
3. Escaneo
Julio Javier Iglesias Pérez
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

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

Tipos de escaneo

Escaneo de vulnerabilidades

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

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

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.

Búsqueda de puertos abiertos

Banderas de comunicación TCP

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

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.

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

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.

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

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.

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

Exploración IDLE

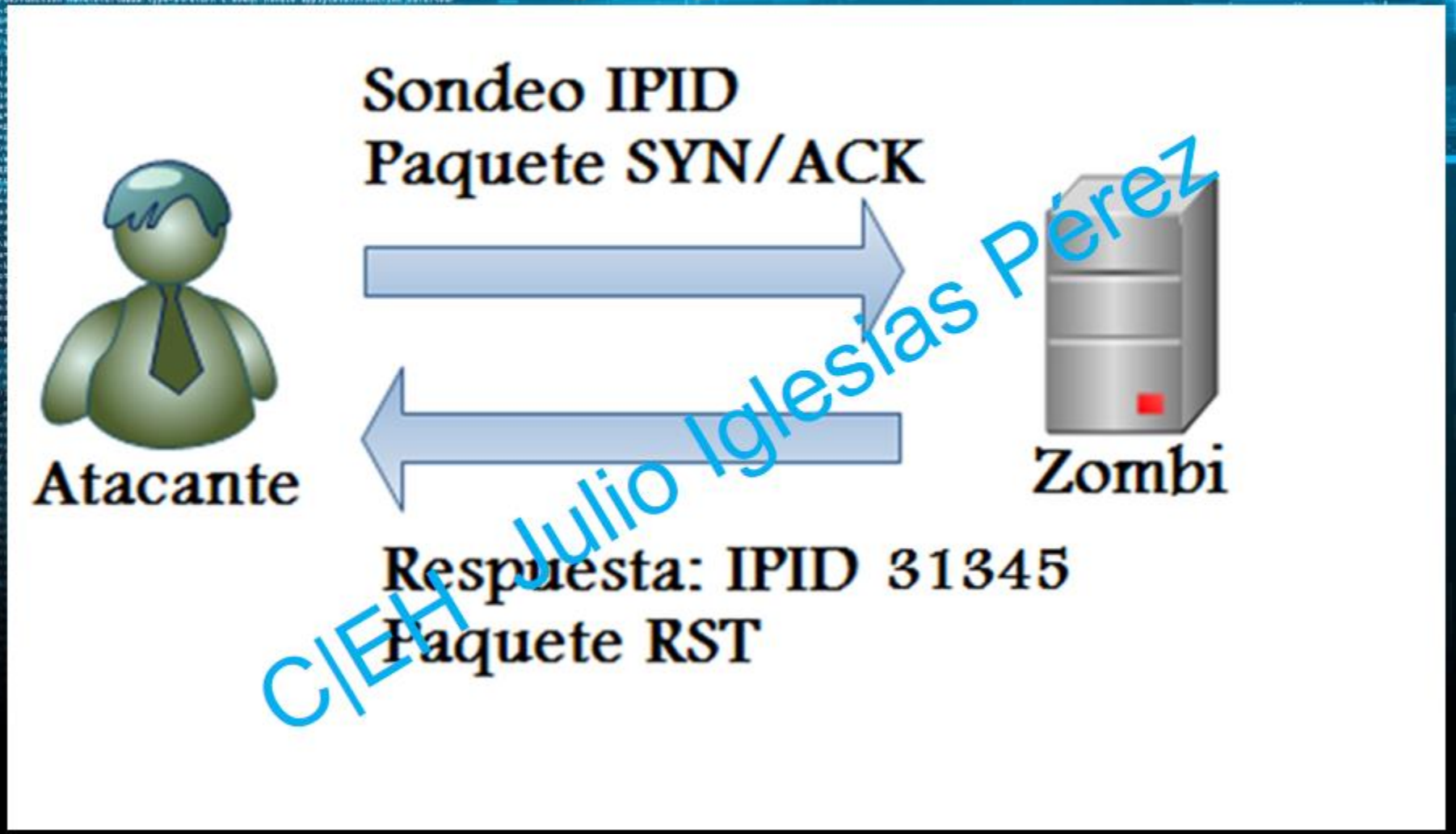
Es una técnica de exploración de puertos. La ventaja es que los atacantes pueden explorar un blanco sin enviar un solo paquete desde su dirección IP.

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".

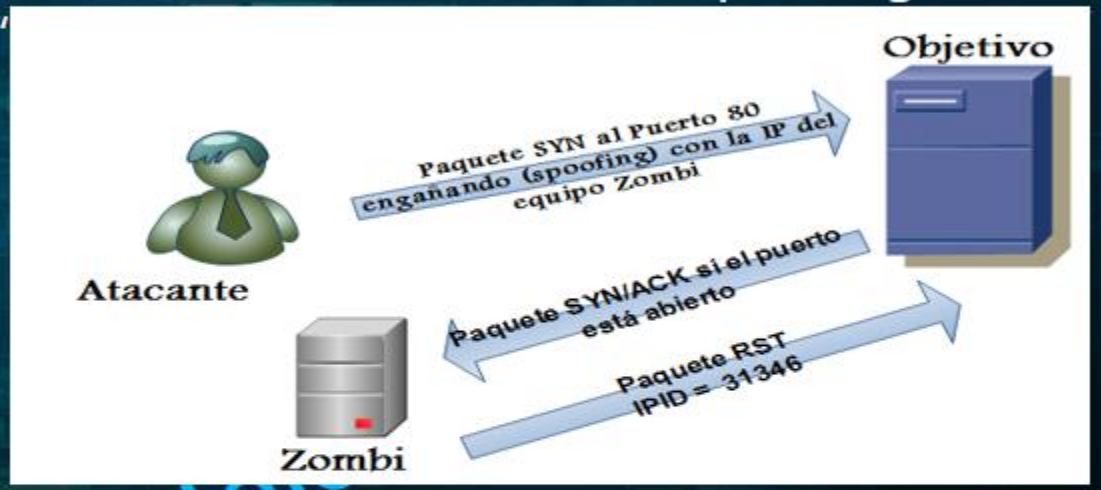
Una manera determinar si el puerto está abierto es enviando un paquete "SYN | ACK". El equipo que recibe este paquete responderá con un RST

Paso 1. Confirmar el IPID del equipo Zombi

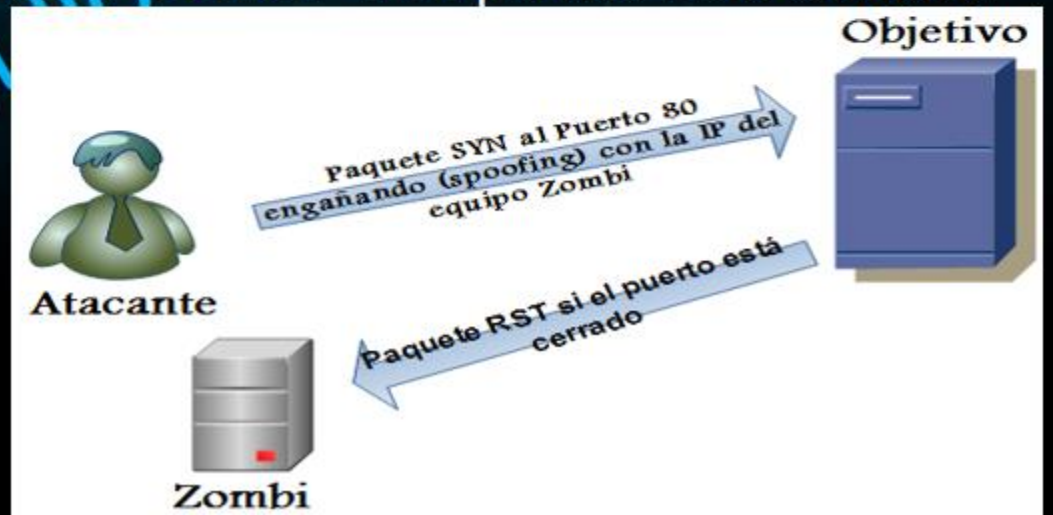


Paso 2

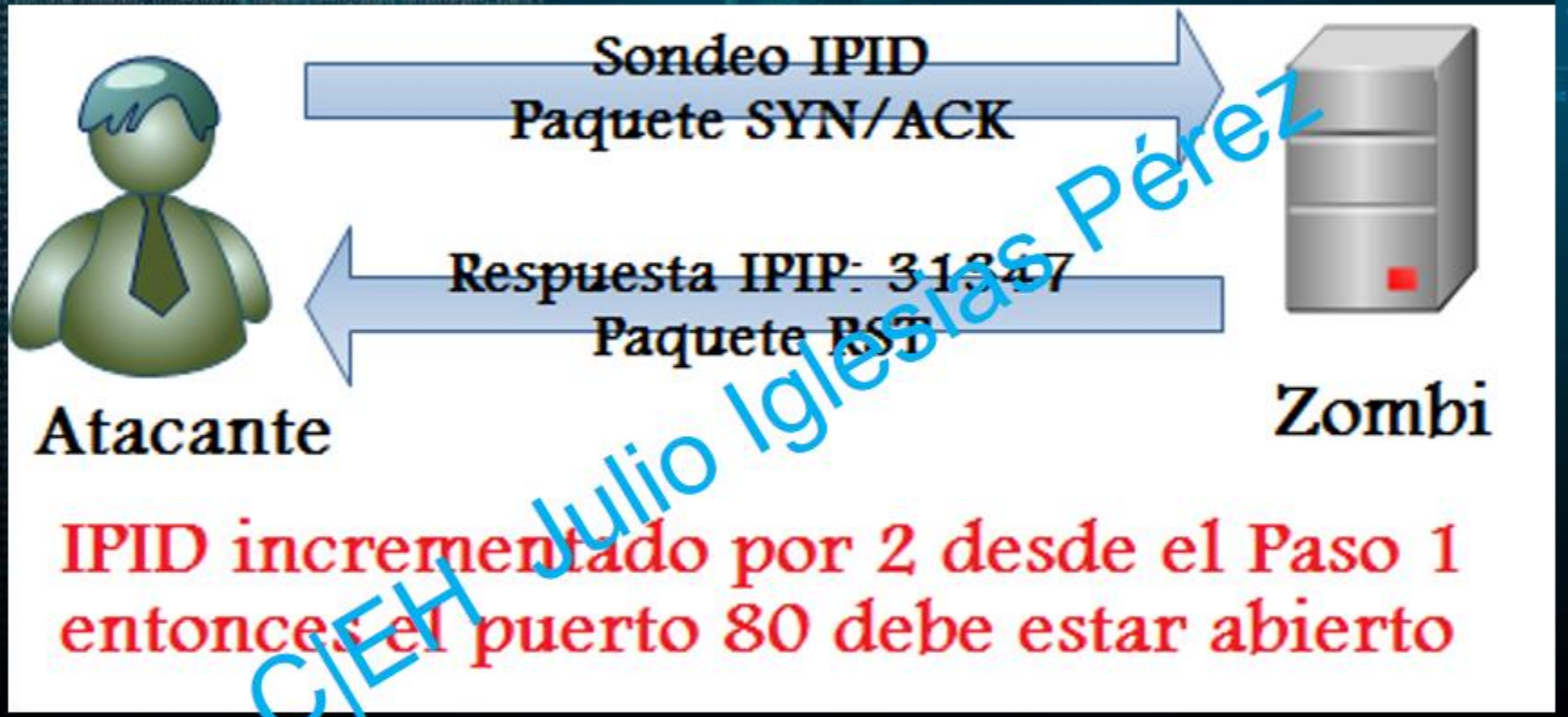
- enviar un paquete SYN al blanco realizando un spoofing a la dirección de "Zombi"



- 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



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

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.

Equipo 1	Equipo2

XMAS dirigido a un puerto abierto:

192.168.9.6:4042 ~~~~~~~~FIN/URG/PSH~~~~~~~~>192.168.9.7:25
192.168.9.6:4042 <~~~~~~~~Sin respuesta~~~~~~~~~~192.168.9.7:25

XMAS dirigido a un puerto cerrado:

192.168.9.6:4042 ~~~~~~~~~~FIN/URG/PSH~~~~~~~~>192.168.9.7:25
192.168.9.6:4042 <~~~~~~~~~~RST/ACK~~~~~~~~~~~~192.168.9.7:25

Herramientas

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

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.

War dialing

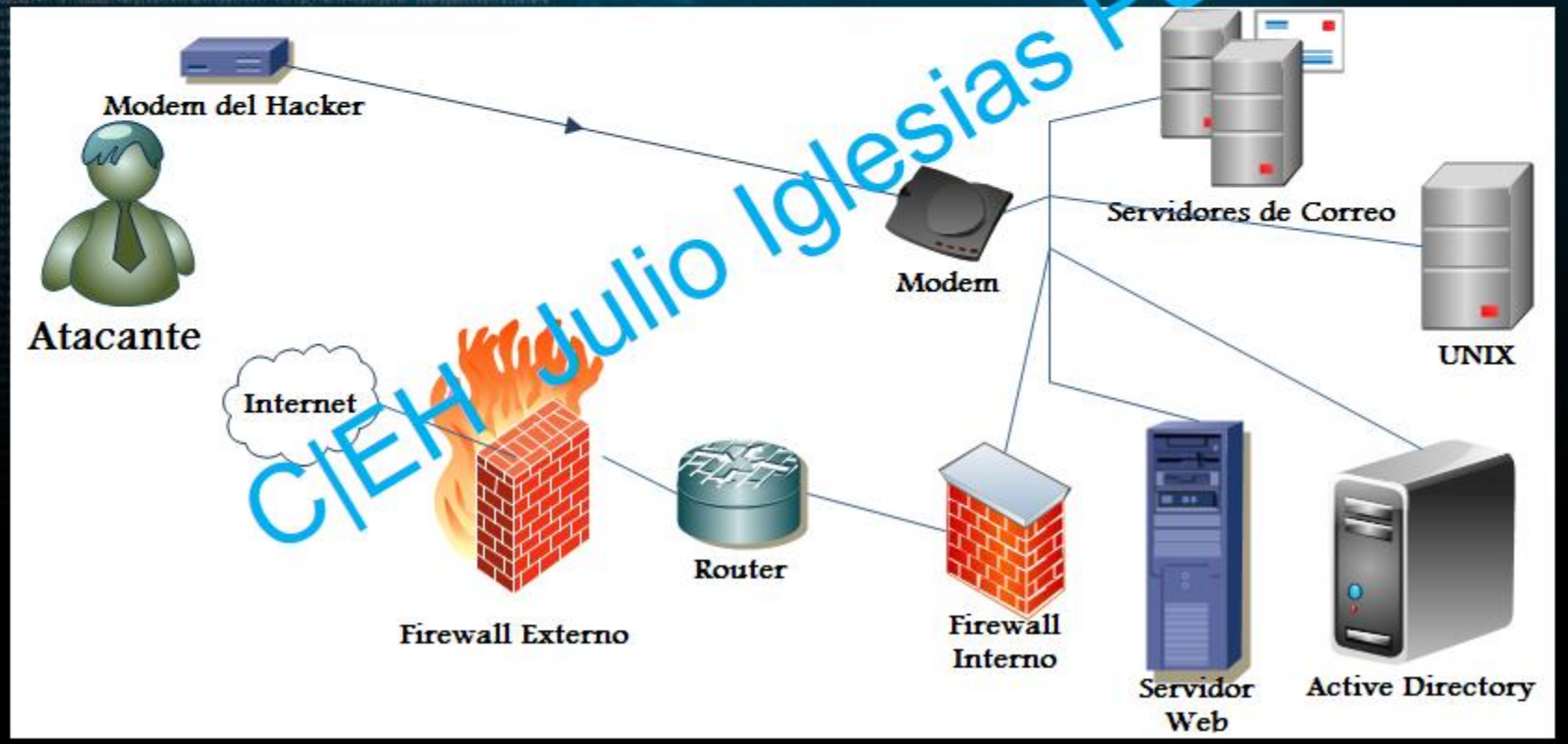
Esta técnica utiliza un programa en conjunto con un modem para penetrar sistemas basados en módems que necesitan de una continua marcación. Las compañías no controlan los puertos como lo hacen con los cortafuegos y las máquinas tienen módems adjuntos en todo lugar.

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.

¿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.



Herramientas War díaling

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

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.

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.

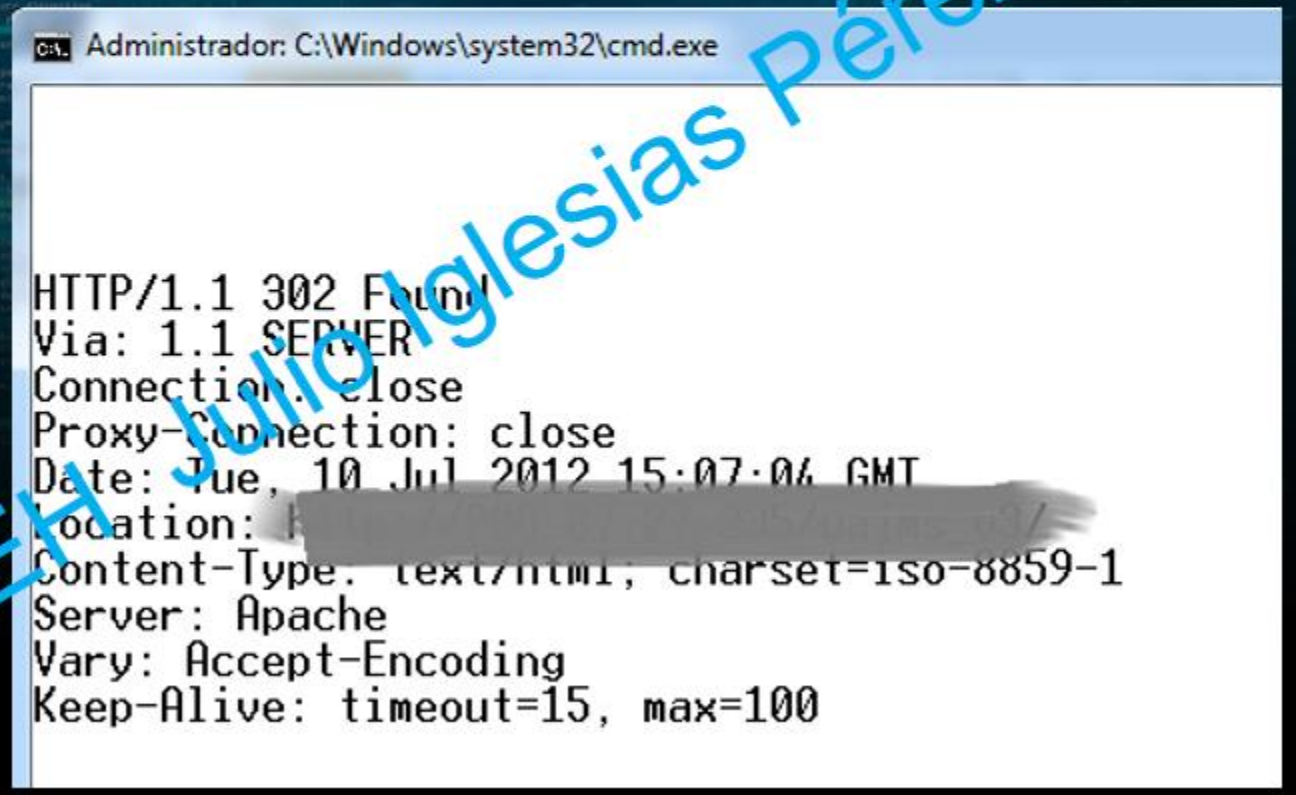
Existen dos distintos tipos de OS Fingerprinting:

- 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



GET Requests

- Mirar el archivo: GET REQUESTS KNOWN_TESTS.htm

Herramientas Banner Grabbing

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

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.

Contramedidas Banner Grabbing

En IIS Server

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

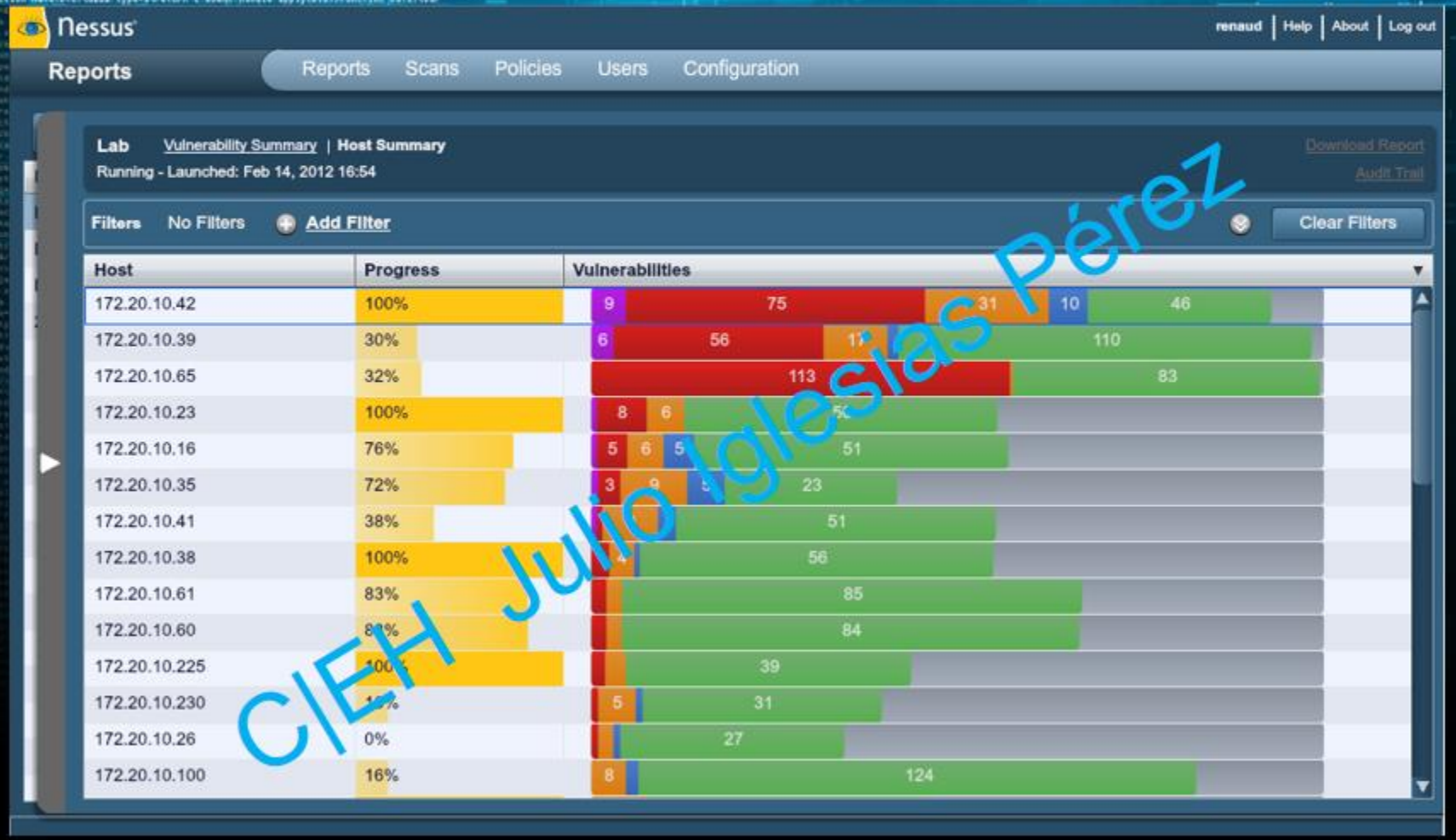
- IIS Lockdown Tool:Es utilizado para quitar características innecesarias para reducir las chances de ser atacados.

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

Escaneo de vulnerabilidades

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

Nessus



SAINT

- Security Administrator's Integrated Network Tool

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.

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.

The Onion Routing (TOR)

Proporciona

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

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).

¿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.

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

Herramientas proxy

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

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.

Anonimizadores

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

Falsificación de direcciones IP (IP Spoofing):

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

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.

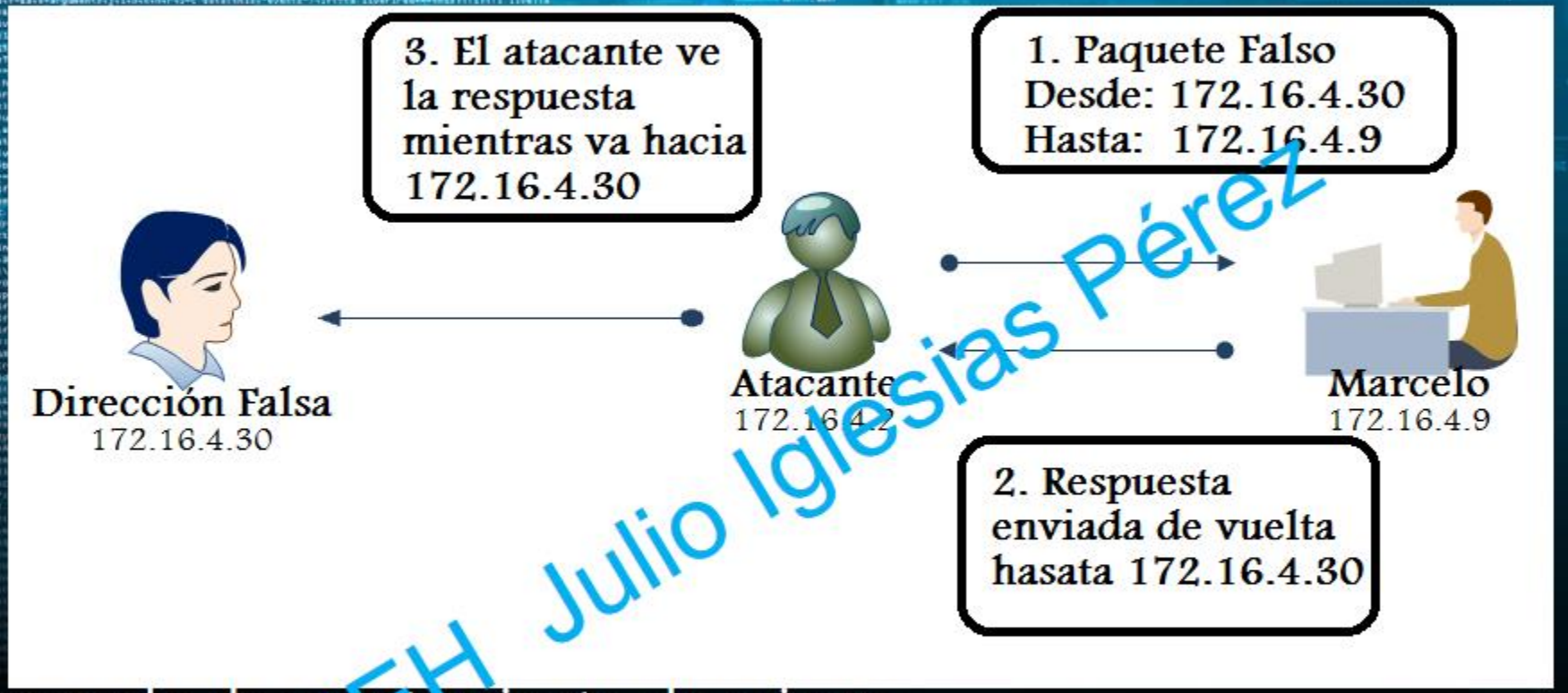
- Enrutamiento de origen estricto o SRS (Strict Source Routing); Se especifica el camino exacto que el paquete debe tomar:

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.



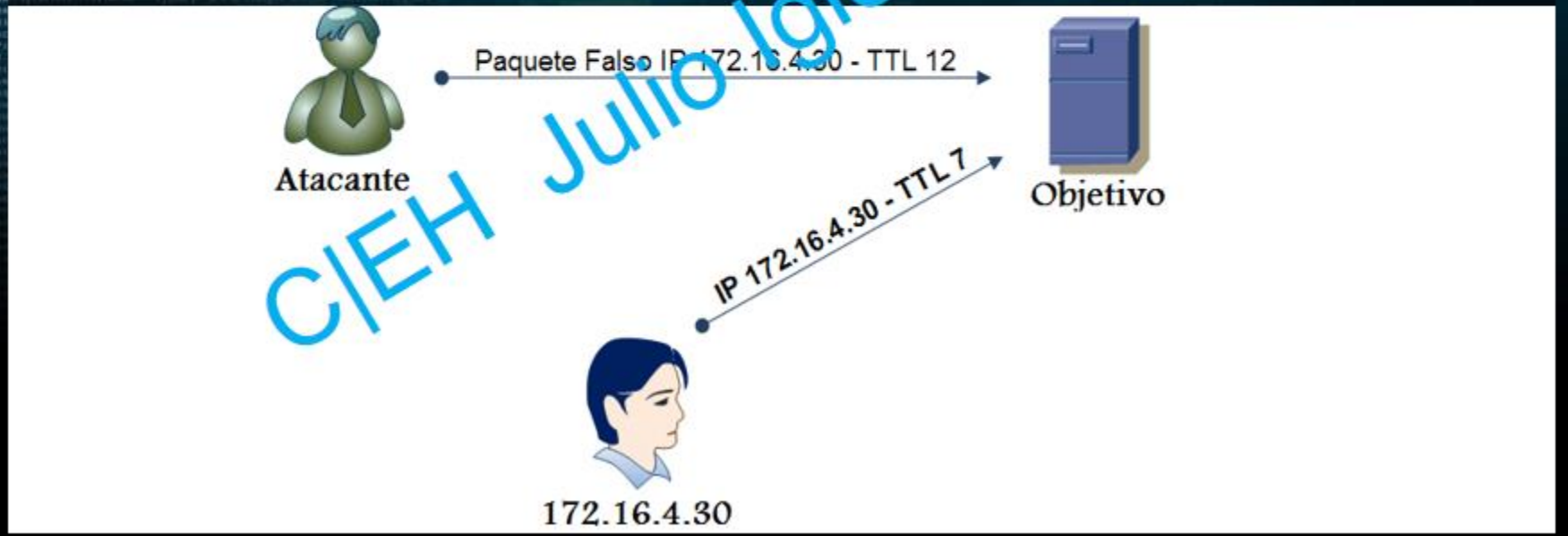
Comando de enrutamiento de origen

- 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.

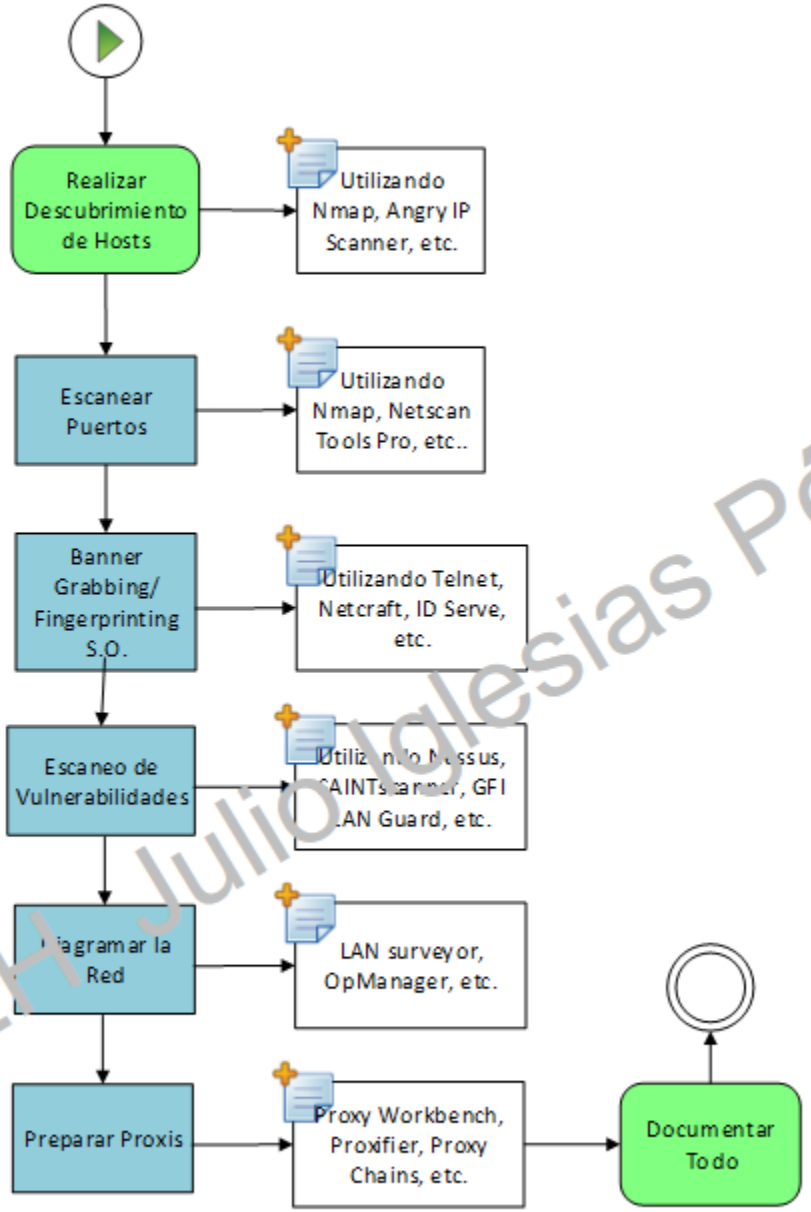


Contramedidas de Exploración

- 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.

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.




¡Muchas Gracias!
C|EH Julio Iglesias Perez