Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 1: Técnicas de intrusión

1- 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.

Puede decirse que Internet es el 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.

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.

2- 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

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

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.

3- 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 (130.206.1.46) 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 de su PC-SC:

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

Entre otros datos interesantes podemos obtener también el servidor de correo de un dominio consultando el registro MX del dominio:

```
$ host –t mx 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 manual de LINUX (*man host*).

Checkpoint 1.1: Mediante consultas DNS busque toda la información que pueda sobre los dominios ***telefonica.com*** y ***navalur.com*** Muestre al profesor toda la información que ha sido capaz de averiguar y coméntela brevemente.

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.opennicproject.org las extensiones de dominio son de lo más curiosas.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

4- 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 correspondiente al mismo. Para ello, en este caso, sólo tiene que teclear el nombre del comando: `whois`

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.

Si prueba a introducir la misma IP en RIPE o desde la línea de comandos de su PC puede darse el caso de que la información devuelta sea diferente o, mejor dicho, más o menos completa. 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.

Investigue qué datos hay sobre el dominio ono.com. Hágalo con todas las herramientas que tiene disponibles hasta ahora (comando `whois` o páginas webWHOIS y consultas a la base de datos del DNS). ¿Qué direcciones IP están asociadas a esta empresa? ¿Qué IPs es capaz de conocer y cuál es su función? Muestre al profesor el rango de IPs que tiene la empresa ONO así como el conjunto de IPs que ha podido descubrir.

Checkpoint 1.2: Suponga que es el responsable de seguridad de una red y que detecta un posible ataque procedente de la dirección 130.206.1.1. ¿A qué dirección de correo electrónico enviaría un mensaje denunciándolo? ¿Y si en vez de un ataque hubiese recibido correo basura (spam)? Muestre al profesor de dónde y cómo ha obtenido la respuesta.

5- Herramientas traceroute

El comando `traceroute` de UNIX 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

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

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, consulte su manual (`man traceroute`) o busque información adicional por la web.

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.

Un método habitualmente empleado por los administradores para evitar exponer información sobre la estructura de red a posibles atacantes es no permitir paquetes ICMP en las redes perimetrales. Esto hace que sea más complicado obtener información, pero aún así la información que obtenemos puede servir para conocer los puntos de entrada, aunque no sepamos la estructura interna de la red. Para evitar esta limitación podemos intentar realizar un `traceroute` utilizando el puerto 53 UDP, que habitualmente es utilizado por los servidores DNS para recibir peticiones, o utilizar el puerto 80, puerto de servidores web. En algunos casos conseguimos acceder a puntos internos, aunque para ello el destino del `traceroute` debe ser un servidor DNS o un servidor web (investiga en la páginas man del comando `traceroute` la opción para cambiar el puerto destino en trazas de red).

Realice trazados de ruta al host `www.arsys.es` desde la web utilizando páginas situadas en países diferentes. Podrá comprobar que el ISP `arsys` tiene más de un enlace a Internet y que el servidor de destino no envía mensajes ICMP de error.

Checkpoint 1.3:¿Cuántos routers de acceso (los últimos en aparecer) puede encontrar que sean de Arsys? Muestre al profesor los routers que cree que son de la empresa Arsys.

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).

6- 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

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

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.

Investigue sobre las siguientes cuestiones:

1. ¿Qué es un exploit?
2. ¿En qué consisten las vulnerabilidades basadas en Buffer Overflow y qué consecuencias trae una vulnerabilidad de este tipo en un sistema?

Checkpoint 1.4: Busque en las bases de datos de vulnerabilidades fallos de seguridad de Windows 2000 referidas a Buffer Overflow. Indique el código CVE de una de ellas. ¿Hay un exploit para dicha vulnerabilidad?

7. Google Hawking (opcional)

Los buscadores son herramientas muy populares, que todos usamos y que todos necesitamos. Los motores de búsqueda son muy potentes y absorben toda la información que encuentran en su camino que no esté debidamente protegida.

Google es hoy por hoy el buscador más popular en uso, siendo sus técnicas de recolección de datos y algoritmos de clasificación muy avanzados, lo que proporciona resultados certeros en las búsquedas a poco que sepamos operar con sus múltiples funcionalidades. Google es, con toda

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

probabilidad, el buscador tecnológicamente más avanzado que existe. Esto facilita que dispongamos de mucha información en la red. Pero también posibilita que podamos hallar información sensible que no ha sido pertinentemente securizada.

Google nos ofrece un mecanismo de consultas avanzadas más allá del uso habitual que le damos. Google tiene comandos especiales, palabras a las que le siguen 2 puntos (:) cuyo significado se corresponde al comando. A continuación se muestra un listado de estos comandos especiales que podremos utilizar en nuestras búsquedas en google:

- **allintext:** Seguido de varias palabras, te da resultados de páginas en la que están todas las palabras en la página.
- **allintitle:** Seguido de varias palabras, te da resultados de páginas en la que están todas las palabras en el título.
- **allinurl:** Seguido de varias palabras, te da resultados de la búsqueda de todas esas palabras en la URL.
- **cache:** Seguido de una URL, te mostrará la página en caché.
- **define:** Seguido de una palabra, la busca en varios diccionarios online y te da la definición.
- **filetype:** Seguido de una extensión determinada, podemos restringir el tipo de documentos que queremos encontrar.
- **intext:** Sólo la primera palabra de las que le siguen, te da resultados de páginas en la que esté la palabra en la página.
- **intitle:** Sólo la primera palabra de las que le siguen, ha de estar en el título.
- **inurl:** Sólo la primera de las palabras que le siguen, ha de estar en la URL.
- **link:** Seguido de una URL, te encuentra todas aquellas páginas que enlazan con la URL dada.
- **site:** Seguido de un dominio, te da los resultados de la búsqueda sólo en ese dominio.
- Y muchos otros…

Google Hacking es aprovechar la información de que dispone Google para realizar búsquedas de información sobre los posibles objetivos de un ataque. Hagamos una demostración. Abra un navegador y vaya a la página de Google (http://www.google.com). Como texto de búsqueda escriba: `"phone * * *" "address *" "e-mail" intitle:"curriculum vitae"`. ¿Qué ha obtenido? Hay mucha información, un atacante, hacker/cracker o spammer, etc. obtendrá mucha y valiosa información.

Pruebe ahora con la siguiente búsqueda: `allintitle:"Outlook Web Access Logon"`. También puede ser interesante si sabemos que un producto determinado tiene alguna vulnerabilidad que explotar…

La Google Hacking Database, base de datos mantenida por Johnny Long en la web http://johnny.ihackstuff.com/, almacena cientos de "googledorks" y es actualizada continuamente. Contiene búsquedas Google para obtención de información y clasifica la base de datos de búsquedas en varias categorías:

- Vulnerabilidades
- Mensajes de error
- Archivos con contraseñas

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

- Portales de entrada
- Detección de servidor web
- Archivos sensibles
- Detección de dispositivos

Una técnica de descubrimiento es la de buscar subdominios de uno que estamos "investigando". Esto se realiza con el modificador site: Por ejemplo:

```
site:unavarra.es -www.unavarra.es
```

Algunos servicios o aplicaciones web, al instalarse, crean una página principal de prueba donde muestran información acerca de la instalación y en algunos casos acerca del servidor donde están instalados. Por ejemplo Apache muestra información en su página de Test sobre la versión de Apache instalada o PHP, cuando se instala, genera una página de test, phpinfo.php, que utiliza la función phpinfo() y que devuelve información sobre la versión, opciones de compilación, servidores donde está instalado, opciones de los módulos y del entorno del servidor. Esta información es en algunos casos información muy interesante para un atacante y muy sensible como para dejarla publicada a la vista de todo el mundo. Os sorprenderá comprobar que esta información se encuentra fácilmente en muchos servidores… Por ejemplo buscando:

```
allinurl:phpinfo.php
```

Investigue el dominio `ono.com` y busque subdominios. Consulte al menos dos o tres páginas de google ¿Qué nuevos servidores aparecen? ¿Qué direcciones IP tienen? ¿Ha encontrado nuevos servidores? ¿Qué consulta ha utilizado en Google para localizarlos?

Checkpoint opcional: Investigue en la Google Hacking Database sobre una búsqueda en Google que le parezca interesante a modo de descubrimiento de objetivos. Deberá explicar al profesor por qué la ha elegido y que información de interés obtiene.

8- 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).

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