Vulnerabilidades e Intrusiones

Redes de Comunicación – Unidad VIII

Universidad AMERICANA

Ing. Luis Müller

Contenido

Unidad VIII – vulnerabilidades e intrusiones

Conceptos básicos. Código malicioso. Vulnerabilidades de los sistemas. Conceptos de la intrusión. Fases de la intrusión. Ejemplos de aplicación.

Seguridad: Metodología de intrusión de red

El objetivo de esta unidad es explicar la metodología que generalmente utilizan los piratas para infiltrarse en un sistema informático. El propósito no es explicar cómo poner en riesgo un sistema sino ayudar a comprender cómo funciona el proceso para que pueda protegerse mejor. La mejor manera de proteger un sistema es usando el mismo enfoque que el pirata para identificar las vulnerabilidades del sistema.

Como tal, este material no proporciona información específica acerca de cómo sacar provecho de las vulnerabilidades, sino cómo detectarlas y corregirlas.

Metodología general

Un hacker que pretenda hackear un sistema informático, primero busca **fallas**, es decir *vulnerabilidades* que puedan afectar la seguridad del sistema en protocolos, sistemas operativos, aplicaciones e incluso a los empleados de una organización. Los términos **vulnerabilidad**, **infracción** y el más informal **carencia de seguridad** también se usan para referirse a las fallas de seguridad.

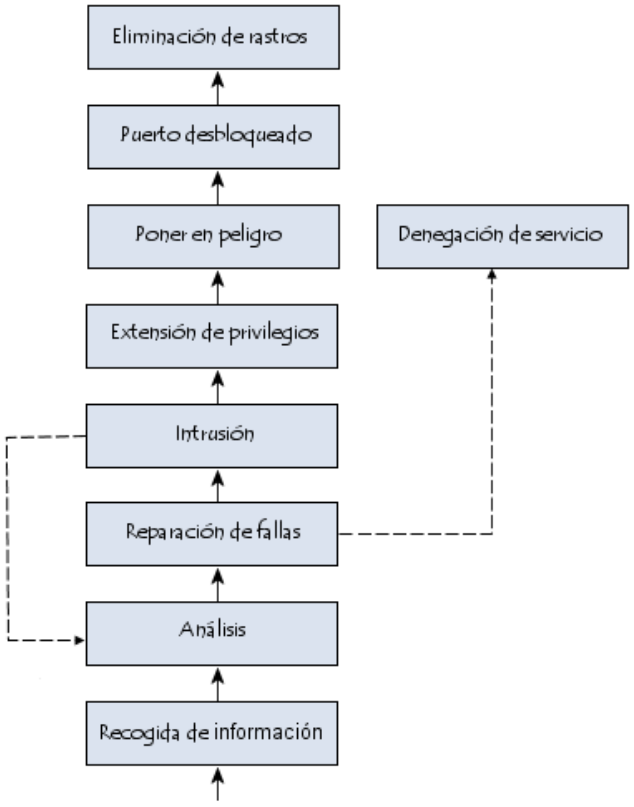
Para poder sacar provecho de un punto vulnerable (el término técnico para *aprovechar una falla*), el hacker primero debe recuperar una cantidad máxima de información acerca de la arquitectura de red y acerca de los sistemas operativos y aplicaciones que se ejecutan en esta red. La mayoría de los ataques son producto de *hackers inexpertos* que intentan usar los puntos vulnerables que encuentran en Internet, sin conocimiento del sistema ni de los riesgos relacionados.

Una vez que el hacker asigna el sistema, podrá aplicar estas formas de explotación de los puntos vulnerables a las versiones de las aplicaciones que ha catalogado. El acceso inicial a un equipo le permitirá expandir su acción para recuperar otra información y posiblemente elevar sus privilegios en el equipo.

Cuando se obtiene acceso de administrador (generalmente se usa el término acceso de *raíz*) decimos que el equipo está en peligro (o, más precisamente, que se ha producido un *peligro de raíz*) ya que los archivos del sistema se han modificado. En este punto, el hacker tiene todos los derechos del equipo.

Si el intruso es un pirata, al finalizar eliminará sus huellas para evitar sospechas por parte del administrador de la red en peligro y para retener el control sobre los equipos en peligro durante el mayor período de tiempo posible.

La siguiente estructura resume toda la metodología:



Recuperación de información del sistema

La información acerca de la dirección de red de destino, a la que generalmente se llama **huella digital**, debe obtenerse antes de realizar un ataque. Esto incluye recabar la máxima cantidad posible de información acerca de las infraestructuras de comunicación de red:

- Direcciones IP,
- Nombres de dominio,
- Protocolos de red,
- Servicios activados,
- Arquitectura del servidor,
- etc.

Consulta de las bases públicas

Al obtener la dirección IP pública de un equipo de red o simplemente el nombre de dominio de la organización, un pirata puede conocer potencialmente las direcciones de toda la red, es decir, el rango de las direcciones IP públicas que pertenecen a la organización de destino y su división en subredes. Para ello, todo lo que necesita es consultar las bases públicas que atribuyen las direcciones IP y los nombres de dominio.

Consulta de los motores de búsqueda

La consulta simple de los motores de búsqueda a veces posibilita recabar información acerca de la estructura de una compañía, los nombres de sus productos principales e incluso los nombres de algunos de los empleados.

Análisis de red

Cuando un pirata conoce la topología de una red, puede analizarla, es decir, usar un software como herramienta (llamado *analizador*) para determinar las direcciones IP activas en la red, los puertos abiertos que corresponden a los servicios accesibles y al sistema operativo utilizado por sus servidores.

Una de las herramientas de análisis de red más conocidas es Nmap, que muchos administradores reconocen como una herramienta esencial para la seguridad de las redes. Esta herramienta actúa mediante el envío de paquetes TCP y/o UDP a un grupo de equipos en una red (determinada por una dirección de red y una máscara) y su posterior análisis de las respuestas. Según la velocidad de los paquetes TCP recibidos, puede determinar el sistema operativo remoto para cada equipo analizado.

Existe otro tipo de analizador, llamado **asignador pasivo** (uno de los más conocidos es Siphon), que permite encontrar la topología de red del proceso físico a través del cual el asignador analiza los paquetes. A diferencia de los analizadores anteriores, esta herramienta no envía paquetes por la red y por lo tanto los sistemas de detección de intrusiones no pueden detectarla.

Además, algunas herramientas permiten recibir conexiones X (un servidor X es un servidor que administra las pantallas en los equipos tipo UNIX). Este sistema está diseñado para usar la pantalla de las estaciones presentes en la red para estudiar qué está publicado en las pantallas y posiblemente interceptar las claves ingresadas por los usuarios de equipos vulnerables.

Obtención del titular

Cuando finaliza el análisis de la red, el pirata necesita examinar el archivo de registro de las herramientas para averiguar las direcciones IP de los equipos conectados y los puertos abiertos en la red.

Los números de los puertos abiertos en los equipos pueden proporcionar información acerca del tipo de servicio abierto e invitarle a interrogar el servicio para obtener información adicional acerca de la versión del servidor en la información conocida con el nombre de "titular".

Para averiguar la versión de un servidor HTTP, un pirata puede comunicarse con el servidor web mediante Telnet en el puerto 80:

```
telnet es.kioskea.net 80
```

y luego solicitar la página de inicio:

```
GET / HTTP/1.0
```

El servidor responde con el siguiente encabezado:

HTTP/1.1 200 OK Date: Thu, 21 Mar 2002 18:22:57 GMT Server: Apache/1.3.20 (Unix) Debian/GNU

Ahora se conoce el sistema operativo, el servidor y su versión.

Ingeniería social

La ingeniería social consiste en manipular personas, es decir, aprovecharse de la inocencia y bondad de los usuarios de redes para obtener información acerca de la red. Este proceso consiste en contactar un usuario de una red, normalmente haciéndose pasar por otra persona, para obtener información acerca del sistema informático y probablemente para obtener directamente una contraseña. En forma similar, se puede crear una falla de seguridad en el sistema remoto al enviar un troyano a alguno de los usuarios de la red. Lo único que se necesita es que uno de los usuarios abra el adjunto para que el atacante externo obtenga el acceso a la red interna.

Éste es el motivo por el que las políticas de seguridad deberían ser más exhaustivas e incorporar los factores humanos (por ejemplo, concienciar a los usuarios acerca de los problemas de seguridad), ya que el nivel de seguridad de un sistema se caracteriza por su eslabón más débil.

Detección de fallas

Después de realizar un inventario del software y probablemente del hardware presentes, el hacker debe determinar si existen fallas o no.

Existen escáneres de vulnerabilidad disponibles que les permiten a los administradores someter a las redes a pruebas de intrusión para averiguar si ciertas aplicaciones tienen fallas de seguridad. Los dos principales son:

- Nessus
- SAINT

También se les aconseja a los administradores de red que visiten regularmente las página Web que mantienen actualizadas las bases de datos de vulnerabilidades:

SecurityFocus/ Vulnerabilidades

Además, algunas asociaciones, en particular los CERT (por la sigla en inglés de *Equipos de Respuesta ante Emergencias Informáticas*) están a cargo de la explotación de las vulnerabilidades y de recabar información sobre los problemas de seguridad.

Intrusión

Cuando un pirata ha asignado los recursos y equipos presentes en una red, está listo para preparar su intrusión.

Para poder infiltrarse en la red, el pirata debe acceder a las cuentas válidas en los equipos que ha catalogado. Para hacerlo, los piratas usan varios métodos:

- La ingeniería social, es decir, el contacto directo con ciertos usuarios de red (por correo electrónico o teléfono) para sacarles información acerca de su identificación de usuario o contraseña. Esto se lleva a cabo normalmente haciéndose pasar por el administrador de red.
- La consulta del directorio o de los servicios de mensajería o de uso compartido de archivos permite encontrar nombres de usuario válidos.
- Irrumpir por la fuerza, que implica varios intentos automáticos de ingreso de contraseñas en una lista de cuentas (por ejemplo, la identificación seguida por un número o la contraseña *password* o *passwd*, etc.).

Aumento de privilegios

Cuando un pirata obtiene uno o más accesos a la red al trabajar en una o más cuentas con niveles de protección bajos, intentará aumentar sus privilegios obteniendo un acceso a la *raíz*. Esto se denomina **elevación de privilegios**.

En cuanto obtiene el acceso a la *raíz* de un equipo, el atacante puede examinar la red para buscar información adicional.

Después podrá instalar un rastreador de puertos, es decir, un software capaz de supervisar (también se usa el término *rastrear*) el tráfico de red que proviene o que está dirigido a los equipos ubicados en el mismo proceso. Gracias a esta técnica, el pirata tiene la esperanza de recuperar los pares *ID/contraseña* que le brindan acceso a las cuentas con privilegios extendidos a otros equipos de red (por ejemplo, el acceso a una cuenta de administrador) para poder controlar a la mayoría en la red.

Los servidores NIS presentes en una red también son destinos preferidos de los piratas ya que abundan en información sobre la red y sus usuarios.

En peligro…

Gracias a los pasos anteriores, el pirata pudo diseñar un completo mapa de la red, de sus equipos y sus fallas, y tiene acceso a la *raíz* de al menos uno de ellos. Ahora puede extender aun más allá su campo de acción al aprovecharse de las relaciones de confianza que existen entre los equipos.

Esta técnica de suplantación de identidad les permite a los piratas penetrar en redes privilegiadas a las que el equipo en peligro tiene acceso.

Puerta trasera

Cuando un pirata logra infiltrarse en la red de una empresa y pone en peligro un equipo, es posible que desee volver. Para hacerlo, instalará una aplicación para crear artificialmente una vulnerabilidad de seguridad. Esto se llama **puerta trasera** y algunas veces también se usa el término *puerta trampa*.

Cubrir las huellas

Una vez que el intruso ha obtenido suficiente control de la red, debe borrar las evidencias de su visita mediante la eliminación de los archivos que creó y los archivos de registro de los equipos a los que accedió, es decir, debe eliminar todas las huellas de actividad relacionadas con sus acciones.

También existen programas llamados "**rootkits**" que permiten remplazar las herramientas de administración del sistema con versiones modificadas para ocultar la presencia del pirata en el sistema. Si el administrador se conecta al mismo tiempo que el pirata, es posible que se dé cuenta de los servicios que el pirata ha ejecutado o que simplemente vea que hay otra persona conectada en simultáneo. El objetivo de un rootkit es, por lo tanto, engañar al administrador al ocultar la realidad.

Conclusión

Todos los administradores de red conectados a Internet son responsables de la seguridad de la red y deberían probar sus fallas.

Éste es el motivo por el que el administrador debe mantenerse informado acerca de las vulnerabilidades en los programas que usa poniéndose "en el lugar del pirata" para intentar infiltrarse en su propio sistema y operar en forma continua en un contexto de paranoia.

Cuando las propias habilidades de la empresa no son las adecuadas para llevar a cabo esta operación, una compañía especializada puede realizar una auditoría de la seguridad informática.

Códigos Maliciosos: Troyanos y Gusanos

Troyanos

Un troyano era en sus comienzos, un programa que camuflado dentro de otro (de ahí el nombre, asociado al caballo que los griegos utilizaron para ganar su guerra contra Troya) para conseguir que un usuario de un ordenador lo ejecutara pensando que en realidad estaba ejecutando un programa lícito.

Estos troyanos, tenían multitud de funciones, algunas destructivas y otras no, y se diferenciaban de los virus comunes en su incapacidad para autoreproducirse, es decir, que no podían crear copias de si mismos para infectar otros ordenadores y dependía de la acción del usuario del ordenador para realizar su fín.

Hablamos en pasado porque, aunque la definición de troyanos sigue siendo válida, los últimos años han visto surgir un gran número de troyanos con unas características especiales, que se han generalizado ampliando su definición al término troyano.

Estos nuevos troyanos, responden más concretamente a la definición de Backdoor o Puerta trasera, es decir, que abren un canal de comunicación en el ordenador infectado que permite que otro ordenador se conecte a él para realizar acciones sin que el usuario legítimo de este ordenador sea consciente de ello.

Estos troyanos pueden realizar tareas "simples", como robar claves, buscando un cierto formato en la información de los usuarios (por ejemplo, las tarjetas VISA se identifican con 4 grupos de 4 números y un grupo más, la fecha de caducidad, que consta de 2 grupos de 2 números separados por una barra) o llegan incluso a permitir al "atacante" que tome control del ordenador, abriendo y cerrando programas, creando y borrando ficheros, etc

Con el advenimiento de la banda ancha (cable o ADSL en nuestro pais) y la posibilidad de mantenerse conectado a Internet durante 24 horas al día, los Troyanos se han puesto de moda, ya que permiten a un atacante, tomar control de un ordenador víctima a través de Internet y manejarlo a su antojo sin ningún tipo de problema. Incluso se pueden crear redes de ordenadores controlados por un solo atacante que puede utilizarlo para actividades ilícitas (por ejemplo atacar un sitio Web y "tumbar" la página).

Gusanos

Otro tipo de código malicioso son los gusanos. Primos hermanos de los virus, su principal misión es reproducirse y extenderse al mayor número de ordenadores posibles.

Internet y el correo electrónico han supuesto el verdadero auge de este tipo de código malicioso, que pueden infectar miles de ordenadores en cuestión de horas.

Posiblemente menos peligrosos para los usuarios domesticos que otros, su mayor poder es en el ataque a grandes sistemas de empresas o los ordenadores que sostienen Internet. Su poder de multiplicación es capaz de colapsar grandes ordenadores rapidamente y "tumbar" los servicios que den (servidores de correo electrónico, de páginas web...).

Su mecanismo de distribución suele ser en la mayoría de los casos muy simple. Camuflados en un mensaje aparentemente inocente, llegan a nuestro correo electrónico. Una vez ejecutado leen nuestra lista de contactos (libreta de direcciones o Address Book) y se reenvían de forma automática a todas las direcciones que contengan. Nuestros contactos recibirán un correo, aparentemente enviado por nosotros, y por tanto lo abrirán sin sospechar nada y vuelta a empezar.

Este tipo de código malicioso utiliza en muchas ocasiones lo que denominamos Ingeniería social, es decir, intenta aparecer atractivo para nosotros, a fín que no sospechemos y lo ejecutemos rapidamente.

Promesas de fotografías, juegos, listados de páginas con contenido erótico... son algunos de los trucos que han usado los creadores de estos engendros para llamar nuestra atención.

LOS DEFENSORES: ANTIVIRUS Y FIREWALLS PERSONALES

Estas y otras razones han hermanado a los antivirus y los firewalls personales.

Pero empecemos por el principio, ¿Qué es un Antivirus?

Un Antivirus es un programa que intenta proteger un ordenador o red de ordenadores de todo tipo de código malicioso que pudiera llegar a este equipo.

Existen antivirus especializados en diferentes entornos, correo, ficheros...

Básicamente un antivirus funciona de una forma muy simple, revisa todo los ficheros (o correo en su caso) que llega al equipo y bloquea todo aquello que cree que puede contener un código malicioso.

¿Cómo sabe que es un código malicioso?, muy sencillo, básicamente existen 2 métodos complementarios. El más habitual es comparar trozos de ese código con una base de datos de firmas que contiene el antivirus y que es actualizada constantemente.

Si coinciden, es que es un código malicioso y no se deja pasar. La otra técnica consiste en ver cual es el comportamiento de ese fichero, buscando acciones extrañas (como formatear el disco duro, infectar ficheros...). Este último método sólo puede dar cierta información de que hay algo raro en el fichero, pero no que virus es.

Los Firewalls personales son un complemento perfecto de los antivirus clásicos, por eso los mejores fabricantes de antivirus los incluyen dentro de sus últimas versiones.

Para entender como funcionan los Firewalls personales, debemos repasar un poco como funcionan las comunicaciones entre ordenadores. De forma simple, podríamos explicarlo como el servicio de correos. Cuando alguien quiere enviar una carta, Correos se encarga de dar el servicio de envío a otro lugar. Es decir, es el "servidor" (el que da el servicio). Cuando se envía una carta esta debe ir en un sobre y con sello, este sobre sería el que posibilita la comunicación por parte del cliente. El sobre es depositado en el buzón o la oficina de correos.

Siguiendo la analogía, el cliente (usted), que es el ordenador que pide el servicio, se comunica con el servidor (correos), que es el ordenador que da el servicio. Para establecer la comunicación utiliza un puerto (el sobre y el sello) y se conecta a otro puerto del servidor (el buzón u oficina de correos).

Lo que hace un Firewall personal es bloquear esa comunicación, cuando se sale de los cauces normales establecidos por el usuario. Es decir, si usted se conecta a una página web con su navegador, esto es una comunicación normal y permitida, por lo que el Firewall lo deja pasar (no bloquea el puerto de esa comunicación), sin embargo si es un troyano el que intenta comunicarse con el ordenador atacante, a fín de tomar control de ese ordenador, intenta comunicarse por un puerto no permitido y el Firewall lo bloquea. Sería como quitar el buzón o cerrar la oficina de correos.