

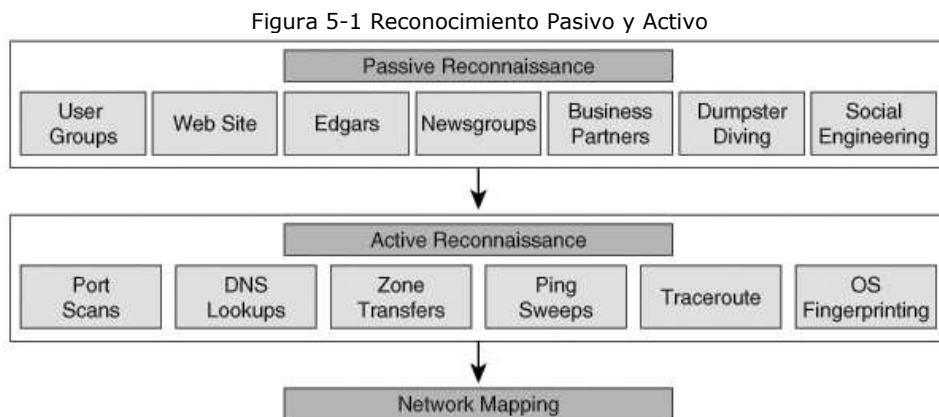
RECONOCIMIENTO

Los usuarios malintencionados también realizan el reconocimiento como primer paso en un eficaz ataque. Lanzar ataques relacionados con vulnerabilidades de UNIX si el objetivo son servidores de Microsoft no tiene sentido. Un poco de tiempo dedicado a investigar ahorra mucho tiempo durante la Prueba de Intrusión.

El objetivo del reconocimiento es descubrir la siguiente información:

- Las direcciones IP de los objetivos de la red
- Puertos Accesibles, UDP y TCP
- Sistemas operativos en los sistemas objetivo

El mapeo de la red puede ser activo o Pasivo, según muestra la figura 5.1



El reconocimiento pasivo, implica la obtención de información por medio de sitios Web, bases de datos, grupos de noticias, socios de negocios, dumpster diving, y la ingeniería social. El reconocimiento pasivo se debe tener paciencia, pero es el más difícil para detectar.

El reconocimiento activo, por el contrario, implica el uso de la tecnología de una manera que la empresa podría detectar. Esto se podría hacer con búsquedas por medio de ping sweeps, traceroute, escaneo de puertos y detección de sistemas operativos. Después de reunir la información de puertos y sistemas operativos se puede saber qué tipo de ataque se realizara.

En este capítulo, aprenderá a descubrir objetivos con diferentes de técnicas. El uso de herramientas de escaneo de puertos, y también aprender la forma de determinar los sistemas operativos de los host. Por último, se aprenderá las mejores prácticas para la detección y prevención de las técnicas de reconocimiento.

Reconocimiento Pasivo de Host

Como se mencionó anteriormente, puede utilizar dos diferentes métodos de reconocimiento para descubrir información sobre los host objetivo de la red, Reconocimiento Pasivo y Activo.

EL reconocimiento Pasivo, recoge datos de una fuente abierta de información. Una fuente abierta significa que la información está disponible gratuitamente para el público. En cuanto a la

información es totalmente legal. Una empresa puede hacer poco para proteger contra la liberación de esta información. Los siguientes son ejemplos fuentes abiertas de información:

- Un sitio de Internet de la sociedad
- Solicitudes de Electronic Data Gathering Análisis y recuperación (EDGAR)
- Protocolo de transferencia de Noticias de la red (NNTP), grupos de noticias USENET
- Reuniones de grupos de usuario
- Socios de negocio
- Dumpster diving
- Ingeniería social

Todos estos, con la excepción del dumpster diving y la ingeniería social, se examinan en este capítulo. Revisión del capítulo 4, "Realización de ingeniería social," para obtener más información acerca de dumpster diving y la ingeniería social.

Un sitio de Internet de la sociedad

Si son contratados para realizar un test de intrusión contra una empresa con presencia en Internet, el primer lugar que usted debería ver, obviamente, es el sitio Internet de la sociedad. Comience por la descarga de la página web para ver sin conexión. Esto le permite dedicar más tiempo a analizar cada una de las páginas sin ser detectado y proporciona beneficios más tarde. En el proceso de descarga del sitio web, usted también puede recolectar las páginas huérfanas. Las páginas huérfanas son las páginas web que podrían haber sido partes del sitio web de la empresa en un momento pero ahora no tienen vínculos a las páginas de ellos. Si bien las páginas deberían ser retiradas del servidor, a menudo no lo son. Ellas pueden contener información útil para la penetración de intrusión.

Dos programas que puede utilizar para descargar un sitio web para revisarlas fuera de línea son: GNU Wget (<ftp://ftp.gnu.org/pub/gnu/wget/>) y Teleport Pro (<http://www.tenmax.com>). GNU Wget es libre bajo la licencia GNU y se puede ejecutar en Linux o Windows. Teleport Pro es un software comercial que funciona sólo en Windows.

Wget es una herramienta por línea de comandos basada en la recuperación del website creando copias locales de sitios web remotos.

La Figura 5-2 muestra la aplicación Wget recuperar las páginas de <http://www.hackmynetwork.com> .

Observe el uso del parámetro `-r`, que permite el duplicado de todas las páginas del sitio. Puede especificar la profundidad máxima del nivel de duplicación con el parámetro `-l`.

Si selecciona la opción `recursive`, Wget sigue los hipervínculos y páginas de descargas de referencia.

Figura 5-2. Wget, recuperación Web

```
C:\wget\wget-1.9.1b>wget -r www.hackmynetwork.com
--09:48:57-- http://www.hackmynetwork.com/
=> `www.hackmynetwork.com/index.html'
Resolving www.hackmynetwork.com... 127.0.0.1
Connecting to www.hackmynetwork.com[127.0.0.1]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8,582 [text/html]

100%[=====>] 8,582      --.-K/s

09:48:57 (8.18 MB/s) - `www.hackmynetwork.com/index.html' saved [8582/8582]

Loading robots.txt; please ignore errors.
--09:48:57-- http://www.hackmynetwork.com/robots.txt
=> `www.hackmynetwork.com/robots.txt'
Reusing connection to www.hackmynetwork.com:80.
HTTP request sent, awaiting response... 404 Not Found
09:48:57 ERROR 404: Not Found.

--09:48:57-- http://www.hackmynetwork.com/design_01.jpg
=> `www.hackmynetwork.com/design_01.jpg'
Connecting to www.hackmynetwork.com[127.0.0.1]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4,441 [image/jpeg]

100%[=====>] 4,441      --.-K/s

09:48:57 (4.24 MB/s) - `www.hackmynetwork.com/design_01.jpg' saved [4441/4441]

--09:48:57-- http://www.hackmynetwork.com/design_02.jpg
=> `www.hackmynetwork.com/design_02.jpg'
Reusing connection to www.hackmynetwork.com:80.
HTTP request sent, awaiting response... 200 OK
Length: 1,774 [image/jpeg]

100%[=====>] 1,774      --.-K/s

09:48:57 (1.69 MB/s) - `www.hackmynetwork.com/design_02.jpg' saved [1774/1774]

--09:48:57-- http://www.hackmynetwork.com/design_03.jpg
=> `www.hackmynetwork.com/design_03.jpg'
Reusing connection to www.hackmynetwork.com:80.
HTTP request sent, awaiting response... 200 OK
Length: 46,794 [image/jpeg]
```

El objetivo de la pruebas no es sólo para ver el acceso que el auditor puede adquirir, sino también lo que el auditor es capaz de hacer sin ser detectado. Para reducir al mínimo la posibilidad de detección cuando se usa wget, puede utilizar los siguientes interruptores:

-- random-wait-Debido a que algunos sitios web realizan el análisis estadístico de la página web para detectar spidering y recuperaciones de web, debe utilizar el parámetro -- random-wait para cambiar la espera de tiempo de recuperación. Wait se refiere al tiempo especificado de espera.

-- wait = segundos-Este parametro especifica el número de segundos entre las recuperaciones. Usted debe utilizar este junto con el -random esperar cambiar.

-- cookies = on/off- Las cookies permiten a los servidores web llevar un registro de visitantes en sus sitios web. Desactivar esta opción evita que el servidor de seguimiento a la visión de su sitio web, sin embargo, es posible que se desee habilitarlo para realizar exploit en base de "cookies" (esto se discutirá más adelante en el capítulo 7, "Realización ataques a Servidores Web.")

-- H- Host permite que Wget abarque no sólo la recolección de las páginas web, sino también permitir el espejo de cualquier sitio de referencia en los hipervínculos a las páginas web. Tenga cuidado con esta opción, puede consumir una cantidad considerable de espacio en el disco duro.

-- D-Este dominio se utiliza con el parámetro -H, haciendo que los límites de recolección que abarque sean sólo a los sectores mencionados.

Dado que es probable utilizar los mismos parámetros cada vez que utilice Wget, puede incluir los parámetros en el archivo wget.rc.

Nota:

Algunos programas CGI pueden causar problemas con Wget. Si se observa Wget intentara descargar el mismo archivo varias veces, utilizar la opción *-ignore-length*. Este parametro elude los problemas originados por los scripts CGI que envían contenido falso de longitud de cabeceras.

Otra variante que puede usar, es la herramienta basada en Windows. La aplicación Teleport Pro de Tennyson Maxwell. Después de lanzar Teleport Pro, se le solicita el nuevo Asistente de Proyecto, tal como se muestra en la Figura 5-3.

Figura 5-3. Teleport Pro, asistente de proyecto nuevo



A efecto de la navegación fuera de línea, seleccione Crear una copia de un sitio web. Después hacer clic en Siguiente, se le pedirá una dirección como en la pantalla de la Figura 5-4.

Figura 5-4. Teleport Pro, pantalla de dirección de inicio de pantalla



En la pantalla, se debe entrar el sitio web que desea almacenar fuera de línea. Tenga en cuenta que la dirección distingue entre mayúsculas y minúsculas. Usted puede elegir la profundidad de exploración del Teleport Pro. El valor por defecto es de hasta tres enlaces, lo cual es suficiente para la mayoría de las recuperaciones. En la siguiente pantalla (Propiedades del proyecto), se muestra en la Figura 5-5, puede especificar qué tipo de archivos desea recuperar. Teleport Pro se limita a recuperar los archivos mostrados en la pantalla opciones de Propiedades del Proyecto. Normalmente, se elige la mejor opción, pero si está con ancho de banda limitado y no son necesarios los gráficos, puede elegir la opción Sólo texto.

Figura 5-5. Teleport Pro, pantalla de propiedades del proyecto

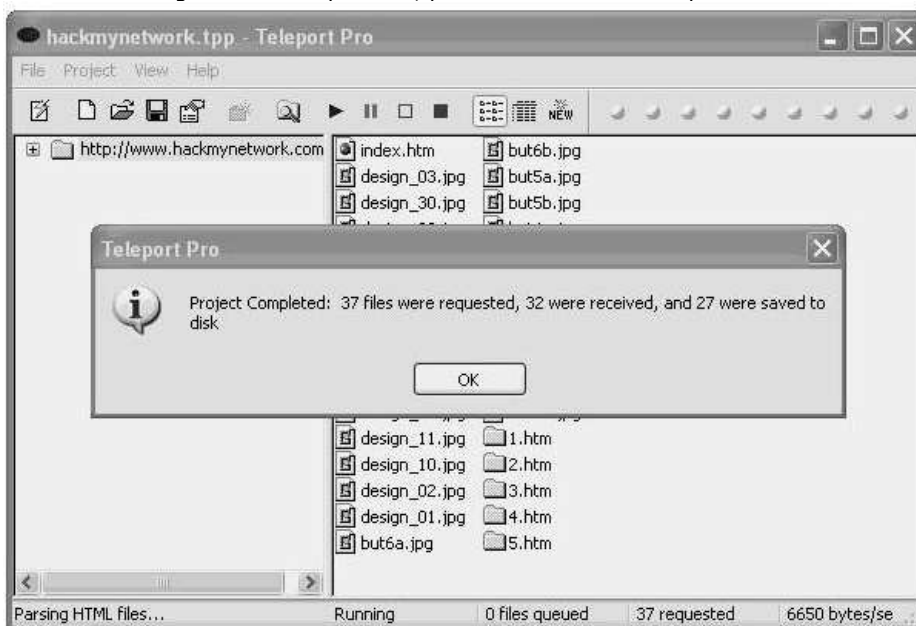


También puede introducir un nombre de cuenta y la contraseña para acceder al sitio si es necesario, es probable que no conozca ningún nombre de usuario o contraseñas en este momento (aprenderá a descubrir estos en el capítulo 7), debe dejar los lugares en blanco .

Después de seleccionar a continuación, se le pedirá que termine el asistente y seleccione la ubicación donde desea guardar el archivo de proyecto.

Cuando esté listo para empezar a copiar el objetivo sitio web, puede ir al menú Proyecto y seleccione Inicio. Cuando el proyecto está terminado, verá una pantalla como la de la Figura 5-6, que le muestra que muchos archivos fueron solicitados y cuántos fueron recibidos. Si el número de solicitudes no es alto, puede cambiar los parámetros de recuperación con la pantalla Propiedades del proyecto en el marco del Proyecto de menú.

Figura 5-6. Teleport Pro, pantalla de final de recuperación

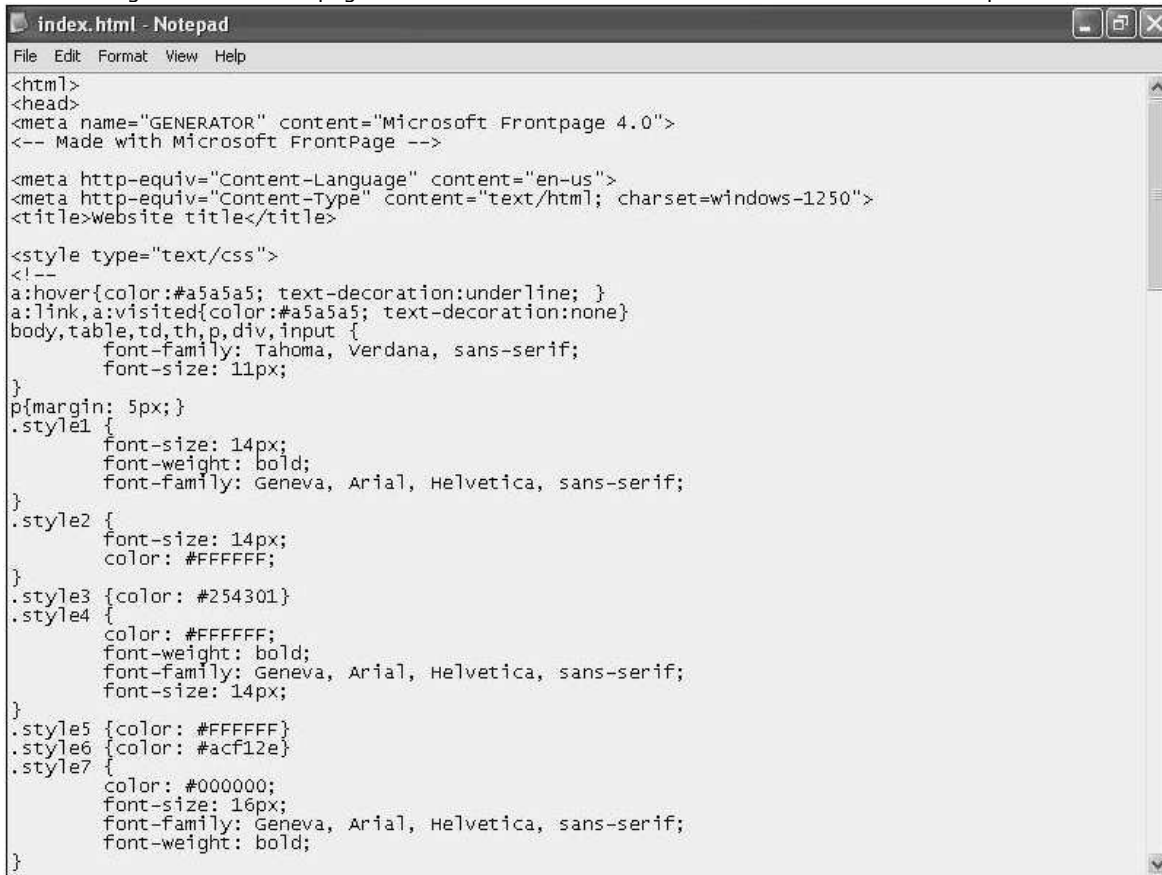


Después de haber copiado el sitio web, ya sea a través de Teleport Pro o Wget, puede navegar en línea. Con respecto al reconocimiento, usted debe estar buscando dos cosas:

- Comentarios en el código fuente
- Información de contacto

Los comentarios en el código fuente podría revelar la plataforma web en que está funcionando, lo cual es útil más adelante cuando trate de infiltrarse en el servidor web de destino. Puede ver el código fuente de las páginas web en un editor HTML, editor de texto, o dentro del navegador. En Internet Explorer, puede ver el código fuente en la pestaña Ver. La Figura 5-7 muestra un ejemplo de código fuente de una página web.

Figura 5-7. Código fuente de una página web. Los comentarios revelan la herramienta utilizada para la creación HTML



```
index.html - Notepad
File Edit Format View Help
<html>
<head>
<meta name="GENERATOR" content="Microsoft Frontpage 4.0">
<!-- Made with Microsoft FrontPage -->

<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1250">
<title>website title</title>

<style type="text/css">
<!--
a:hover{color:#a5a5a5; text-decoration:underline; }
a:link,a:visited{color:#a5a5a5; text-decoration:none}
body,table,td,th,p,div,input {
font-family: Tahoma, Verdana, sans-serif;
font-size: 11px;
}
p{margin: 5px;}
.style1 {
font-size: 14px;
font-weight: bold;
font-family: Geneva, Arial, Helvetica, sans-serif;
}
.style2 {
font-size: 14px;
color: #FFFFFF;
}
.style3 {color: #254301}
.style4 {
color: #FFFFFF;
font-weight: bold;
font-family: Geneva, Arial, Helvetica, sans-serif;
font-size: 14px;
}
.style5 {color: #FFFFFF}
.style6 {color: #acf12e}
.style7 {
color: #000000;
font-size: 16px;
font-family: Geneva, Arial, Helvetica, sans-serif;
font-weight: bold;
}
}
```

Los comentarios al principio con el <! - Etiqueta HTML y terminan con ->. Figura 5-7 muestra que la página web ha sido escrito con Microsoft FrontPage. Los exploits deberán estar relacionados con Microsoft FrontPage.

La Figura 5-8 muestra otro ejemplo de comentario que puede ser información útil. En este ejemplo se puede que el sitio fue desarrollado por XYZ Web Design Company. Aunque a primera vista esto podría no revelar mucho, es realmente útil la información. Muchas empresas de diseño web anuncian qué tipo de plataforma utilizan para desarrollar sitios, como Microsoft o UNIX. Al ir al sitio XYZ Web Design, se puede ver que se especializan en ASP, .NET, y FrontPage. Se puede concluir con certeza, ya que estas son utilizados en todas las plataformas de Microsoft, el objetivo web está funcionando en Microsoft Internet Information Server (IIS). Si XYZ Web Design anuncia que utilizan Perl, CGI, PHP, y Python, el objetivo web es más probable que se ejecuta en una plataforma basada en UNIX. A pesar de todas estas tecnologías también pueden correr en Windows, pero son más comunes en la plataforma UNIX.

Figura 5-9. Muestra la información del contacto página web



Sobre esta página web, se puede ver los nombres de los ejecutivos, junto con sus números de teléfono e información de e-mail. Esto puede ser útil para realizar ingeniería social, tal como se describe en el capítulo 4. Los números de teléfono en la Figura 5-9 también son útiles para la realización de war dialing, en la que se marca una serie de números de teléfono con un software como el ToneLoc o THC war dialer y tratar de establecer la conectividad de acceso remoto. En la figura, todos los números de teléfono comienzan con el prefijo 503 555-1 seguidas por el número de extensión. Armado con este conocimiento, puede configurar su software de war dialing para marcar todos los números dentro del rango 503 555-1000 a través de 503 555-1999 y detectar los módems utilizados para el acceso remoto.

Si es posible, las empresas sólo deben incluir los números 800 en su sitio de Internet que conecta a la persona que llama a una recepcionista para minimizar el riesgo de ataque de war dialing. Si el empleado es información que se mostrará, asegúrese de que las políticas están en su lugar y que lo proteja contra los ataques de ingeniería social.

Nota:

Las empresas que proporcionan soluciones de tecnología están particularmente en riesgo porque suelen anunciar su plataforma de elección en su página web. Por ejemplo, algunas empresas bancarias en línea anuncian que corren exclusivamente Microsoft IIS y servidores SQL. A pesar de que esta información podría ser útil para fines de marketing, no debe ser de conocimiento público. En lugar de ello, el personal de ventas puede dar a conocer la información a los posibles clientes que lo soliciten.

Registros EDGAR

Los registros EDGAR son las solicitudes de Electronic Data Gathering Analysis and Recovery. Las sociedades con cotización oficial en los Estados Unidos están obligadas a presentarse ante la Comisión de la seguridad de Bolsa (SEC). Puede acceder a esta información a través de la base de datos EDGAR, que se puede ver en <http://www.sec.gov/edgar.shtml> . Las búsquedas pueden revelar la información financiera y comunicados de prensa. Algunas compañías anuncian la tecnología utilizada en su organización en un comunicado de prensa enviado a EDGAR. Esto ahorra tiempo al intentar determinar el sistema operativo a través de otros medios.

NNTP grupos de noticias USENET

Si alguna vez has tenido para solucionar un problema difícil, ustedes saben el valor del trabajo en red con otros para encontrar una solución. Uno de los métodos que utilizan los ingenieros para buscar ayuda es mediante la publicación de preguntas sobre los grupos de noticias USENET. Por desgracia, algunos exponen demasiada información cuando está buscando ayuda.

El Ejemplo 5-1 muestra un ingeniero realizando una pregunta sobre un problema que está experimentando. En su mensaje, él describe que se está ejecutando Red Hat Linux 6,2. Ninguna empresa debería exponer esta información de manera libre al público.

Ejemplo 5-1. Ejemplo de envío de grupos de noticias

From: bsmith@hackmynetwork.com
Subject: Apache Problem
Newsgroups: comp.infosystems.www.servers.unix, comp.os.linux,
alt.apache.configuration, comp.lang.java.programmer
Date: 2004-07-07 09:19:28 PST

I am having a problem with Apache reverse proxy not communicating with web applications using HTTP 1.1 keepalive. I am using Apache 1.3.23 on Red Hat Linux 6.2. It is compiled with mod_proxy and mod_ssl.
Any ideas would be greatly appreciated.

Thank you.

bsmith@hackmynetwork.com
Sr. Systems Administrator
Hackmynetwork.com

El Ejemplo 5-1 también muestra la dirección de correo electrónico de Bill: bsmith@hackmynetwork.com. Esto no sólo revela el nombre de la empresa en que trabaja Bill (Hackmynetwork), también puede reflejar su cuenta de usuario en la red. Por desgracia, muchas empresas todavía utilizan el mismo código de acceso de red como su nombre de e-mail. Se debe documentar su dirección de correo electrónico al realizar el reconocimiento. Debido a que trabaja en la producción de servidores de la sociedad afectada, es posible que pueda obtener pleno acceso a su red si crackea su contraseña. (se abordara este tema en el capítulo 9, "Crackeo de Contraseñas.")

Se puede navegar por los grupos de noticias utilizando software como Microsoft Outlook Express, Netscape, Xnews, y muchos otros. Por otra parte, y tal vez de manera más eficaz, también se puede buscar grupos de noticias a través de Google. Sólo se debe introducir el nombre de la empresa objetivo, y obtendrá todas las noticias de los mensajes enviados o relacionados con su empresa.

Reuniones de Grupo de Usuarios

Se puede tratar de asistir a reuniones de grupos de usuario. La mayoría de las ciudades tienen grupos de usuarios que celebran reuniones relacionadas con diversas tecnologías, como Microsoft, tecnologías Cisco, Linux, e incluso pruebas de intrusión. Los Usuarios que participan en las reuniones de grupos brindan una oportunidad para las personas en una comunidad a recibir información y cumplir con otros que trabajan con la misma tecnología.

Asistir a grupos de usuarios es una buena manera de practicar sus habilidades de ingeniería social adquirida en el capítulo 4. Al llegar temprano o quedarse tarde después de la reunión, puede obtener información de otros y descubrir lo que las gentes que trabajan en las empresas y qué tecnologías utilizan.

Socios de Negocios

Se puede comprobar los socios comerciales del objetivo para obtener más información. A pesar de que el objetivo podría proteger su información técnica, los socios tal vez no.

Los sitios de Internet de empresas a menudo revelan los nombres de sus socios de negocios, un medio más eficaz de obtener información de los socios es utilizando búsquedas en Google. Por ejemplo, si introduce link: www.hackmynetwork.com en el cuadro de búsqueda de Google, tira todos los sitios que tienen enlace al sitio destino.

Al ir a todos los sitios enumerados en los resultados de búsqueda, es posible descubrir las tecnologías del objetivo. Si aparece una empresa de red que se especializa en soluciones de Sun Solaris, puede asumir con seguridad que su objetivo se está ejecutando en los servidores Sun Solaris.

Reconocimiento Activo

A pesar de que el reconocimiento pasivo de medios es eficaz, a menudo se necesita mucho tiempo y no siempre producen los resultados exactos.

En el reconocimiento activo, se utilizan técnicas con las herramientas para descubrir información sobre los Hosts que están activos en su objetivo (este tipo de reconocimiento es muy completo). El inconveniente del reconocimiento activo, es que es más fácil de detectar.

Algunas de las herramientas que son útiles para reconocimiento activo son las siguientes:

Nslookup / Whois / Dig

SamSpade

Visual Route / Keops

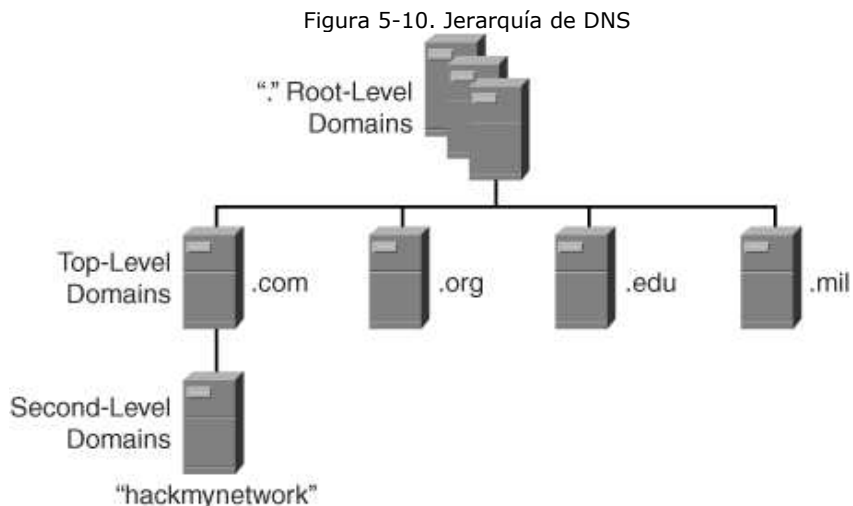
Pinger / WS_Ping_Pro

Nslookup / whois lookups

Cuando se esta realizando una prueba en una Black-Box y no se les da información detallada sobre el objetivo de la red, el cliente puede dar tan sólo una red rango de direcciones IP a prueba. A menudo, puede ser que sólo se conceda la dirección del sitio web, dejando a descubrir el rango de red por su cuenta. En este caso, se tiene que realizar algunas búsquedas DNS para averiguar las direcciones IP asociadas con el sitio web.

Nota:
RFC 1034 y 1035 definen el funcionamiento del DNS. Puede leer sobre ellos en <http://www.ietf.org> .

Jerarquía de DNS, es una distribución de bases de datos compartidas entre servidores y preguntan por Hosts y otros servidores. El nivel más alto de la jerarquía es la última etiqueta en un nombre de dominio. Los nombres de nivel superior pueden ser de dos o tres designaciones de organización, tales como .com con fines comerciales o .edu para organizaciones educativas, .biz para las empresas de negocios, o dos letras del país, designaciones, tales como .uk para el Reino Unido o .au para Australia. La Figura 5-10 muestra la jerarquía de DNS para el sitio web <http://www.hackmynetwork.com> . Las empresas que registran sus DNS en autoridades, tales como ARIN en los Estados Unidos o en Europa RIPE.



Una porción contigua al nombre DNS se denomina zona. Una zona puede contener uno o más nombres de dominio. Cuando se necesita una actualización que debe hacerse a una zona DNS, se hace a una zona principal en un servidor maestro. Las zonas secundarias son copias de la zona primaria que se han repetido desde el servidor maestro. Un servidor puede albergar varias zonas. Cuando un servidor DNS secundario necesita hacer una replica el servidor maestro, realiza una zona de transferencia. En la sección que trata sobre la herramienta "SamSpade," más adelante en este capítulo, analizan las zonas de transferencias.

Incluido en la información de zona están los Resource Records (RRs). Varios tipos de registros de recursos definen la información sobre los hosts en un dominio. La Tabla 5-1 define los diferentes tipos de tipos de registro.

Tabla 5-1. Registros de recursos DNS

Record	Type	Used for
A	Host record	Single hosts
MX	Mail record	Mail servers
PTR	Pointer record	IP to name reverse lookups
CNAME	Alias record	Creating aliases
NS	Name Service record	DNS servers
SOA	Start-of-Authority record	A master record for the entire zone

Cuando se va a ejecutar una Prueba de intrusión, se deben realizar búsquedas DNS para obtener la dirección IP de Hosts en su red objetivo. Las búsquedas DNS también pueden darle información

sobre el propósito de su uso. Por ejemplo, si un registro MX tiene peticiones a smtp.hackmynetwork.com, se sabe que está siendo utilizado para el correo electrónico MX porque es el récord de intercambio de correo.

Si los servidores DNS son las puertas para descubrir un host a través de un sitio web objetivo, Whois, NSLookup, y Dig son las claves para desbloquear esas puertas.

Whois (RFC 812) se encuentra instalado por defecto en la mayoría de sistemas UNIX y plataformas Linux, pero en Windows, usted necesita software de terceros, como SamSpade Whois para realizar consultas.

Whois, que en sus primeros tiempos se llamó NICNAME, es una transacción TCP basada en la consulta/respuesta que sirve para buscar información de registro de un dominio específico. Puede obtener Whois a <http://www.linux.it/~md/software> . Por defecto, los servidores Whois realizan consultas establecidas por la NICNAMSERVER y WHOISSERVER las variables de entorno, y si no, las preguntas se realizan a sewhois.crsnic.net. Escribiendo whois sin ninguna opción revela el servidor por defecto que se utilizan en la consulta. El Ejemplo 5-2 muestra la salida de una consulta en hackmynetwork.com.

Ejemplo 5-2. Ejemplo de consulta Whois

```
#whois hackmynetwork.com
```

```
Registrant:  
HackMyNetwork (hackmynetwork-DOM)  
123 Main Street  
Portland, OR 97415  
Domain Name: hackmynetwork.com
```

```
Administrative Contact:  
John Nobody (RJXX2-ORG) hackmynetwork@HD1.VSNL.NET.IN
```

```
HackMyNetwork  
123 Main Street  
Portland, OR 97415
```

```
Technical Contact:  
John Nobody (VSXX) jnobody@hackmynetwork.com
```

```
123 Main Street  
Portland, OR 97415  
Record expires on 14-Nov-2006  
Record created on 13-Nov-2003
```

```
Dataabase last updated on 17-May-2004
```

```
Billing contact:  
John Nobody  
123 Main Street  
Portland, OR 97415
```

```
Domain servers in listed order:  
NS1.hackmynetwork.com 172.29.140.12  
NS2.hackmynetwork.com 172.22.145.12
```

Las consultas Whois son útiles para dos propósitos:

-Se aprende la información del contacto administrativo que es útil en ingeniería social. (Para más información sobre ingeniería social, véase el Capítulo 4.)

-Se aprende la autoridad y nombres de los servidores DNS. Como podrán ver en breve, esto es útil cuando se desea intentar una transferencia de zona DNS con una herramienta como SamSpade.

NSLookup, Dig, también son herramientas de línea de comandos que se puede utilizar para descubrir información sobre su objetivo red. NSLookup está disponible tanto en UNIX como en plataformas de Windows, aunque NSLookup no esta en la mayoría de los sistemas Linux, esta sustituido por la herramienta Dig. NSLookup adicionalmente puede revelar las direcciones IP y los nombres de los servidores. El Ejemplo 5-3 muestra una consulta NSLookup.

Ejemplo 5-3. NSLookup Query

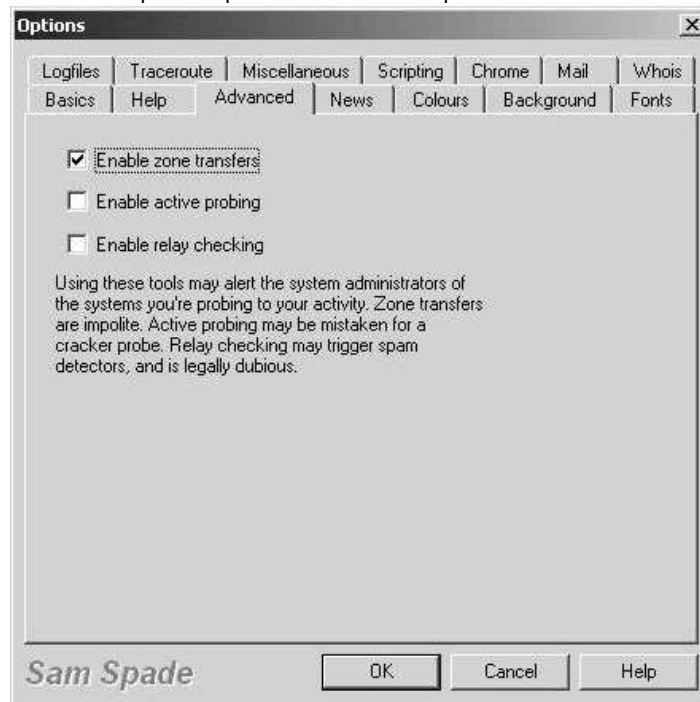
```
#nslookup
>set type=mx
>hackmynetwork.com
Server: smtp.hackmynetwork.com
Address: 172.28.135.16
Non-authoritative answer:
hackmynetwork.com
  origin = hackmynetwork.com
  mail addr: webmaster.hackmynetwork.com
  serial = 20108130
  refresh = 720 (2H)
  retry = 3600 (1H)
  expire = 1728000 (2w6d)
  minimum ttl = 7200 (2H)
hackmynetwork.com  nameserver = ns1.hackmynetwork.com
```

Aunque NSLookup y Dig son instrumentos eficaces, son limitados en comparación con SamSpade.

SamSpade

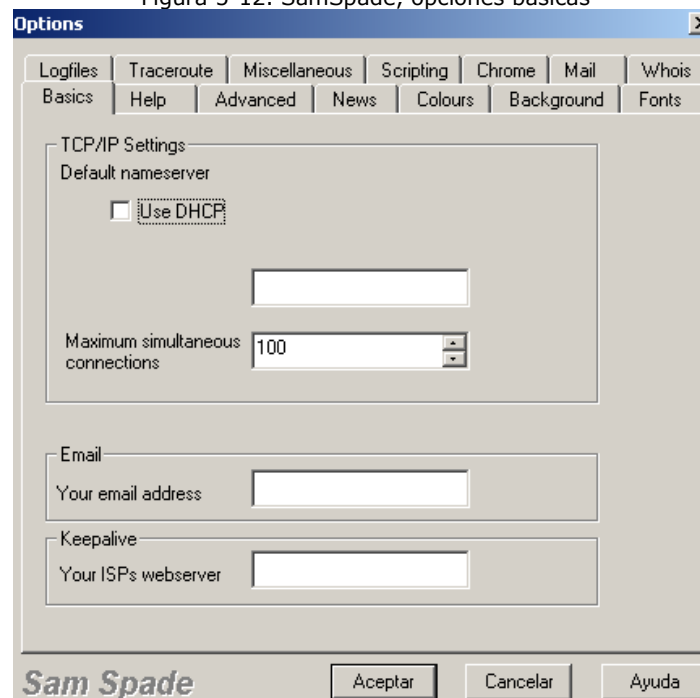
A pesar de que se puede utilizar herramientas de línea de comandos como Dig para realizar las transferencias, es posible que se prefiera una herramienta gráfica como SamSpade (<http://www.samspade.org>). SamSpade es una herramienta libre de Windows creada por Steve Atkins. Se puede realizar un gran número de funciones, incluyendo búsquedas DNS, control de correo, y analizar el sitio web. SamSpade también puede hacer transferencias de zona, sin embargo, la zona de transferencias es desactivada por defecto. Para habilitar la función de zona de transferencia, es necesario ir al menú Edición y seleccione Opciones. Desde allí, seleccione la ficha Opciones avanzadas, tal y como se muestra en la Figura 5-11. Compruebe que la opción de zona transferencias este habilitada.

Figura 5-11. SamSpade. Opciones avanzadas: permitir la transferencia de zona



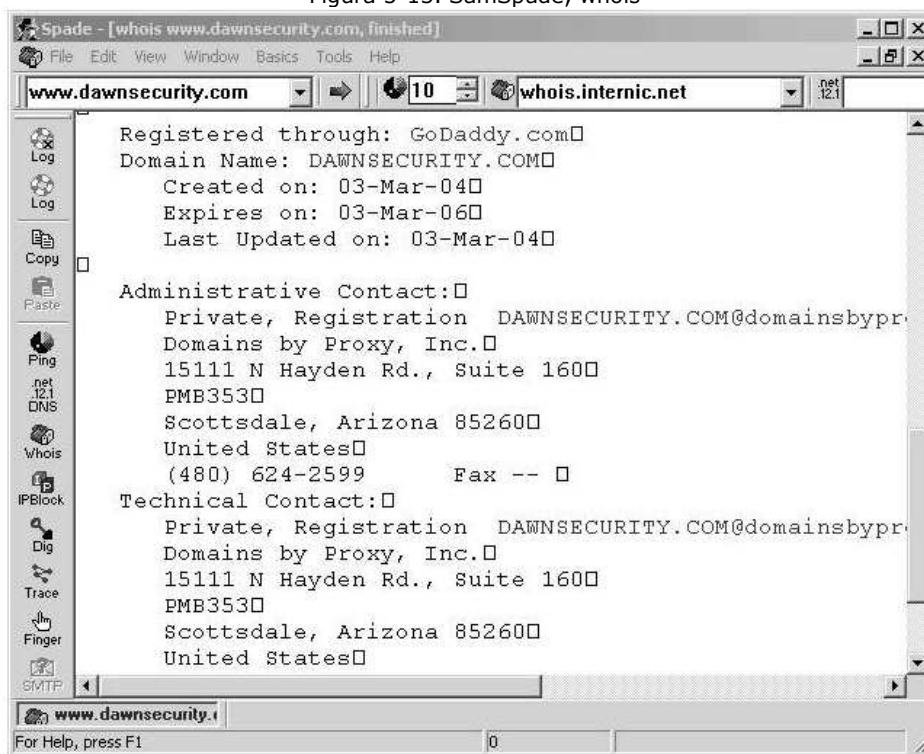
Antes de poder realizar una transferencia de zona, lo que necesita saber cuál es el servidor de nombres con autoridad. Introduzca la dirección IP del servidor DNS, tal y como se muestra en la Figura 5-12. En virtud de TCP / IP, puede elegir ya sea para aprender de su información a través de DHCP o de forma estática ingresando la dirección IP del servidor DNS. Después de esto salir de la pantalla de Opciones.

Figura 5-12. SamSpade, opciones básicas



Ahora puede realizar una búsqueda DNS ingresando en el cuadro de dirección el sitio web de nombres de dominio. En la Figura 5-13, el nombre de dominio ingresado es `www.dawnsecurity.com`. El resultado revela el nombre de la empresa que registró este nombre de dominio, además de devuelve información de contactos administrativos y técnicos. No se muestra en el gráfico la autoridad de la dirección del servidor DNS de `PARK15.SECURESERVER.NET`, que también se incluye en la búsqueda DNS Lookups. Equipado con esta dirección, usted puede intentar una transferencia de zona DNS.

Figura 5-13. SamSpade, whois



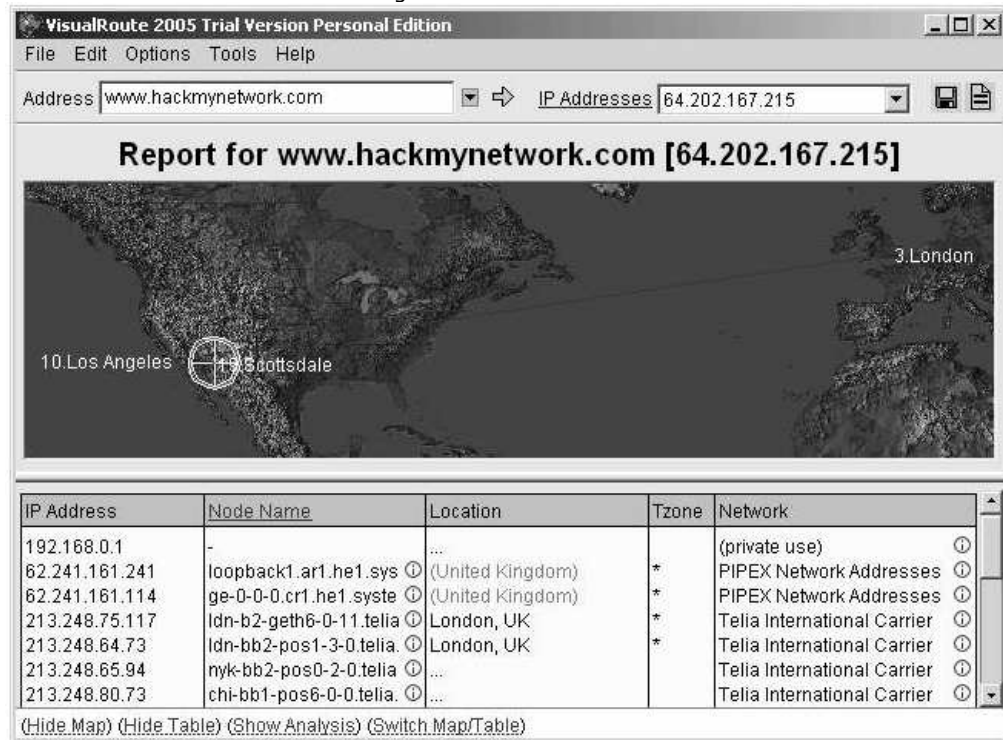
Comience el intento de ir al menú Herramientas y escoger la zona de transferencia. Como en la Figura 5-13, introduzca el nombre de dominio de su destino y la dirección IP del servidor DNS con autoridad en que usted descubrió en el paso anterior. Se tiene la posibilidad de mostrar la salida en SamSpade en un archivo. En primer lugar, ver la información dentro de SamSpade para determinar si puede realizar una zona de transferencia. A continuación, si se tiene éxito, se puede guardar la salida en un archivo para verlo más adelante.

Visual Route

Aunque SamSpade ofrece una excelente salida y debe formar parte de cualquier conjunto de herramientas de pruebas de intrusión, no ofrece mapas gráficos o información detallada a lo largo del camino hasta el punto de destino. Para ver una representación de un paquete a través de Internet a un destino, se necesita una herramienta como Visual Route (<http://www.visualware.com>), que funciona sobre Linux, Windows, Solaris, y Mac OS X.

La Figura 5-14 muestra la pantalla visual del camino que recorre el paquete. Un rastro se ejecuta desde una computadora en Londres a la página web <http://www.hackmynetwork.com> . Visual Route lista cada tramo a lo largo del camino hacia el sitio, junto con las direcciones IP y tiempos de demora.

Figura 5-14. Visual Route



Lo que hace interesante a Visual Route, es que con hacer un doble clic en cualquiera de los saltos a lo largo del camino se puede realizar una consulta Whois. La información es la misma que se consigue en una búsqueda Whois, pero Visual Route es gráficamente más atractivo y hace que sea fácil buscar información. Puede guardar tanto las búsquedas Whois y la visual en el mapa como Jpg o Png, lo que lo hace ideal para preparar informes para los clientes.

Exploración de Puertos

Ahora que se conocen los hosts accesibles de la red, se necesita determinar qué puertos están abiertos en estos hosts. Se puede hacer esto a través del escaneo de puertos, que es el proceso para determinar que puertos TCP y UDP son accesibles.

La mayoría de las aplicaciones de red de hoy corren por sobre TCP o UDP. Estos protocolos son el mecanismo de transporte utilizado por aplicaciones tales como FTP, Simple Mail Transfer Protocol (SMTP), Dynamic Host Configuration Protocol (DHCP), y HTTP.

TCP es un protocolo orientado a la conexión, lo que significa que proporciona la fiabilidad de establecer una conexión entre hosts, por el contrario, UDP no ofrece fiabilidad.

TCP es análoga a la entrega de un paquete a través de correo prioritario en los que el destinatario tiene que firmar el paquete, haciendo que la entrega fiable. En comparación, UDP es similar al correo postal ordinario, lo que no proporciona garantía de que el paquete será entregado. Las aplicaciones UDP, como DHCP, se basan en la capa aplicación para proporcionar la fiabilidad, si es necesario. Las aplicaciones que utilizan TCP (como FTP) cuentan con mecanismos incorporados en el protocolo TCP para proporcionar fiabilidad, o sea sobre la misma capa de transporte.

TCP y UDP identifican las aplicaciones que transportan a través de números de puerto. El Cuadro 5-2 enumera los números de puerto TCP y UDP más comunes. Tiene sentido, entonces, determinar qué aplicaciones se están ejecutando en el host objetivo. Se debe ver los puertos TCP y UDP que están abiertos, realizando de un escaneo de puertos.

Tabla 5-2. Números de puerto

TCP		UDP	
Application	Port Number(s)	Application	Port Number(s)
FTP	20-21	DNS	53
Telnet	23	DHCP	67-68
SMTP	25	TFTP	69
DNS	53	NTP ^[1]	123
HTTP	80	SNMP ^[2]	161
POP ^[3]	110		
NNTP ^[4]	119		
HTTPS ^[5]	443		

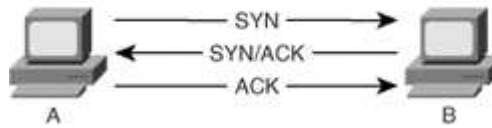
- [1] NTP= Network Time Protocol
- [2] SNMP= Simple Network Management Protocol
- [3] POP= Post Office Protocol
- [4] NNTP= Network News Transfer Protocol
- [5] HTTPS= Hypertext Transfer Protocol Secure

El Escaneo de Puertos esta disponible en muchos tipos, incluyendo los siguientes:

- TCP Connect()scan
- SYN
- NULL
- FIN
- ACK
- Xmas-Tree
- Dumb scan
- Reverse Ident

El escaneo de puertos TCP connect() intenta crear una relación con el objetivo. Una conexión establecida, es la que ha completado el acuerdo de tres vías, que ocurre cuando dos hosts inician la comunicación, como se ilustra en la Figura 5-15.

Figura 5-15. Acuerdo de tres vías (Three Way Handshake)



Como muestra la figura, cuando una computadora busca crear una conexión TCP a la computadora B, envía un paquete de sincronización (SYN) con su número de secuencia inicial (ISN). El número de secuencia inicial pseudo aleatorio es un número entre 0 y 2 elevado a la 32 menos 1 (4294967295).

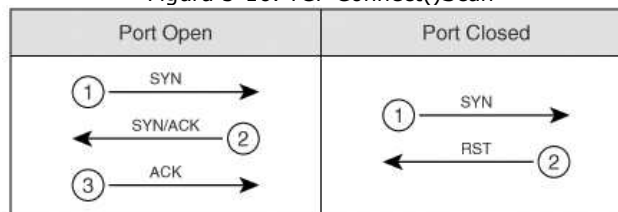
La Computadora B envía un recibo (ACK) de nuevo con el ISN+1, lo que indica el siguiente número de secuencia que predice. La Computadora B también establece el flag SYN e incluye su propio ISN.

La Computadora A, responde a la computadora B, con un ACK para reconocer el paquete recibido SYN/ACK. El número de secuencia es el ISN+1 de la Computadora B, lo que indica el siguiente número de secuencia que espera de la computadora B. Con este acuerdo inicial proporciona fiabilidad porque cualquier desviación del proceso o de cualquier discrepancia de número de secuencia causa que las computadoras envíe un paquete con flag reset (RST), por lo tanto, se pierde la conexión.

TCP Connect()Scan

Un TCP Connect() intenta explorar cada puerto TCP por medio del acuerdo de tres vías. En la Figura 5-16 se muestra como se realiza un escaneo de puertos. Sin embargo, este tipo de exploración es también más fácil de detectar por los firewalls y los sistemas de detección de intrusos (IDS). Por lo tanto, se debe buscar el uso de otros tipos de exploraciones que tienen una mejor oportunidad de evitar la detección.

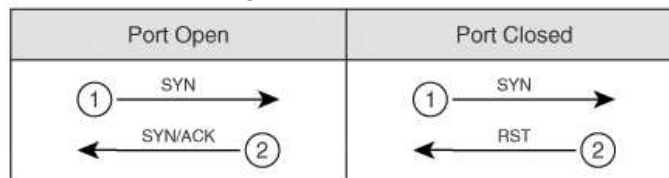
Figura 5-16. TCP Connect()Scan



SYN Scan

Una exploración que es más difícil de detectar, es la exploración SYN. Como se mencionó anteriormente, en TCP las tres fases implican SYN, SYN/ACK, y ACK (en ese orden). Un SYN scan sólo envía el SYN inicial al destino. Como se muestra en la Figura 5-17, si el puerto está abierto, el objetivo responde con un SYN-ACK. Si está cerrado, responde con un RST.

Figura 5-17. SYN Scan



En este punto, el comportamiento de un SYN scan es exactamente como un TCP Connect()scan. Lo que lo hace diferente, es que la host no responde con un paquete ACK, como se esperaría del

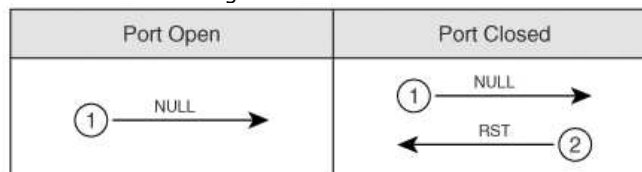
acuerdo de tres vías. En lugar de ello, el host responde con un paquete RST, pasando la conexión. Al caer la conexión antes de ser establecida, el SYN scan pueden pasar desapercibido ante algunos Firewall. Sin embargo, muchos sistemas de detección de intrusos (IDSS) detectan escaneos SYN.

NULL Scan

En una exploración NULL, un paquete sin flag es enviado a un puerto TCP. En condiciones normales de la comunicación TCP, el ultimo flag esta seteado en 1. En una exploración NULL, sin embargo, no se establecen este bit.

La RFC 793 establece que en caso de que un segmento TCP no llega con el flan necesario, el host receptor descarta el segmento y envía un RST. Como se muestra en la figura 5-18, cuando se envía paquetes a cada puerto TCP sin el flan necesario, el objetivo responde con un paquete RST si el puerto está cerrado. Si el puerto está abierto, el host hace caso omiso de lo recibido y lo descarta, así la respuesta no llega.

Figura 5-18. NULL Scan



Esto es, por supuesto, suponiendo que todos los hosts cumplan con la RFC 793. En realidad, Windows no cumple con esta RFC. Posteriormente, no se puede utiliza un NULL scan contra una host con Microsoft Windows para determinar qué puertos están activos.

Cuando un sistema operativo de Microsoft recibe un paquete que no tiene el flag, envía un paquete RST en respuesta, o sea no se puede diferenciar si el puerto esta abierto o cerrado.

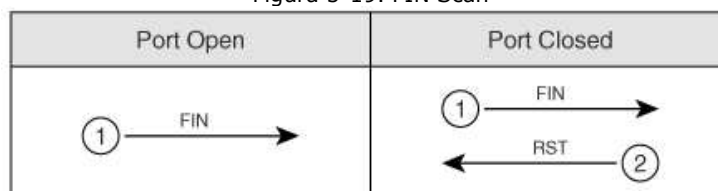
Los sistemas basados en UNIX cumplen con la RFC 793, por lo que envían los paquetes RST cuando el puerto está cerrado y no envía nada si el puerto está abierto.

Tenga en cuenta que este es el efecto contrario a la exploración SYN y TCP Connect(), en estas exploraciones, una respuesta indica un puerto abierto, pero en un NULL scan, una respuesta indica un puerto cerrado. Este es el motivo por el cual el NULL scan se le llama exploración inversa stealthier.

FIN Scan

Otro tipo de exploración inversa es el FIN scan. Al igual que el escaneo NULL, esta es stealthier. En un escaneo FIN, un paquete es enviado a cada puerto TCP con el flag FIN-bit seteado en 1. El bit FIN indica el final de un período de sesiones TCP. Al igual que todas las exploraciones inversas, una respuesta RST indica el puerto que está cerrado, y si no hay respuesta indica que el puerto está a la escucha. Tenga en cuenta, sin embargo, que Windows no se ajusta a la RFC 793, por lo que no proporciona resultados precisos con este tipo de exploración. La Figura 5-19 muestra la respuesta a un FIN scan.

Figura 5-19. FIN Scan



ACK Scan

En condiciones normales de operación de TCP, los acuses de recibo (ACKs) se envían después de que el número de paquetes se especifica en la publicación del tamaño de la ventana de la recepción.

Con un ACK scan, puede ser útil para descubrir la configuración de un Firewall. Si un puerto está filtrado por un firewall, no vuelve nada. Si un puerto está sin filtrar (el tráfico destinado a ese puerto se permite a través del Firewall), sin embargo, un RST es enviado de vuelta. Al escuchar los mensajes RST, puede aprender cuales son los puertos filtrados y sin filtrar.

Xmas-Tree scan

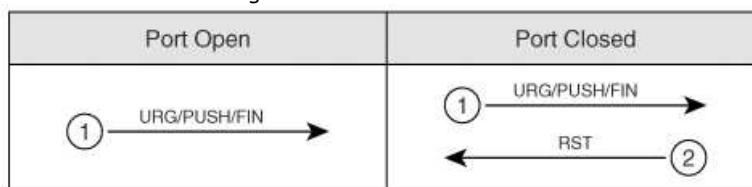
La Figura 5-20 muestra la formación de un paquete en un Xmas-tree scan, el cual envía un paquete TCP con las siguientes banderas:

URG: Indica que el dato es urgente y debe ser procesado inmediatamente

PSH: Fuerza al dato a entrar al buffer

FIN: Se utiliza cuando terminar un período de sesiones TCP

Figura 5-20. Xmas-tree Scan



El truco en esta exploración no es el objetivo de estos flags por separados, el objetivo es de utilizarlos juntos. Una conexión TCP no debe poder hacer nada con los tres de estos parámetros seteados activos. Se obtienen los mismos resultados que otras exploraciones inversas y, posteriormente, tiene las mismas limitaciones cuando se utiliza contra las plataformas Windows.

Dumb Scan

El Dumb scan (también llamada exploración ocupada inversa) fue descubierta por Salvatore Sanfilippo (Ver el documento en <http://www.kyuzz.org/antirez/papers/dumbscan.html>). Dumb scan es un método alternativo de exploración que utiliza un tercer host zombie para actuar como un Dumb en el proceso de escaneo de su objetivo. Un zombie es un host comprometido por que esta ocupado. Generalmente, este no almacena los datos sensibles, y el acceso a ella es a menudo inadvertido. Muchas empresas tienen ocupadas aquellos hosts que se utilizan para la transferencia de datos a través de modems dial-up. Se puede descubrir fácilmente estos mediante el uso de los softwares War dialers como ToneLoc. Por ejemplo, las pequeñas sucursales de cooperativas de crédito podrían utilizar una gran cantidad accesos vía dial-up a la empresa de informes de crédito para reunir los informes financieros de clientes. Si usted puede tener acceso a estos hosts, se puede acceder normalmente al resto de su red de datos.

Usuarios malintencionados suelen utilizar los sistemas ocupados en Internet que están comprometidos. Esta es la razón por la red no está a salvo de piratas informáticos maliciosos.

Al igual que un SYN scan normal, con un Dumb scan, un SYN es enviado al destino. Esta vez, sin

embargo, el zombie lo envía. Si un puerto está a la escucha, el objetivo responde con el SYN/ACK de respuesta. Si el puerto está cerrado, el objetivo responde con un mensaje de RST. En esta etapa, nada distingue el normal SYN scan y al Dumb Scan.

Lo que hace un Dumb scan diferente es que la exploración no es enviada desde su propio host, sino desde un host zombie. Mientras la exploración se lanzó desde el zombie, se lleva a cabo un ping desde un equipo X contra el zombie. Observando el ID en el campo de respuesta de eco del zombie, se puede determinar qué puertos están abiertos y cuales están cerradas en el sistema destino. Por ejemplo, utilizando la utilidad HPING de Linux con el parámetro -r para ver el incremento en el ID, se puede ver la siguiente salida de ping al zombie:

```
HPING B (eth0 172.16.15.12): no flags are set, 40 data bytes
```

```
60 bytes from 172.16.15.12: flags=RA seq=0 ttl=64 id=41660 win=0 time=1.2 ms
60 bytes from 172.16.15.12: flags=RA seq=1 ttl=64 id=+1 win=0 time=88 ms
60 bytes from 172.16.15.12: flags=RA seq=2 ttl=64 id=+1 win=0 time=93 ms
60 bytes from 172.16.15.12: flags=RA seq=3 ttl=64 id=+1 win=0 time=75 ms
60 bytes from 172.16.15.12: flags=RA seq=4 ttl=64 id=+1 win=0 time=93 ms
60 bytes from 172.16.15.12: flags=RA seq=5 ttl=64 id=+1 win=0 time=80 ms
```

En este sentido, los puertos no están abiertos. Comienza con la identificación inicial de 41660 y luego cada ping tiene un incremento. El host X continúa su ping al zombie, pero esta vez cuando el zombie envía un SYN a un puerto abierto del objetivo, la respuesta cambio:

```
60 bytes from 172.16.15.12: flags=RA seq=1 ttl=64 id=+1 win=0 time=87 ms
60 bytes from 172.16.15.12: flags=RA seq=2 ttl=64 id=+2 win=0 time=90 ms
60 bytes from 172.16.15.12: flags=RA seq=3 ttl=64 id=+1 win=0 time=91 ms
60 bytes from 172.16.15.12: flags=RA seq=4 ttl=64 id=+1 win=0 time=92 ms
60 bytes from 172.16.15.12: flags=RA seq=5 ttl=64 id=+1 win=0 time=92 ms
```

En la segunda línea de esta salida, el ID esta incrementando en dos. Esto indica que, cualquiera que sea el puerto que este siendo escaneado en el momento de que se realiza el ping es un puerto de escucha en el objetivo.

Nmap

Ahora que se aprendió las diferentes opciones de exploraciones, se aplicaran estas técnicas utilizando una herramienta llamada nmap.

En general se tiene una caja de herramientas de aplicaciones de software utilizadas con frecuencia en los ensayos, en la cual una herramienta muy importante esta Nmap, escrito por Fyodor y disponibles en <http://www.insecure.org> , está disponible en ambas plataformas Windows y Linux, este capítulo utiliza la versión de Linux con fines explicativos.

Nota:

Nmap, aunque es el más popular, no es el único explorador de puertos. Otros exploradores de puertos que pueden ser incluidos son SuperScan, Scanline, VScan, y Angry IP. Véase el Apéndice B, "Herramientas", para obtener información sobre estos y otros exploradores de puertos.

Nmap es descrito como una herramienta para "permitir que los administradores de sistemas y personas curiosas exploren grandes redes y ver qué servicios están ofreciendo." (Para ver el manual, teclee man nmap a la línea de comandos de Linux). Nmap permite realizar muchas de las exploraciones anteriormente mencionadas.

Nmap Parámetros y técnicas

Los parámetros disponibles en nmap que corresponden a las exploraciones anteriores son los siguientes:

-sT : TCP Connect() scan

-sS : SYN scan

-sF : FIN scan

-sX : Xmas tree scan

-sN : NULL scan

-sI : Dumb scan (también llamada Idle scan)

-sA : ACK scan

Además, otros parámetros son útiles son:

-P0 : No hace ping al hosts antes de escanear.

-PP : Utiliza la petición de respuesta ICMP timestamp (ICMP tipo 13) para encontrar host que estén a la escucha. Normalmente, los intentos de ping a un hosts utilizan la solicitud de eco ICMP (ICMP tipo 1) para ver si el host está ahí. Algunos firewalls y routers bloquean las peticiones de eco, sin embargo, pueden permitir otro tipo de tráfico. Este parámetro también utiliza ICMP para determinar si un host esta activo, pero utiliza un tipo diferente de paquete ICMP para este fin.

-6 : Permite soporte IPv6. Se puede realizar un escaneo de puertos en contra de un nombre de host a través de DNS (suponiendo que el servidor DNS tiene registros AAAA de IPv6) o a través de la dirección IP.

-oN logfilename : envía el resultado a un archivo de formato legible para el usuario.

-oX logfilename : Lo mismo que -oN, pero esta vez lo enviará en formato XML.

-oG logfilename : Lo mismo que -oN, pero almacena todos los resultados en una sola línea para consultar a través del programa Grep.

--append_output : añade la salida a sus archivos de registro existentes en lugar de sobrescribir.

-p : Especifica el número de puerto (o también la lista de puertos) a explorar. TCP y UDP tiene un total de 65.536. También puede especificar si se desea hacer un ping a puertos UDP o TCP. Por ejemplo, para escanear los puertos TCP 23 (Telnet), 25 (SMTP), y 80 (HTTP), puede escribir lo siguiente:

```
nmap -p T:23,25,80
```

-v : modo verbose.

-vv : Muy modo verbose. Activar esto para ver la salida más detallada.

-M max sockets : Establece el número máximo de sockets utilizados por Nmap. La limitación de este valor disminuye la velocidad de exploración, lo cual es útil a la hora de escanear varios hosts de la red que han sido conocidos por accidente cuando se escaneen. Por supuesto, al descubrir estos hosts accidentalmente es una vulnerabilidad que se debe documentar en su informe.

-T {paranoid | sneaky | polite | normal | aggressive | insane}: Cambia el tiempo de exploraciones según las políticas. El valor por defecto es normal, que trata de escanear lo más rápido posible. Paranoid es útil para evitar los sistemas IDS y espera cinco minutos entre cada envío de paquetes. Sneaky envía paquetes cada 15 segundos.

Polite espera cada 0,4 segundos y está diseñado para evitar agredir al host objetivo.

Aggressive e Insane las exploraciones son muy aceleradas, si el sigilo es muy importante, debería evitar esto a menos que haya un motivo justificado.

--host_timeout milisegundos: Especifica cuánto tiempo esperara una respuesta antes de detener el de escaneo de un host. Si nmap parece que se cuelga, puede que desee ajustar este temporizador.

--scan_delay milisegundos: análogas a -T, este especifica cuánto tiempo esperara entre los sondeos. El aumento de este valor podría dejar pasar desapercibido ante los sistemas IDS.

-O: Intenta detectar el sistema operativo.

Además de los parámetros que aparecen en la lista, Nmap es capaz de realizar técnicas más avanzadas, como cambiar la fuente número de puerto, fragmentar paquetes, explorar con rendimiento en Identd, y haciendo rebotar el escaneo con FTP:

--source_port número de puerto: Precisa el número de puerto. Los Firewalls y Routers podrían bloquear un intento de escaneo si el número de puerto está por encima de 1023. Sin embargo, muchos permiten tráfico DNS (puerto 53) o FTP (puerto 21). Si se tiene dificultades para obtener el paso por un firewall, se debe cambiar su número de puerto a 53 o 21.

-f: Fragmenta los paquetes. Al dividir la exploración en pequeños fragmentos TCP, a menudo no son detectados por los dispositivos de seguridad que no procesan los paquetes fragmentados de una exploración que se está llevando a cabo.

-I: Realiza una Identd scan. El protocolo Identd (RFC 1413) permite la divulgación del nombre de usuario asociado con un proceso de TCP. Esto permite conectarse a servidores web y averiguar si se están ejecutando privilegios de root. Esta exploración pocas veces funciona, porque la mayoría de los hosts desactivan el servicio Identd por esta misma razón.

-b: Realiza una exploración desde FTP. Se trata de una exploración antigua, que al igual que el Identd scan, rara vez funciona. Se basa en tener el acceso a un servidor proxy FTP y realizar una exploración desde ese servidor. Una vez más, la mayoría de los administradores tomaron las precauciones necesarias para prevenir este tipo de exploraciones.

Compilando y probando nmap

La compilación de nmap es similar a la compilación de otros programas en Linux. Los pasos son los siguientes:

Paso 1. Descargue la versión más reciente de <http://www.insecure.org> .

Paso 2. Descomprimir nmap utilizando el programa gzip.

Paso 3. Desempaquete nmap utilizando la herramienta tar.

Paso 4. Navegue hasta el directorio que contiene los archivos de nmap y escriba ./configure.

Paso 5. Escriba make install.

Paso 6. Escriba ./install.

A continuación, realice una conexión TCP () scan contra la dirección IP 64.202.167.192. En la línea de comandos, escribir lo siguiente:

```
Nmap-sT-vv -p T:1-1023 -P0 -O 64.202.167.192
```

Esto lleva a cabo una exploración TCP Connect() con salida verbose, escaneado los puertos TCP 1 al 1023 y no realiza ping para ver si el host esta activo. Por último, se permite intentar determinar el sistema operativo con -O.

Basándose en los resultados, se sabe que los puertos TCP 80 y 443 están disponibles. Esto indica que este servidor está funcionando como un servidor web. Como nmap no logra determinar el tipo de sistema operativo en este caso particular, si se encuentran los puertos 137, 138, y 139 abiertos, se sabe que el objetivo es muy probable que ejecuta un sistema operativo Windows, ya que estos puertos son utilizados con NetBIOS (un servicio comúnmente visto en los sistemas Windows). Nmap sabe más de 500 diferentes sistemas operativos y pueden detectar los sistemas operativos no sólo de servidores, sino también de dispositivos de red, como routers, firewalls, y otros.

Fingerprinting

La determinación del sistema operativo del objetivo es importante porque muchos de los exploits son específicos según la plataforma. El proceso de descubrir el sistema operativo subyacente se llama FingerPrinting. Además de utilizar esta característica de nmap, puede probar otras técnicas, tales como Telnet o solicitudes HTTP.

Por ejemplo, se sabría que el objetivo ejecuta HP-UX si se realiza un Telnet a un dispositivo y se obtiene la siguiente respuesta:

```
Trying 10.0.0.1...
```

```
Connected to server.hackmynetwork.com
Escape character is '^]'.
HP-UX B.10.01 A 9000/715 (tty3)
login:
```

Dado que la mayoría de las redes no permiten el acceso Telnet, podría tratar de ejecutar Telnet a otro puerto, como el puerto TCP 21 (FTP). Se sabe que el objetivo ejecuta el sistema operativo Sun por la siguiente respuesta:

```
#telnet 10.0.0.1 21
```

```
220 ftp FTP server (UNIX(r)System V Release 4.0) ready.
SYST
215 UNIX Type: L8 Version: SUNOS
```

También puede probar realizar una petición HTTP GET. La salida que podría recibir si el objetivo ejecuta Microsoft IIS es la siguiente:

```
#echo 'GET / HTTP/1.0\n' | grep '^Server'  
Server: Microsoft-IIS/5.0
```

Otra forma de detectar el sistema operativo del sistema de destino es a través de pila de Fingerprinting. El Stack fingerprinting activamente envía paquetes a la pila TCP/IP del objetivo y analiza la respuesta. La pila TCP/IP difiere entre sistemas operativos, y hace de éste un medio esencial para la detección. Se puede realizar una pila Fingerprinting a través de los siguientes métodos:

BOGUS Probe: Esta técnica detecta los mayores sistemas Linux. En él se establecen los bits 7 y 8 de la cabecera TCP en un paquete SYN. El Kernel de los Sistemas Linux anteriores a la versión 2.0.35 responden con los mismos bits seteados. Estos bits fueron originalmente indefinidos, pero ahora se utilizan para declarar un dispositivo con notificación explícita de congestión (ECN). Los Routers que utilizan Random Early Detection (RED) puede establecer la experiencia de congestión (CE) a fin de notificar a las estaciones de la congestión que se produjo.

TCP ISN sampling: Esta técnica se encuentra en los patrones de números de secuencia inicial (ISN) utilizado en peticiones de conexión. Algunos sistemas UNIX utilizan el 64000 como número de secuencia. Nuevas versiones de Solaris y FreeBSD, sin embargo, emplean los incrementos aleatorios. En comparación, las computadoras de Windows se incrementan por una pequeña cantidad fija cada vez. Por último, algunos de los dispositivos de red siempre comienzan con el mismo ISN. Los Hubs 3Com, por ejemplo, comience con 0x803, y las impresoras Apple comienzan con 0xC7001.

TCP initial Windows size: Esta técnica analiza el tamaño de la ventana sobre el retorno de paquetes. AIX envía un tamaño de la ventana de 16165; Microsoft, OpenBSD, FreeBSD, utilizan 16430; Linux utiliza 32120.

RTO delay: A veces se denomina análisis de la respuesta temporal, se trata de una técnica más complicada porque requiere la adición de un dispositivo Firewall. Un Firewall está configurado para negar los paquetes TCP con las banderas SYN y ACK. Se envía un SYN, pero cuando el objetivo responde con SYN/ACK, éste se encuentra bloqueado. A continuación, se toma el tiempo que transcurre entre las transmisiones (retransmisión time-out) y luego se compara los resultados con una base de datos de firmas. Un parche para Nmap llamado nmap-ringv2 utiliza esta técnica. Ringv2 tiene una técnica parecida a las medidas de la RTO de los paquetes FIN.

IP ID sampling: Cada sistema utiliza un ID de campo en la cabecera IP cuando los datos tiene que ser fragmentados en múltiples paquetes. La mayoría incrementa el valor de a uno, pero algunos no lo hacen, lo cual dará la oportunidad de detectar los sistemas operativos que son una excepción a la regla. OpenBSD, por ejemplo, utiliza una IP aleatoria. Microsoft tiene su propio estilo, incrementa cada vez por 256.

MSS response: Se puede examinar el tamaño máximo de segmento (MSS) de respuesta para determinar si su objetivo correr el sistema operativo Linux. Si se envía un paquete con un pequeño valor MSS a una máquina Linux, responde con un MSS de valor nuevo. Otros sistemas operativos le dan valores diferentes.

Otras herramientas para realizar Fingerprinting son: Xprobe2, Ettercap, p0f V2, Queso, SS y CheckOS

Nota:

Xprobe2 es una herramienta única en el sentido de que utiliza fuzzy . Mantiene una base de datos de Fingerprinting con firmas conocidas, sino que también incluye resultados probabilísticos para reconocer un sistema operativo.

Footprinting

Se debe tener cuidado de confundir con Fingerprinting, Fingerprinting es el proceso de determinar el sistema operativo de un dispositivo, mientras que Footprinting es la combinación de técnicas de reconocimiento activos y pasivos para el fin de establecer una estrategia de ataque.

Después de terminar el Footprinting (recopilando toda la información que sea pertinente al destino), puede dibujar un mapa de red. El mapa de red deben contener lo siguiente:

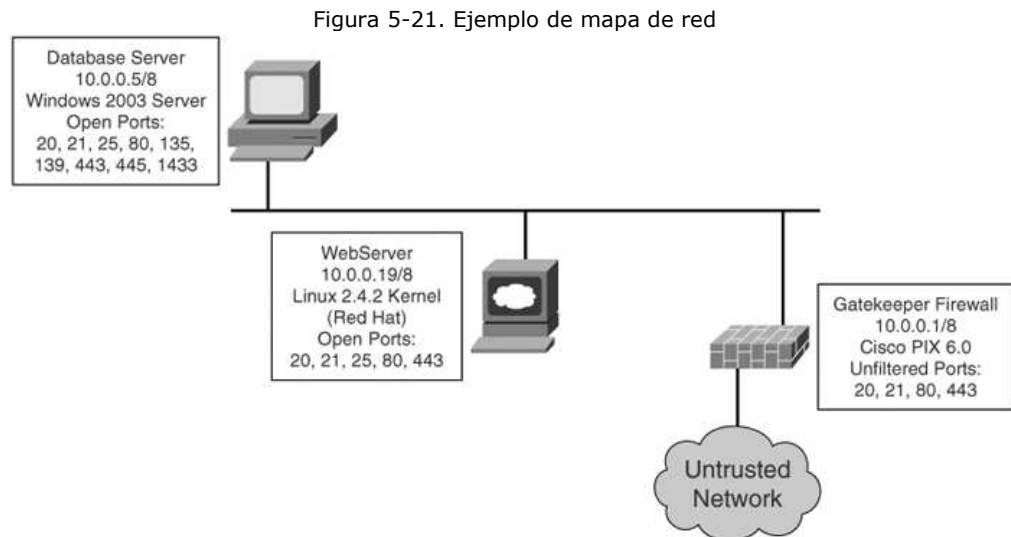
Nombres de host

Direcciones IP

Números de puerto de escucha

Sistemas operativos

La Figura 5-21 muestra un ejemplo de un mapa de red.



Supongamos que se detecto tres servidores y un Firewall. Un servidor ejecuta Microsoft Windows, ya sea 2000 o edición 2003. Aunque no se sabe con seguridad qué tipo de aplicación de base de datos está en funcionamiento, la probabilidad de que ejecute Microsoft SQL Server es alta debido a que es el sistema preferido de bases de datos en Windows.

Armado con esta valiosa información, se puede comenzar a elaborar estrategias en cuanto a qué tipo de ataques se pueden lanzar contra el objetivo. Los ataques se centran en las vulnerabilidades encontradas en los sistemas operativos Windows y sus aplicaciones.

Todas las técnicas mencionadas hasta el momento, aunque no necesariamente de intrusión a una red, puede conducir a consecuencias peligrosas. Por lo tanto, una empresa debe hacer todo lo posible para mitigar los riesgos asociados contra los ataques de reconocimiento.

Detección de escaneo

Esta sección cubre el uso de un Sistema de Detección de Intrusos (Cisco IDS-4215) para vigilar y detectar una red explorada con nmap.

La creación de una barricada de defensa para proteger contra escaneo con nmap implica varios componentes. Antes de profundizar en la detección, es necesario examinar estos componentes de seguridad, tal como se describe en las secciones que siguen.

Detección de intrusos

El IDSS es similar a los sistemas de seguridad que vigilan la entrada o incumplimiento en un lugar. Al igual que un sistema de seguridad, el IDSS tiene un registro de alarmas de entrada en la red. A diferencia de la mayoría de sistemas domésticos, se puede configurar un IDS para detectar entradas a la red, donde se puede analizar la mayor cantidad de tráfico posible.

Sistemas de detección de anomalías

El sistema de detección de Anomalías (también llamado sistema de detección basado en perfiles) está diseñado para vigilar usuarios o un cierto perfil de la red. Por ejemplo, un sistema de detección de anomalías es activar una alarma cuando la red se encuentra utilizada entre un 30 y 90 por ciento por un largo período.

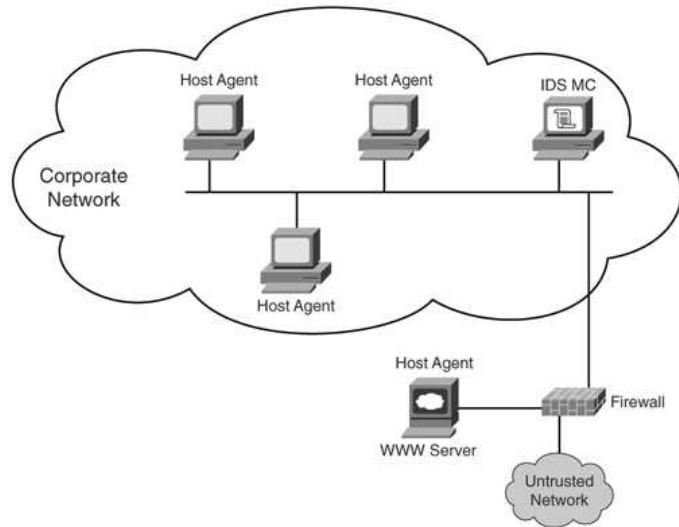
Sistema de detección de uso indebido

Estos sistemas contienen una base de datos de cientos de patrones y firmas que se utilizarán para controlar tráfico en una red. Por ejemplo se puede detectar, con el uso de un software antivirus, patrones en los programas y archivos que representan alteraciones maliciosas. Estos son los sistemas más utilizados de hoy. Sin embargo, pueden convertirse rápidamente en sistemas obsoletos cuando surgen nuevos ataques que no están dentro de las bases de datos.

IDSS basado en Host

El IDSS basado en Host está instalado localmente en un computador central y se utiliza para detectar llamadas al sistema local, realizar logs de auditoría, enviar mensajes de error y analizar tráfico de la red. El beneficio de este sistema IDS es la protección y las alertas que pueden aportar a un sistema específico. Sin embargo, no están diseñados para proteger toda la red, sólo protege un lugar específico. La Figura 5-22 ilustra la manera de desplegar un sistema IDS basado en Host.

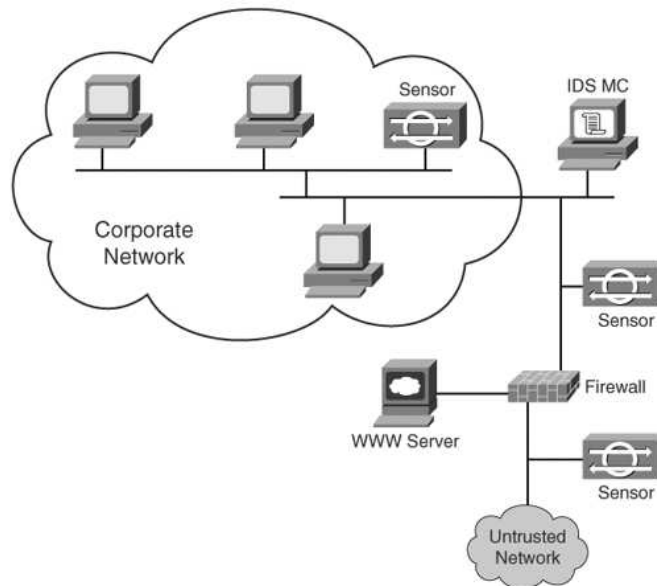
Figura 5-22. Despliegue de IDS basado en Host



IDSS basados en red

El IDSS basado en red, como la serie Cisco 4200, son los aparatos dedicados a una tarea de supervisión de toda la red. Están ubicados en puntos especiales donde pueden controlar el tráfico de la red que está dirigido a cualquier Host. La Figura 5-23 ilustra la manera de desplegar un IDS basado en red.

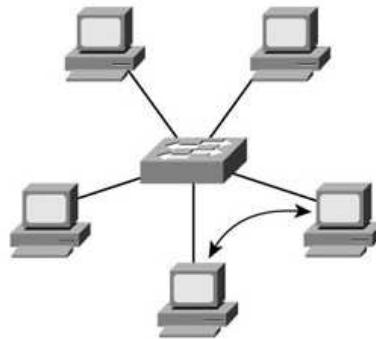
Figura 5-23. Despliegue de IDS basado en Red



Redes Conmutadas

El Switch proporciona una topología de estrella tal como se la podría implementar con un Hub, sin embargo, el Switch no interconecta todos los Hosts con el mismo bus. El Switch está diseñado para operar en Capa 2, el mismo implementa una tabla de direcciones MAC que corresponde a las direcciones aprendidas por sus puertos. Esto aumenta el rendimiento ya que evita las colisiones. Ahora, cuando un Host necesita comunicarse, sus tramas se envían sólo a la interfaz específica que contiene el destino, como ilustra la figura 5-24.

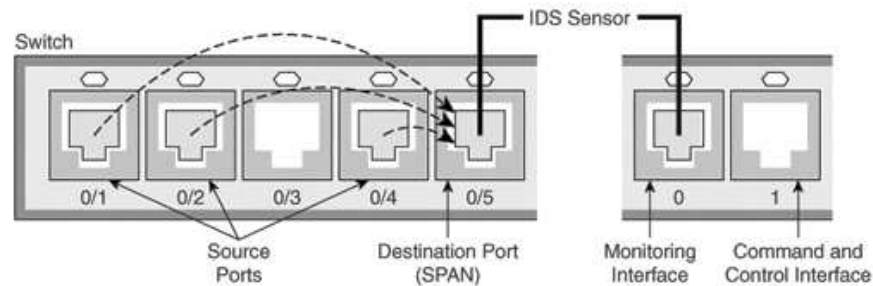
Figura 5-24. Red conmutada



Debido a este diseño básico, donde el tráfico es enviado sólo cuando es necesario, se puede implementar el sistema IDS sobre un puerto de monitoreo o supervisión conocido como SPAN (Switch Port Analyzer Network). La función SPAN permite al administrador de red seleccionar el puerto específico de monitoreo donde espejara todo el tráfico que se requiera para el análisis.

Como ilustra la figura 5-25, el Switch de la derecha está configurado para SPAN. El tráfico ingresa en los puertos 0/1, 0/2 y 0/4 se copian en el puerto destino 0/5 (Puerto con SPAN). El Puerto 0/5 es posteriormente conectado a la interfaz de monitoreo (puerto 0) en el sensor IDS.

Figura 5-25. Puerto utilizando SPAN



Ejemplos de detección de Escaneo

En las secciones siguientes se realizarán ejemplos concretos de la detección de puertos ejecutando nmap. Los ejemplos utilizan una instalación básica de la Cisco IDS 4215 conectado a la red con el software IDS Event Viewer (IEV) para controlar las alarmas de sensores en tiempo real.

Detectando TCP Connect() Scan

El escaneo TCP Connect(), como se mencionó anteriormente, es una técnica confiable de escaneo que determina la condición del puerto (abierto o cerrado). Sin embargo, los sensores IDS detectan con facilidad una conexión TCP normal. El Ejemplo 5-4 muestra la sintaxis utilizada y el resultado del escaneo a un equipo con Windows 2003 Server.

Ejemplo 5-4. El uso de nmap TCP Connect()Scan a un equipo con Windows 2003 Server

```
C:\>NMap -sT -vv -P0 192.168.200.100
```

```
Starting NMap 3.81 ( http://www.insecure.org/NMap ) at 2005-03-21 19:19 GMT  
Standard Time
```

Initiating Connect() Scan against WEB1 (192.168.200.100) [1663 ports] at 19:19

Discovered open port 53/tcp on 192.168.200.100
Discovered open port 23/tcp on 192.168.200.100
Discovered open port 1433/tcp on 192.168.200.100
Discovered open port 1026/tcp on 192.168.200.100
Discovered open port 1031/tcp on 192.168.200.100
Discovered open port 1025/tcp on 192.168.200.100
Discovered open port 139/tcp on 192.168.200.100
Discovered open port 1434/tcp on 192.168.200.100
Discovered open port 445/tcp on 192.168.200.100
Discovered open port 135/tcp on 192.168.200.100
Discovered open port 1029/tcp on 192.168.200.100
The Connect() Scan took 52.38s to scan 1663 total ports.

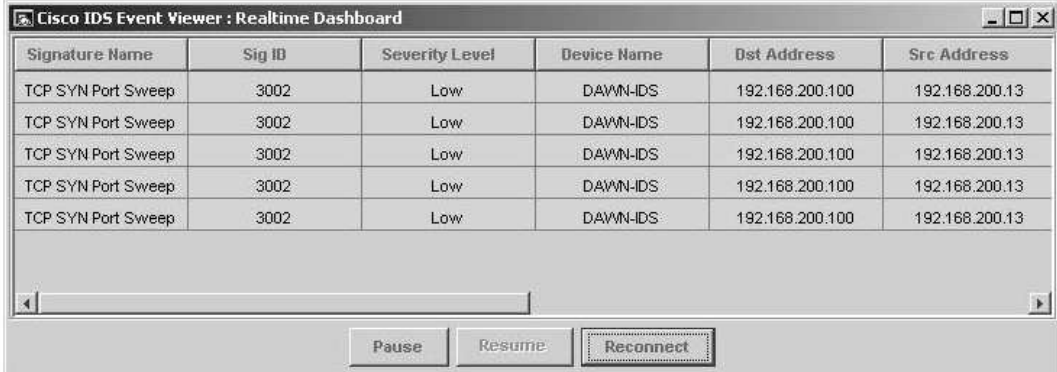
Host WEB1 (192.168.200.100) appears to be up ... good.
Interesting ports on WEB1 (192.168.200.100):
(The 1652 ports scanned but not shown below are in state: filtered)

PORT STATE SERVICE

23/tcp open telnet
53/tcp open domain
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
1029/tcp open ms-lsa
1031/tcp open iad2
1433/tcp open ms-sql-s
1434/tcp open ms-sql-m

Una vez realizado el escaneo con éxito, se observa en tiempo real la salida del IEV de Cisco. En la Figura 5-26 se puede ver que el sensor detecta con exactitud el escaneo.

Figura 5-26. TCP Connect () Scan Detectado



The screenshot shows the Cisco IDS Event Viewer interface with a table of detected events. The table has six columns: Signature Name, Sig ID, Severity Level, Device Name, Dst Address, and Src Address. There are five rows of data, all showing 'TCP SYN Port Sweep' events with a severity level of 'Low'.

Signature Name	Sig ID	Severity Level	Device Name	Dst Address	Src Address
TCP SYN Port Sweep	3002	Low	DAWN-IDS	192.168.200.100	192.168.200.13
TCP SYN Port Sweep	3002	Low	DAWN-IDS	192.168.200.100	192.168.200.13
TCP SYN Port Sweep	3002	Low	DAWN-IDS	192.168.200.100	192.168.200.13
TCP SYN Port Sweep	3002	Low	DAWN-IDS	192.168.200.100	192.168.200.13
TCP SYN Port Sweep	3002	Low	DAWN-IDS	192.168.200.100	192.168.200.13

Detectando SYN Scan

El escaneo SYN es un poco más difícil de detectar, porque solo deja conexiones abiertas y confía que el timeout borre la conexión. El Ejemplo 5-5 muestra la sintaxis utilizada y los resultados generados en el momento del escaneo del equipo con Windows 2003 Server.

Ejemplo 5-5. SYN Scan en un Windows 2003 Server

```
C:\>NMap -sS -vv -P0 192.168.200.100
```

Starting NMap 3.81 (<http://www.insecure.org/NMap>) at 2005-03-21 19:22 GMT

Standard Time
Initiating SYN Stealth Scan against WEB1 (192.168.200.100) [1663 ports] at 19:22

Discovered open port 23/tcp on 192.168.200.100
Discovered open port 53/tcp on 192.168.200.100
Discovered open port 445/tcp on 192.168.200.100
Discovered open port 1031/tcp on 192.168.200.100
Discovered open port 1025/tcp on 192.168.200.100
Discovered open port 1433/tcp on 192.168.200.100
Discovered open port 139/tcp on 192.168.200.100
Discovered open port 1026/tcp on 192.168.200.100
Discovered open port 135/tcp on 192.168.200.100
Discovered open port 1434/tcp on 192.168.200.100
Discovered open port 1029/tcp on 192.168.200.100

The SYN Stealth Scan took 0.11s to scan 1663 total ports.
Host WEB1 (192.168.200.100) appears to be up ... good.

Interesting ports on WEB1 (192.168.200.100):
(The 1652 ports scanned but not shown below are in state: closed)

PORT STATE SERVICE

23/tcp open telnet
53/tcp open domain
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
1029/tcp open ms-lsa
1031/tcp open iad2
1433/tcp open ms-sql-s
1434/tcp open ms-sql-m

MAC Address: 00:50:56:EE:EE:EE

NMap finished: 1 IP address (1 host up) scanned in 0.344 seconds
Raw packets sent: 1663 (66.5KB) | Rcvd: 1663 (76.5KB)

Como se dijo anteriormente, SYN scan deja la conexión abierta. Se trata de una anomalía que se espera tenga lugar entre dos Host si uno esta caído o simplemente que nunca retorne el último ACK. El escaneo SYN es más difícil para detectar por los sensores a causa de su aparición natural "en estado salvaje", sin embargo, en caso de que se inunde la red con ellos, se activara una alarma, como se ve en la Figura 5-27. Se debe tener en cuenta que la firma de la alarma es igual a la del escaneo -sT. Sin embargo, sólo 1 alarma se detectó en contraposición a 6 u 8 alarmas que desencadenó en una normal escaneo -sT. Esto demuestra que el escaneo -sS es menos detectados.

Figura 5-27. Detectando SYN Scan

Signature Name	Sig ID	Severity Level	Device Name	Dst Address	Src Address
TCP SYN Port Sweep	3002	Low	DAWN-IDS	192.168.200.100	192.168.200.13

Detección FIN, NULL, y Xmas-tree scan

Ahora que realizaron las exploraciones básicas TCP Connect() y SYN scans, en esta sección investiga las tres exploraciones inversa. El Ejemplo 5-6 muestra la sintaxis de exploración y resultados contra un Host con Windows 2003 Server. Como se puede ver, en el escaneo todos los puertos están cerrado.

Ejemplo 5-6. Escaneo FIN, NULL, y Xmas-tree

```
C:\>NMap -sF -vv -P0 192.168.200.100
```

```
Starting NMap 3.81 ( http://www.insecure.org/NMap ) at 2005-03-21 19:26 GMT
Standard Time
```

```
Initiating FIN Scan against WEB1 (192.168.200.100) [1663 ports] at 19:26
The FIN Scan took 0.09s to scan 1663 total ports.
Host WEB1 (192.168.200.100) appears to be up ... good.
All 1663 scanned ports on WEB1 (192.168.200.100) are: closed
```

```
MAC Address: 00:50:56:EE:EE:EE
```

```
NMap finished: 1 IP address (1 host up) scanned in 0.312 seconds
Raw packets sent: 1663 (66.5KB) | Rcvd: 1663 (76.5KB)
```

```
C:\>NMap -sN -vv -P0 192.168.200.100
```

```
Starting NMap 3.81 ( http://www.insecure.org/NMap ) at 2005-03-21 19:24 GMT Stan
dard Time
```

```
Initiating NULL Scan against WEB1 (192.168.200.100) [1663 ports] at 19:24
The NULL Scan took 0.08s to scan 1663 total ports.
Host WEB1 (192.168.200.100) appears to be up ... good.
All 1663 scanned ports on WEB1 (192.168.200.100) are: closed
```

```
MAC Address: 00:50:56:EE:EE:EE
```

```
NMap finished: 1 IP address (1 host up) scanned in 0.312 seconds
Raw packets sent: 1663 (66.5KB) | Rcvd: 1663 (76.5KB)
```

```
C:\>NMap -sX -vv -P0 192.168.200.100
```

```
Starting NMap 3.81 ( http://www.insecure.org/NMap ) at 2005-03-21 19:27 GMT Stan
dard Time
```

```
Initiating XMAS Scan against WEB1 (192.168.200.100) [1663 ports] at 19:27
The XMAS Scan took 0.08s to scan 1663 total ports.
```

Host WEB1 (192.168.200.100) appears to be up ... good.
All 1663 scanned ports on WEB1 (192.168.200.100) are: closed

MAC Address: 00:50:56:EE:EE:EE

NMap finished: 1 IP address (1 host up) scanned in 0.312 seconds
Raw packets sent: 1663 (66.5KB) | Rcvd: 1663 (76.5KB)

Sin embargo, el sensor detecta el escaneo inverso e incluso muestra la exploración ejecutada. La Figura 5-28 muestra en tiempo real las alarmas de la detección de escaneo FIN, NULL, y un OOB error que se genera como efecto secundario del Xmas-tree scan.

Figura 5-28. Detectando escaneos inversos



Signature Name	Sig ID	Severity Level	Device Name	Dst Address	Src Address
TCP FIN Packet	3042	High	DAWN-IDS	192.168.200.100	192.168.200.13
Netbios OOB Data	3300	High	DAWN-IDS	192.168.200.100	192.168.200.13
TCP NULL Packet	3040	High	DAWN-IDS	192.168.200.100	192.168.200.13
TCP FIN Packet	3042	High	DAWN-IDS	192.168.200.100	192.168.200.13
TCP Null Port Sweep	3015	High	DAWN-IDS	192.168.200.100	192.168.200.13
TCP FIN High Port Sweep	3011	High	DAWN-IDS	192.168.200.100	192.168.200.13
TCP FIN Port Sweep	3005	High	DAWN-IDS	192.168.200.100	192.168.200.13

DetECCIÓN de OS

La última detección para llevar a cabo es el sistema operativo. Nmap usa el parámetro -O para la detección de OS del objetivo. El Ejemplo 5-7 muestra la sintaxis de exploración y resultados contra un Host con Windows 2003 Server.

Ejemplo 5-7. Escaneo para determinar sistema operativo del objetivo

```
C:\>NMap -O -vv -P0 192.168.200.100
```

```
Starting NMap 3.81 ( http://www.insecure.org/NMap ) at 2005-03-21 19:28 GMT Standard Time
```

```
Initiating SYN Stealth Scan against WEB1 (192.168.200.100) [1663 ports] at 19:28
```

```
Discovered open port 23/tcp on 192.168.200.100  
Discovered open port 53/tcp on 192.168.200.100  
Discovered open port 1434/tcp on 192.168.200.100  
Discovered open port 139/tcp on 192.168.200.100  
Discovered open port 1031/tcp on 192.168.200.100  
Discovered open port 445/tcp on 192.168.200.100  
Discovered open port 1029/tcp on 192.168.200.100  
Discovered open port 1025/tcp on 192.168.200.100  
Discovered open port 1026/tcp on 192.168.200.100  
Discovered open port 1433/tcp on 192.168.200.100  
Discovered open port 135/tcp on 192.168.200.100
```

The SYN Stealth Scan took 0.09s to scan 1663 total ports.

For OSScan assuming port 23 is open, 1 is closed, and neither are firewalled

Host WEB1 (192.168.200.100) appears to be up ... good.
Interesting ports on WEB1 (192.168.200.100):
(The 1652 ports scanned but not shown below are in state: closed)

PORT STATE SERVICE

23/tcp open telnet
53/tcp open domain
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
1029/tcp open ms-lsa
1031/tcp open iad2
1433/tcp open ms-sql-s
1434/tcp open ms-sql-m

MAC Address: 00:50:56:EE:EE:EE

Device type: general purpose

Running: Microsoft Windows 2003/.NET|NT|2K/XP

OS details: Microsoft Windows 2003 Server or XP SP2P

OS Fingerprint:

TSeq(Class=TR%IPID=I%TS=0)

T1(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=MNWNNT)

T2(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)

T3(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=MNWNNT)

T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)

T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)

T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)

T7(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)

PU(Resp=Y%DF=N%TOS=0%IPLEN=B0%RIPTL=148%RIPCK=E%UCK=E%ULEN=134%DAT=E)

TCP Sequence Prediction: Class=truly random

Difficulty=9999999 (Good luck!)

TCP ISN Seq. Numbers: 69D80142 413B414C 4E54B424 74F4775C 1DE05ABB AC9A1054

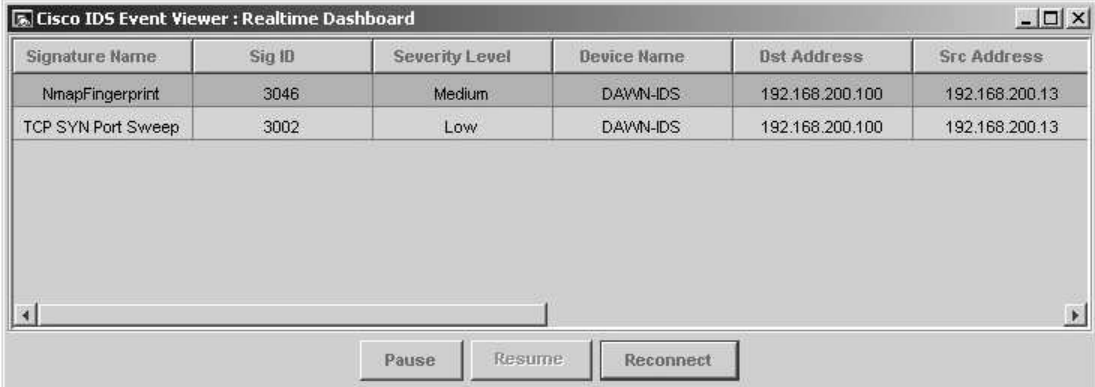
IPID Sequence Generation: Incremental

NMap finished: 1 IP address (1 host up) scanned in 1.062 seconds

Raw packets sent: 1676 (67.3KB) | Rcvd: 1677 (77.4KB)

Lo interesante de esta exploración es que se logra reconocer exactamente el sistema operativo. Sin embargo, sí reduce a que puede ser Windows 2003 Server o XP con SP2. Al utilizar un poco de razonamiento deductivo y observando los puertos que están abiertos, tales como TCP 23, que se utiliza para un servidor Telnet, tendrá que inclinarse más hacia el servidor Windows 2003 en lugar de XP. En cuanto a las alarmas generadas en la Figura 5-29, se puede ver que el IDS detecta el escaneo de OS con un error llamado NmapFingerprint. Esta exploración es fácilmente detectable.

Figura 5-29. Detectando escaneo de OS



Signature Name	Sig ID	Severity Level	Device Name	Dst Address	Src Address
NmapFingerprint	3046	Medium	DAWN-IDS	192.168.200.100	192.168.200.13
TCP SYN Port Sweep	3002	Low	DAWN-IDS	192.168.200.100	192.168.200.13

Caso de Estudio

En este caso de estudio Evil Jimmy (Hacker) escanea una pequeña empresa llamada Little Company Network (LCN). Utiliza DNS para reunir información antes de pasar a Nmap para iniciar su diagramación de la red.

La escena se fija cuando LCN rechaza Evil Jimmy para una posición de trabajo. LCN ni siquiera lee su resumen hasta el final, Jimmy planea hacer uso de sus habilidades en una forma no autorizada. Jimmy sabe el nombre DNS de su objetivo LCN.com, por lo que conecta su ordenador portátil y comienza su ataque. Sabiendo que la preparación es vital para un resultado exitoso, Jimmy comienza por hacer un plan y la recolección de sus herramientas. Los siguientes pasos ilustran la ejecución.

Paso 1. Evil Jimmy utiliza la herramienta Wget para descargar todo el sitio web de la compañía. Él puede después buscar en su tiempo libre información de direcciones de correo electrónico, y cualquier otro detalle sobre la compañía que más tarde podría resultar útil.

Paso 2. Evil Jimmy utiliza SamSpade para descubrir la Dirección de la empresa, contacto, registro y la información publicada por el sitio en el momento en que se ha creado. El siguiente ejemplo muestra estos detalles del resultado en el SamSpade.

Registrant:

LITTLE COMPANY NETWORK
100 NW JOHN OLSEN PLACE
HILLSBORO, OR 97123
US

Domain Name: LCN.COM
Administrative Contact, Technical Contact:
Little Company Network jbates@LCN.COM
100 NW JOHN OLSEN PL
HILLSBORO, OR 97123
US
503-123-5555 fax: - 503-123-5555

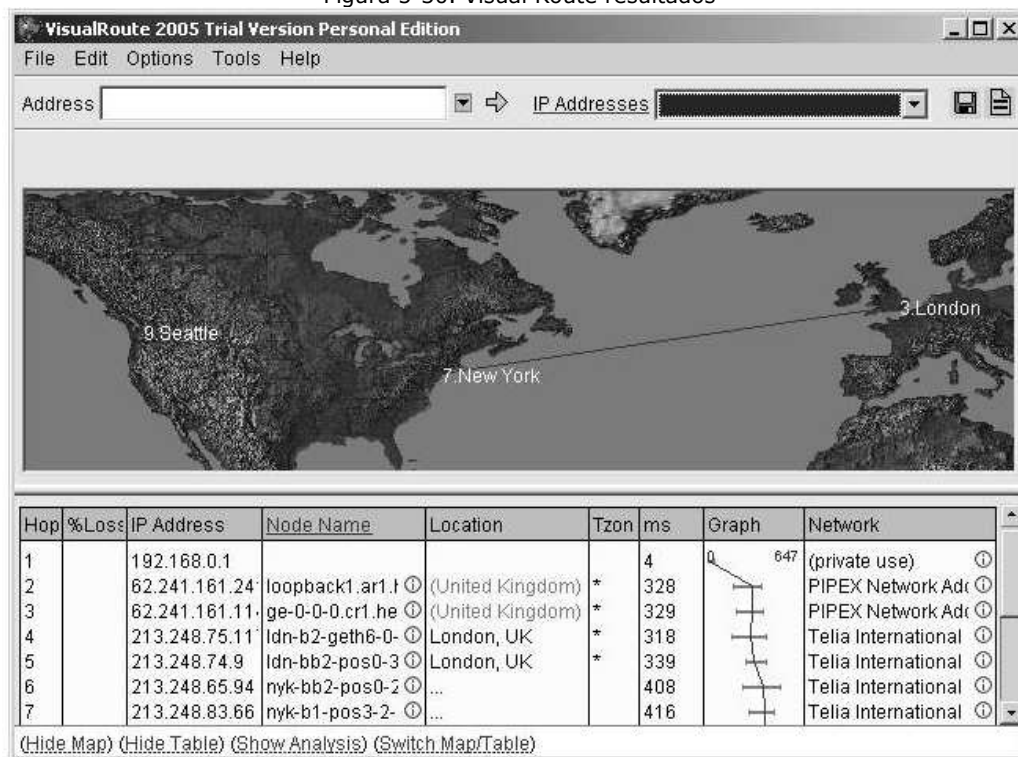
Record expires on 11-Apr-2005.
Record created on 10-Apr-1997.
Database last updated on 20-Mar-2005 17:16:56 EST.

Domain servers in listed order:

NS1.SECURESERVERS.NET
NS2.SECURESERVERS.NET

Paso 3. Usando la herramienta Visual Route, Jimmy obtiene una idea general de donde esta el servidor web. Como muestra la Figura 5-30, el servidor web se encuentra en Seattle.

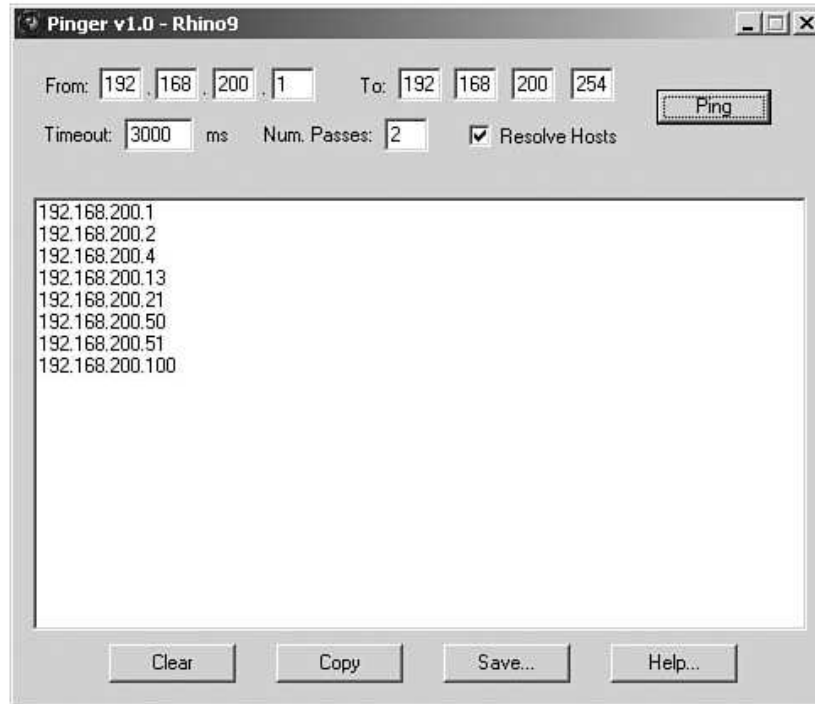
Figura 5-30. Visual Route resultados



Paso 4. Armado con la información Dirección de la empresa, Jimmy Evil se dirige a la empresa y se conecta a la red para hacer un escaneo.

Paso 5. Ahora que Jimmy tiene acceso a la red local, puede realizar un ping sweep a la red. Usando Pinger, Jimmy descubre varios ordenadores a través de la red. La Figura 5-31 muestra los Host de la red que responden a peticiones ICMP estándar.

Figura 5-31. Resultados Pinger



Paso 6. A continuación, Jimmy comienza a escanear los puertos de los Hosts para enumerar los detalles de los programas que están funcionando en cada computadora. Por otra parte, Jimmy utiliza el nmap -O para detectar el sistema operativo que está funcionando. El siguiente ejemplo muestra la información del resultado:

```
C:\>NMap -sS -O 192.168.200.21,100
```

```
Interesting ports on Desk1 (192.168.200.21):
```

```
(The 1658 ports scanned but not shown below are in state: closed)
```

```
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
5713/tcp  open  proshareaudio
```

```
MAC Address: 08:00:46:F3:14:72
```

```
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP SP2
NMap finished: 2 IP addresses (2 hosts up) scanned in 3.203 seconds
```

```
Starting NMap 3.81 ( http://www.insecure.org/NMap ) at 2005-03-21 21:07
```

```
GMT
Standard Time
```

```
Interesting ports on WEB1 (192.168.200.100):
```

```
(The 1652 ports scanned but not shown below are in state: closed)
```

```
PORT      STATE SERVICE
23/tcp    open  telnet
53/tcp    open  domain
```

135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
1029/tcp open ms-lsa
1031/tcp open iad2
1433/tcp open ms-sql-s
1434/tcp open ms-sql-m

MAC Address: 00:50:56:EE:EE:EE

Device type: general purpose
Running: Microsoft Windows 2003/.NET|NT/2K/XP
OS details: Microsoft Windows 2003 Server or XP SP2

Paso 7. Jimmy finaliza su reconocimiento. Afortunadamente para Jimmy, el equipo de detección de intrusos se tomó varios minutos para detectar el escaneo antes de que pudieran empezar a buscar a los culpables.

Paso 8. Jimmy Evil regresa a su casa y comienza a recopilar la información para una fácil lectura del diagrama que muestra las direcciones de Host, servicios abiertos y sistemas operativos.

Resumen

El reconocimiento se puede dividir en dos categorías; pasiva, que es similar a un ladrón que espía una casa caminando a lo largo de la calle, y activa, donde examina por las ventanas para ver si alguna esta abierta.

El reconocimiento pasivo puede llevar mucho tiempo y el rendimiento tiene diversos grados de éxito. El más obvio punto de partida es la página web del objetivo. Dos populares herramientas están disponibles para ayudar a capturar todo el sitio para la navegación fuera de línea:

- Wget (herramienta por línea de comandos)
- Teleport Pro (herramienta gráfica)

Analizando el contenido del sitio puede revelar información como la siguiente:

- Hardware, sistema operativo y la información comentada dentro del código fuente
- Información de contacto para su uso en los ataques de ingeniería social

También se puede extraer información potencialmente útil a partir de fuentes públicas, incluyendo los siguientes:

- Presentaciones EDGAR
- Grupos de noticias USENET
- Reuniones de grupos de usuario
- Socios de negocio

El reconocimiento Activo puede ser mucho más revelador, pero el inconveniente es que es un proceso riesgoso y es más fácil detectar.

Para identificar hosts en la red objetivo, se pueden utilizar las siguientes herramientas:

- NSLookup
- Whois
- SamSpade
- Visual Route

Basta con realizar un nsLookup para buscar una dirección IP en forma pasiva, pero al momento de comenzar a hacer una zona de transferencia, se está empezando a realizar un reconocimiento activo.

Después de identificar los Hosts, se puede utilizar escaneo de puerto para identificar posibles vulnerabilidades. Las técnicas de escaneo de puertos disponibles son:

- TCP Connect () scan
- SYN scan
- FIN scan
- Xmas-tree scan
- NULL scan
- Dumb scan

Además, este capítulo examino nmap, que es una popular herramienta de escaneo de gran alcance.

El fingerprinting es el proceso de examen de las características del Host para identificar su sistema operativo subyacente. Aunque este capítulo se utilizó nmap, otras herramientas están disponibles:

- Xprobe2
- Ettercap
- p0f V2
- Queso
- SS
- CheckOS

Todas estas medidas (reconocimiento activo y pasivo) constituyen el footprinting de un objetivo de la red. Tras la información completa, se debe ser capaz de crear un mapa de red que contenga información como la siguiente:

- Nombres de Host
- Direcciones IP
- Números de puertos
- Sistemas operativos

El reconocimiento contra un blanco de red, como el que se describe en este capítulo, puede ser detectado mediante un IDS, lo cual puede tomar varias formas:

- Detección de anomalía
- Detección de uso indebido
- Detección basado en Host
- Detección basados en la red