Práctica 5.3: Escaneo y enumeración de sistemas, aplicaciones web y redes

Juan Boubeta Puig

Seguridad en los Sistemas Informáticos
Grado en Ingeniería Informática

Curso 2019 – 2020

UCA
Universidad de Cádiz

Índice

- Configuración del laboratorio de hacking.
- Escaneo y enumeración.
- Ping *sweepers.*
- TCP-ping.
- Estados de puertos.
- Técnicas de escaneo.
- Analizadores de vulnerabilidades.
- Análisis de vulnerabilidades con OpenVAS.
- Enumeración de varios protocolos con Netcat.

Configuración del laboratorio de hacking (I)

- Descarga la máquina virtual Metasploitable2, que contiene vulnerabilidades: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
- Usaremos Metasploitable2 como host víctima.
- Usaremos Kali Linux como estación hacker.
- La estación hacker debe poder conectarse con el host víctima.
- Para ello, configuramos en VirtualBox la tarjeta de red en modo “Adaptador solo anfitrión” para ambas máquinas virtuales.
- Iniciamos sesión en Metasploitable2 con usuario *msfadmin* y contraseña *msfadmin*.
- Iniciamos sesión en Kali Linux.

Configuración del laboratorio de hacking (II)

- Accedemos a la terminal de cada máquina virtual y comprobamos las IP asignadas automáticamente:
  - ifconfig
- Supongamos que las IP son las siguientes:
  - Estación hacker: 192.168.1.5
  - Host víctima: 192.168.1.6
- En la terminal de Kali, comprobamos que podemos hacer ping con éxito al host víctima:
  - ping 192.168.1.6

Configuración del laboratorio de hacking (III)

- Es importante que el ping se realice con éxito para poder realizar la práctica.
- Aclaración: al configurar las tarjetas de red en modo “Adaptador solo anfitrión”, las máquinas no tendrán acceso a Internet. En caso de necesitar conexión a Internet en la máquina de Kali (por ejemplo, para descargar OpenVAS), deberá cambiarse a modo “Adaptador puente” momentáneamente.

Escaneo y enumeración

- Tras obtener el rango de direcciones IP de nuestro objetivo durante la fase de reconocimiento, en esta fase de **escaneo**:
  - Identificaremos los hosts que estén activos.
  - Buscaremos los puertos abiertos en dichas máquinas.
  - A partir de los puertos abiertos, obtendremos información del sistema operativo, aplicaciones, servicios…
- Una vez identificados el sistema operativo, servicio, etc. podremos decidir si realizar la **enumeración** (escaneo más intenso) para tratar de obtener cuentas de usuario, procesos…
- Si existen vulnerabilidades, estas podrán ser posteriormente explotadas.

Ping *sweepers*

- Son herramientas de barrido de ping.
- Permiten definir un rango de IPs donde enviar solicitudes de respuesta (*echo request*) utilizando el protocolo ICMP.
- Se marcarán como activos aquellos hosts que respondan a la solicitud.
- Consideraciones importantes:
  - Los *firewalls* suelen bloquear las solicitudes de ping realizadas desde el exterior.
  - Los sistemas de prevención de intrusos (IPS) podrían detectar el escaneo y enviar órdenes al *firewall* para bloquear ciertas IP.

TCP-ping

- Permite comprobar si un host está activo utilizando el protocolo TCP (en vez de ICMP).

Estados de puertos

- La herramienta de escaneo de puertos más conocida es NMAP.
- Esta herramienta define los siguientes estados de puerto:
  - **Abierto**: está disponible y escuchando. Por ejemplo: UDP/53 (DNS), TCP/80 (HTTP) y TCP/443 (HTTPS).
  - **Cerrado**: está accesible pero no tiene un servicio/aplicación que responda a solicitudes de conexión.
  - **Filtrado**: no está accesible. Un router con ACL implementadas o *firewall* impide saber si el puerto está abierto o cerrado.
  - **No-filtrado**: accesible, pero no se sabe si está abierto o cerrado.
  - **Abierto|Filtrado**: el escáner no sabe si está abierto o filtrado.
  - **Cerrado|Filtrado**: el escáner no sabe si está cerrado o filtrado.

Técnicas de escaneo (I)

- **Escaneo SYN o *half-open***:
  - Identifica puertos con servicios que usan TCP como protocolo de transporte.
  - En primer lugar, se envía una solicitud de sincronización (SYN) a la víctima.
  - Si se recibe como respuesta de la víctima:
    a) La sincronización junto con un acuse de recibo (SYN + ACK) → puerto abierto.
    b) Un reset (RST) → puerto cerrado.
    c) Sin respuesta → puerto filtrado.

Técnicas de escaneo (II)

- **Escaneo *full* o *connect-scan***:
  - También utiliza el protocolo TCP.
  - En esta técnica, sí se finaliza la conexión con el envío del acuse de recibo final (ACK) a la máquina objetivo.
  - Requiere más tiempo para ejecutarse.
  - Podría quedar un registro de la conexión en los logs de eventos de la máquina objetivo.

Técnicas de escaneo (III)

- **Escaneo UDP**:
  - Utiliza el protocolo de transporte UDP.
  - Envía un paquete UDP a los puertos de los hosts remotos y espera respuesta.
  - Si la respuesta es:
    a) Un segmento UDP → puerto abierto.
    b) Un mensaje ICMP *port-unreacheable* → puerto cerrado.
    c) Otro tipo de error ICMP → puerto filtrado.

Técnicas de escaneo (IV)

- **Escaneo ACK**:
  - Permite comprobar si existe un *firewall*.
  - Envía un segmento con la bandera ACK encendida al puerto destino de la víctima.
  - Si la respuesta es:
    a) RST → puerto no filtrado (*unfiltered*), accesible (el puerto puede estar abierto o cerrado).
    b) Sin respuesta o mensaje de error ICMP → puerto filtrado.

Técnicas de escaneo (V)

- **Ejercicio 1**:
  - Busca información en Internet en qué consisten los escaneos especiales Fin-Scan, XMAS-Scan y Null-Scan.
  - Encuentra un gráfico que permita visualizar gráficamente la secuencia de pasos que se realizan en cada técnica de escaneo:
    - SYN o *half-open*.
    - Full o *connect-scan*.
    - UDP.
    - ACK.
    - Fin-Scan.
    - XMAS-Scan.
    - Null-Scan.

Técnicas de escaneo (VI)

- **Ejercicio 2**:
  - Accede a la documentación de NMAP: http://www.nmap.org
  - Describe la sintaxis completa con las opciones del comando *nmap*.
  - Describe y ejecuta el comando *nmap* junto con las opciones necesarias para realizar:
    - Un escaneo en modo *half-scan* de la red 192.168.1.0/24.
    - Un escaneo tipo *connect* que permita detectar el sistema operativo del host víctima (máquina Metasploitable2).
    - Un escaneo en modo *half-scan* que permita detectar el sistema operativo, la versión de los servicios y la obtención de *banners* del host víctima (máquina Metasploitable2).

Técnicas de escaneo (VII)

- **Ejercicio 3**:
  - Describe y explica los resultados obtenidos tras ejecutar el comando *nmap* junto con las opciones necesarias para realizar:
    - Un escaneo en modo *half-scan* del servidor scanme.nmap.org
    - Un escaneo tipo *connect* que permita detectar el sistema operativo del servidor scanme.nmap.org
    - Un escaneo en modo *half-scan* que permita detectar el sistema operativo, la versión de los servicios y la obtención de *banners* del servidor scanme.nmap.org

Técnicas de escaneo (VIII)

- **Ejercicio 4**:
  - Repite el Ejercicio 3 pero utilizando la herramienta gráfica Zenmap (*Applications > Information Gathering > Zenmap*).
  - Teniendo como objetivo el servidor (scanme.nmap.org), trate de obtener más información utilizando otras opciones y perfiles proporcionados por la herramienta gráfica.
  - Obtenga la topología de red (de un modo gráfico).
  - Indica ventajas/inconvenientes de Zenmap frente a línea de comandos.

Analizadores de vulnerabilidades

- Permiten ejecutar escaneos y enumeraciones sobre el objetivo.
- Identifican vulnerabilidades del objetivo.
- Clasifican las vulnerabilidades según el riesgo:
  - **Alto**: el equipo objetivo tiene una o más vulnerabilidades críticas explotables fácilmente por un atacante. Se requiere una acción correctiva inmediata.
  - **Medio**: tiene una o más vulnerabilidades severas que requieren una mayor complejidad para ser explotadas. Se requiere atención a corto plazo.
  - **Bajo**: tiene una o más vulnerabilidades moderadas que podrían ofrecer información al atacante. No requiere atención urgente.
- Analizadores: OpenVas, Nessus, Nexpose…

Análisis de vulnerabilidades con OpenVAS (I)

- Abrimos la terminal en Kali Linux e instalamos OpenVAS:
  - apt-get update
  - apt-get install openvas
- Configuramos OpenVAS ejecutando el comando:
  - openvas-setup
- Tras finalizar la configuración:
  - Se inician automáticamente los servicios de OpenVAS.
  - Se crea la cuenta de usuario *admin* con una clave aleatoria.
  - Se abre un navegador web conectado a la interfaz de administración (https://localhost:9392)
  - Se muestra la contraseña del usuario *admin* en la terminal.

Análisis de vulnerabilidades con OpenVAS (II)

- **Ejercicio 5**:
  - Tomamos nota de la contraseña porque se usará más tarde.
  - En el navegador abierto, accedemos a las opciones avanzadas y agregamos una excepción para el certificado autogenerado.
  - Accedemos a la interfaz de administración *Greenbone Security Assistant* introduciendo el usuario *admin* y la contraseña anotada.
  - Creamos un nuevo escaneo con la opción *Scans* > *Tasks* > (icono *Wizard*).
  - En la caja de diálogo introducimos la IP de nuestro objetivo (la máquina Metasploitable2) y pulsamos en *Start Scan*.

Análisis de vulnerabilidades con OpenVAS (III)

- Accedemos a los informes generados con la opción *Scan > Reports*.
- Accedemos a la lista de vulnerabilidades asociadas a un informe, pulsando sobre el nombre del informe en cuestión.
- Analizamos qué tipos de riesgo (alto, medio o bajo) se han encontrado.
- Exportamos el informe generado en formato XML.

Enumeración de varios protocolos con Netcat (I)

- Netcat es una herramienta de código abierto que permite:
  - Escanear puertos.
  - Abrir puertos de escucha en un equipo y realizar conexiones remotas.
  - Transferir ficheros.
- Usaremos Metasploitable2 como host víctima.
- Usaremos Kali Linux como estación hacker.
- **Ejercicio 6**:
  - Abre la terminal en Kali, ejecuta el siguiente comando y describe la sintaxis de netcat:
    - nc -h

Enumeración de varios protocolos con Netcat (II)

- Utilizando el comando nc, realiza un escaneo de la máquina virtual Metasploitable2 con las siguientes opciones:
  - Información detallada (*verbose*) de la conexión por consola.
  - Tiempo de espera por conexión de 3 segundos.
  - Modo de escaneo de puerto (zero I/O).
  - Puertos del 15 al 1000.
  - ¿Qué información se obtiene?
- **Ejercicio 7**: repite el Ejercicio 6 pero en esta ocasión escaneando todos los puertos (1-65535).
- **Ejercicio 8**: ¿qué opción permite escanear los puertos UDP?

Enumeración de varios protocolos con Netcat (III)

- **Ejercicio 9**:
  - Usa netcat para conectarte desde Kali al puerto 80 de la máquina Metasploitable2.
  - Una vez conectado, ejecuta el siguiente comando:
    - GET / HTTP /
  - ¿Qué información se muestra en la consola de Kali?
- **Ejercicio 10**:
  - Busca por Internet más información sobre Netcat.
  - ¿Qué otro tipo de información/operación podríamos obtener/realizar haciendo uso de este comando?

Bibliografía

- K. Astudillo B. Hacking Ético: Cómo Convertirse en Hacker Ético en 21 Días o Menos, 3ª edición. ISBN 978-84-9964-767-8. Ra-Ma, 2018.
- M. Á. Caballero Velasco y D. C. Serrano. El Libro del Hacker. ISBN 978-84-415-3964-8. Anaya Multimedia, 2018.
- P. González, G. Sánchez y J. M. Soriano. Pentesting con Kali Linux Rolling Release 2017, 2ª edición. ISBN 978-84-697-6035-2. 0xWORD, 2017.
- R. Hertzog, J. O'Gorman y M. Aharoni. Kali Linux Revealed: Mastering the Penetration Testing Distribution. ISBN 978-0-9976156-0-9. Offsec Press, 2017.


slidesgo