**FASES DE UN ATAQUE MODELO**

* Reconocimiento
* Acceso remoto
* Escalada de privilegios
* Objetivo concreto del ataque
* Mantenimiento del acceso
* Borrado de huellas

**1. RECONOCIMIENTO**

Sus objetivos son:

1. Analizar la red en busca de un objetivo valioso.
2. Descubrir los posibles puntos de ataque.
3. Planificar el ataque.

Para ello utiliza una serie de técnicas de reconocimiento entre las que están:

**Footprinting**

Consiste en averiguar todo lo posible sobre la posible red objetivo y su seguridad. Hay diferentes técnicas en función del objetivo.

* Navegar por la Web de la entidad objetivo.
* Consultas en buscadores y bases de datos.
* Bases de datos WHOIS: asocian nombres de dominios o IPs a entidades.
* Consultas DNS: asocian nombres de dominio a direcciones IP.
* Traceroute: muestra la ruta que sigue un paquete hasta su destino.

Para prevenir esto se necesita conocer y controlar la información que se expone en webs y bases de datos de acceso público, configurar adecuadamente nuestros servidores DNS y configurar un control de acceso adecuado en los firewalls.

**Scanning**

Realiza un escaneo de puertos y de pings para obtener información de las máquinas y servicios activos en ellas.

Para prevenirlo, hay que permitir el paso a la red exclusivamente a los paquetes necesarios y tener mecanismos de detección y de reacción.

**Enumeración**

Una vez detectados qué servicios están activos en las máquinas, se obtiene información sobre ellos como el nombre de usuario o la versión del software del servicio para encontrar posibles vulnerabilidades.

Para evitarlo, hay que deshabilitar los servicios innecesarios, poner especial atención en la configuración de seguridad de los servicios que ofrecen información de la red y bloquear conexiones a determinados servicios a nivel de firewall.

**Vulnerability Mapping**

Asocia la información obtenida del sistema objetivo con potenciales vulnerabilidades. Busca los atributos del sistema en bases de datos de vulnerabilidades, utiliza *exploits* disponibles en la red y los lanza contra la máquina objetivo y herramientas automatizadas de búsqueda de vulnerabilidades.

**2. ACCESO REMOTO**

En esta fase, conseguimos tener acceso a la máquina y ejecutar órdenes *shell*. Para acceder remotamente a un sistema hay que hacerlo a través de servicios a la escucha, usuarios que puedan facilitarnos el acceso o interfaces en modo promiscuo mediante ataques de fuerza bruta, ataques basados en datos y errores de validación de entrada.

**3. ESCALADA DE PRIVILEGIOS**

Una vez obtenido acceso remoto, se empieza careciendo de privilegios (nobody) con lo que hay que explotar vulnerabilidades lovales para obtener los privilegios necesarios para el objetivo del ataque (ya sea ser root o algún nivel intermedio). Esto se puede conseguir por ejemplo, mediante password cracking del fichero en donde se almacenan las contraseñas, por una maña gestión de los permisos de acceso a ficheros o ejecutando ficheros SUID.

Esto se puede detectar con los sistemas de detección de intrusiones y prevenir mediante el control de los permisos de acceso a ficheros y los ficheros SUID, teniendo el software y sistema operativo actualizado y con todos los parches de seguridad y no no permitir la ejecución de *stack* o *heap* (a nivel de SO).

**5. OBJETIVO CONCRETO DEL ATAQUE**

**6. MANTENIMIENTO DEL ACCESO**

**7. BORRADO DE HUELLAS**

Depende de cuál haya sido nuestro ataque, así deberá de ser la forma de borrar nuestras huellas.

La más drástica es la destrucción del sistema deshabilitando el login y borrar los ficheros y directorios más importantes del sistema. Esto debe de hacerse cuando la evidencia es imposible de ocultar.

Si se realizó un ataque web, bastaría con capturar y borrar los Access log del servidor, por ejemplo, Apache.

Lo más común es eliminar el historial Bash antes de salir de la víctima, eliminar todo rastro de nuestros exploits, tener cuidado con los cambios en el sistema que se realizaron y devolverlos a su estado original, eliminar las cuentas creadas y eliminar los backdoors cuando no los utilicemos ya que con el tiempo lo descubrirán. Durante todo el proceso hay que tener especial cuidado con los usuarios logados en el sistema puesto que pueden llegar a darse cuenta de los cambios y detectarnos.

Por último, una lista de ficheros a tener especialmente en cuenta tomados de la web [1]:

**- utmp:** Guarda un registro (log) de los usuarios que están utilizando el sistema mientras estan conectados al sistema. Directorios: */var/adm/utmp* y */etc/utmp*

**- wtmp:**Guarda un log cada vez que un usuario se introduce en el sistema o sale del sistema.

**- lastlog:**Guarda un log del momento exacto en que un usuario entro por última vez.

**- acct o pacct:** Registra todos los comandos ejecutados por cada usuario (aunque no registra los argumentos con que dichos comandos fueron ejecutados).

Troyanos: versiones modificadas de ficheros binarios del sistema. El mecanismo de detección es realizar controles de integridad.

Sniffers: capturan paquetes de la red. Pueden obtener contraseñas y otra información valiosa de la víctima y de otras máquinas. El mecanismo de prevención es la criptografía y el de detección IDS.

Keyloggers: capturan pulsaciones de teclado.

Rootkits: incluyen varias de las herramientas anteriores. Suelen incluir también mecanismos que evitan la detección.

Kernel Rootkits: modifican directamente el núcleo del sistema, permiten ocultar ficheros, procesos, conexiones de red. Casi imposible de detectar.

Limpieza de logs: borrado de huellas, localización de logs. Puede requerir empleo de utilidades específicas. Elimina la historia de órdenes de la shell.

Mecanismos de seguridad: una vez comprometido el sistema es muy difícil valorar el alcance de la intrusión. Para prevenir se utiliza IDS. Se almacenan los logs en soportes no modificables. Y se utilizan estrategias de respuesta ante incidentes (kits de recogida de evidencias).

Bibliografia:

[1] <https://www.blackploit.com/2011/08/eliminar-rastro-y-huellas-post.html>

Curso de ciberseguridad de <https://www.edx.org/es>