Práctica de Seguridad en Redes

Juan Boubeta Puig
y Antonio García Domínguez

Seguridad y Competencias Profesionales

Departamento de Ingenieria Informatica
Universidad de Cadiz

Curso 2012-2013

1. Descripción general

En esta práctica (4 horas de duración) los estudiantes llevarán a cabo ataques a dos servidores web, que se encontrarán instalados en una red de área local.

2. Configuración de los equipos de la red local

Los estudiantes formarán grupos de 4 o 5 personas. Cada grupo utilizará 2 ordenadores con el software que se detalla a continuación. Para ello, se seguirán los siguientes pasos:

1. Descargar el software de virtualización *Oracle VM VirtualBox* de `https://www.virtualbox.org/wiki/Downloads` (en la sección *VirtualBox platform packages*).

2. Instalar *Oracle VM VirtualBox*.

3. Descargar una máquina virtual para *Oracle VM VirtualBox* proporcionada por OWASP (`https://www.owasp.org/index.php/Category:OWASP_Live_CD_Project`), que ya trae instalado el software que se utilizará para realizar los ataques a los servidores. Es posible descargarla directamente de `http://appseclive.org/apt/downloads/owasp-wte-Feb-2011.vdi.rar`.

4. Descomprimir la máquina virtual (*owasp-wte-Feb-2011.vdi.rar*). Téngase en cuenta que la descompresión da problemas en algunas versiones de Windows; se recomienda realizarla desde una distribución GNU/Linux Ubuntu.

5. Crear la máquina virtual en *Oracle VM VirtualBox*. Los pasos a seguir son: Abrir *Oracle VM VirtualBox* → Nueva → Siguiente → Nombre: "OWASP" → Sistema Operativo: "Linux" → Versión: "Others" → Memoria: 512 MiB o 1024 MiB (dependiendo de la memoria total del ordenador) → Usar un disco duro existente (seleccionar la ruta donde se encuentra el fichero descomprimido) → Crear.

6. Configurar el adaptador de red de la máquina virtual. Los pasos a seguir son: Máquina → Configuración → Red → Adaptador 1 → Conectado a: "Adaptador puente".

7. Comprobar que arranca la máquina virtual. Para ello, seleccionar la máquina virtual creada y hacer clic en el botón "Iniciar".

8. Asignar una dirección IP estática (proporcionada por el profesorado) a la máquina arrancada.

3. Herramientas a emplear

En esta práctica se utilizarán las siguientes herramientas (ya instaladas en la máquina virtual):

- *nmap* es una herramienta que permite explorar los nodos de una red, identificando las características de las máquinas y los servicios disponibles.

  Es muy popular en el ámbito de la seguridad informática, y se halla bajo activo desarrollo: la versión 5.00 se publicó en julio de 2009. Implementa muchas técnicas avanzadas, y es particularmente interesante su capacidad de identificar remotamente los sistemas operativos y versiones de los servidores que ofrecen cada servicio, utilizando un amplio arsenal de técnicas heurísticas.

  Una herramienta como *nmap* tiene muchos usos para un administrador de la seguridad de un sistema informático:

  - Mantener una imagen actualizada de todos los nodos disponibles en la red y las rutas existentes entre ellos. Además de la ayuda que supone para el inventariado de las máquinas, puede ser útil para localizar puntos de acceso inalámbricos conectados de forma no autorizada por el personal.
  - Evaluar la seguridad de las máquinas críticas en la red, evitando ofrecer al exterior más servicios de lo estrictamente necesario. Todo servicio aporta una funcionalidad que puede incluir vulnerabilidades aprovechables por un atacante.
  - Localizar servidores con versiones antiguas con vulnerabilidades críticas conocidas, que requieran una puesta a punto.

- Verificar la efectividad de las reglas de nuestros cortafuegos, sistemas IDS (como *snort*) y sistemas IPS. Por ejemplo, es posible lanzar *nmap* desde una red externa al perímetro de seguridad del cortafuegos y verificar si es posible rodearlo de alguna forma, o si no se ha cerrado el acceso a los puertos necesarios.

- *wireshark*: se trata de uno de los analizadores de protocolos más avanzados existentes. Dispone de una interfaz gráfica desde la cual un usuario puede inspeccionar todo el tráfico que pasa por las redes locales en que se encuentran sus interfaces de red. Para ello, normalmente requieren permisos de administrador (**root** en sistemas basados en UNIX), ya que han de cambiar las interfaces a «modo promiscuo».

  wireshark puede extraer los campos de los distintos PDU de cada paquete desde el nivel de aplicación OSI (HTTP o FTP, por ejemplo) hasta el nivel de enlace OSI (trama Ethernet, entre otras). Resulta muy útil como herramienta de depuración, pero también puede usarse para otros fines.

  Si lo que se desea es únicamente realizar un volcado del tráfico, pueden usarse programas más sencillos desde la línea de órdenes, como *tcpdump*.

Otra de las herramientas que podría utilizarse es *snort*, pero debido a la limitación de tiempo para desarrollar la práctica su uso será opcional:

- *snort* es el referente actual en sistemas de detección de intrusiones (*Intrusion Detection Systems* o IDS). Monitoriza el tráfico de la red (cambiando la interfaz también a «modo promiscuo») y aplica una serie de reglas para determinar si se está llevando a cabo algún ataque (como, por ejemplo, un escaneo de puertos con *nmap*).

  Muchas veces simplemente se registran estos ataques a un registro de auditoría para posterior referencia: sirven como evidencia de un ataque y también para evaluar la seguridad real de la red.

  En algunos casos, se da un paso más allá y se integra el IDS con un Sistema de Prevención de Intrusiones (*Intrusiones Prevention Systems* o IPS), que modifica las reglas de los cortafuegos en función de los ataques detectados.

4. Guión de la práctica

A nivel general, en esta práctica se comprobará la forma en que un atacante puede extraer información valiosa de una red sin más conocimientos previos que la existencia de dos servidores web (uno de ellos con una zona privada). De partida se desconoce la IP y el puerto en el que se halla cada servidor.

Se han hecho una serie de suposiciones para simplificar la práctica y hacerla factible en el tiempo de que se dispone:

- Los atacantes tienen una conexión a la red local donde se encuentran las máquinas atacadas. Normalmente tendrían que pasar antes por varios dispositivos de red y posiblemente rodear algún que otro cortafuegos.

- Las propias máquinas atacadas no disponen de cortafuegos. La mayoría de cortafuegos ralentizan el escaneo de puertos, ya que no responden a los mensajes enviados a puertos cerrados, y obligan a *nmap* a esperar. De todos modos, esto es rodeable modificando los tiempos de espera y los métodos de escaneo utilizados.
- En una de las máquinas se emplea una versión antigua y con conocidas vulnerabilidades críticas de un servidor web. En la otra máquina se encuentra instalado de forma insegura un servidor web y un sistema de gestión de base de datos.

Los miembros de cada grupo se distribuirán los siguientes roles:

- Dirigir el ataque activo sobre los dos servidores web, mediante la interfaz gráfica *zenmap* para la herramienta *nmap*.
- Describir la forma en que *nmap* averigua la versión usada del servidor web Apache y observar lo que van haciendo el resto de usuarios.
- Inspeccionar todo el tráfico que pasa por la red local en que se encuentran sus interfaces de red, mediante la herramienta *wireshark*.
- Opcionalmente, detectar los ataques de los demás grupos mediante *snort*, preferiblemente en una máquina distinta a la que ejecuta *nmap*.

Se entregará un informe por grupo con una descripción general de los resultados obtenidos en estos roles a través del Campus Virtual de la asignatura. Se valorará el contenido, la ortografía, el formato y las ilustraciones.

5. Pasos del ataque activo

Los pasos generales a seguir para realizar el ataque activo son:

1. Listar las máquinas de la red. Podríamos enviar peticiones de eco ICMP a todas las direcciones IP del rango de direcciones de la red, pero como estamos conectados a la LAN, puede emplearse un ping ARP, que es mucho más eficiente y difícil de detectar.
2. Obtener algo más de información de las máquinas de la red: sistemas operativos y puertos abiertos. Ello debería ir dando ya más pistas de qué máquinas pueden ser las que alojen el servidor web.
3. Realizar escaneos a fondo de los candidatos a alojar el servidor web, identificando el puerto bajo el que se halla, el software usado y la versión empleada, si es posible.
4. Acceder a los dos servidores, para comprobar qué clase de información alojan.

5. Si la información deseada no se encuentra disponible directamente, por hallarse protegida con diversos mecanismos de seguridad, aprovechar alguna de las vulnerabilidades conocidas para rodearla. Para ello, pueden usarse bases de datos públicas oficiales (como la CVE del MITRE, entre otras), bases de datos no oficiales, la guía de realización de pruebas de OWASP (`https://www.owasp.org/index.php/OWASP_Testing_Guide_v3_Table_of_Contents`) o la información publicada por los propios desarrolladores.