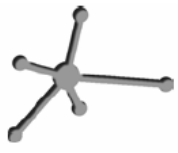
Universidad Pública de Navarra

Grupo de Redes, Sistemas y Servicios Telemáticos



SEGURIDAD EN SISTEMAS INFORMÁTICOS

Práctica 1
Técnicas de Intrusión: los “preliminares”

Introducción

Internet es una red pública de escala planetaria formada por la interconexión de multitud de redes y equipos individuales que se comunican mediante distintos protocolos, entre los que destaca TCP/IP.

Si buscamos una definición más completa podemos acudir a la Wikipedia: http://es.wikipedia.org/wiki/Internet; pero cuidado, aunque esta sea una herramienta muy útil ha de tomarse, al igual que todo en Internet, con precaución: SIEMPRE hemos de intentar contrastar la información y la fuente, antes de tomarlas como veraces.

En el caso de Internet, creo que podemos afirmar que es uno de los avances tecnológicos que ha cambiado el mundo a mejor, y no sólo para quien tiene acceso a La Red. Sin lugar a dudas se trata del medio de comunicación más libre creado hasta la fecha. Es la libertad de expresión (casi) en estado puro. Los usuarios no son meros agentes pasivos que se limitan a recibir información ya elaborada (al estilo de la radio o la televisión), sino que, si lo desean, pueden convertirse en agentes activos e inyectar su propio tráfico, dotándola de contenidos propios. Incluso, en algunos casos, son capaces de tomar sus propias decisiones administrativas.

Este carácter libre es, en principio, muy interesante pero La Red es una herramienta utilizada y conformada por personas y, como tal, imperfecta; es un reflejo de nuestra propia sociedad y, por lo tanto, también contiene aspectos negativos (incluso delictivos) que han de ser perseguidos y castigados por la ley, pero no a cualquier precio. Las nuevas legislaciones sobre Internet tienden al control de la información y los usuarios, a coartar las libertades adquiridas y restringir el acceso a contenidos y su utilización. Como usuarios y votantes no debemos permitir tales actuaciones, ni las de las empresas que aceptan restricciones de las libertades de los usuarios, impuestas por regímenes totalitarios (como es el caso de Yahoo y Google en China).

Pero también trae consigo consecuencias no deseadas, que sus creadores y primeros usuarios jamás pudieron imaginar. Como ya se habrá explicado en clase de teoría, Internet fue concebida inicialmente con fines militares y nunca se pensó que su uso se haría extensivo al público en general, por lo que a la hora de diseñarla no se tuvo en cuenta su seguridad; se diseñó para ser muy flexible y fiable (es decir, para no fallar nunca por avería de un nodo de comunicaciones) pero no para ser segura ya que en aquella época nunca se pensó que Internet (Arpanet, en realidad) se emplearía más allá de unos pocos ordenadores muy controlados y a los que muy poca gente tuviera acceso en todo el mundo. En la actualidad, Internet es una red muy grande y de carácter transnacional. Esto facilita la labor de los usuarios no deseados, al permitirles camuflar sus actividades, o escapar de la justicia si residen en otros países.

Estructura organizativa de Internet

Sin lugar a dudas, la gestión no centralizada es lo que ha hecho posible el rápido crecimiento de Internet. Existen organizaciones centrales, pero no se encargan de todos los detalles administrativos, sino que delegan la autoridad y la gestión en niveles inferiores.

Algunas organizaciones involucradas en la gestión y organización de Internet son:

- IANA (http://www.iana.org)
- RIPE (http://www.ripe.net)
- ICANN (http://www.icann.org)
- ESNIC (http://www.nic.es)

Visitando las páginas anteriores podrá conocer qué función desarrolla cada una de las organizaciones mencionadas y qué relación hay entre ellas. Este conocimiento nos será

muy útil a la hora de saber qué información podemos extraer de sus bases de datos (públicas). También puede buscar los términos anteriores en la enciclopedia libre Wikipedia (http://www.wikipedia.org) o en su versión en español (http://es.wikipedia.org) también muy útil, aunque algo menos completa.

Bases de datos DNS

El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. DNS es capaz de asociar a cada nombre de dominio distintos tipos de información, que se almacena en registros. Los más comunes son los registros de tipo A (que nos indican las relaciones nombre-IP), CNAME (nombres o alias que tiene esa máquina), MX (servidores de correo que se deben utilizar para un dominio concreto) y NS (servidores de nombre asociados), aunque existen otros registros tan curiosos como LOC, que permite introducir datos sobre la localización geográfica de una máquina sobre la superficie terrestre (latitud y longitud en grados minutos y segundos) además de otros datos complementarios.

Los usos más comunes son la *resolución* de nombres, que consiste en la conversión de nombres de dominio (www.rediris.es) a direcciones IP (130.206.1.2) y la localización de los servidores de correo electrónico de cada dominio. Otro uso habitual es el proceso de conversión de direcciones IP (159.237.12.60) a nombres de dominio (www.unav.es), conocido con el original nombre de *resolución inversa*.

Puede acceder a esta base de datos mediante el comando *host* de UNIX. Por ejemplo para averiguar qué dirección IP está asociada al nombre *www.telefonica.com* debería teclear en una *shell*:

```
$ host -a www.telefonica.com
```

Si lo que quiere es realizar la conversión inversa, teclee:

```
$ host -a 194.224.55.221
```

Si quiere saber más sobre el comando *host*, consulte su página del manual de LINUX (*man 1 host*).

Como curiosidad, además del espacio de nombres DNS "oficial" (el que contiene los dominios .com, .org, .net, … etc., y que depende en último término del Departamento de Comercio de EEUU), existen otros alternativos. Uno de ellos, el OpenNIC, ha surgido como iniciativa de la comunidad de usuarios frente al control que las corporaciones ejercen en el DNS tradicional. Puede encontrar información adicional en wikipedia o en la propia web de la organización http://www.opennic.unrated.net/; las extensiones de dominio son de lo más curiosas.

En sistemas operativos Windows tenemos una herramienta de funcionalidad similar a *host*, cuyo nombre es *nslookup*. Para ver su funcionamiento, es necesario que abramos un "terminal" de línea de comandos. Para ello, vaya a *Inicio>Ejecutar* y, en la ventana que se abre, teclee *cmd* y pulse *Aceptar*. Una vez abierto el terminal, puede teclear *nslookup*, para que se abra el modo interactivo de la aplicación, y una vez ahí teclee *help*, para ver las distintas opciones que presenta el programa. Para realizar una búsqueda concreta, recomiendo que anote las opciones que quiera incluir en la línea de comandos, salga del modo interactivo (*exit*) y teclee el comando, con las opciones y el dominio/IP que quiera consultar.

Bases de datos whois

WHOIS es un protocolo TCP basado en preguntas/repuestas que es usado para consultar bases de datos que proporcionan información sobre los propietarios de dominios, rangos de direcciones IP y dominios autónomos.

Para acceder a estas bases de datos se puede utilizar el comando *whois* de UNIX; siempre que hablemos de un nuevo comando UNIX/LINUX es muy recomendable consultar la página del manual (*man*) correspondiente al mismo.

Otra opción es acceder a dicha información utilizando una interfaz web. Hay muchas disponibles. Se diferencian en su estética y el número de bases de datos *whois* que nos permiten consultar. Por ejemplo, la de la institución RIPE proporciona información sobre los rangos de direcciones IP y además algunos de los datos de contacto del propietario/a. Pruebe a acceder a la dirección http://www.ripe.net/db/whois/whois.html y busque la cadena 130.206.0.0. Deberá aparecer información del rango de direcciones IP 130.206.0.0/16. Este rango es el asignado a RedIRIS, la institución que proporciona conectividad a Internet a las universidades y centros de investigación españoles. Pruebe también la interfaz de la página www.completewhois.com. Permite realizar cualquier tipo de consulta y funciona bastante bien.

Si prueba a introducir la misma IP en RIPE y en *completewhois.com* puede darse el caso de que la información devuelta sea diferente o, mejor dicho, más o menos completa; esto puede comprobarlo también si realiza la misma consulta con *whois* desde línea de comandos. En concreto, existe una opción en el comando *whois* que nos permite forzar nuestra búsqueda sobre la base de datos de un servidor concreto (INTERNIC, ARIN, RIPE, ESNIC,…). Si no forzamos la búsqueda, el comando realizará la búsqueda en un servidor u otro en función, por ejemplo, de la extensión del dominio que estemos buscando.

A la hora de obtener el resultado deseado, también son importantes los términos de búsqueda que empleemos. Pruebe a forzar la búsqueda de la cadena *google.com* sobre el servidor de ARIN (*whois.arin.net*); pruebe ahora con sólo *google* (sin extensión), verá que los resultados obtenidos son diferentes.

Herramientas traceroute

El comando *traceroute* de UNIX (y su equivalente en Windows *tracert*) sirve para averiguar qué ruta siguen los paquetes que se mandan de un *host* a otro. Lo que hace básicamente es mandar paquetes IP al *host* de destino incrementando progresivamente el valor del campo TTL (*Time To Live*). De esta forma, los *routers* que están por el camino van enviando mensajes ICMP de error y así podemos saber qué máquinas hay en el camino. Si quiere aprender algo más sobre este comando, puede leer la página del manual o buscar información adicional.

Esta utilidad se concibió como una herramienta de ayuda a la administración y gestión de redes. Por ejemplo, si no tenemos conectividad entre dos máquinas, podemos determinar en qué enlace o *router* se encuentra el problema e informar al administrador responsable.

Pero también es posible utilizarla con otros fines más “oscuros”. El ejemplo típico sería estudiar qué *routers* y enlaces de acceso a Internet tiene una organización para, de entre ellos, elegir la puerta de entrada más débil para posibles ataques.

Al igual que sucedía con las bases de datos *whois*, además del comando que podemos ejecutar desde nuestras máquinas, existen varios interfaces web que implementan la herramienta *traceroute*. Esta opción resulta especialmente interesante ya que, por cuestiones como por ejemplo el balance de carga, una entidad puede presentar distintas puertas de entrada, según cual sea el origen de los paquetes. Los interfaces web nos permiten trazar rutas a un mismo punto de destino desde servidores situados en distintos lugares del planeta. En la página http://www.traceroute.org/ tiene una lista exhaustiva de servidores, organizada por países.

Como curiosidad, existen herramientas que permiten realizar trazados de ruta gráficos. Un ejemplo es el software propietario de la empresa VisualWare Inc., sobre el que puede

encontrar más información en la página web de la compañía (http://www.visualware.com/) o en la del propio producto: http://www.visualroute.com/.

Servicios de anonimato y privacidad

La finalidad de este tipo de servicios es preservar el anonimato y la privacidad de las comunicaciones.

Los pioneros fueron ciertos servidores de correo SMTP que borraban las cabeceras que permitían trazar al emisor del mensaje (p.ej., la que contiene la dirección IP) y las sustituían por las correspondientes al propio servicio de anonimato. Además, algunos no guardaban registros de las transacciones realizadas, por lo que el usuario tenía la seguridad de que el anonimato era casi total. Si los registros no existían, ningún curioso podría nunca acceder a ellos. Ni ninguna corte judicial.

En la actualidad existen empresas que ofrecen acceso a cualquier puerto, no sólo al del correo (SMTP). Básicamente, lo que hacen es proporcionar un servidor de SOCKS seguro (con encriptación). Si le interesa el tema, puede encontrar más información en la web http://www.findnot.com/.

Es evidente que la existencia de estos servicios constituye una dificultad adicional para trazar el origen de posibles ataques.

APÉNDICE: *Búsqueda de Vulnerabilidades (Bug Tracking)*

El origen etimológico del término "bug" se remonta al siglo XIX, en el que se empleaba dentro de la jerga de los ingenieros para describir pequeños fallos o defectos de origen inexplicable. De ahí pasó al mundo de las telecomunicaciones, durante los primeros días del telégrafo, y de éste al de la informática, en el cual se generó, además, el término "debug".

El término "bug" puede referirse a fallos en el hardware o en el software, aunque de forma general se suele utilizar para referirse a fallos en el software (dado que son los más numerosos). El problema surge cuando estos fallos no impiden el correcto funcionamiento de los programas (por lo que son aparentemente invisibles), pero dejan al descubierto determinados agujeros de seguridad que pueden ser aprovechados por usuarios remotos para realizar ataques.

Una vez un atacante ha extraído, toda la información posible acerca de la red objetivo de su ataque (empleando, entre otras, las herramientas que hemos visto hasta ahora), sabrá qué *hosts* están activos, qué sistemas operativos corren dichos *hosts* y qué servicios están activos en los mismos. A partir de ahí empezará por buscar las vulnerabilidades conocidas empleando algún software específico de *bug tracking* como Bugzilla, Eventum o Mantis, o a través de las múltiples bases de datos existentes en La Red, como:

- http://www.cert.org/
- http://nvd.nist.gov/
- http://www.us-cert.gov/
- http://isc.sans.org/index.php

Estos registros almacenan información actualizada a cerca de fallos de seguridad en general y posibles amenazas, recogiendo incidencias de productos de distinta índole y procedencia.. Pero también los propios fabricantes de equipos y empresas o colectivos de desarrolladores de software mantienen y actualizan sus propios registros:

- http://seclists.org/
- http://www.securityfocus.com/
- http://www.debian.org/security/
- http://www.ubuntu.com/usn
- http://bugs.gentoo.org/
- http://cve.mitre.org

Por ello, un responsable de seguridad tiene que estar puesto al día y conocer estos fallos. Saber cuáles son, en qué consisten exactamente, qué consecuencias pueden tener y qué sistemas están afectados. Y lo más importante: cómo proteger los sistemas vulnerables. En la mayoría de las ocasiones, para proteger los sistemas afectados se debe aplicar un parche de seguridad. Mientras tanto, la alternativa más segura (aunque pocas veces factible) consiste en el cese temporal en la prestación del servicio asociado.