

Conociendo al Enemigo

EL ATACANTE INFORMÁTICO

Protocolos de Comunicación
Ambientes Operativos

DoS

Buffer Overflow

Exploits

Enumeración

CAPÍTULO 4

ENUMERACIÓN Y RECONOCIMIENTO

Rookits

Virus

Criptografía

Metodologías y Estándares



Jhon César Arango Serna

www.itforensic-la.com

Agradecimientos a Leonardo Piñer y “Chema” Alonso, sin los conocimientos adquiridos a través de ellos, la re estructuración de este capítulo no hubiera sido posible.

CAPITULO 4

ENUMERACIÓN Y RECONOCIMIENTO

REUNIENDO INFORMACIÓN:

Muchas compañías, cuando empiezan a construir una infraestructura de seguridad, se preocupan solamente por proteger sus sistemas de un determinado ataque, cuando lo que necesitan saber es que barreras deben colocar a sus sistemas y cuando las colocan. Sin embargo, no se dan cuenta que a través de un reconocimiento y de recolectar información, un atacante puede adquirir gran cantidad de información a través de sus sitios Web.

Antes de efectuar una ofensiva, el atacante necesita conocer el entorno del sitio y empieza por reunir la mayor cantidad de información que le sea posible.

Mientras un atacante inexperto, ataca directamente enviando indiscriminadamente mensajes de error de Internet a los sistemas más desprotegidos, sin importar a quien pertenecen, los atacantes más experimentados se toman su tiempo reuniendo detalles, como número de máquinas, tipo, sistemas operativos y haciendo reconocimientos previos antes de lanzarse a asaltar una red; así sus posibilidades de tener éxito serán mayores.

Para entender mejor por qué un reconocimiento es tan importante, imagine a alguien que quiere robar un banco. Los ladrones no precisamente, se levantan un día y determinan un objetivo (determinado banco). Ellos, primero necesitan reunir una información preliminar. Visitarán las principales sucursales para observar los horarios de entrada y salida de los guardas de seguridad, localizarán las cámaras de seguridad, sistemas de alarma y quizás su fabricante. Adicionalmente los bandidos usarán las páginas blancas para localizar direcciones y levantarán un mapa de la entidad para planear una ruta de entrada.

Exactamente como en los robos de bancos, el primer paso para atacar maquinas es investigar el objetivo, utilizando la información que esté disponible. En la mayoría de los casos, el éxito del ataque depende de la cantidad de información reunida acerca del objetivo. Si la información ha sido reunida correctamente y con todo detalle, el acceso a los sistemas está garantizado.

Por consiguiente, la clave de una compañía para prevenir un ataque, es conocer que tipo de información puede adquirir el atacante y minimizar el posible daño.

PASOS PARA OBTENER INFORMACION:

Sin necesidad de haber tocado jamás un computador, un atacante está apto para sacar provecho de una información susceptible que tenga determinada empresa. Utilizando una variedad muy extensa de técnicas, puede conocer fácilmente contraseñas, puntos de acceso, detalles sobre la arquitectura y sistemas de documentación de una red y hasta información altamente confidencial, pasando por encima de todas las medidas y personal de seguridad, sin ningún tropiezo.

Antes de empezar se debe establecer dos cosas: la primera nuestra herramienta de trabajo, para nuestro caso utilizaremos la última versión de BackTrack¹ y la segunda es tener claro quién será nuestro objetivo, es de aclarar que los resultados de los ejemplos mostrados en este capítulo serán alterados para conservar el anonimato de la fuente real.

La enumeración y el reconocimiento tienen como objetivo, entre las más importantes conocer la siguiente información:

- Posibles usuarios y contraseñas
- Rangos de direcciones IP's
- Equipos activos
- Nombres de equipos
- Correos electrónicos del personal afiliado a nuestro objetivo
- Puertos y Servicios que están disponibles en los diferentes equipos de la víctima.
- Datos sensibles sobre la víctima u usuarios pertenecientes a nuestro objetivo.
- Reconocimiento general de la Red de datos (Switches, Routers, Firewall, Puntos de Acceso, Etc)

Los siguientes son los seis pasos básicos que un atacante deberá seguir para obtener información más completa del caso.

Paso 1 - Encontrar la información inicial

- Ping
- Whois
- Análisis de Metadatos
- OSINT

Paso 2 - Identificar el Rango de la Red

- Arin / Lacinic / Ripe / Internic
- Traceroute
- Hping
- Descubrimiento con DNS

Paso 3 - Buscar Maquinas Activas

- Nmap

¹ [http:// www.backtrack-linux.org/](http://www.backtrack-linux.org/)

Paso 4 - Buscar puertos y Servicios

- Introducción puertos y servicios
- Portscanners
- Nmap

Paso 5 - Encontrar versiones de Sistemas Operativos y Aplicaciones

- Nmap

Paso 6 – Búsqueda de Información Complementaria

- Escarbando Basureros.
- Búsqueda de Imágenes Satelitales
- Búsqueda de Redes Inalámbricas
- Escuchando el Trafico de Red

A continuación daremos un vistazo a cada uno de los siete pasos y examinaremos como trabaja cada herramienta. No solamente veremos cómo pueden dichas herramientas ser empleadas por un agresor para comprometer un sistema, sino que les mostraremos como pueden ustedes utilizarlas para proteger su propio sistema.

Muchas personas tienen una perspectiva negativa hacia las herramientas que pueden ser utilizadas para implicar sistemas, porque no siempre son confiables. Si usted las conoce y utiliza correctamente, ellas pueden contribuir a aumentar la seguridad y protección de su sitio y disminuir su valor para un atacante. En la medida en que usted conozca y entienda como un atacante puede irrumpir en su red, está en capacidad de aumentar la seguridad de su sitio.

ENCONTRAR LA INFORMACION INICIAL:

Para que un atacante irrumpa en una maquina necesita tener alguna información previa, como por ejemplo, una dirección IP o un nombre de dominio. Normalmente la dirección IP descubierta es de tipo estática, la cual es fiel a la mayoría de los servidores.

Ahora, si ese ataque tiene un nombre de dominio dado, el intruso necesitará obtener información del sitio. Direcciones IP o gente que trabaja en el sitio, puede ser usada para perpetrar un ataque exitosamente.

Miremos algunas maneras como un atacante puede obtener información inicial:

Comando Ping

Es el primer paso de todo atacante, un simple Ping me da información útil dependiendo de la salida que nos de. El hacer un ping al nombre del dominio, lo primero que el programa hace es tratar de analizar la dirección IP del host e imprimirla en la pantalla.

Algunas salidas posibles pueden ser:

```
root@itforensic-la:~# ping www.eltiempo.com
PING www.eltiempo.com (200.41.9.39) 56(84) bytes of data.
64 bytes from www.eltiempo.com.co (200.41.9.39): icmp_seq=1 ttl=246 time=229 ms
64 bytes from www.eltiempo.com.co (200.41.9.39): icmp_seq=2 ttl=246 time=97.5 ms
64 bytes from www.eltiempo.com.co (200.41.9.39): icmp_seq=3 ttl=246 time=358 ms
```

Esta salida nos muestra una respuesta de un IP 200.41.9.39, inmediatamente podemos deducir que es una dirección de clase C, podemos también deducir que el servidor no tiene el ICMP filtrado ya que responde el Ping, lo que podría suponer que nos encontramos con un servidor que no posee esquemas de seguridad o por el contrario con un administrador inteligente que nos pone a perder tiempo.

Por otro lado observamos que las peticiones DNS están funcionando adecuadamente ya que al escribir el nombre de dominio este nos devuelve la IP, se debe tener en cuenta que posiblemente nuestro objetivo se puede encontrar en un Hosting.

```
root@itforensic-la:~# ping www.corpocaldas.gov.co
PING www.corpocaldas.gov.co (216.121.7.94) 56(84) bytes of data.
- codename [ pwns
```

En este caso vemos que el DNS resuelve adecuadamente, sin embargo no obtenemos las respuestas a la solicitud. Aquí podemos deducir que las respuestas al ICMP están bloqueadas por lo que nos podemos estar enfrentándonos a un equipo que tiene establecidos unos parámetros de seguridad básica o por el contrario a un cortafuego que esta rechazando esta solicitud.

```
root@itforensic-la:~# ping www.amazon.com
PING www.amazon.com (207.171.166.252) 56(84) bytes of data:
From xe-0-4-0-7.r01.asbnva02.us.ce.gin.ntt.net (168.143.191.26) icmp_seq=57 Pack
et filtered
```

Y en este último caso, responde el DNS y al tiempo responde un IP totalmente diferente a la arrojada inicialmente, por lo que podemos deducir que nos encontramos con un red que con seguridad esta filtrada.

WHOIS

Es una herramienta utilizada para comprobar la disponibilidad de un dominio y para obtener información sobre la persona o entidad que lo posee.

Además de hacer búsquedas, la variedad de bases de datos whois en internet es demasiado útil como fuente de información. Estas bases de datos contienen una gran variedad de elementos con respecto a la asignación de direcciones en internet, nombres de dominio y contactos individuales.

Además de nombres de dominio y direcciones de red, algunas bases de datos whois están llenas de información correspondiente a los empleados que son responsables de los servidores y la conectividad de dichas organizaciones inclusive otros muestran la ubicación geo referenciada del dominio. Esta información puede ser utilizada por el atacante con el fin de crear un perfil de las personas que crearon el dominio o por el contrario para reunir información de dichas personas, lo suficiente; como para realizar un ataque de Ingeniería Social.

Muchas versiones de UNIX vienen comando “whois” incluido; sin embargo las grandes posibilidades de Internet y la evolución de los navegadores, nos permite utilizar herramientas vía Web más certeras.

En la la mayor parte de países existen los dominios nic.xx, donde la xx represente las iniciales del país, así tenemos:

<http://www.nic.ve/> (Venezuela)

<http://www.nic.ar/> (Argentina)

<http://www.nic.cl/> (Chile)

<http://nic.es/> (España)

<http://nic.mx/> (Mexico)

Otros como nic.co, nic.pe, se re direccionan a otros dominios, sin importar la pagina utilizada la idea es buscar la utilidad “whois” en cada una de ellas dependiendo del origen de nuestro objetivo.

<http://www.whois.co> (Colombia)

<http://www.punto.pe/whois.php> (Peru)







<http://www.whois.mx/form.jsf> (Mexico)

Como complemento para buscar los dominios .com, .org, .net, entre otras podríamos utilizar alguna de estas páginas:

<http://www.internic.com/whois.html>
<http://hexillion.com/asp/samples/AutoWhois.vbs.asp>
<http://www.domaintools.com/>

Dependiendo del dominio, utilizaremos la herramienta “whois” adecuada, nuestro objetivo es obtener los correos y nombres de las personas que solicitaron la creación del dominio.

Así por ejemplo si nuestro objetivo es el “ucaldas.edu.co”, tendríamos que buscarla con la herramienta “whois” de Colombia (<http://www.whois.co>), donde podríamos apreciar la siguiente salida:

Nombre del Dominio	UCALDAS.EDU.CO
ID del Dominio	D612146-CO
Entidad responsable del Registrador	.CO INTERNET S.A.S.
ID del Registrador	111111
URL (Servicio Registro) Registrador	www.cointernet.com.co
Estado del Dominio	ok
Numero Identificación de Registrante	14568-REG
Nombre del Registrante	UNIVERSIDAD DE CALDAS
Compañía/Organización de Registrante	UNIVERSIDAD DE CALDAS
Dirección del Registrante	CALLE 65 NO. 26-10
Ciudad del Registrante	MANIZALES
País de Registrante	Colombia
Código de País del Registrador	CO
Teléfono de Registrante	 +571.0000000 
Correo electrónico del Registrante	sistemas@ucaldas.edu.co
Numero Identificación de Contacto Administrativo	14568-ADMIN
Nombre de Contacto Administrativo	abelardo rodriguez giraldo
Dirección de Contacto Administrativo	CALLE 65 NO. 26-10
Ciudad de Contacto Administrativo	manizales
País de Contacto Administrativo	Colombia
Código de País de Contacto Administrativo	CO
Teléfono de Contacto Administrativo	 +571.0000000 
Correo electrónico de contacto administrativo	sistemas@ucaldas.edu.co
Numero Identificación de Contacto de Pago	14568-BILLING
Nombre de Contacto de Pago	universidad de caldas
Dirección de Contacto de Pago	CALLE 65 NO. 26 - 10
Ciudad de Contacto de Pago	manizales
País de Contacto de Pago	Colombia
Código de País de Contacto de Pago	CO
Teléfono de Contacto de Pago	 +571.0000000 

Ahora si nuestro objetivo es “eltiempo.com”, tendría que utilizar una de las paginas antes mencionadas, a continuación se mostrara la salida utilizando la página <http://www.domaintools.com/>



Wildcard search of all current/deleted/expired whois domains.
Domain Suggestions Engine serves over 10 Billion suggestions a year.

[Whois](#) [Suggestions](#) [Domain Search](#) [For Sale](#) [DNS Tools](#)

Whois Lookup:

```
Registrant:
Casa Editorial El Tiempo
Avenida El Dorado 59-70
Bogota, D.C., Cundinamarca N/A
COLOMBIA

Domain Name: ELTIEMPO.COM

Administrative Contact:
Rodriguez, Sandra sandro@eltiempo.com.co
Casa Editorial El Tiempo
Carrera 69 No. 25 B - 44 piso 3
Bogota D.C., Bogota D.C.
CO
57-1-5700222 fax: 57-1-2940159 ext. 5460

Technical Contact:
Role Account, DNS dns@eltiempo.com.co
Casa Editorial El tiempo
AV EL DORADO # 59-70
Bogota, DC 00000
CO
57-1-4266550

Record expires on 10-Oct-2012.
Record created on 11-Oct-1995.

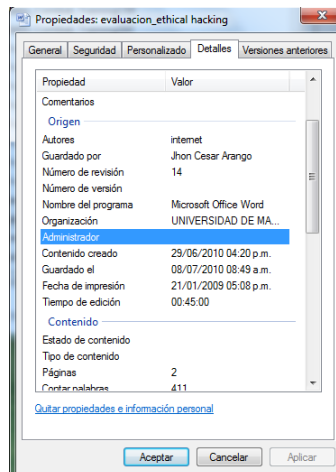
Domain servers in listed order:
NS1.IMPSTAT.NET.CO
DNS.ELTIEMPO.COM.CO
JUNO.IMPSTAT.NET.CO
```

Como se puede observar, explorando un registro de dominio, se suministra información relacionada con números telefónicos, fax, e-mail y otros datos que pueden ser de mucha utilidad a la hora de realizar un ataque.

Análisis de Metadatos

Los metadatos son datos que describen otros datos, un metadato es la propiedad que tiene cada archivo para indicar datos con relación al documento como fecha de creación, autor, fecha de modificación, equipo que lo almaceno, etc.

Al dar un Click derecho sobre un documento y ver sus propiedades podemos ver exactamente de lo que estamos hablando:



Ahora bien el objetivo de utilizar esta técnica es que mediante herramientas especializadas para la búsqueda de metadatos podamos obtener información adicional que permita perfilar más nuestro objetivo.

Las herramientas más certeras para la búsqueda de metadatos las podemos resumir en Metagoofil² y Foca³; estas hacen la búsqueda de documentos a través de los buscadores más populares; en el caso de Metagoofil se utiliza Google y el caso de Foca, herramienta más completa y especializada; la búsqueda lo hace a través de Google, Bind y Exalead

Metagoofil

La instalación de Metagoofil es sencilla, solo hay que descargarla del sitio oficial y una vez se descomprime se ejecuta a través de Python en un ambiente operativo Linux.

El comando a utilizar es: **“python metagoofil.py -d www.victima.com -l 20 -f pdf -o out.html -t out-files”**

-d = dominio de la victima

-l = numero de archives maximos a descargar

-f = tipo de archivos (pdf, doc, xls, all)

-o = como se guardara el resultado

-t = directorio que contendrá los archivos descargados

² <http://www.edge-security.com/metagoofil.php>

³ <http://www.informatica64.com/DownloadFOCA/>

```

root@itforensic-la:~# cd /pentest/enumeration/google/metagoofil/
root@itforensic-la:/pentest/enumeration/google/metagoofil# python metagoofil.py -d www.u
es.edu.co -l 20 -f pdf -o um.html -t um-files

*****
*MetaGooFil Ver. 1.4b
*Coded by Christian Martorella
*Edge-Security Research
*cmartorella@edge-security.com
*****

[+] Command extract found, proceeding with leeching
[+] Searching in www.u[REDACTED].edu.co for: pdf
840
[+] Total results in google: 840
[+] Limit: 20
[+] Searching results: 0
[ 1/20 ] http://www.u[REDACTED].edu.co/pagare.pdf
[ 2/20 ] http://www.u[REDACTED].edu.co/PagaresBlancoAutorizacion.pdf
[ 3/20 ] http://www.u[REDACTED].edu.co/ceanj/lopulicoparagrupojovenes.pdf#BUC6
[ 4/20 ] http://www.u[REDACTED].edu.co/odontologia/convocatoria_servicio_odontologia.pdf
[ 5/20 ] http://www.u[REDACTED].edu.co/ceanj/tesis/TesisDollyMagnoliaGonzalez.pdf
[ 6/20 ] http://www.u[REDACTED].edu.co/ceanj/tesis/TesisRocioAbelloCorrea.pdf
[ 7/20 ] http://www.u[REDACTED].edu.co/ceanj/tesis/TesisTomasSanchez.pdf

```

Una vez termine de procesar, el resultado esperado sería algo como:

```

Title(UNIVERSIDAD D[REDACTED])

Usernames found:
=====
AA-Abu-AA!
o-AA!ZA
A!A-AAuAA
AA-6tA'Âe
Administrador
AcAMAXAA
Author(usuario)

Paths found:
=====
\
(Windows\)\Author(usuario)\Company(um)\
[+] Process finished

```

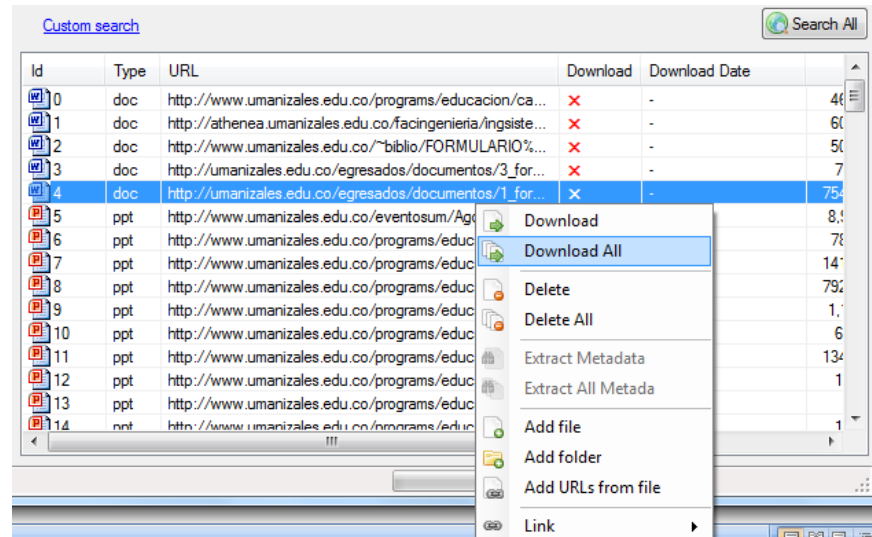
Foca

Solo funciona bajo Windows y es quizás la herramienta mas especializada para lo obtención de metadatos que permite encontrar: Usuarios, Sistemas Operativos, Recursos Compartidos, Impresoras, Nombres de Servidores Internos, Versiones de Software, entre otras.

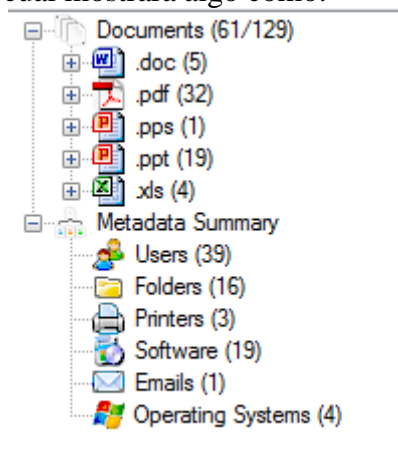
Una vez descargado e instalado Foca, creamos un nuevo proyecto para ello vaya a la opción de “File” → “New Project”, complete la información solicitada y luego presione el botón “Create”. En la siguiente ventana, seleccione para que la búsqueda la realice por los buscadores deseados y luego se elije los archivos a buscar, luego selecciona el botón de “Search All”

Entre más archivos busque, mas metadatos encontrara.

Una vez termine la búsqueda, sobre el área de los archivos encontrados, presione click derecho y escoja la opción “Download All” para descargar todos los archivos.



Finalizado, presione click derecho sobre los archivos descargados y escoja la opción de “Extract All Metadata”, para extraer todos los metadatos, lo cual mostrara algo como:



Solo basta con hacer un click en cada opción para conocer los resultados.

Para manejar esta herramienta recomiendo el manual oficial que puede obtener en:

<http://elladodelmal.blogspot.com/2010/07/foca-25-free-manual-de-usuario-1-de-6.html>

OSINT

Las redes sociales cada día cobran más fuerzas, es así como muchos usuarios crean sus perfiles indicando sus gustos, hobbies, profesiones, amigos y en fin una variedad de información que un atacante podría utilizar con el fin de realizar a futuro un ataque de Ingeniería Social.

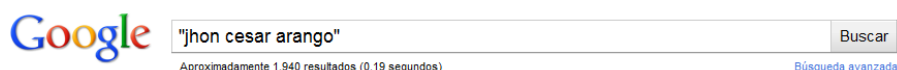
Es aquí donde nace OSINT que es un acrónimo anglosajón (Open Source Intelligence) usado para referirse a los recursos libremente accesibles con información de inteligencia. La recopilación y análisis de la información contenida en esas fuentes permiten crear un perfil completo de las personas que fueron descubiertas en las técnicas de “whois” o la “Análisis de Metadatos”.

Las unidades de gestión humana de cada empresa, empiezan a utilizar esta técnica con el fin de conocer realmente el perfil de la persona a emplear.

Algunos sitios públicos que se pueden utilizar:

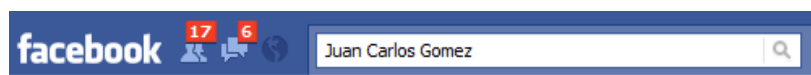
- <http://pipl.com/>
- <http://www.123people.com/>
- <http://whoozy.es/>
- <http://whostalkin.com/>
- <http://namechk.com/>
- <http://www.linkedin.com/>
- <http://www.facebook.com/>
- <http://delicious.com/>
- <http://twitter.com/>
- <http://google.com/>

Como ejemplo, tomemos el caso del nombre mio “Jhon Cesar Arango”, una búsqueda en Google me arroja algo más de 1900 resultados.



Si ingreso a cada enlace de esta búsqueda, puedo entender perfectamente el ambiente en que la persona se mueve, que estudios tiene, su experticia y en fin cualquier otra información útil.

Como otro ejemplo tomemos el buscador de FaceBook:



A preguntar por Juan Carlos Gomez, encontramos sus fotos de matrimonio, comentarios de sus amigos, los amigos mismos, videos, viajes, hobbies, etc.

Ya el lector se dará cuenta de lo importante de esta técnica.

IDENTIFICAR EL RANGO DE LA RED

Ahora que se tiene una dirección IP, nuestro objetivo es determinar el rango de red o la máscara de subred de nuestro objetivo.

Por ejemplo, con la dirección 10.10.10.5, desconociendo la máscara de subred, el atacante no tiene manera de conocer el rango de la dirección. La principal razón por la que desea conocer el rango de la dirección es para estar seguro de concentrar sus esfuerzos contra una red y no forzarse en varias, esto lo hace por dos razones:

- 1) Tratar de explorar una dirección clase A completa, le tomará mucho tiempo.
- 2) Algunas compañías tienen mejor seguridad que otras. Explorar una dirección más larga, aumenta el riesgo porque ahora un atacante debe forzarse en una compañía que tiene seguridad propia y esa compañía deberá reportar el ataque y poner en marcha la alarma.

Por ejemplo, si la máscara de subred es 255.0.0.0, entonces la red 10 completa pertenece a esa compañía y un atacante puede ir después a cualquier máquina. Por otro lado, si la máscara de subred es 255.255.255.0, entonces él puede solamente ir hasta 10.10.10.X, porque 10.10.11.X pertenece a alguien más.

Tal como se vio en el Capítulo 2, Una dirección IP está compuesta de dos partes: Una porción para red y una porción para host. Todos los computadores conectados a la misma red, deben tener la misma porción de dirección de red pero diferentes direcciones de host. Esto es similar a las casas: Dos casas en la misma manzana deben tener la misma dirección de la calle, pero diferente número de casa.

La máscara de subred se utiliza para indicarle al sistema cual parte de la dirección IP está en la porción de red y cual parte en la porción del host.

Un atacante puede obtener esta información de varias maneras:

- Arin / Apnic / Ripe /Lacnic
- Traceroute
- Hping
- Descubrimiento con DNS

Arin / Apnic /Lacnic

Además de la información suministrada por el supervisor de la red objetivo, otra fuente de información es el American Register for Internet Numbers, ARIN (<https://www.arin.net/>), Asia Pacific Network Information Center (<http://www.apnic.net/>), RIPE Network Coordination Centre (<http://www.ripe.net/>) y el Latin American and Caribbean Internet Address Registry (<http://www.lacnic.net/>).

Estas mantienen una base de datos al estilo “whois”, accesible desde Internet, que permite a los usuarios obtener información acerca de sus propios rangos de direcciones IP conferidos, o nombres de dominio, para organizaciones en Nortue América (Arin), Sur América y Caribe (Lacnic), Europa (Ripe) y las zonas asiáticas (Apnic). Así, mientras el registrador de la base de datos whois, le proporciona al usuario información particular de los nexos, la base de datos de estas fuentes, contiene todas las direcciones IP asignadas a una organización particular.

El problema que aquí radica es que al consultar estas fuentes, normalmente no vemos el rango de IP’s asignado a X empresa, si no que vemos el Rango de IP’s asignado al proveedor de servicios de la empresa objetivo, tal como se muestra en la grafica de la salida de lacnic, sin embargo el conocimiento ya del proveedor de servicios de Internet de la víctima es también un dato muy importante.



The screenshot shows the LACNIC website's Whois search interface. At the top, there's a navigation bar with links for LACNIC System, System Guide, Registration Documents, Fees, Statistics, F.A.Q, and Help. Below this, the 'REGISTRATION SERVICES' section is active, and the 'Whois' tab is selected. A search input field contains '200.1.0/17' and a 'SEARCH' button. The results display a series of status messages and a detailed registration record for the IP range 200.1.0/17, which is allocated to COLOMBIA TELECOMUNICACIONES S.A. ESP.

```

% Joint Whois - whois.lacnic.net
% This server accepts single ASN, IPv4 or IPv6 queries
% LACNIC resource: whois.lacnic.net

% Copyright LACNIC lacnic.net
% The data below is provided for information purposes
% and to assist persons in obtaining information about or
% related to AS and IP numbers registrations
% By submitting a whois query, you agree to use this data
% only for lawful purposes.
% 2010-08-05 13:17:20 (BRT -03:00)

inetnum: 200.1.0/17
status: allocated
owner: COLOMBIA TELECOMUNICACIONES S.A. ESP
ownerid: CO-CTSE-LACNIC
responsible: Administradores Internet
address: Transversal, 49, 105-84
address: N - BOGOTA -
country: CO
phone: +57 1 5935399 [1539]
owner-c: JRJ
tech-c: JRJ
abuse-c: CTE3
inetrev: 201.228.0/17
nserver: DNS5.TELECOM.COM.CO
nsstat: 20100802 AA
nelastaa: 20100802
created: 20051027
changed: 20091029
  
```

TracerRoute:

Es un programa de servicios de Internet que muestra por un lado el tiempo requerido para la llegada del paquete de datos del computador origen al computador destino a través de Internet y por otro lado permite descubrir el camino que el paquete o mensaje lleva desde la fuente hasta el destino.

Para entender mejor como trabaja traceroute es necesario tener algunos conocimientos básicos sobre ICMP y Ping, teniendo en cuenta que ping es un programa basado en el protocolo de control de mensajes por Internet (ICMP) y este es el que nos dice si hay una respuesta por parte del host o no.

Tal como vimos en el paso 1, el ping puede mostrar diferentes salidas cuando encuentra el destino dependiendo de la seguridad que este tenga, sin embargo; cuando no está disponible el objetivo, la salida sería algo como:

```
root@itforensic-la:~# ping thehackingday.com
ping: unknown host thehackingday.com
root@itforensic-la:~#
```

Si se desea conocer la ruta que toman los paquetes en la red, el programa que se debe utilizar es traceroute, el cual modifica el tiempo de vida TTL (Tracerouting relies on the time to live), en el encabezado IP. El campo TTL indica por cuantos puntos de conexión pasará un paquete antes de descender por los routers.

El programa traceroute envía paquetes con un TTL de 1; luego de 2; luego de 3 y así sucesivamente hasta llegar a su destino y refuerza cada router a lo largo de la vía, para enviar de regreso, mensajes de tiempo excedido, los cuales pueden ser usados para seguir la pista de cada punto de conexión desde la fuente hasta el destino.

```
root@itforensic-la:~# traceroute www.lapatria.com
traceroute to www.lapatria.com (198.104.188.87), 30 hops max, 40 byte packets
 1 192.168.1.254 (192.168.1.254) 4.348 ms 3.186 ms 1.408 ms
 2 epm200-13-227-187.epm.net.co (200.13.227.187) 30.237 ms * *
 3 static-epm200-13-229-158.epm.net.co (200.13.229.158) 33.610 ms 33.987 ms
36.856 ms
 4 adsl200-13-248-42.epm.net.co (200.13.248.42) 72.735 ms 72.374 ms 72.314 m
s
 5 190.248.0.14 (190.248.0.14) 40.266 ms 41.939 ms 43.961 ms
 6 190.248.0.45 (190.248.0.45) 84.277 ms 190.248.0.157 (190.248.0.157) 65.745
ms 65.509 ms
 7 xe-7-3.r03.miamfl02.us.bb.gin.ntt.net (157.238.179.105) 88.249 ms 86.352 m
s 78.497 ms
 8 ae-0.r20.miamfl02.us.bb.gin.ntt.net (129.250.2.18) 67.726 ms 67.941 ms 69
.856 ms
 9 as-2.r21.asbnva01.us.bb.gin.ntt.net (129.250.2.184) 98.423 ms 100.087 ms
100.149 ms
10 xe-1-1.r01.stngva01.us.bb.gin.ntt.net (129.250.2.85) 102.761 ms 118.852 ms
106.710 ms
11 ge-0-0-0.r00.stngva01.us.wh.verio.net (129.250.27.187) 99.564 ms 100.988 m
s 99.497 ms
12 pc-1.a0632.stngva01.us.wh.verio.net (198.66.145.90) 109.001 ms 95.265 ms 93.907 ms
13 val-lm00164.vwh.net (140.174.99.135) 98.224 ms 98.293 ms 93.497 ms
14 lapatria.com (198.104.188.87) 94.322 ms 94.716 ms 93.020 ms
root@itforensic-la:~#
```


Cada vez que un paquete viaja por la red, el TTL decrece.

TTL no se refiere a tiempo sino a puntos de conexión; por lo cual fue creado para que los paquetes tuvieran un tiempo de vida finito y no se tuvieran paquetes fantasmas circulando por la red infinitamente.

Cuando un router recoge un paquete con TTL 0, dicho paquete no llega a su destino. Si lo recoge con un TTL 1, el router determina si el siguiente punto de conexión del paquete es el destinatario. Si no lo es, el paquete se cae y debe ser lanzado nuevamente y se envía de regreso al emisor, un mensaje ICMP de “tiempo excedido”

Compañías que están conectadas a Internet tienen un router externo que conecta sus redes a sus ISPs (Internet Service Provider) o un Firewall. Entonces, cuando se inicia un Traceroute el último punto de contacto deberá ser la máquina destino; la segunda salida deberá ser el Firewall y la tercera deberá ser el router externo.

Los atacantes de redes utilizan la herramienta TTL para decidir la ruta que sus paquetes tomarán a través de la red y utilizan traceroute para determinar el camino para cada punto de conexión descubierto durante el barrido del ping.

Una vez hecho el barrido del ping y se determine cuáles hosts están activos, el atacante tiene que aprender la topología de la red y emplear el traceroute para conocer la variedad de routers y puertos que forman la estructura de la red objetivo.

Al finalizar la exploración con traceroute, el atacante analizará los resultados para cada objetivo y reconocerá los routers y entradas y creará un diagrama de la red. El no conocerá los propósitos de cada sistema, ni los elementos de la red, pero con un dibujo sencillo de la infraestructura, empezará a elaborar metódicamente la arquitectura del ataque.

Ahora bien, la utilización de esta técnica está siendo reemplazada por otra, la razón hoy en día existen muchos Firewall bloqueando nuestros paquetes, por lo que la siguiente técnica evitara los bloqueos de los cortafuegos.

Hping:

Hping es una excelente herramienta de tipo generador de paquetes TCP, UDP, ICMP, etc. Que nos permite hacer innumerables cosas, entre ellas, testear firewalls, scanner de puertos (mediante flags), Os Fingerprint, Traceo de rutas, e incluso D.o.S. Hping2 es una utilidad principalmente creada para auditar redes.

Utilizando el comando adecuado, podemos utilizar Hping como un trazador de rutas, solo basta con identificar un puerto que sepamos que el servidor objetivo, tenga abierto.

En un tracert realizado en una página del gobierno, se obtuvo el siguiente resultado:

```
root@itforensic-la:~# tracert www.████████.gov.co
tracert to www.████████.gov.co (190.████████.128.2████████), 30 hops max, 40 byte packets
 1 192.168.1.254 (192.168.1.254) 1.421 ms 1.763 ms 2.114 ms
 2 epm200-13-227-187.epm.net.co (200.13.227.187) 69.425 ms * *
 3 static-epm200-13-229-158.epm.net.co (200.13.229.158) 71.582 ms 72.593 ms
 4 adsl200-13-248-38.epm.net.co (200.13.248.38) 74.087 ms 74.575 ms 77.884 m
 5 190.248.0.14 (190.248.0.14) 78.105 ms 79.405 ms 80.171 ms
 6 190.248.0.110 (190.248.0.110) 82.288 ms 190.248.0.130 (190.248.0.130) 33.2
110 (190.248.0.110) 30.618 ms
 7 etb1-nap.ccit.org.co (206.223.124.193) 35.489 ms 190.248.0.81 (190.248.0.81
.954 ms
 8 * etb1-nap.ccit.org.co (206.223.124.193) 38.501 ms *
 9 10.5.2.238 (10.5.2.238) 44.643 ms * 44.285 ms
10 10.5.2.238 (10.5.2.238) 46.915 ms 47.146 ms 10.246.67.1 (10.246.67.1) 64.
11 10.246.67.1 (10.246.67.1) 64.442 ms * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
```

Como podran ver a partir del salto 12, no se muestra la salida; lo que nos hace suponer que existen dispositivos configurados de tal forma que bloquea la información entregada en esta petición.

Ahora bien, el mismo objetivo sabemos que el puerto 80 (Web Server) funciona sin problema alguno, porque al cargar la victima desde un navegador nos muestra su contenido. Ello nos indica que sus posibles cortafuegos tienen permitido el puerto 80.

Intentemos trazar la ruta con el siguiente comando, desde la consola de BackTrack:

“hping -S -n -z -p 80 -t 1 www.victima.com”

Una vez que este en marcha este comando, se presiona las teclas “CTRL+Z” para que se incremente la TTL y descubra todos los routers, hasta llegar al objetivo final.

```
root@itforensic-la:~# hping -S -n -z -p 80 -t 1 www.██████████.gov.co
HPING www.██████████.gov.co (eth0 190.██████████.128.203): S set, 40 headers + 0 data bytes
TTL 0 during transit from ip=192.168.1.254
TTL 0 during transit from ip=192.168.1.254
TTL 0 during transit from ip=192.168.1.254
2: TTL 0 during transit from ip=200.13.227.187
TTL 0 during transit from ip=200.13.227.187
TTL 0 during transit from ip=200.13.227.187
3: TTL 0 during transit from ip=200.13.229.158
TTL 0 during transit from ip=200.13.229.158
TTL 0 during transit from ip=200.13.229.158
TTL 0 during transit from ip=200.13.229.158
4: TTL 0 during transit from ip=200.13.248.38
TTL 0 during transit from ip=200.13.248.38
TTL 0 during transit from ip=200.13.248.38
5: TTL 0 during transit from ip=190.248.0.14
TTL 0 during transit from ip=190.248.0.14
TTL 0 during transit from ip=190.248.0.14
6: TTL 0 during transit from ip=190.248.0.130
TTL 0 during transit from ip=190.248.0.110
TTL 0 during transit from ip=190.248.0.130
TTL 0 during transit from ip=190.248.0.110
7: TTL 0 during transit from ip=206.223.124.193
TTL 0 during transit from ip=190.248.0.81
TTL 0 during transit from ip=206.223.124.193
TTL 0 during transit from ip=190.248.0.81
8: TTL 0 during transit from ip=190.248.0.81
8: TTL 0 during transit from ip=190.248.0.81
TTL 0 during transit from ip=206.223.124.193
TTL 0 during transit from ip=206.223.124.193
TTL 0 during transit from ip=206.223.124.193
9: TTL 0 during transit from ip=10.5.2.238
TTL 0 during transit from ip=10.5.2.238
TTL 0 during transit from ip=10.5.2.238
TTL 0 during transit from ip=10.5.2.238
10: TTL 0 during transit from ip=10.5.2.238
TTL 0 during transit from ip=10.246.67.1
TTL 0 during transit from ip=10.5.2.238
11: TTL 0 during transit from ip=190.24.128.194
TTL 0 during transit from ip=10.246.67.1
TTL 0 during transit from ip=190.24.128.194
TTL 0 during transit from ip=10.246.67.1
TTL 0 during transit from ip=190.24.128.194
12: TTL 0 during transit from ip=190.24.128.194
TTL 0 during transit from ip=190.24.128.194
13: len=46 ip=190.██████████.128.203 ttl=51 DF id=0 sport=80 flags=SA seq=59 win=5840 rtt=57.8 ms
len=46 ip=190.██████████.128.203 ttl=51 DF id=0 sport=80 flags=SA seq=61 win=5840 rtt=52.7 ms
14: len=46 ip=190.██████████.128.203 ttl=51 DF id=0 sport=80 flags=SA seq=63 win=5840 rtt=197.0 ms
len=46 ip=190.██████████.128.203 ttl=51 DF id=0 sport=80 flags=SA seq=64 win=5840 rtt=86.1 ms
len=46 ip=190.██████████.128.203 ttl=51 DF id=0 sport=80 flags=SA seq=65 win=5840 rtt=185.8 ms
len=46 ip=190.██████████.128.203 ttl=51 DF id=0 sport=80 flags=SA seq=66 win=5840 rtt=100.3 ms
len=46 ip=190.██████████.128.203 ttl=51 DF id=0 sport=80 flags=SA seq=67 win=5840 rtt=97.5 ms
^C
```

Como pudo ver en los gráficos, este tracer si llego hasta su destino final.

Los parámetros utilizados en este comando, lo dejo como tarea para el lector para que investiguen el uso de esta herramienta.

Descubrimiento con DNS

Esta técnica permite extraer la información de los DNS del objetivo, entre los cuales podría encontrar: Sus servidores Mx (correo electrónico), nombres de servidores, direcciones IP de los diferentes servidores dentro del segmento IP analizado, etc.

Algunas páginas como:

<http://centralops.net/co>
<http://www.intodns.com/>
<http://news.netcraft.com/>

Me permiten mostrar su configuración o la salud del DNS del objetivo de una manera pasiva, lo cual incrementaría la información que estoy recolectando de la víctima.

Algunas ideas de cómo utilizar estas herramientas son:

Este reporte me genera los registros del DNS, el “whois” del dominio y la “whois” de la red con la que puedo establecer la máscara de red utilizada por el objetivo.



The screenshot shows the CentralOps.net website with the 'Domain Dossier' tool active. The tool's interface includes a sidebar with various utilities like Domain Dossier, Domain Check, Email Dossier, Browser Mirror, Ping, Traceroute, Nslookup, AutoWhois, TcpQuery, and AnalyzePath. The main area is titled 'Domain Dossier' and 'Investigate domains and IP addresses'. It features a search bar with 'thehackingday.com' entered. Below the search bar are checkboxes for 'domain whois record', 'DNS records', 'tracert', 'network whois record', and 'service scan'. A 'go' button is present. At the bottom, there is a user status bar showing 'user: 190.28.52.217 [anonymous] 47/50' and a 'log in | get account' link. A promotional banner at the bottom says 'New: Compare web hosting plans across multiple providers: shared | VPS | dedicated'.

Este reporte me entrega la salud de la configuración del DNS del objetivo.



The screenshot shows the intoDNS beta website. It features a logo with a blue and grey pixelated design. Below the logo is a search bar containing 'thehackingday.com' and a 'Report' button. At the bottom, there is a promotional banner that says 'NEW! Follow IntoDNS on Twitter'.

Este reporte me muestra todos los dominios que tienen la palabra hackingday.com, como su posible huella del sistema operativo.



The screenshot shows the PETCRAFT website. It features a logo with the word 'PETCRAFT' in a stylized font. Below the logo is a search bar with the text 'What's that site running?' and a search button. The search bar contains 'thehackingday.com'.

Ahora bien, como se que nos gusta el camino difícil, explicare brevemente la forma de utilizar el comando “host” y el comando “dig”, para conocer el posible dimensionamiento de la red de nuestro objetivo.

Antes que nada debemos conocer que el descubrimiento de DNS se divide en 3 tipos: Forward Lookup, Reverse Lookup y Zone Transfers.

Forward Lookup

Esta técnica me permite conocer la dirección IP, si conozco de antemano el dominio que deseo consultar, la utilización de este comando desde BackTrack seria:

```
root@itforensic-la:~# host www.apple.com
www.apple.com is an alias for www.isg-apple.com.akadns.net.
www.isg-apple.com.akadns.net is an alias for www.apple.com.edgekey.net.
www.apple.com.edgekey.net is an alias for e3191.c.akamaiedge.net.
e3191.c.akamaiedge.net has address 96.16.253.15
```

Reverse Lookup

Esta técnica me permite conocer el dominio dada una IP, la utilización de este comando desde BackTrack seria:

```
root@itforensic-la:~# host 96.16.253.15
15.253.16.96.in-addr.arpa domain name pointer a96-16-253-15.deploy.akamai.com.
```

Zone Transfer

La transferencia de zonas, me permite conocer sobre un dominio si tiene servidores propios de DNS y así consultarlos para ver como tiene identificados los servidores con IP's publicas que pasan por su dominio.

Para ello utilizamos el comando "dig" como se muestra a continuación:

```
root@itforensic-la:~# dig compu[redacted].com.co

; <<>> DiG 9.5.0-P2.1 <<>> compu[redacted].com.co
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6290
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;compu[redacted].com.co.      IN      A

;; ANSWER SECTION:
compu[redacted].com.co.    6449    IN      A      200.1.54.165
compu[redacted].com.co.    6449    IN      A      200.1.243.243
compu[redacted].com.co.    6449    IN      A      200.1.54.164

;; AUTHORITY SECTION:
compu[redacted].com.co.    84938   IN      NS      DNS3.compu[redacted].com.co.
compu[redacted].com.co.    84938   IN      NS      DNS.compu[redacted].com.co.

;; ADDITIONAL SECTION:
DNS.compu[redacted].com.co. 6129    IN      A      200.1.243.243
DNS3.compu[redacted].com.co. 30461   IN      A      200.1.54.165

;; Query time: 36 msec
;; SERVER: 192.168.1.254#53(192.168.1.254)
;; WHEN: Fri Aug 6 08:08:13 2010
;; MSG SIZE rcvd: 152
```

Tal como muestra el grafico anterior, nuestro objetivo es ubicar los servidores DNS, los cuales se muestran enmarcados en el cuadro verde y si vemos un poco más abajo podemos ver por cada servidor DNS (dns y dns3) su dirección IP. Ya con esta información podemos complementar el comando “dig” para que nos muestre la información de las diferentes IP y servidores que son resueltos por uno de estos DNS. El comando a utilizar es “**dig @IP_DNS nombre_dominio axfr**”, el resultado seria

```

root@itforensic-la:~# dig @200.54.165.compu.com.co axfr

; <<>> DiG 9.5.0-P2.1 <<>> @200.54.165.compu.com.co axfr
; (1 server found)
;; global options: printcmd
compu.com.co. 86400 IN SOA dns3.compu.com.co. afrendon\compu.com.co. 2006021741 10800 1800 3600000 86400
compu.com.co. 86400 IN A 200.243.243
compu.com.co. 86400 IN A 200.54.164
compu.com.co. 86400 IN A 200.54.165
compu.com.co. 86400 IN NS DNS.compu.com.co.
compu.com.co. 86400 IN NS dns3.compu.com.co.
compu.com.co. 86400 IN MX 0 MAIL.compu.com.co.
compu.com.co. 86400 IN MX 10 MX3.compu.com.co.
ADI.compu.com.co. 86400 IN A 200.243.252
ALMACENAR.compu.com.co. 86400 IN A 200.244.245
APLICACIONES.compu.com.co. 86400 IN A 200.244.244
ASOFONDOS.compu.com.co. 86400 IN A 200.54.162
BANACOL.compu.com.co. 86400 IN A 200.244.244
BRASILIA.compu.com.co. 86400 IN A 200.244.246
CENISS.compu.com.co. 86400 IN A 200.54.163
COMFENALCO.compu.com.co. 86400 IN A 200.244.244
CRBOG.compu.com.co. 86400 IN A 200.54.164
CRUCERO.compu.com.co. 86400 IN A 200.243.243
CRYSTAL.compu.com.co. 86400 IN A 200.244.245
CSMARCO.compu.com.co. 86400 IN A 200.244.245
DELIMA.compu.com.co. 86400 IN A 200.244.246
DNS.compu.com.co. 86400 IN A 200.243.243

```

Como pueden apreciar, obtuvimos una lista de servidores e IP's las cuales me permiten dimensionar la red, además me permite deducir si se trata de una empresa que tiene sus propios servidores con IP pública o simplemente un Hosting, como este caso.

Tenga en cuenta que no necesariamente los equipos que se muestran en este resultado, existen. Seria tarea nuestra de ver la efectividad de cada servidor con el comando “ping” o el comando “hping”.

Otras herramientas disponibles en BackTrack como “dnsrecon” y “fierce”, nos permite en cierta forma obtener los mismos resultados.

A continuación veremos la salida de estos dos comandos y los parámetros a utilizar:

Como podemos ver en la siguiente salida, el comando “dnsrecon” nos muestra el segmento IP que nos permite determinar que la IP detectada es una clase “C” y también nos muestra posibles maquinas dentro de dicho segmento.

```

^Croot@itforensic-la:/pentest/enumeration/dnsrecon# ruby dnsrecon.rb -b um [redacted] .edu.co hosts.txt
admin.u [redacted] es.edu.co,201. [redacted] 8.3.8
correo.t [redacted] es.edu.co,201. [redacted] 8.3.11
ftp.u [redacted] .edu.co,201. [redacted] 3.3.3
gateway.t [redacted] .edu.co,201. [redacted] 8.3.2
mail.u [redacted] es.edu.co,74.125.47.121
router.t [redacted] es.edu.co,201. [redacted] 3.3.1
um.t [redacted] .edu.co,201. [redacted] 8.3.3
venus.u [redacted] .edu.co,201 [redacted] 3.3.18
www.t [redacted] .edu.co,201. [redacted] 8.3.3

```

En la siguiente salida de “fierce”, podemos ver un resultado más completo:

```

root@itforensic-la:/pentest/enumeration/fierce# perl fierce.pl -dns u [redacted] s.edu.co -wordlist
hosts.txt
DNS Servers for u [redacted] .edu.co:
ns.u [redacted] .edu.co

Trying zone transfer first...
Testing ns.u [redacted] .edu.co
Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 1896 test(s)...
201. [redacted] 3.3 ns.u [redacted] .edu.co
201. [redacted] 3.1 router.u [redacted] .edu.co
201. [redacted] 3.2 gateway.t [redacted] .edu.co
201. [redacted] 3.6 campusvirtual.t [redacted] .edu.co
201. [redacted] 3.7 virtual.u [redacted] .edu.co
201. [redacted] 3.8 admin.t [redacted] .edu.co
201. [redacted] 3.9 athenea.t [redacted] .edu.co
201. [redacted] 3.10 ingenieria.t [redacted] .edu.co
201. [redacted] 3.11 correo.u [redacted] .edu.co
201. [redacted] 3.12 aiesec.t [redacted] .edu.co
201. [redacted] 3.13 virtualmoodle.t [redacted] .edu.co
201. [redacted] 3.15 atilla.t [redacted] .edu.co
201. [redacted] 3.17 prometeo.t [redacted] .edu.co

```

BUSCAR MAQUINAS ACTIVAS

Después de que un atacante obtiene el rango de direcciones, puede continuar acumulando información mediante la búsqueda de servidores activos en la red.

Con mucha frecuencia las compañías tienen rangos de direcciones mayores de los que necesita y pueden crecer aun más, diferentes máquinas pueden estar activas por diferentes períodos de tiempo durante el día y entran nuevamente en las horas de la noche. Los servidores pueden estar activos durante todo el día y las estaciones de trabajo entrar solamente en jornada normal de trabajo.

Para un atacante que está todo el día explorando máquinas activas, le queda muy fácil diferenciar entre servidores y estaciones de trabajo. Sin embargo, esta técnica aporta al atacante muy poca información dado que en la actualidad, más y más compañías están empleando la traducción de direcciones de red (NAT) a redes privadas. Por ejemplo, si solo se tienen dos aparatos con dirección publica y todos los demás con Firewall, un atacante fácilmente puede pensar que solo hay dos máquinas, cuando en realidad hay muchas más.

Este es uno de los beneficios de utilizar direcciones privadas y NAT porque con NAT una compañía usa direcciones privadas para sus maquinas internas, en cualquier momento estas maquinas necesitan acceso a internet, y utilizando NAT, por lo general el firewall o router, traslada una dirección privada a una dirección publica.

Por otro lado aparece un esquema muy utilizado cuando de seguridad y de IP publicas escasas se tratan y es el “Reenvio de Puertos”, un cliente puede hacer una petición a un puerto determinado de una IP publica, automáticamente el firewall reenvía la petición a un equipo de la Intranet con IP privado a otro puerto asociado.

Como podrán notar el descubrimiento de maquinas activas es hoy un tarea compleja que no se resuelve solamente con un simple “ping”, para ello utilizaremos técnicas especializadas con una sola herramienta llamada “nmap”.

Desde la versión 5.0 NMap⁴ es una de las herramientas preferidas por los expertos en seguridad y por los atacantes, Fyodor's su creador, ha tenido mucho trabajo, realizo mas de 600 cambios lo que convierte a esta versión 5.0 de NMap, la mas importante desde su lanzamiento en 1997.

Algunas características del NMap son:

- Identificar computadores de una red
- Identifica puertos abiertos en un computador objetivo.
- Determina qué servicios está ejecutando.
- Determinar qué sistema operativo y versión utiliza dicha computadora, (fingerprinting).

⁴ <http://nmap.org>

- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

Para nuestro caso “identificar computadores de una red”, utilizaremos dos tipos de búsquedas:

- Búsqueda de Maquinas Activas Básico.
- Búsqueda de Maquinas Activas Optimizado.

Búsqueda de Maquinas Activas Básico

El descubrimiento básico o por defecto de Nmap, se conoce con el nombre de “Nmap Ping”, su funcionamiento radica en enviar a nuestro objetivo un ICMP Echo Request (Ping) y un paquete ACK al puerto 80.

El comando para realizar este descubrimiento es:

“nmap -n -sP IP_Victima/CIDR”

Como podrá notar en los pasos previos, fue necesario descubrir una Dirección IP y por supuesto el posible numero de Bits de su máscara, para aplicar este comando, con lo cual tendríamos una salida como:

```
root@itforensic-la:~# nmap -n -sP 201.1.1.3.0/24
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-08-09 13:43 COT
Nmap scan report for 201.1.1.3.1
Host is up (0.075s latency).
Nmap scan report for 201.1.1.3.9
Host is up (0.076s latency).
Nmap scan report for 201.1.1.3.11
Host is up (0.070s latency).
Nmap scan report for 201.1.1.3.12
Host is up (0.091s latency).
Nmap scan report for 201.1.1.3.17
Host is up (0.065s latency).
Nmap scan report for 201.1.1.3.20
Host is up (0.089s latency).
Nmap scan report for 201.1.1.3.21
Host is up (0.072s latency).
Nmap scan report for 201.1.1.3.30
Host is up (0.070s latency).
Nmap scan report for 201.1.1.3.33
Host is up (0.078s latency).
Nmap scan report for 201.1.1.3.40
Host is up (0.067s latency).
Nmap scan report for 201.1.1.3.41
Host is up (0.072s latency).
Nmap scan report for 201.1.1.3.44
Host is up (0.086s latency).
Nmap scan report for 201.1.1.3.111
Host is up (0.073s latency).
Nmap done: 256 IP addresses (13 hosts up) scanned in 4.29 seconds
```

En esta salida se descubren 13 equipos.

Búsqueda de Maquinas Activas Optimizado

El comando anterior aunque hoy es utilizado, puede ser poco efectivo a la hora de descubrir los equipos que realmente están activos en la red.

¿Que sucede con los equipos cuyo firewall rechazan el ping o como si fuera poco con los firewall configurados con la opción de filtrado por

paquetes statefull, que no permitiría pasar peticiones al puerto 80 tan fácilmente ya que verifica la conexión entre el origen y el destino?: La respuesta sencilla, con el comando anterior estos equipos nunca hubieran sido descubiertos.

Antes de continuar es necesario aclarar la diferencia entre un Firewall con filtrado de paquetes StateLess y otro StateFul.

El Filtrado de paquetes StateLess sólo intenta examinar los paquetes IP independientemente, lo cual corresponde al nivel 3 del modelo OSI. Sin embargo, la mayoría de las conexiones son admitidas por el protocolo TCP, el cual administra sesiones, para tener la seguridad de que todos los intercambios se lleven a cabo en forma correcta. Asimismo, muchos servicios (por ejemplo, FTP) inician una conexión en un puerto estático. Sin embargo, abren un puerto en forma dinámica (es decir, aleatoria) para establecer una sesión entre la máquina que actúa como servidor y la máquina cliente.

De esta manera, con un filtrado de paquetes StateLess, es imposible prever cuáles puertos deberían autorizarse y cuáles deberían prohibirse.

El Filtrado de paquetes StateFul, se basa en la inspección de las capas 3 y 4 del modelo OSI, lo que permite controlar la totalidad de las transacciones entre el cliente y el servidor.

Un firewall con "inspección stateful" puede asegurar el control de los intercambios. Esto significa que toma en cuenta el estado de paquetes previos cuando se definen reglas de filtrado. De esta manera, desde el momento en que una máquina autorizada inicia una conexión con una máquina ubicada al otro lado del firewall, todos los paquetes que pasen por esta conexión serán aceptados implícitamente por el firewall.

El hecho de que el filtrado dinámico sea más efectivo que el filtrado básico de paquetes no implica que el primero protegerá el ordenador contra los hackers que se aprovechan de las vulnerabilidades de las aplicaciones. Aún así, estas vulnerabilidades representan la mayor parte de los riesgos de seguridad.

La idea de buscar maquinas activas con un comando optimizado es la de utilizar diferentes técnicas que nos permitan pasar por el control de la red objetivo, para ello es necesario entender los parámetros que maneja "Nmap".

Si queremos descubrir equipos detrás de un Firewall StateFul deberíamos utilizar paquetes SYN, ya que si utilizamos paquetes ACK y no existe un registro previo en la tabla de estado del Firewall, el ACK seria descartado.

Esto lo podríamos realizar aplicando a Nmap el parámetro: "-PS".

Por otro lado, si los equipos a descubrir están detrás de un Firewall StateLess la recomendación es utilizar paquetes ACK, ya que como el Firewall no posee una tabla de estado creará que el paquete pertenece a una conexión pre establecida y lo dejara pasar.

Esto lo podríamos realizar aplicando a Nmap el parámetro: "-PA".

Ambos parámetros van acompañados de unos puertos, la presentación hecha por Fyodor⁵ en Defcon⁶ 16 de 2008 se publico un listado de los 10 puertos más utilizados en internet, los cuales podemos utilizar en nuestros parámetros.

Top 10 TCP ports	Top 10 UDP ports
- 80 (http)	- 137 (netbios-sn)
- 23 (telnet)	- 161 (snmp)
- 22 (ssh)	- 1434 (ms-sql-m)
- 443 (https)	- 123 (ntp)
- 3389 (ms-term-serv)	- 138 (netbios-dgm)
- 445 (microsoft-ds)	- 445 (microsoft-ds)
- 139 (netbios-ssn)	- 135 (msrpc)
- 21 (ftp)	- 67 (dhcps)
- 135 (msrpc)	- 139 (netbios-ssn)
- 25 (smtp)	- 53 (dns)

Ejemplos: "-PS80,22,25,443,21" y/o "-PA80,22,25,443,21"

Otra opción sería realizar un descubrimiento mediante puertos UDP, para el caso sería buscar puertos cerrados que nos devuelvan un erro ICMP Port Unreachable, ya que si enviamos un paquete sin contenido a un puerto UDP abierto, el sistema que lo reciba no sabrá que hacer con él y simplemente los descartara. Para este caso la recomendación seria elegir un puerto UDP alto que con seguridad no este en uso, Fyodor también recomienda sumar el puerto 53 (DNS).

Esto lo podríamos realizar aplicando a Nmap el parámetro: "-PU".

Ejemplo: "-PU33221,53"

El clásico "Nmap Ping", utiliza "ICMP Echo Request" que suele estar filtrado por los Firewalls, por lo que es recomendable agregar otro tipo de Echo Request diferente del paquete ICMP, como por ejemplo el "Timestamp Request" o el "Netmask Request".

⁵ <http://www.kungfoosion.com/2008/10/cmo-optimizar-el-host-discovery-en-nmap.html>

⁶ <http://www.defcon.org/>

Esto lo podríamos realizar aplicando a Nmap el parámetro: “-PE” (Echo Req) y “-PP” (Timestamp Req).

En conclusión, si seguimos todas las recomendaciones vistas anteriormente nuestro comando “nmap” visto en la búsqueda básica, cambiaría a algo como:

**“nmap -n -sP -PSlista_puertos_tcp -PALista_puertos_tcp
-PULista_puertos_udp -PE -PP IP/CIDR”**

Ejemplo Búsqueda Básica donde se encuentra 114 Hosts.

```
root@itforensic-la:~# nmap -n -sP 200.69.107.0/24
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-08-20 10:20 COT

Nmap done: 256 IP addresses (114 hosts up) scanned in 135.29 seconds
root@itforensic-la:~#
```

Ejemplo Búsqueda optimizada donde se encuentra 116 Hosts.

```
root@itforensic-la:~# nmap -n -sP -PE -PP -PS21,23,25,80,110,443,445,3389 200.69.107.0/24
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-08-20 12:06 COT

Nmap done: 256 IP addresses (116 hosts up) scanned in 367.85 seconds
```

BUSCAR PUERTOS Y SERVICIOS

Ahora que el atacante tiene un mapa bastante bueno de la red y sabe con exactitud cuales máquinas están activas y cuáles no, puede empezar a calcular la vulnerabilidad de las máquinas. Un atacante actúa exactamente igual a un ladrón de casas, el cual busca los puntos vulnerables por donde dirigir el ataque, tales como puertas y ventanas, por donde pueda acceder con facilidad. Un atacante informático busca los puertos que estén abiertos, los puntos más vulnerables de la red y los pocos puertos que estén seguros.

Para detectar en un sistema los puertos que están abiertos, un atacante puede usar un programa llamado Port Scanner (Explorar puertos), el cual se ejecuta a través de una serie de puertos y va detectando los que están abiertos, los cuales son altamente vulnerables.

Si una compañía está tratando de conocer la vulnerabilidad de sus máquinas, es un trabajo muy dispendioso explorar cada una en forma individual, por lo que es muy recomendable tener en su propiedad un explorador de puertos, el cual agrupa todos los rangos de puertos del programa y explora todas las máquinas a la vez. Es importante anotar que la exploración se debe hacer a los puertos TCP y UDP y no solamente a uno de los dos. Muchas compañías exploran solo los puertos TCP, lo cual es conocido por los atacantes que se esconderían entonces en los puertos UDP.

Mediante la exploración de puertos comunes en cada una de las direcciones IP potenciales, es posible determinar que host están activos, localizando aquellos puertos del sistema que se encuentren abiertos.

Uno de los pioneros en el desarrollo de las diversas técnicas de exploración de puertos es Fyodor., el cual ha incorporado numerosas técnicas de exploración de puertos, en su herramienta Nmap.

INTRODUCCIÓN PUERTOS Y SERVICIOS

Después de conocer los puertos que están abiertos un atacante necesita saber que servicios corren en cada puerto. Conocer el servicio específico que ejecuta cada puerto le facilita al atacante buscar el ataque y lanzar estos conocimientos contra los servicios más vulnerables. Lo primero que debe hacer es utilizar la información por defecto.

Basado en una configuración común y un software el atacante puede hacer un cálculo de que servicios se están ejecutando y en que puertos; por ejemplo: si él sabe que el sistema operativo es Unix y el puerto que está abierto es el 80 le queda fácil suponer que se está ejecutando un Apache Web Server (httpd) y si el sistema operativo es Windows 2008 y el puerto que está abierto es el 80 puede suponer que hay un Internet Information Server instalado, esto es una manera fácil de comprender

cuales servicios se están ejecutando, pero saber que el puerto 80 está abierto, no es garantía absoluta de que se está ejecutando un programa de Web Server.

Para entender los puerto y servicios que se corren en cada servidor es conveniente que observe los archivos “services” que encuentra en los diferentes sistemas operativos, para el caso de Linux este lo puede encontrar en la ruta “/etc/services”, para el caso de Windows en la ruta “Windows/System32/Drivers/Etc/Services”.

PORTSCANERS

Llegado a este punto, un atacante ya sabe identificar que sistemas están activos en una red, mediante el uso de barridos ping, TCP o ICMP; tiene un entendimiento básico de la topología de la red y sabe como reunir información ICMP. Ahora ya está preparado para descubrir el propósito de cada máquina y aprender las entradas potenciales dentro de la máquina por la exploración de los puertos de cada sistema.

La exploración de puertos es el proceso de conexión a puertos UDP y TCP, del sistema objetivo, para determinar que servicios se están ejecutando o si está en un estado de LISTENING (de escucha).

Identificar los puertos UDP y TCP que están a la escucha, es de suma importancia para un atacante determinar el tipo de sistema operativo y aplicaciones que se están utilizando. Los servicios activos que estén a la escucha pueden permitir que el atacante tenga acceso a sistemas mal configurados o que ejecuten una versión de software que tenga problemas de seguridad.

Cada máquina con una pila TCP/IP tiene 65.535 puertos TCP y 65.535 puertos UDP. Cada puerto con un servicio de escucha es una entrada potencial, para un atacante, el cual cuidadosamente hará un recuento de los puertos abiertos. Por ejemplo, si se está ejecutando un servidor Web, la escucha es más probable en un puerto TCP 80. Si se está ejecutando un servidor DNS, se abrirá el puerto UDP 53. Si la máquina provee espacios (hosting) en un servidor de mail de internet, muy probablemente se abre el puerto TCP 25. Por supuesto, cualquier servicio puede ser configurado para escuchar en cualquier puerto, pero el principal servicio escucha en una variedad de números de puertos bien conocidos.

Con una lista de puertos abiertos, el atacante puede tener una idea de cuales servicios están en uso, consultando RFC 1700⁷, números asignados, la cual contiene una lista de números de puertos más comúnmente usados.

⁷ <http://www.faqs.org/rfcs/rfc1700.html>

Es muy peligroso que un atacante tenga acceso a esta información, porque si él irrumpe dentro de una máquina y abre un puerto como una puerta trasera o secreta, él abrirá un puerto muy elevado, por ejemplo el puerto 40.000, con la esperanza de que la compañía no lo note.

La mayoría de las herramientas para explorar puertos, puede rastrear una lista de puertos específicos, o todos los puertos TCP y UDP posibles.

Algunas técnicas de exploración de puertos son:

Exploración de conexión TCP:

Es el tipo más común de exploración. El programa trata de conectar cada puerto a una máquina usando el sistema de llamadas e intentando completar un acuerdo completo de tres direcciones. Si la máquina destino responde, el puerto está activo.

Exploración TCP SYN:

Esta técnica es conocida como exploración semi abierta, porque no se realiza una conexión TCP completa. Por el contrario, se envía un paquete SYN al puerto objetivo. Si se recibe un SYN/ACK de este puerto se puede decir que está en el estado de LISTENING (a la escucha) y si se recibe un RST/ACK, quiere decir que no está a la escucha y por lo tanto no se lleva a cabo una conexión completa. Esta técnica tiene la ventaja de ser muy cautelosa y puede no ser detectada por el sistema objetivo.

Exploración TCP FIN:

Esta técnica envía un paquete FIN al puerto destino. Después de que está establecida la conexión, dos máquinas envían mensajes atrás y adelante. Cuando está hecha la comunicación se envía un paquete con el conjunto bits FIN y se rompe la comunicación. Ahora bien, la manera como trabaja TCP consiste en que si se envía un paquete a un puerto cerrado, el sistema responde con un comando RST diciendo que el puerto no está abierto. La manera como trabaja este explorador es enviando un paquete con el conjunto de bits FIN. Si el puerto está abierto, se ignora, pero si el puerto está cerrado, se obtiene un RTS por respuesta. Este tipo de exploración es muy escurridizo porque la mayoría de los sistemas no llevan un registro de estos paquetes.

Exploración Nula TCP:

Esta técnica desactiva todas las banderas (flags).

Exploración TCP ACK:

Esta técnica se utiliza para definir los conjuntos de reglas del firewall. Puede ayudar a determinar si el firewall es un simple filtro de paquetes que solo permitirá las conexiones predefinidas (Conexiones con el conjunto de bits ACK) o se trata de un firewall completo que realiza un filtrado de paquetes completo.

Exploración de ventanas TCP:

Esta técnica puede detectar puertos abiertos, así como puertos filtrados y no filtrados de algunos sistemas. Por ejemplo AIX y FreeBSD, debido a una anomalía en el sistema de información sobre el tamaño de las ventanas TCP.

Exploración UDP:

Esta técnica envía un paquete UDP al puerto objetivo. Si el puerto responde con un mensaje similar a “puerto ICMP no alcanzable”, el puerto está cerrado; si no se recibe dicho mensaje, el puerto está abierto. Dado que UDP es un protocolo sin conexión, la fiabilidad de esta técnica depende en gran medida de muchos factores relacionados con la utilización de los recursos del sistema y la red.

La exploración UDP es un proceso muy lento si se desea analizar un dispositivo que utilice filtrado pesado de paquetes, por tanto los resultados son poco confiables.

NMAP ('NETWORK MAPPER'):

Como ya se había mencionado, Nmap es la mejor herramienta disponible para la exploración de puertos y cuenta con funciones básicas de exploración UDP y TCP.

Nmap es el explorador de puertos más recomendado para ambientes Linux, y es la pieza necesaria en una caja de herramientas de seguridad.

Con un parámetro adicional a las instrucciones antes vistas de Nmap, podemos hacer que esta herramienta nos saque un reporte de los puertos y de los servicios de la o las máquinas escaneadas, el parámetro es la opción “-v”.

Ejemplo del comando a ejecutar:

“nmap -v -PE -PS22,25,80 -PA21,23,80,3389 IP_Victima”


```

root@itforensic-la:~# nmap -v -PE -PS22,25,139,80 -PA21,23,80,3389 192.168.1.159

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-08-26 08:30 COT
Initiating ARP Ping Scan at 08:30
Scanning 192.168.1.159 [1 port]
Completed ARP Ping Scan at 08:30, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:30
Completed Parallel DNS resolution of 1 host. at 08:30, 0.37s elapsed
Initiating SYN Stealth Scan at 08:30
Scanning 192.168.1.159 [1000 ports]
Discovered open port 139/tcp on 192.168.1.159
Discovered open port 135/tcp on 192.168.1.159
Discovered open port 445/tcp on 192.168.1.159
Discovered open port 1025/tcp on 192.168.1.159
Discovered open port 5000/tcp on 192.168.1.159
Completed SYN Stealth Scan at 08:30, 0.12s elapsed (1000 total ports)
Nmap scan report for 192.168.1.159
Host is up (0.00047s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
5000/tcp   open  upnp
MAC Address: 00:0C:29:F3:16:78 (VMware)

```

Nmap hace posible ejecutar todos los diferentes tipos de exploraciones y tiene muchas características útiles. Supongamos que después de realizar un rastreo a una organización, se descubre que como cortafuegos (firewall) principal dicha empresa está usando un dispositivo sencillo de filtrado de paquetes. Se puede utilizar la opción `-f` de Nmap para fragmentar los paquetes. Esencialmente, esta opción distribuye las cabeceras TCP de los paquetes, por lo que los dispositivos de control de acceso y los sistemas IDS (sistema de detección de intrusos) tendrán más dificultades a la hora de detectar la exploración.

Cuanto mas sofisticadas sean las redes y host objetivo, más fácil será para un atacante detectar las exploraciones que realice. Nmap dispone de funciones adicionales de señuelo diseñadas para saturar el sitio objeto de información redundante, mediante el uso de la opción `-D`, al tiempo con la información real. El sistema objeto tendrá el trabajo adicional de intentar rastrear todas las exploraciones y determinar las legítimas y las falsas, para lo cual la dirección objetivo debe estar activa, o las exploraciones podrían producir desbordamientos SYN en el sistema objetivo y provocar una negación de servicio.

Después de ejecutar la exploración de puertos y servicios en la red objetivo, un atacante tiene una idea real muy buena de los puntos de acceso dentro de los sistemas de cómputo.

ENCONTRAR VERSIONES DE SISTEMAS OPERATIVOS Y APLICACIONES:

Ahora que el atacante ha hecho una cantidad significativa de progresos en su decisión de atacar un objetivo, tales como conocer perfiles de personas, que máquinas están activas y que puertos están abiertos, debe empezar a calcular cuales sistemas operativos se están ejecutando en cada pc victima, así como su versión y debe establecer las versiones de las aplicaciones que están corriendo en los diferentes puertos descubiertos.

La información sobre el Sistema Operativo y las versiones de las aplicaciones que se encuentren, será de mucha utilidad durante la fase de búsqueda de vulnerabilidades asociadas al sistema objetivo.

Se pueden utilizar técnicas muy sencillas de captura de información a partir de los servicios FTP, telnet, SMTP y otros. Esta es la forma más sencilla de detectar sistemas operativos y el número de la versión asociado al servicio que se está ejecutando. Sin embargo, una herramienta mas precisa que dispone un atacante es la todo poderoso Nmap, esta cuenta con rastreo de pilas. (Stack Fingerprinting).

El rastreo de pilas es una técnica extremadamente potente que permite averiguar rápidamente y con gran probabilidad de acierto, cuál es el sistema operativo instalado en el hosts y cuáles son las versiones de aplicaciones que un PC está ejecutando en sus diferentes puertos. Para obtener la máxima fiabilidad, el seguimiento de pilas necesitará que al menos un puerto esté a la escucha.

Nmap realizará una hipótesis razonable del sistema operativo que se está utilizando mediante opciones de sondeos los cuales hace mediante el envío de paquetes.

Algunas opciones de sondeo son los siguientes:

Sondeo FIN:

Se envía un paquete FIN a un puerto abierto. RFC 793 establece que el comportamiento correcto es no contestar; sin embargo muchos desarrollos de pilas como Windows responderán con un paquete FIN/ACK.

Sondeo Bogus Flag:

Se introduce una bandera TCP indefinida en la cabecera TCP de un paquete SYN algunos sistemas operativos como LINUX responderán con esta bandera en su paquete de respuesta.

Tamaño de ventana inicial TCP:

Se analiza el tamaño de ventana inicial recibido en los paquetes de respuesta. En algunos desarrollos de pilas, este tamaño es único y puede ayudar bastante en la precisión del mecanismo de seguimiento.

Valor ACK:

Las pilas IP difieren en el valor de la secuencia que usan en el campo ACK, por lo que algunos desarrollos responderán con el mismo número de secuencia que han recibido y otros responderán con ese número de secuencia +1.

Cita de mensajes ICMP:

Los sistemas operativos difieren en la cantidad de información que se cita cuando aparecen mensajes de error ICMP. Si se examina el mensaje citado, se podrán realizar ciertas hipótesis sobre cuál es el sistema operativo destino.

Opciones TCP:

Las opciones TCP se definen en RFC 793 y de forma mas reciente, en RFC 1323. Enviando un paquete para el que se han definido una serie de opciones, por ejemplo, no operación, tamaño máximo de segmento, factor de escala de ventana y estampación de hora, es posible realizar algunas hipótesis sobre cuál es el sistema operativo destino.

Muchas de las herramientas de detección de exploración de puertos, pueden utilizar también para la detección de sistemas operativos. Aunque no indican específicamente que se está llevando a cabo una detección de sistemas operativos, pueden detectar una exploración con determinadas opciones definidas, como por ejemplo la bandera SYN.

Las técnicas de detección de pilas son activas por naturaleza. Se envían paquetes a cada sistema para determinar la idiosincrasia específica de la pila de red, esta acción permite adivinar el sistema operativo que se está utilizando. Como se han enviado paquetes al sistema objetivo, será relativamente sencillo para un sistema IDS basado en red, determinar que se ha ejecutado una prueba de identificación del sistema operativo. Por esto, este método no es una de las técnicas más silenciosas que pueden emplear los atacantes.

Otro sistema de rastreo de pilas es el rastreo de pilas pasivo, similar al activo; sin embargo, en lugar de enviar paquetes al sistema objetivo, el atacante se limita a observar de forma pasiva el tráfico que circula por la red para determinar el sistema operativo que se está utilizando. De esta forma, supervisando el tráfico de red que circula entre varios sistemas se puede determinar los sistemas operativos que se están empleando en la misma.

Es mucho más fácil emplear herramientas como "Nmap" la cual realiza en cuestión de segundos cientos de pruebas, algunas de ellas extremadamente sofisticadas que solamente un atacante experto podría entender, y que le informan con lujo de detalles las características del sistema operativo, servicios, configuraciones, etc.

La opción “-v” como vimos anterior mente me indica los puertos y los servicios que está corriendo, pero si agregamos el parámetro “-A”, Nmap nos mostrara la versión de los aplicativos que corren en cada puerto y la versión del sistema operativo.

Aplicando este parámetro a los comandos antes visto nos quedaría algo como:

“nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 IP_Victima”

```
root@itforensic-la:~# nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.1.147

Host is up (0.023s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Serv-U ftpd 5.0
139/tcp   open  netbios-ssn  Microsoft Windows XP microsoft-ds
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
2869/tcp  closed iclslap
MAC Address: 00:0C:29:B3:6D:72 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP3
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows

Host script results:
| nbstat:
|_ NetBIOS name: JHON-D315C432A2, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:b3:6d:72 (VMware)
|_ Names
|_ JHON-D315C432A2<00> Flags: <unique><active>
|_ SISTEMAS<00> Flags: <group><active>
|_ JHON-D315C432A2<20> Flags: <unique><active>
|_ SISTEMAS<1e> Flags: <group><active>
|_ SISTEMAS<1d> Flags: <unique><active>
|_ \x01\x02_MSBRWSE_\x02<01> Flags: <group><active>
|_ smb2-enabled: Server doesn't support SMBv2 protocol
```

BÚSQUEDA DE INFORMACION COMPLEMENTARIA

Con la ejecución de los pasos anteriores, se tiene bastante información como para planear un ataque a nuestro objetivo, sin embargo no está por demás en realizar este último paso; en el que una información de fuentes complementarias puede complementar aun más el perfil de nuestra víctima.

A continuación explicare el uso de estas fuentes complementarias:

ESCARBANDO BASUREROS

Mucho se puede aprender acerca de las personas con sólo observarlos, pero puede aprender más de lo que siempre quiso saber con solo observar su basura.

Escarbar Basureros (Dumpster Diving), pretende buscar información, documentos y medios electrónicos que son útiles para un atacante. Obviamente, que la información aquí encontrada alguna será más útil que la otra.



Dentro de la información que podría encontrar en un basurero, se tiene:

- Datos de Empleados
- Cuentas de Correo Electrónico
- Firmas de Directivos
- Extractos Bancarios
- Anotaciones Personales
- Agendas
- Nombres de Usuarios y Contraseñas
- Medios Electronicos (CD's, DVD's, Discos Duros, Etc)
- Facturas de Compra

El problema a lo que nos podemos enfrentar es que momento escarbo las basuras? dentro de las instalaciones de nuestro objetivo, donde puedo estar pasando por encima de la ley o cuando la basura llega a la calle que pasa a ser de dominio público, en donde cualquier persona puede acceder a ella y no tener que preocuparse por romper la ley.

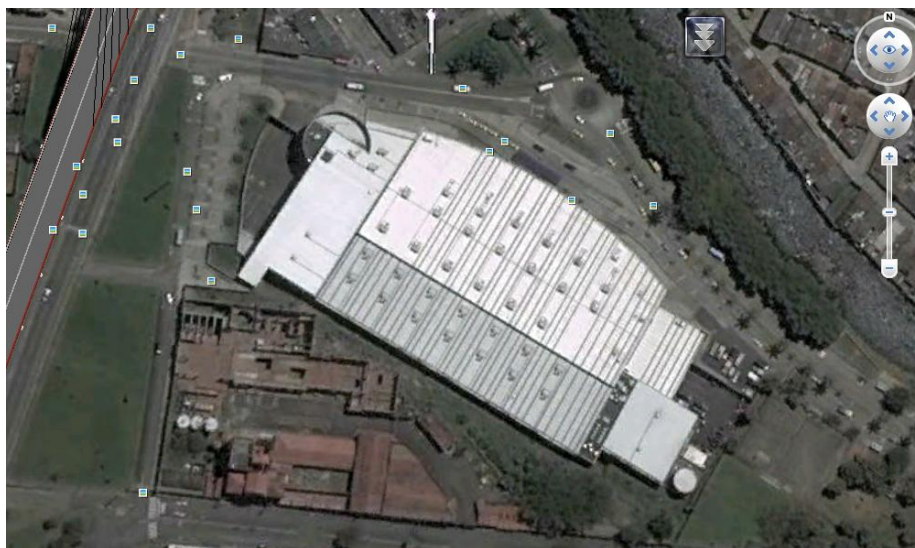
La información que encuentre, también depende de la época del año; por ejemplo buscar información en el primer mes del año nos trae buenas sorpresas con las agendas que contienen información que nos puede ser útil.

La información en medios magnéticos encontrada y la combinación de técnicas de cómputo forense nos puede llevar a la obtención de información sensible que el atacante puede utilizar.

BÚSQUEDA DE IMÁGENES SATELITALES

Existen numerosas fuentes públicas de imágenes de satelitales, pero en estos días el que se destaca por el momento es Google Earth (<http://earth.google.com>).

Google Earth es un mosaico sin fisuras de fotografías de satélite tomadas de diferentes fuentes y que son actualizadas periódicamente. En realidad, es mucho más que eso, ya que nos puede mostrar fotografías en alta resolución de lugares poblados como las ciudades.



Aparte de obtener una vista general del entorno del objetivo, puedo obtener información útil como la ubicación de las entradas, salidas, parqueaderos, contenedores de basura, aéreas libres, etc.

Obviamente para poder obtener las coordenadas sobre los objetivos es necesaria la utilización de una unidad GPS.

BÚSQUEDA DE REDES INALÁMBRICAS

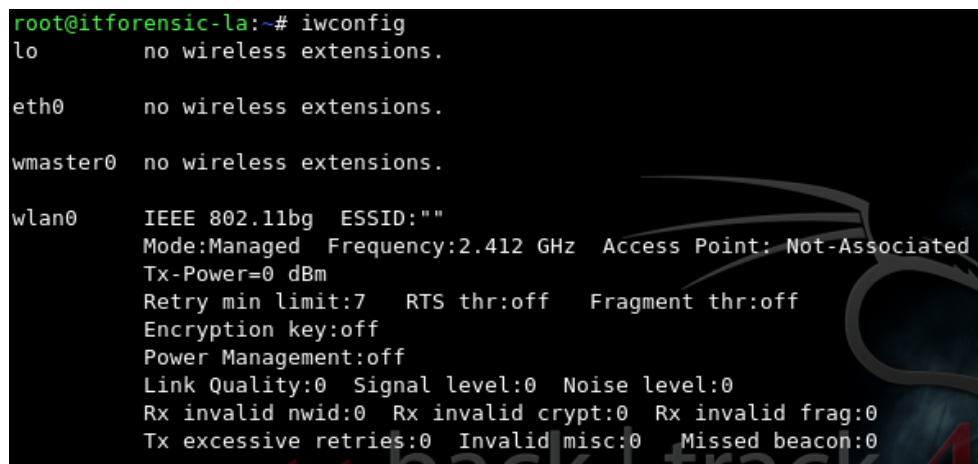
Los puntos de acceso inalámbricos nos pueden brindar una entrada directa a nuestro objetivo e inclusive nos puede permitir sobrepasar los cortafuegos perimetrales, muchos de los accesos inalámbricos son enrutadores y muchos de ellos vienen con contraseñas por defecto que nos permite de manera inmediata entrar a la configuración de dichos dispositivos.

Por esto es importante dentro de la información que se recolecta el conocer la redes inalámbricas que posee nuestra víctima, para ello basta con utilizar una tarjeta de red inalámbrica que la posee cualquier portátil y una herramienta que permita identificar entre otros, la siguiente información:

- Nombres de los SSID
- Canal
- Tipo de Ciframiento
- Mac Address

La herramienta que nos permite esto; se llama **“airodump-ng”** y esta incluida dentro de las utilidades de nuestro mencionado **“BackTrack”**.

Lo primero es conocer la manera como **“BackTrack”** reconoció su tarjeta inalámbrica (OnBoard o Usb) en su sistema, para ello se digita el comando **“iwconfig”**



```
root@itforensic-la:~# iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

wmaster0    no wireless extensions.

wlan0       IEEE 802.11bg  ESSID:""
           Mode:Managed  Frequency:2.412 GHz  Access Point: Not-Associated
           Tx-Power=0 dBm
           Retry min limit:7   RTS thr:off   Fragment thr:off
           Encryption key:off
           Power Management:off
           Link Quality:0  Signal level:0  Noise level:0
           Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
           Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

Lo siguiente es ejecutar el comando **“airodump-ng”** con la interfaz adecuada de la tarjeta de red inalámbrica reconocida por el sistema, en nuestro ejemplo **“wlan0”**; el comando completo quedaría:

“airodump-ng wlan0”

Una vez identifiquemos los parámetros antes mencionados de los puntos de acceso inalámbrico de nuestra víctima, presionamos **“CTRL+C”** para terminar el monitoreo.

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:16:41:BE:C3:E9	-75	845	2	0	10	54e	WEP	WEP		r3net
00:0C:42:26:FA:0B	-76	874	2237	4	7	11	WEP	WEP		uniforum11
00:30:4F:5A:87:0E	-83	319	0	0	12	54e	OPN			WEP-40bit(1000)
00:0E:8E:0F:CE:84	-84	388	0	0	1	54	WPA2	TKIP	PSK	Uniforum (H&L)
00:02:6F:33:39:75	-83	164	1355	7	5	11	OPN			Uniforum-0
00:30:4F:5A:87:6F	-83	549	3	0	9	54e	OPN			WEP-40bit(1000)
00:30:4F:52:CB:D2	-84	84	71	0	10	11	WEP	WEP		Uniforum (H&L)
00:17:9A:76:6F:8A	-84	154	0	0	1	54	WEP	WEP		ASPCA
00:17:B7:20:08:80	-86	222	126	0	13	11	OPN			WEP-40bit(1000)
00:0E:8E:0F:CB:2C	-85	230	0	0	9	54	WPA2	TKIP	PSK	Uniforum (H&L)
00:4F:62:0B:E0:A4	-85	221	180	1	10	11	OPN			WEP-40bit(1000)
00:0E:8E:7E:D8:E7	-87	107	96	1	1	11e	WEP	WEP		Uniforum (H&L)
00:30:4F:42:90:16	-88	135	0	0	7	54	OPN			WEP
00:30:4F:52:D6:9B	-88	102	128	0	6	11	WEP	WEP		ALL
00:60:B3:19:A7:23	-89	31	113	0	8	11	WEP	WEP40		WEP
00:21:27:CD:7C:6E	-89	76	192	0	9	11	OPN			WEP-40bit(1000)
00:0C:42:60:60:61	-90	12	0	0	9	54	OPN			WEP-40bit(1000)
00:30:4F:4C:E0:F1	-90	4	1	0	4	11	WEP	WEP		WEP-40bit(1000)
00:30:4F:42:0F:E3	-91	2	1	0	8	11	OPN			WEP-40bit(1000)
00:02:6F:4F:A9:76	-87	23	15	0	13	11	WEP	WEP		uniforum11

ESCUCHANDO EL TRAFICO DE LA RED

Llegamos a nuestro último paso, la idea es conectar un equipo dentro de la red local de nuestro objetivo; sea por punto de red o vía inalámbrica y escuchar todo el tráfico que circunda por ella. Esta técnica se hace mediante un programa llamado Sniffer y si somos lo suficientemente pacientes, podemos obtener información muy importante, como:

- Usuarios y contraseñas
- Mensajes de broadcast de dispositivos de red (switches, routers, impresoras, etc)
- Protocolos que pasan por la red.
- Solicitudes ARP
- Entre otras

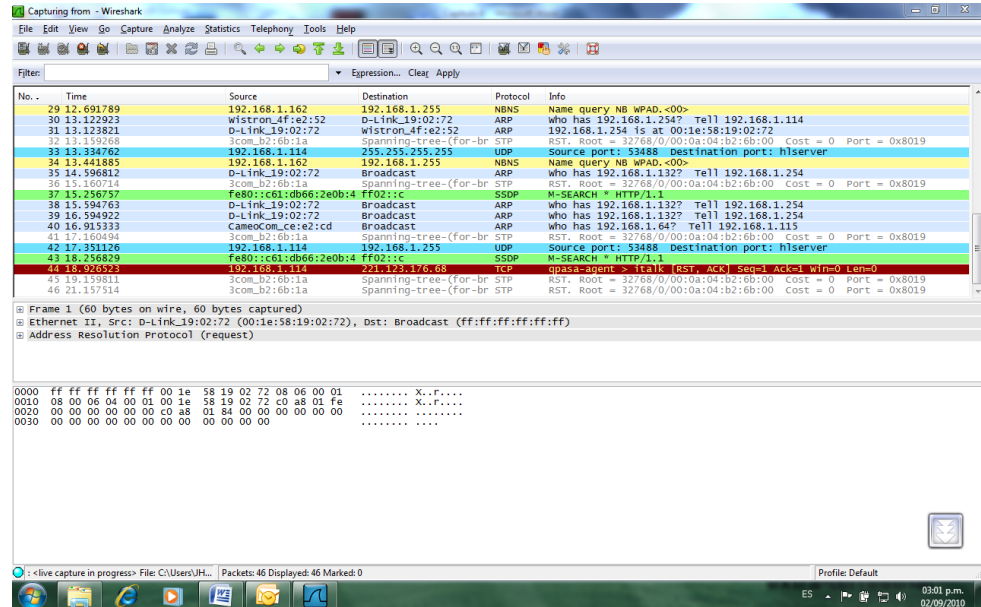
Un Sniffer es un programa que permite capturar las tramas de la red.

Dentro de los programas de distribución libre más destacados para esta labor se encuentra el “Wireshark⁸”, antes conocido como Ethereal.

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark.

⁸ <http://www.wireshark.org/>

Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.



BIBLIOGRAFÍA

LIBROS

- ED SKOUDIS, Counter Hack Reloaded.
- NORTHCUTT. Stephen. Detección de Intrusos: Prentice Hall
- COLE. Eric, Hacker Beware
- RYAN Russell, Hack Proofing Your Network
- NITESH Dhanjani, Hacking The Next Generation
- SHON Harris, Gray Hat Hacking
- DAVID Melnichuck, The Hacker's Underground Handbook
- WIL Allsop, Unauthorised Access Physical Penetration Testing For IT Security Teams

ENLACES

<http://www.backtrack-linux.org/>
<http://www.dragonjar.org>
<http://www.kungfoosion.com/>
<http://www.elladodelmal.com/>

TABLA DE CONTENIDO

ENUMERACIÓN Y RECONOCIMIENTO.....	- 2 -
REUNIENDO INFORMACIÓN:.....	- 2 -
PASOS PARA OBTENER INFORMACION:	- 3 -
<i>ENCONTRAR LA INFORMACION INICIAL:</i>	- 5 -
Comando Ping	- 5 -
WHOIS	- 6 -
Análisis de Metadatos.....	- 9 -
OSINT	- 12 -
<i>IDENTIFICAR EL RANGO DE LA RED</i>	- 13 -
Arin / Apnic /Lacnic	- 13 -
TracerRoute:	- 15 -
Hping:	- 16 -
Descubrimiento con DNS	- 18 -
<i>BUSCAR MAQUINAS ACTIVAS</i>	- 23 -
Búsqueda de Maquinas Activas Básico.....	- 24 -
Búsqueda de Maquinas Activas Optimizado.....	- 24 -
<i>BUSCAR PUERTOS Y SERVICIOS</i>	- 28 -
INTRODUCCIÓN PUERTOS Y SERVICIOS	- 28 -
PORTSCANERS	- 29 -
NMAP ('NETWORK MAPPER'):	- 31 -
<i>ENCONTRAR VERSIONES DE SISTEMAS OPERATIVOS Y APLICACIONES:</i>	- 33 -
<i>BÚSQUEDA DE INFORMACION COMPLEMENTARIA</i>	- 36 -
ESCARBANDO BASUREROS	- 36 -
BÚSQUEDA DE IMÁGENES SATELITALES	- 37 -
BÚSQUEDA DE REDES INALAMBRICAS	- 38 -
ESCUCHANDO EL TRAFICO DE LA RED	- 39 -
BIBLIOGRAFÍA	- 41 -