Módulo 5.1

Redes y Seguridad
Gr. Ing. Informática
J.L. Vázquez Poletti

Objetivo

En este módulo aprenderemos a manejar una solución de detección de vulnerabilidades que nos ofrecerá información muy interesante de la máquina objetivo. Además, trabajaremos su integración en una herramienta mayor, piedra imprescindible en cualquier auditoría de seguridad seria.

Punto de partida

La multinacional EUROCORP está mejorando la versión 6 de su chip DART que irá implantada de forma exclusiva en sus agentes. Dicha mejora permite a su portador evaluar los objetivos a los que se tiene que enfrentar de una forma sistemática.

Se ha ubicado un objetivo en la red de EUROCORP para probar esta nueva funcionalidad. Por motivos de seguridad, el Consejo de Administración de la multinacional no autoriza la vulneración del objetivo durante este módulo.

- El agente (**RyS-Backtrack**) tendrá la IP 192.168.1.2.
- El objetivo de pruebas (**RyS-Víctima**) tendrá la IP 192.168.1.3.

Escaneo con Zenmap

Zenmap es una interfaz gráfica para **nmap** que permite acceder a todo su potencial de forma sencilla (incluyendo la enumeración de servicios) y mostrar los resultados de una forma categorizada.

- Arrancar **zenmap**.
- Indicar el objetivo que se quiere escanear con la opción de escaneo intenso.

¿Cuántos puertos hay abiertos?
¿En cuántos puertos está escuchando un servidor FTP? ¿Y uno HTTP?
¿Cuántos gestores de bases de datos se están ejecutando?

NOTA: No cerrar **zenmap** ya que sus resultados servirán más adelante.

Nessus

Nessus es un sistema de detección de vulnerabilidades de código cerrado pero gratuito para entorno doméstico y educativo. La base de su negocio es la suscripción a su repositorio de vulnerabilidades, una de las más actualizadas, aunque existen alternativas libres y gratuitas.

Este sistema no viene instalado por defecto en **Backtrack**, pero su instalación es muy sencilla.

Máquinas Virtuales

- RyS-Backtrack (root:toor)
- RyS-Victima (msfadmin:msfadmin)

Más información

Backtrack: http://www.backtrack-linux.org/

Zenmap: http://nmap.org/zenmap/

Snort: http://www.snort.org/

Nessus: http://www.tenable.com/products/nessus/

MSF: http://www.metasploit.com/

En **RyS-Backtrack**:

1. Abrir en **Firefox** la web **https://localhost:8834**.
2. Saldrá un aviso relativo al certificado de la máquina. Indicar que se entienden los riesgos y seguir adelante.
3. Desbloquear la ejecución de scripts mediante el botón "**Options…**" de abajo a la derecha.
4. Una vez que **Nessus** se ha iniciado (tarda un cierto tiempo), introducir el nombre de usuario **nessus** y la contraseña **nessus**.

En **RyS-Víctima**:

1. Detener el demonio **snort**.
2. Editar **snort.conf**:
   - HOME_NET debe ser la IP de **RyS-Víctima**.
   - EXTERNAL_NET debe ser !$HOME_NET.
3. Borrar el fichero de alerta.
4. Arrancar **snort** (desde **/etc/snort/**).

CONSEJO: En otra terminal se puede visualizar los cambios del fichero de alertas utilizando el comando **tail** y la opción **-f**.

De vuelta a **RyS-BackTrack**:

1. Ir a la pestaña **Scans**.
2. Añadir un nuevo escaneo.
   - Asignarle el nombre **RyS-Víctima Externo**.
   - Indicar que se quiere un escaneo del tipo1 **red externa**.
   - Indicar la IP de **RyS-Víctima** como objetivo.
3. Lanzar el escaneo.

A continuación el escaneo creado aparecerá en la lista con el estado **Running**. Se puede hacer doble click encima del mismo para ir viendo los resultados apenas van apareciendo. Un simple click encima del resultado ofrece información extendida.

Apenas termine el escaneo, la tarea desaparecerá de la pestaña **Scans** y se creará una nueva entrada en **Reports**.

4. Ir a la pestaña **Reports**.
5. Hacer click en la entrada relativa al escaneo y luego seleccionar **Dowload**.
6. Indicar que se desea el informe en formato **PDF** con los tres capítulos disponibles.

¿Cuántos puertos revela el escaneo TCP SYN?
¿Cuántos servicios se están ofreciendo a través de RPC?
¿Cuántas amenazas y de qué severidad detecta el escaneo?

¿Hay alguna puerta trasera instalada en **RyS-Víctima**?
¿Qué diferencia hay con lo obtenido con **zenmap**?
¿Cuántas alertas ha emitido **snort**? (usar el comando **grep** y encadenarlo con **wc**)

A continuación se pedirá a **Nessus** que aborde el objetivo desde otra perspectiva.

1. Borrar el archivo de alerta de **snort** en **RyS-Víctima** y reiniciarlo.
2. Crear un nuevo escaneo llamada **RyS-Víctima Interna**, pero esta vez que trate a **RyS-Víctima** como un objetivo en **red interna**.

¿Cuántas amenazas y de qué severidad detecta el escaneo?
¿Hay alguna diferencia con los resultados obtenidos del escaneo anterior?
¿Cuántas alertas ha emitido **snort**?

Ahora se creará una política de escaneo específica para el objetivo.

1. Borrar el archivo de alerta de **snort** en **RyS-Víctima** y reiniciarlo.
2. Ir a la pestaña **Policies** y seleccionar la opción de **añadir**.
3. En la pestaña **General**:
   - Introducir **Personalizada** como nombre.
   - Dejar **SYN Scan** como única opción en el escaneo de puertos.
4. En la sección de **Plugins**:
   - Desmarcar todas las familias.
   - Marcar las correspondientes a los resultados encontrados por **Zenmap**. Algunos pueden estar en categorías más genéricas.
5. Crear un nuevo escaneo llamado **RyS-Víctima Personalizada** indicando la política creada anteriormente.

¿Cuántas amenazas y de qué severidad detecta el escaneo?
¿Hay alguna diferencia con los resultados obtenidos de los escaneos anteriores?
¿Cuántas alertas ha emitido **snort**?
¿De qué manera se puede optimizar el escaneo?

Integración Nessus/MSF

Metasploit Framework (MSF) es una solución de auditoría de seguridad muy potente y modular. Desde la misma se pueden realizar escaneos a través de otras herramientas (como **Nessus**), estudiar los resultados y lanzar ataques dirigidos a vulnerabilidades específicas.

1. Arrancar **MSF** en modo consola con **msfconsole**.
2. Visualizar los comandos disponibles con **help**.

   NOTA: se puede pasar un parámetro en particular a **help**.

3. Cargar el módulo de **nessus** con **load nessus**.
4. Mostrar los comandos relacionados con este módulo con **nessus_help**.
5. Conectar al servicio **Nessus** con el siguiente comando: **nessus_connect *<Usuario>:<Contraseña>*@localhost ok**. El último parámetro indica que se usará SSL, útil cuando el servicio **Nessus** se encuentra en una máquina remota.
6. Obtener la sintaxis para arrancar un nuevo escaneo con **nessus_scan_new**.
7. Crear un nuevo escaneo de **RyS-Víctima** con nombre **"MSFinterna"** y política de **red interna**.
8. Mostrar el estado del escaneo con **nessus_scan_status**.
9. Mostrar la lista de informes con **nessus_report_list**.

Apenas termine el escaneo, se podrá importar el informe a la base de datos de **MSF** para posteriores operaciones.

1. Agregar el informe a la base de datos de **MSF** con **nessus_report_get** seguido del ID asignado al mismo.
2. Mostrar las máquinas objetivo cargadas.
3. Mostrar los servicios cargados.
4. Mostrar las vulnerabilidades cargadas.

¿Cuántos servicios de **RyS-Víctima** tiene registrados **MSF**?
¿Cuántas vulnerabilidades de **RyS-Víctima** tiene registradas **MSF**?

PISTA: no es necesario visualizar la lista de los anteriores.