Criptografía y seguridad
Intrusión y detección de intrusos

Montoya Montes Pedro
Universidad Nacional Autónoma de Mexico

November 20, 2019

Contents

PAGINA INTENCIONALMENTE EN BLANCO

1 Intrusión

Primeramente vamos a definir que una intrusión es el acceso de forma ilicita a un sistema.
Existen dos tipos de intrusión:

1. Directa: Es aquella en la que se tiene acceso directo al equipo al que se quiere tener acceso.

2. Indirecta: Es la que mediante una red, ya sea pública o privada, se tiene acceso a un equipo.

2 Vulnerabilidad

Como define Toni Puig, una vulnerabilidad "es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre un activo". [1]
La podemos dividir en tres grupos:

- Vulnerabilidad intrínseca, es aquella que sólo depende del activo y de la amenaza en sí.

- Vulnerabilidad efectiva, es la resultante luego de que se aplican las medidas correspondientes.

- Vulnerabilidad residual, es la resultante luego de que se aplican las medidas complementarias.

Al mismo tiempo existen tres tipos de intrusos.[2]

- Usuario fraudulento: Hace referencia a un usuario que accede de manera ilegal a recursos de la organización o que, teniendo los permisos, hace uso indebido de la información disponible.

- Suplantador: Es una persona que no tiene nada que ver con los accesos legales en la organización pero que logra llegar hasta el nivel de tomar la identidad de un usuario legitimo para acceder y realizar el daño.

- Usuario clandestino: Es una persona que puede tomar el control de auditoria del sistema de la organización.

[1] Toni Puig, "Gestión de riesgos de los sistemas de información" en http://www.mailxmail.com/curso-gestion-riesgos-sistemas-informacion/identificacion-vulnerabilidades-impactos, 12/02/201

[2] https://www.solvetic.com/page/recopilaciones/s/profesionales/tipos-de-ataques-informaticos-e-intrusos-y-como-detectarlos

3 Ataques

Existen varios tipos de ataques que ayudan a detectar distintas caracteristicas de la victima y así poder efectuar un ataque de mejor manera, a destacar serian los siguientes:

3.1 Barrido de puertos

Esta técnica nos es útil para saber la situación de cierto puerto, es decir, si se encuentra abierto, cerrado o tras un firewall.
Existen los siguientes tipos de barrido de puertos:

3.1.1 Escaneo de puertos TCP

Cada vez que se establece una conexión TCP (Transmission Control Protocol), se sigue una negociación conocida como Three-way-handshake, que consiste en:
La máquina de origen envía un paquete con bandera SYN activa.
La máquina destino responde con una bandera SYN/ACK.
La máquina origen envía un paquete en la bandera ACK.
Una vez finalizado, la conexión se ha completado entre la máquina origen y destino.
El escáneo de puertos TCP envía a la victima varios paquetes SYN, y dependiendo la respuesta puede intepretar los siguiente:

- Si la respuesta es un SYN/ACK, entonces el puerto está abierto.
- Si la respuesta es un paquete RST, significará que el puerto está cerrado.
- Si la respuesta es un paquete ICMP (Internet Control Message Protocol) como puerto inalcanzable, será porque dicho puerto está protegido por un firewall.

3.1.2 Escaneo de puertos UDP

A pesar de que el protocolo UDP (User Datagram Protocol) no está orientado a conexiones, si se envia un paquete a dicho puerto y se encuentra cerrado, se recibirá un mensaje de puerto inalcanzable, si embargo, si no se obtiene respuesta alguna, se difiere que está abierto, aunque si dicho puerto está protegido por un firewall la respuesta obtenida no será concisa.

3.2 Identificación de firewalls

Se podría definir a un firewall como un dispositivo informático, ya sea software ohardware que protege a una red privada al definir un perímetro de

seguridad, y definírsele reglas de filtrado de paquetes. La función principal del firewall es la de examinar paquetes en busca de coincidencias con las reglas que se le han fijado y dependiendo de ellas, permitirles o negarles el acceso. Además, los firewalls pueden también generar alarmas y crear listas negras .[3] Existen tres tipos:

3.2.1 Firewall de filtrado por paquetes

Trabaja en la capa tres del modelo OSI, analizando el encabezado del paquete de procedencia y destino, con estos datos se determina si se permine o niega el paso al paquete.

3.2.2 Firewall de filtrado por estado

Este permite guardar un registro de las conexiones existentes. Además, es capaz de trabajar con los protocolos tales como IP, TCP, UDP, ICMP, FTP e IRC. No trabajan filtrando paquetes individuales, sino sesiones enteras, permitiendo una optimización del trabajo de filtrado. [4]

3.2.3 Firewall de filtrado por contenido

También conocido como de filtrado por aplicación, analiza la trama a nivel de la capa de aplicación del modelo OSI, así, controla además de los puertos y sesiones, los protocolos que se utilizan para la comunicación evitando que se puedan suplantar servicios.

3.3 Ientificación del sistema operativo

Para está técnica, que se utiliza para saber el sistema operativo donde se corre el sistema a atacar, y se tienen dos variantes activa y pásiva.
La primera se dedica a enviar y recibir paquetes para posteriormente analizar y saber el sistema operativo.
Mientras que la segunda, se dedica a recabar paquetes enviados por el usuario.

4 Explotación y obtención de acceso a sistemas y redes

Existen distintas formas con las que un atacante obtiene acceso al sistema de su víctima para así obtener privilegios de instalación, ejecución de software, modificación, creación de archivos, de las que podemos destaca:

[3] http://tindes.com/jj/index.php?option=com_content&view=article&id=41:seguridad-red&catid=1:actualidad&Itemid=27&0de28b3435550b272401162583c2c73f=tqyhgghphlnuox

[4] http://www.alegsa.com.ar/Dic/seguridad/$%$50informatica.php

4.1 Robo de identidad

Está técnica usa phising para obtener datos de forma directa del usuario a traves de spam, páginas y mensajes engañosos, con el fin de que el usuario entregue sin saber datos que puedan y serán usados para atacarle.

4.2 Engaño de firewalls e IDS's

La manera más sencilla para engañar un firewall es la creación de "túneles", que consiste en encapsular un protocolo de red dentro de otro, con esto se pretende superar los parámetros del firewall.

4.3 Vulnerabilidades de software

Una vulnerabilidad de software se puede ver como un fallo en algún programa o sistema que puede ser utilizado por un virus o por un intruso, quien tendrá acceso al sistema.
Existen dos tipos:

- Buffer overflows: Esto se da gracias a algunos lenguajes de bajo nivel que permiten una mezcla entre datos introducidos por el usuario y la información del control de flujo.
- Heap Bufferoverflow: Es un caso especial del primero, donde se utiliza el heap, y su facilidad para ser sore-escrito.
- Vulnerabilidad de formato de cadena: Se da cuando no se válida información enviada por el usuario mediante alguna entrada.
- SQL injection: Es la posibilidad de inyectar sentencias SQL (Structured Query Languaje) arbitrarias en, por ejemplo, formularios estándar publicados en un sitio web.

4.4 Ataques a contraseñas

Este tipo de ataque se centra en obtener alguna contraseña para obtener acceso a mutlitud de servicios.

4.5 Ataques a redes inalámbricas

4.6 Detección de intrusos

Como hemos visto, los ataques son algo que se puede dar de multiples formas, y con ello aparte de protocolos, firewalls, precacusión, se requieren metodos para detectar si es que el equipo tiene un intruso.
Para ello se tiene dos tipos principales de auditorias:

4.6.1 Registros de auditoría específicos para detección

Podemos implementar dichos registros para que sólo nos muestre la información requerida por el sistema de detección de intrusión.

4.6.2 Registros nativos de auditoría

Es la herramienta que viene por defecto en los sistemas operativos y almacena toda la actividad de los usuarios, por ejemplo, el visor de eventos de Microsoft Windows.

4.7 Detección de anomalías

Gracias a ciertas anomalías en el perfil de un usuario de un sistema podemos detectar alguna intrusión:

- Contador: Es un valor que puede incrementarse mas no disminuirse hasta que sea iniciado por alguna acción
- Calibre: Es un número que puede aumentar o disminuir, y mide el valor actual de una entidad
- Intervalo de tiempo: Hace referencia al periodo de tiempo entre dos acontecimientos
- Uso de recursos: Implica la cantidad de recursos que se consumen en un determinado tiempo

Para una eficiente detección se recomienda una combinación entre análisis de comportamiento y auditorias.