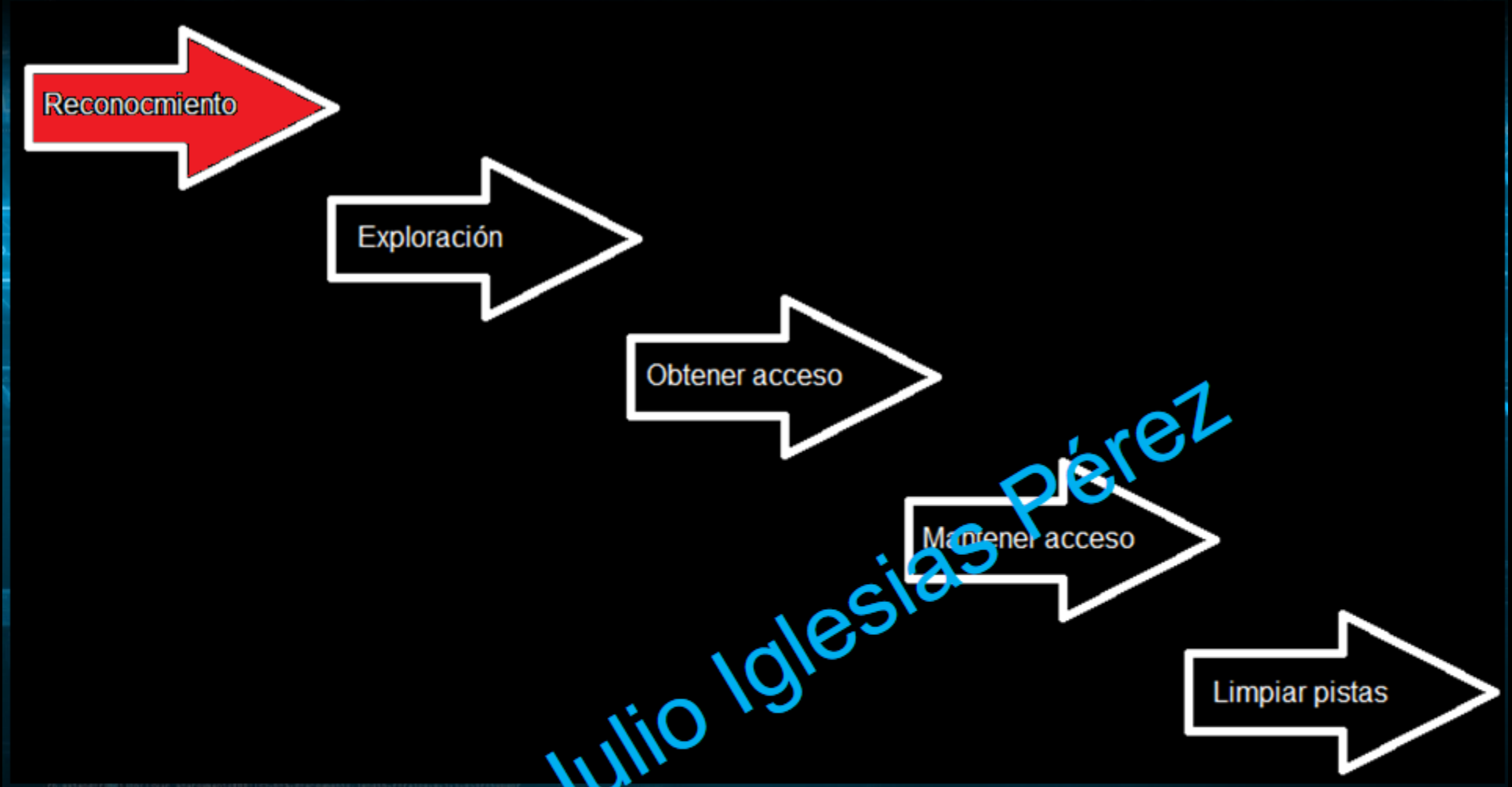
2. Reconocimiento

Certified Ethical Hacker

C|EH 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.

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.

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

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

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.

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.

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

Herramientas para footprinting

Algunas herramientas footprinting son las siguientes:

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

Herramientas Whois

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

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)

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.

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

Herramientas de extracción de información DNS

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

Localizando rangos de red

Comúnmente incluye:

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

- Herramientas: Angry IP Scanner, etc.

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

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.

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.

HTTrack Web Site Copier

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

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.

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

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

Ejemplos

intitle:intranet inurl:intranet site:.bo

Aproximadamente 28.100 resultados (0,22 segundos)

Google Hacking Data Base

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

Otras Herramientas Google Hacking

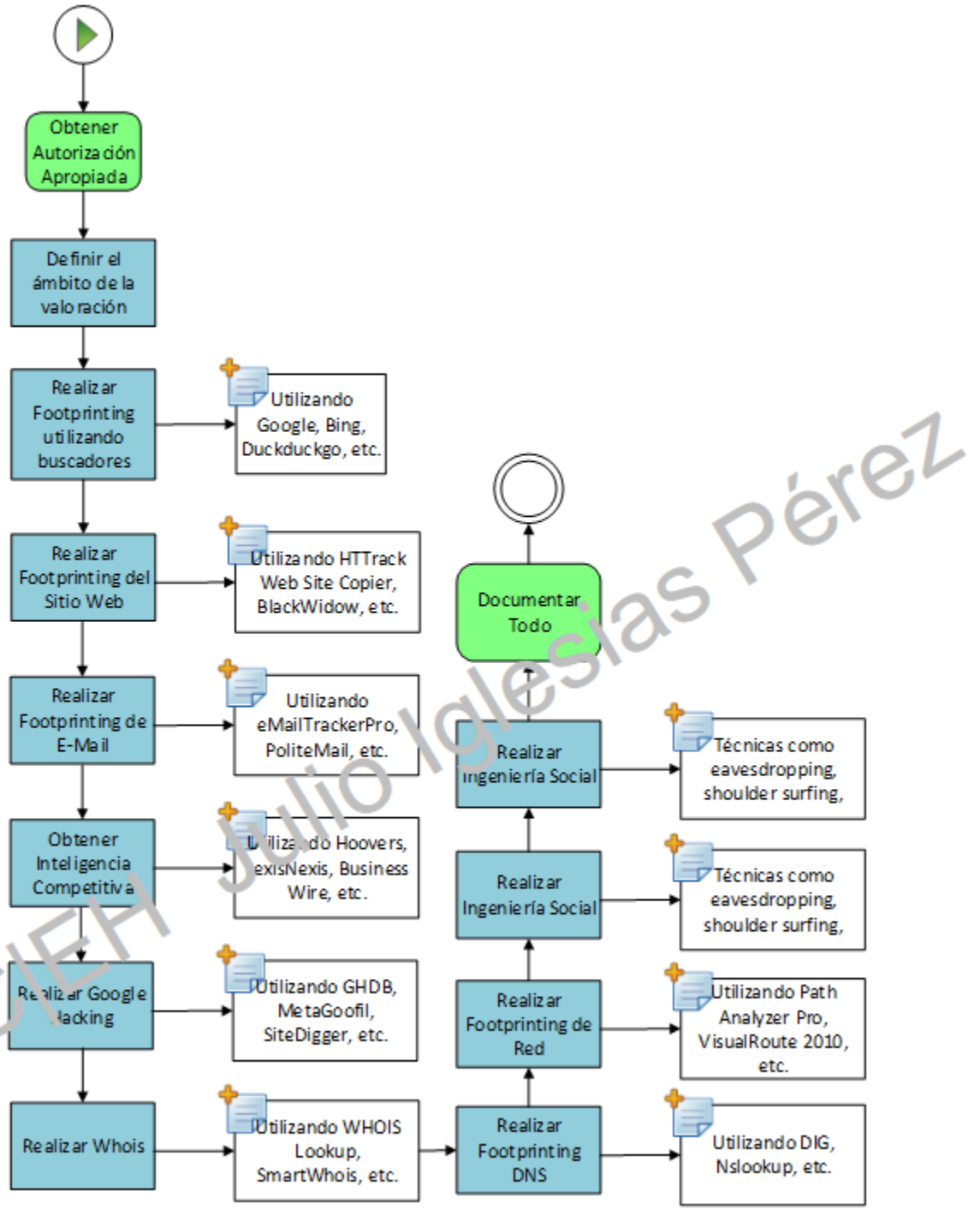
- MetaGoofil. http://www.ghacks.net
- SiteDigger. http://www.foundstone.com
- Bile Suite. http://www.sensepost.com
- GMapCatcher. http://www.code.google.com

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.

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



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:

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:	

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:	

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:

Plantillas para Test de Intrusión

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

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:


¡Muchas Gracias!
C|EH Julio Iglesias Perez