Práctica II.: Ejemplos de categorías de ataque et al. (? sesiones – ?h)

Prof. A. Santos del Riego
Legislación y Seguridad Informática (LSI)
Facultad de Informática. Universidad de A Coruña
Fecha propuesta.: enero 2003
Última revisión.: agosto 2023

El objetivo de esta práctica es comprender y probar el funcionamiento de los *sniffers*, los ataques [D]DoS, así como diversos temas relacionados con lo que hemos llamado la trilogía ("host discovery", "port scanning" y "fingerprinting"). La gestión de la información de auditoría es otro de los objetivos de esta práctica. En las sesiones de laboratorio se propondrán posibles herramientas a utilizar.

a) Instale el ettercap y pruebe sus opciones básicas en línea de comando.
b) Capture paquetería variada de su compañero de prácticas que incluya varias sesiones HTTP. Sobre esta paquetería (puede utilizar el wireshark para los siguientes subapartados)
    - Identifique los campos de cabecera de un paquete TCP
    - Filtre la captura para obtener el tráfico HTTP
    - Obtenga los distintos "objetos" del tráfico HTTP (imágenes, pdfs, etc.)
    - Visualice la paquetería TCP de una determinada sesión.
    - Sobre el total de la paquetería obtenga estadísticas del tráfico por protocolo como fuente de información para un análisis básico del tráfico.
    - Obtenga información del tráfico de las distintas "conversaciones" mantenidas.
    - Obtenga direcciones finales del tráfico de los distintos protocolos como mecanismo para determinar qué circula por nuestras redes.
c) Obtenga la relación de las direcciones MAC de los equipos de su segmento.
d) Obtenga la relación de las direcciones IPv6 de su segmento.
e) Obtenga el tráfico de entrada y salida legítimo de su interface de red ens33 e investigue los servicios, conexiones y protocolos involucrados.
f) Mediante *arpspoofing* entre una máquina objetivo (víctima) y el *router* del laboratorio obtenga todas las URL HTTP visitadas por la víctima.
g) Instale metasploit. Haga un ejecutable que incluya un Reverse TCP meterpreter payload para plataformas linux. Inclúyalo en un filtro ettercap y aplique toda su sabiduría en ingeniería social para que una víctima u objetivo lo ejecute.
h) Haga un MITM en IPv6 y visualice la paquetería.
i) Pruebe alguna herramienta y técnica de detección del *sniffing* (preferiblemente arpon).
j) Pruebe distintas técnicas de *host discovey*, *port scanning* y *OS fingerprinting* sobre las máquinas del laboratorio de prácticas en IPv4. Realice alguna de las pruebas de *port scanning* sobre IPv6. ¿Coinciden los servicios prestados por un sistema con los de IPv4?.
k) Obtenga información "en tiempo real" sobre las conexiones de su máquina, así como del ancho de banda consumido en cada una de ellas.
l) Monitorizamos nuestra infraestructura.:
    - Instale prometheus y node_exporter y configúrelos para recopilar todo tipo de métricas de su máquina linux.
    - Posteriormente instale grafana y agregue como fuente de datos las métricas de su equipo de prometheus.
    - Importe vía grafana el dashboard 1860.
    - En los ataques de los apartados m y n busque posibles alteraciones en las métricas visualizadas.

m) PARA PLANTEAR DE FORMA TEÓRICA.: ¿Cómo podría hacer un DoS de tipo *direct attack* contra un equipo de la red de prácticas? ¿Y mediante un DoS de tipo *reflective flooding attack?*.
n) Ataque un servidor apache instalado en algunas de las máquinas del laboratorio de prácticas para tratar de provocarle una DoS. Utilice herramientas DoS que trabajen a nivel de aplicación (capa 7). ¿Cómo podría proteger dicho servicio ante este tipo de ataque? ¿Y si se produjese desde fuera de su segmento de red? ¿Cómo podría tratar de saltarse dicha protección?
o) Instale y configure modsecurity. Vuelva a proceder con el ataque del apartado anterior. ¿Qué acontece ahora?
p) Buscamos información.:
    - Obtenga de forma pasiva el direccionamiento público IPv4 e IPv6 asignado a la Universidade da Coruña.
    - Obtenga información sobre el direccionamiento de los servidores DNS y MX de la Universidade da Coruña.
    - ¿Puede hacer una transferencia de zona sobre los servidores DNS de la UDC?. En caso negativo, obtenga todos los nombres.dominio posibles de la UDC.
    - ¿Qué gestor de contenidos se utiliza en www.usc.es?
q) Trate de sacar un perfil de los principales sistemas que conviven en su red de prácticas, puertos accesibles, *fingerprinting*, etc.
r) Realice algún ataque de "password guessing" contra su servidor ssh y compruebe que el analizador de logs reporta las correspondientes alarmas.
s) Reportar alarmas está muy bien, pero no estaría mejor un sistema activo, en lugar de uno pasivo. Configure algún sistema activo, por ejemplo OSSEC, y pruebe su funcionamiento ante un "password guessing".
t) Supongamos que una máquina ha sido comprometida y disponemos de un fichero con sus mensajes de log. Procese dicho fichero con OSSEC para tratar de localizar evidencias de lo acontecido ("post mortem"). Muestre las alertas detectadas con su grado de criticidad, así como un resumen de las mismas.

Método de evaluación.: Como resultado de esta práctica, el profesor evaluará las habilidades adquiridas por el alumno mediante una sesión de trabajo en máquina.