FOOTPRINTING

Tarqui Mita Yessica Fabiola
Universidad Mayor de San Andrés
Carrera de Informática
Análisis y Diseño de Sistemas de Información
yessy.faby@gmail.com

RESUMEN

En este artículo se podrá observar que el Footprinting es donde el atacante obtiene, reúne y organiza toda la información posible sobre su objetivo o su víctima, mientras más información obtiene con mayor precisión y éxito puede lanzar un ataque.

Palabras Claves

Recolectar información, red, sistema, organización, victima.

1. INTRODUCCIÓN

El primer pasó del hacker ético es el "*Footprinting";* que es un proceso que se hace antes de hacer un ataque a alguna organización. Básicamente hace una recopilación de toda la información necesaria para hacer un perfecto ataque. En esta parte del Footprinting es donde el atacante obtiene, reúne y organiza toda la información posible sobre su objetivo o víctima, mientras más información obtiene, con mayor precisión puede lanzar un ataque.

La recopilación de información es también conocida como "*huella o Reconocimiento"*. La información que el hacker está buscando en la fase del Reconocimiento es algo que da indicios sobre la arquitectura de la red, el servidor y los tipos de aplicaciones, donde almacenan los datos valiosos de una organización o víctima. Antes de lanzar un ataque, los tipos de aplicación deben ser descubiertos, utilizando las metodologías y herramientas necesarias, esto para que el ataque sea más efectivo y pueda ser lanzado y obtener lo que se está buscando del objetivo específico.

2. FOOTPRINTING

Es el modelado de un perfil de seguridad y el proceso de creación de un mapa de las redes y sistemas de una organización, el Footprinting es la forma de recopilar información, comienza por determinar el objetivo, para luego averiguar información específica utilizando métodos no intrusivos, una herramienta fundamental son las búsquedas online, utilizando Google u otro servidor. Es importante conocer en profundidad las características avanzadas de búsqueda.

Junto al Scannign y Enumeration, el Footprinting es una de las tres fases de *obtención de información* en un pre-ataque.

Un atacante suele pasar el 90% del tiempo sacando información y formando perfiles de la organización y otros,y un 10% de tiempo en el lanzamiento del ataque. [1]
El resultado del footprinting es un perfil general de la organización respecto a sus redes, estas pueden ser: internet, intranet, extranet, wireles, etc y también todos los sistemas que hay en él.

3. METODOLOGIA DE FOOTPRINTING

La metodología del Footprinting es parte de la obtención o recopilación de información, que considera las tres etapas ya mencionadas: Footprinting, Scannign y Enumeration. De manera general puede ser divida en nueve pasos:

- Ubicación del rango de red.
- Comprobación de equipos activos.
- Descubrimiento de puertos abiertos y aplicaciones que se están ejecutando en ellos.
- Detección versiones del sistema operativo.
- Nombres de Dominios (DNS: Sistema de Nombres de Dominio).
- Bloques de Red.
- Dirección IP (Protocolo de Internet) especificas.
- Mapeo de red (País, ciudad donde se encuentra los servidores).
- Información del contacto (números telefónicos, emails, etc.).

Mucha de la información, antes mencionada, como Domain Name (Nombre de Dominio), algunas direcciones IP, País, Ciudad, e información de contacto se la obtienen buscando en las bases de datos de WHOIS.

3.1 Enumeración de red

La red de enumeración (Red enumeration) es una actividad de computación en el que los nombres de usuario, y la información sobre los grupos, las acciones y servicios de equipos en red se recuperan. No se debe confundir con el mapeo de red, sólo recupera información acerca de los servidores que están conectados a una red específica y qué sistema operativo se ejecutan en ellos. Esto incluye la identificación del nombre de dominio, así como la búsqueda de la información de registro, desde dominios de compañías que están listados con la información de su registro. El hacker sólo necesita saber qué registró la compañía. Hay cuatro tipos de consultas que figuran en esta sección, que son los siguientes:

3.1.1 Consultas Whois

Consultas Secretario o WHOIS es una consulta y protocolo de respuesta que es ampliamente utilizado para la consulta de bases de datos que almacenan los usuarios registrados o sucesores de un recurso de Internet, como: un nombre de dominio, un bloque de direcciones IP, o un sistema autónomo, pero también se utiliza

para una gama más amplia de otra información. El protocolo almacena y entrega de contenido de base de datos en un formato legible. [2]
Esta consulta es la más usada ya que, las bases de datos WHOIS mantienen detalles de direcciones IP registradas en 5 regiones del Mundo. Estas bases de datos son manejadas por 5 organizaciones llamadas Regional Internet Registry (RIR) (Registro Regional de Internet).

Las 5 bases de datos WHOIS están localizadas en:

- América del Norte (ARIN),
- América del Sur, América Central y el Caribe (LACNIC),
- Europa, el Medio Este y Asia Central (RIPE NCC),
- Asia del Pacifico (APNIC) y
- Africa (AfriNIC).

3.1.2 Consultas de organización

Esta es la búsqueda de un registro específico para obtener todas las instancias del nombre del objetivo. Los resultados muestran muchos dominios diferentes asociados con la empresa, ya que puede utilizar un gran número de dominios con su servidor o sistema que se puede decir dedicado.

3.1.3 Domain Consulta (Consulta de Dominio)

Una consulta de dominio se basa fuera de los resultados encontrados en una organización consulta. Con una consulta de dominio, se puede encontrar la dirección de la empresa, nombre de dominio, administrador, su número de teléfono, y los servidores de dominio del sistema, mientras que el registro de un dominio de este se incluye en el foro de registro. El contacto administrativo podría ser muy útil para un hacker, ya que proporciona un propósito de cómo hacer ingeniería social. Así que aquí es donde la ingeniería social entra en juego. Muchos administradores ahora publican los números de teléfono falsos para protegerse a sí mismos de esta manera que no pueden ser engañados tan fácilmente.

3.1.4 DNS interrogatorio

Una vez recopilada la información necesaria usando las técnicas anteriores, un hacker podría comenzar a consultar el DNS utilizando herramientas. Un problema común con los administradores del sistema es permitir que los usuarios no confiables, o peor aún, desconocidos, para realizar una transferencia de zona DNS. Muchas herramientas de software libre se pueden encontrar en Internet y se puede utilizar para llevar a cabo interrogatorios DNS. Las herramientas como lookup (búsqueda), para PC, también en el sabor muchas aplicaciones de código abierto de Linux están presentes para este fin.

3.1.4.1 DNS Zone Transfer (DNS Zona de Transferencia)

Los datos contenidos en una zona DNS son sensibles por naturaleza. Individualmente, los registros DNS no son sensibles pero si un atacante obtiene una copia entera de la zona DNS de un Dominio, obtiene una lista competa de todos los huéspedes de ese dominio.
Un atacante no necesita herramientas especiales para obtener una zona DNS completa, solo que el DNS este mal configurado y que permita a cualquiera realizar una transferencia de zona. La transferencia de zona s necesaria y no pueden ser deshabilitadas completamente. Pero solo deben ser permitidas entre servidores DNS y clientes que necesitan de estas.

En general solo los servidores DNS dependientes necesitan realizar transferencia de zona.

3.1.4.2 DNS Denial of Service (DNS de Negación de Servicio)

Si un atacante puede realizar una transferencia de Zona, también puede realizar ataques de denegación de servicio contra esos servidores DNS realizando múltiples peticiones.

3.1.4.3 Identificación de los Tipos de Registros DNS [14]

- A (address: dirección): Hace un trazado IP del huésped.
- MX (mail Exchange: Intercambio de Correo): Identifica el servidor del correo del Dominio.
- NS (name server: Servidor de Nombres): Identifica otros nombres de servidores para el dominio.
- CNAME (canonical name: Nombre Canónico): Provee nombres adicionales o alias para dicho registro.
- SOA (start of authority: Inicio de Autoridad): Indica la autoridad para un dominio.
- TXT (text: Texto): Registro de texto genérico. Permite a los dominios identificarse de modos arbitrarios.
- HINFO (host information: Información de Acogida): Nos muestra la información del huésped, equipo y sistema operativo.
- LOC: Permite indicar coordenadas del dominio.
- SVR (service: Servicio): Identifica servicios que ofrece el dominio.
- WKS: Es la generalización del registro MX para indicar los servicios que ofrece el dominio. Está obsoleto a favor de SRV.
- PTR (pointer: Puntero): Mapea direcciones IP a nombre de algún huésped.

3.2 Footprinting Fuente

Es un tipo de reconocimiento más segura, ya que se encuentra en los límites legales y usted puede hacerlo sin ningún temor, si usted está haciendo cualquier tarea, algo ilegal. Incluye la búsqueda de información básica, mayormente presentes para uso público también, igual que la búsqueda de los números de teléfono, direcciones de correos electrónicos, que está llevando a cabo la solicitud de nombre de dominio, buscando a través de tablas DNS y escaneo ciertas direcciones IP a través de herramientas automatizada y buscando algunos medios comunes de búsqueda de información sobre el sistema de servidor y propietario. Muchas de las Empresas dan una gran cantidad de información acerca de ellos mismo, en la propia página web sin darse cuenta del hecho de que puede ser útil para un hacker, a veces en HTML y comentarios de codificación estás a su vez da a los hackers una gran cantidad de información acerca de codificación. Ya que en como comentar, es una forma de codificación que la realiza un programador sobre la función de un código específico.

4. HERRAMIENTAS ONLINE PARA FOOTPRINTING

1. **4.1 SamSpade**
2. El SamSpade [3] es una herramientas Whois, que contiene:
3. – Búsqueda de nombres de dominios.
4. – Lugares comúnmente incluidos.
5. – Contactos (teléfonos y correo electrónico).

6. – Fuentes de información.
7. – Código abierto.

4.2 DNSstuff
La herramienta DNSstuff, [4] nos proporciona múltiples elementos para extraer información de los DNS.

4.3 People Search and Intellius
People Search, [5] y Intellius, [6] son herramientas que nos proporcionan es el buscador de personas e información de contacto.

4.4 NetCraft
La herramienta NetCraft, [7] es un detector del sistema operativo de una organización.

4.5 Whois
La herramienta Whois, [2] realiza la consulta Secretario denominada también Whois, es esta página se pone el URL de una organización y nos muestra el dominio, IP y otro tipo de información.

5. SOFTWARE PARA FOOTPRINTING

5.1 SamSpade
SamSpade, [8] también es un software que provee información sobre el DNS, WHOIS y permite informarse profundamente sobre el objetivo.

5.2 Web Data Extractor Tool
Web Data Extractor Tool, [9] es un software que extrae las fechas de los enlaces, email, números telefónicos, fax, entre otras cosas y permite almacenarlos en el disco duro.

5.3 Spiderfoot
Spiderfoot, [10] esta herramienta nos provee información sobre sub-dominios, versión del web server, dominios similares, emails y bloques de red (Netblocks).

5.4 Traceroute
Traceroute, [11] es un software en línea de comandos que viene instalada en la mayoría de los sistema operativos, se usa para encontrar la ruta de un sistema, muestra los detalles de paquetes IP que viajan entre dos sistemas. Puede trazar el número de routers (enrutadores) por donde viajan los paquetes y la duración del tiempo en tránsito del viaje entre dos routers. Traceroute trabaja explotando una característica del Internet Protocol (IP) llamada TTL (Time To Live: Tiempo de Vida).

5.6 NsLookup
Nslookup, es una herramienta valiosa para hacer consultas a los DNS para la resolución de nombres de huéspedes. Viene instalado en los sistemas operativos UNIX y Windows.

5.7 3DTraceroute
3DTraceroute, [12] es el trazador de ruta en tres dimensiones, realiza el monitoreo visual de conexiones de Internet (websites: Sitio Web), escanea puertos, WHOIS, entre otras cosas.

5.8 GEOSpider
GEOSpider te ayuda a detectar, identificar y monitorear tu actividad de red en un mapa mundial. Puedes ver websites, y localizaciones mundiales de direcciones IP. También puede trazar un Hacker, investigar un website y trazar su nombre de dominio.

6. CONCLUSIÓN
El Footprinting es una de las tres fases de la obtención de información, que realiza el hacker ético donde nos muestra las formas más eficientes del muestreo que se puede plasmar, tomando en cuenta la metodología, las herramientas y los distintos software del footprinting, todo esto para un ataque exitoso hacia una persona u organización, del cual se extrae como resultado un perfil, con información pública muy valiosa de un dominio.

Dependiendo lo que se quiera hacer hay métodos que ayudan a los hackers a infiltrarse en las redes del internet, pero también existen grandes consecuencias dependiendo el grado de hackeo que se esté realizando.

El footprinting, resulta también necesario ya que si se lo hace de una manera sistemática y metódicamente nos puede garantizar que todas las piezas de información relacionadas con las tecnologías mencionadas, se puedan identificar. Además al realizarlo en una compañía puede ayudar a los administradores de red saber qué tipo de información reside fuera de la compañía y las potenciales amenazas que esa información posee. Se deben usar medidas preventivas para asegurarse de que la información expuesta no pueda ser usada para “explotar” el sistema.

7. REFERENCIAS
[1] Titulo: La Biblia del Footprinting. Autor: Juan Antonio Calle García, Pablo Gonzales Pérez, 2011, Disponible en: http://www.flu-project.com/la-biblia-del-footprinting-i-de-vii.htmls. Fecha de acceso: 7/06/13 Hora. 10:30.

[2] Titulo: Footprinting e ingeniería Social. http://www0.unsl.edu.ar/~moalaniz/taar/teorias/02A_Footprintin_IngenieriaSocial.pdf fecha de Acceso: 6/06/13 Hora. 10:30.
[3] http://www.samspade.org/
[4] http://member.dnsstuff.com/pages/tools.php?ptype=free
[5] http://www.people.yahoo.com
[6] http://www.intellius.com/
[7] http://www.netcraft.com/
[8] http://www.softpedia.com/get/NetworkTools/NetworkToolsSuites/Sam-Spade.shtml
[9] http://rafasoft.com/
[10] http://binarypool.com/spiderfoot/
[11] http://www.cnn.com/
[12] http://www.d3tr.de/
[13] http://www.oreware.com/viewprogram.php?prog=22
[14] Titulo: Hacking Ético, Autor: Constantino Malagón disponible en: http://www.nebrija.es/~cmalagon/seguridad_informatica/transparencias/Modulo_0.pdf. Fecha de Acceso: 7/06/13 Hora. 14:30