Anexo VI

Actividades de reconocimiento de sistemas

Álvaro Gómez Vieites

ANEXO VI

ACTIVIDADES DE RECONOCIMIENTO DE SISTEMAS

Estas actividades directamente relacionadas con los ataques informáticos, si bien no se consideran ataques como tales ya que no provocan ningún daño, persiguen obtener información previa sobre las organizaciones y sus redes y sistemas informáticos, realizando para ello un escaneo de puertos para determinar qué servicios se encuentran activos o bien un reconocimiento de versiones de sistemas operativos y aplicaciones, por citar dos de las técnicas más conocidas.

INFORMACIÓN SOBRE NOMBRES DE DOMINIO, PÁGINAS WEB Y DIRECCIONES IP

En primer lugar, se puede obtener importante información sobre las organizaciones y empresas presentes en Internet, los nombres de dominio y las direcciones IP que éstas tienen asignadas, por medio de consultas en servicios como Whois, que mantiene una base de datos sobre direcciones IP y nombres de dominio necesaria para el correcto funcionamiento de Internet. Así, se podrían consultar las siguientes fuentes de información sobre nombres de dominio y asignación de direcciones IP en Internet:

- Base de datos Whois de InterNIC (*Internet Network Information Center*): www.internic.net/whois.html.

- Servicio de Información de RIPE-NCC (*Réseaux IP Européens Network Coordination Center*) para Europa: www.ripe.net.

- Servicio de Información de ARIN (*American Registry for Internet Numbers*): www.arin.net.

- Servicio de Información de APNIC (*Asian Pacific Network Information Center*), para la región de Asia-Pacífico: www.apnic.net.

- Servicio de Información de LACNIC (*Latin America and Caribean Internet Addresses Registry*): http://lacnic.net.

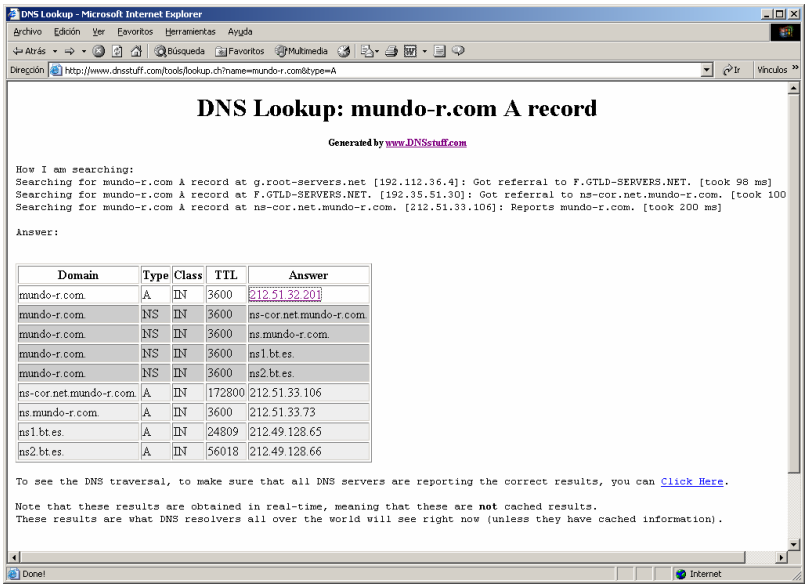

Figura 1: Consulta de la ficha de información sobre un determinado nombre de dominio, perteneciente en este caso a un operador de telecomunicaciones

En las consultas a servicios como Whois también se puede obtener información relevante sobre las personas que figuran como contactos técnicos y administrativos en representación de una organización (podría facilitar diversos ataques basados en la "Ingeniería Social"); datos para la facturación ("*billing address*"); direcciones de los servidores DNS de una organización; fechas en que se han producido cambios en los registros; etcétera.

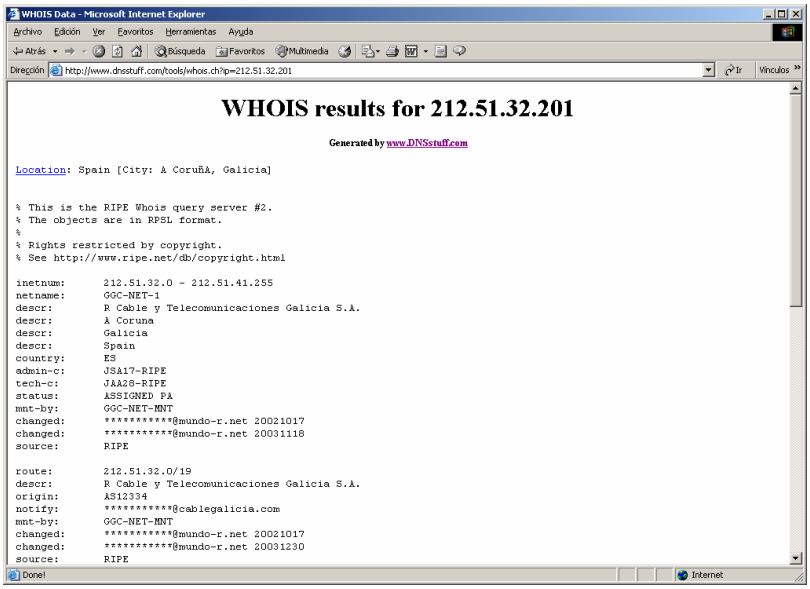

Figura 2: Acceso a la base de datos WHOIS

Por otra parte, se podrían utilizar herramientas que facilitan todos estos tipos de consultas, como podría ser el caso de "DNS Stuff" (www.dnsstuff.com).

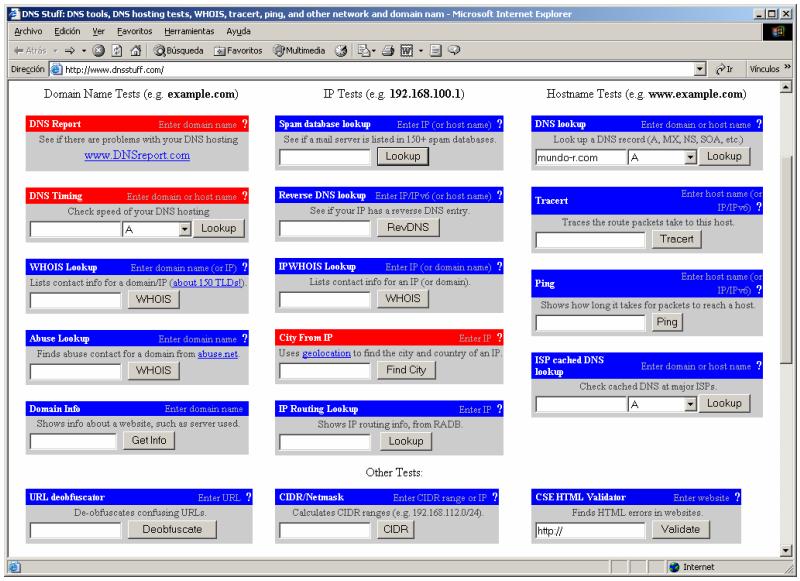

Figura 3: DNS Stuff

Los intrusos también podrían recurrir a la información que facilitan los propios servidores de nombre de dominio de la organización (servidores DNS). Para realizar consultas a un servidor DNS se pueden utilizar herramientas como "nslookup". Si el servicio DNS no se ha configurado adecuadamente, un usuario externo podría realizar una consulta de transferencia de zona completa, obteniendo de

este modo toda la información sobre la correspondencia de direcciones IP a nombres de equipos, las relaciones entre equipos de una organización, o el propósito para el que emplean. Asimismo, mediante una consulta al servicio de nombres de dominio se pueden localizar los servidores de correo de una organización (los cuales figuran como registros MX en una base de datos DNS). Por todo ello, conviene configurar los servidores DNS (o filtrar el tráfico hacia estos servidores en los cortafuegos) para evitar este tipo de transferencias hacia equipos externos.

Para detectar cuáles son los ordenadores conectados a una red informática y obtener información adicional sobre su topología se podrían utilizar herramientas como "*Ping*" o "*Traceroute*".

Así, el servicio PING[1] (*Packet Internet Groper*) permite detectar si un determinado ordenador se encuentra activo y conectado a la red. Para ello, se envía un paquete de control ICMP (paquete "ECHO") a la dirección IP del equipo y se espera la respuesta por parte de éste (paquete "REPLY").

Por su parte, la herramienta "Traceroute" proporciona una relación de todos los equipos incluidos en una ruta entre dos equipos determinados. Para ello, se envían una serie de paquetes de control ICMP que permiten determinar el número de saltos (nodos o equipos que hay que atravesar) necesarios para alcanzar un determinado equipo ("*host*") destinatario. El número de saltos se determina mediante el campo TTL de la cabecera IP de un paquete, que actúa como un contador de saltos que se va decrementando en una unidad cada vez que el paquete es reenviado por un *router*. Existen herramientas gráficas con una funcionalidad similar a "Traceroute" que permiten visualizar las correspondientes asociaciones de cada elemento IP y su localización en un mapa mundial.

También se puede obtener información interesante sobre una organización recurriendo al análisis de sus páginas Web publicadas en Internet, en especial de la revisión del código fuente y de los comentarios incluidos en el propio código de las páginas HTML, ya que permitirán averiguar qué herramientas utilizó el programador para su construcción, así como alguna otra información adicional sobre el sistema (tipo de servidor o base de datos utilizada, por ejemplo).

Otra posibilidad a tener en cuenta es la búsqueda en los foros y grupos de noticias (USENET) para recabar información sobre usuarios de una organización, así como ciertos detalles sobre los sistemas implantados, que podría ser utilizada posteriormente en ciertos engaños y ataques basados en la "Ingeniería Social".

[1] El nombre de PING proviene del mundo del sonar, siendo en este caso el pulso sonoro enviado para localizar objetos en un medio submarino.

INFORMACIÓN REGISTRADA EN BUSCADORES COMO GOOGLE

La localización de referencias sobre la organización en buscadores de Internet como Google o Yahoo! podría facilitar más información de interés para un atacante.

Google es la herramienta de búsqueda más conocida de Internet, capaz de indexar miles de millones de páginas Web. Sin embargo, en ocasiones el motor de búsqueda de Google tiene acceso a determinadas páginas o contenidos de una organización que no deberían ser accesibles directamente desde Internet:

- Directorios o páginas internas a las que no se debería poder acceder de forma directa (técnicas de "navegación transversal").
- Páginas de prueba o evaluación que incluyen todo el código fuente.
- Páginas con determinados mensajes de error que no se deberían mostrar al usuario.
- Ficheros con listas de usuarios y contraseñas, etcétera.

De hecho, resulta importante impedir que los atacantes puedan tener acceso a información sensible a través de buscadores como Google. Para ello, se podría evitar que Google u otros buscadores procedieran a la indexación de las páginas Web de la organización, mediante alguna de las siguientes medidas:

- Bloqueo de buscadores en el propio fichero "robots.txt"[2] del servidor Web:
  - User-agent: googlebot
  - Disallow: /directorio/archivos
- Inclusión de etiquetas en las páginas Web para que no puedan ser indexadas y/o almacenadas en la memoria caché del buscador:
  - Etiquetas para no indexar la página Web en cuestión: <META NAME="GOOGLEBOT" CONTENT="NOINDEX, NOFOLLOW">

[2] Se trata de un fichero que deben consultar todos los motores de búsqueda (o por lo menos, aquellos que cumplen correctamente con las especificaciones de Internet) al acceder a un determinado servidor Web, para determinar si éste permite que sus páginas y recursos puedan ser indexados por el buscador.

- Etiquetas para que no se pueda almacenar la página Web en la memoria caché del buscador: <META NAME="GOOGLEBOT" CONTENT="NOARCHIVE">

- Eliminación de determinadas páginas Web y otros contenidos de la caché de Google directamente desde la página Web: http://services.google.com/urlconsole/controller.

IDENTIFICACIÓN DE SISTEMAS Y ESCANEO DE PUERTOS

Para llevar a cabo la identificación de versiones de sistemas operativos y aplicaciones instaladas es necesario obtener lo que se conoce como "**huellas identificativas**" del sistema: cadenas de texto que identifican el tipo de servicio y su versión, y que se incluyen en las respuestas a las peticiones realizadas por los equipos clientes del servicio en cuestión.

Se conoce con el nombre de "***fingerprinting***" al conjunto de técnicas y habilidades que permiten extraer toda la información posible sobre un sistema. Los atacantes utilizarán esta información para tratar de explorar las vulnerabilidades potenciales del sistema en cuestión.

En este sentido, muchos ataques comienzan llevando a cabo un análisis de las respuestas que genera un sistema informático a determinadas peticiones en un servicio o protocolo, ya que existen distintas implementaciones de servicios y protocolos TCP/IP (distintas interpretaciones de los estándares propuestos en los documentos que describen el funcionamiento de Internet –RFCs–). Para ello, los intrusos se encargan de monitorizar los bits de estado y de control de los paquetes IP, los números de secuencia generados, la gestión de la fragmentación de paquetes por parte del servidor, el tratamiento de las opciones del protocolo TCP (RFCs 793 y 1323), etcétera.

En cuanto a las actividades de escaneo de puertos, éstas tienen lugar una vez que se ha localizado e identificado un determinado equipo o servidor conectado a Internet, para descubrir los servicios que se encuentran accesibles en dicho sistema informático (es decir, cuáles son los puntos de entrada al sistema).

Se puede recurrir a distintas técnicas de escaneo, siendo las más conocidas las que se describen a continuación:

a) Técnica "*TCP Connect Scanning*"

Esta técnica de escaneo es la más sencilla, ya que consiste en el envío de un paquete de intento de conexión al puerto del servicio que se pretende investigar, para comprobar de este modo si el sistema responde aceptando la conexión o denegándola. No obstante, esta técnica es fácilmente detectable, por lo que se puede configurar al sistema informático para que no responda a este tipo de acciones.

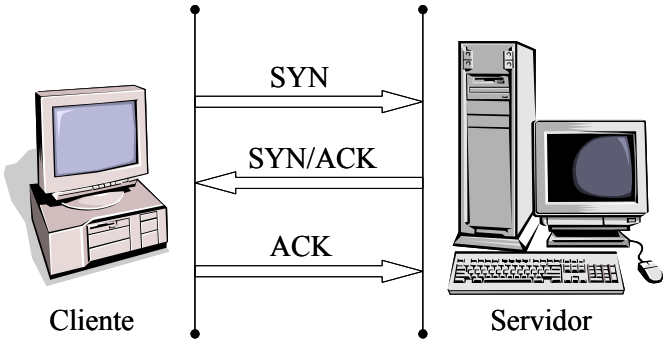

Figura 4: Técnica "TCP Connect Scanning"

b) Técnica "*TCP SYN Scanning*"

En esta técnica de escaneo se intenta abrir la conexión con un determinado puerto para a continuación, en cuanto se confirma que el puerto está abierto, enviar un paquete "RST" que solicita terminar la conexión. Esta técnica de escaneo no es registrada por algunos servidores.

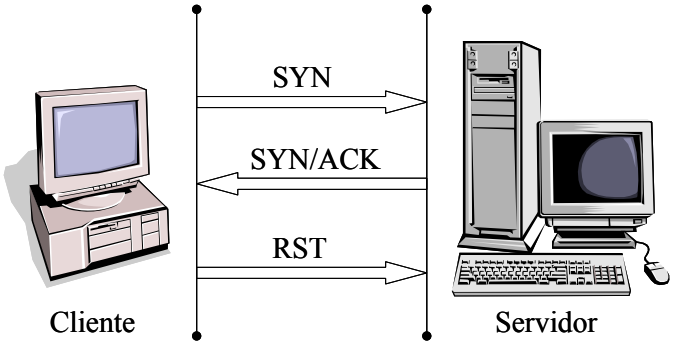

Figura 5: Técnica "TCP SYN Scanning"

c) Técnica "*TCP FIN Scanning*"

También conocida como "*Stealth Port Scanning*" (Escaneo Oculto de Puertos), ha sido propuesta como una técnica de escaneo que trata de evitar ser registrada por los cortafuegos y servidores de una organización.

Se trata, por lo tanto, de una técnica más avanzada que las anteriores, que consiste en el envío de un paquete "FIN" de exploración, de forma que si el puerto está abierto, el servidor ignorará este paquete, mientras que si el puerto está cerrado, el servidor responderá con un paquete "RST". Algunos sistemas, como los de Microsoft, no cumplen de forma estricta el protocolo TCP, respondiendo siempre con un paquete "RST" ante un paquete "FIN", independientemente de si el puerto se encuentra abierto o cerrado (por este motivo, no son vulnerables a este tipo de técnica de escaneo).

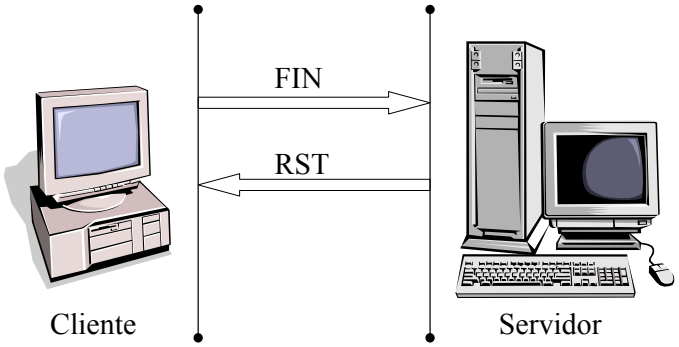

Figura 6: Técnica "TCP FIN Scanning"

d) Otras técnicas de escaneo de puertos:

- **"*TCP Null Scanning*"**: en esta técnica se envía un paquete TCP con todos los "*flags*" a cero en su cabecera.
- **"*TCP ACK Scanning*"**: técnica que permite determinar si un cortafuegos actúa simplemente como filtro de paquetes o mantiene el estado de las sesiones.
- **"*TCP Fragmentation Scanning*"**: técnica de escaneo que recurre a la fragmentación de paquetes TCP.
- **"*TCP Window Scanning*"**: permite reconocer determinados puertos abiertos a través del tamaño de ventana de los paquetes TCP.
- **"*TPC RPC Scanning*"**: en los sistemas UNIX esta técnica permite obtener información sobre puertos abiertos en los que se ejecutan servicios de llamada a procedimientos remotos (RPC).
- **"*UDP ICMP Port Unreachable Scanning*"**: técnica que emplea paquetes UDP para tratar de localizar algunos puertos abiertos.
- Técnicas que se basan en el análisis de los mensajes de error generados ante paquetes de control ICMP malformados enviados a un equipo: modificación maliciosa de la cabecera del paquete, uso de valores inválidos, etcétera.

Los atacantes pueden utilizar numerosas herramientas disponibles en Internet que facilitan el escaneo de puertos:

- NMAP (para UNIX): www.insecure.org/nmap/.
- NMAP (Windows): www.eeye.com/html/Research/Tools/nmapnt.html.

- NetScan Tools (para Windows): www.nwpsw.com.
- WinScan (para Windows): www.prosolve.com
- CyberCop Scanner de Network Associates, etcétera.