


Facultad de Ciencias
UNAM

Criptografía y Seguridad
Práctica 01: Recopilación de Información en Pentesting
Uziel Vidal Cruz Vargas
Emilio Arsenio Raudry Rico

1. Introducción

La seguridad informática es un aspecto crítico en la actualidad, ya que la información es uno de los activos más valiosos de cualquier organización Las pruebas de penetración, o *pentesting*, son evaluaciones de seguridad diseñadas para identificar vulnerabilidades en sistemas y redes antes de que puedan ser explotadas por actores malintencionados (Mitnick & Simon, 2002).

En esta práctica, se enfoca la fase de **recopilación de información**, una etapa esencial del *pentesting* en la que se recolectan datos clave sobre el objetivo para evaluar posibles puntos débiles. Para ello, se emplearán diversas herramientas y metodologías que permiten obtener información de manera estructurada y efectiva (Campbell & Beach, 2016).

Este documento presenta los requisitos, las fuentes de información utilizadas, el proceso de adquisición de datos, el procesamiento de la información obtenida, el análisis de resultados y una serie de preguntas clave relacionadas con la seguridad informática y el *pentesting*. Finalmente, se ofrecerá una conclusión sobre los hallazgos obtenidos y su relevancia en el ámbito de la ciberseguridad.

2. Preguntas de Pentesting: Recopilación de Información

2.1 Menciona los tipos de protocolos de red.

Los protocolos de red se pueden clasificar en diferentes capas del modelo OSI, dependiendo de su función:

Capa de Enlace de Datos: Controlan la comunicación dentro de una red local.

- Ethernet (IEEE 802.3)
- Wi-Fi (IEEE 802.11)
- PPP (Point-to-Point Protocol)

Capa de Red: Administran la transmisión de datos entre dispositivos en diferentes redes.

- IP (Internet Protocol): IPv4, IPv6
- ICMP (Internet Control Message Protocol): Diagnóstico y reporte de errores en redes.
- ARP (Address Resolution Protocol): Traducción de direcciones IP a direcciones MAC.

Capa de Transporte: Garantizan la entrega fiable de datos entre aplicaciones.

- TCP (Transmission Control Protocol): Conexión confiable y orientada a flujo.
- UDP (User Datagram Protocol): Conexión rápida pero sin garantía de entrega.

Capa de Aplicación: Facilitan la comunicación entre aplicaciones.

- HTTP/HTTPS (Hypertext Transfer Protocol Secure): Transferencia de información en la web.

- FTP (File Transfer Protocol): Transferencia de archivos.
- DNS (Domain Name System): Resolución de nombres de dominio en direcciones IP.
- SMTP/POP3/IMAP: Protocolos de correo electrónico.
- SSH (Secure Shell): Acceso remoto seguro.

Protocolos de Seguridad: Proporcionan cifrado y autenticación.

- TLS/SSL (Transport Layer Security / Secure Sockets Layer)
- IPSec (Internet Protocol Security)

2.2 ¿Cómo funcionan los protocolos de red y para qué sirven?

Los protocolos de red operan en distintos niveles del modelo OSI (Open Systems Interconnection) y del modelo TCP/IP para permitir la transmisión de datos. Su funcionamiento se basa en la encapsulación de información en paquetes que son transportados de un punto a otro dentro de una red.

Funcionamiento: Cada protocolo tiene reglas específicas sobre cómo se deben enviar, recibir y procesar los datos. Por ejemplo, TCP divide la información en paquetes, los transmite y garantiza su correcta entrega y orden.

Utilidad:

- Permiten la comunicación entre dispositivos.
- Garantizan que los datos lleguen completos y sin alteraciones.
- Optimización del uso de recursos de red.
- Seguridad y autenticación de datos.

2.3 ¿Qué es un sniffer?

Un *sniffer* es una herramienta que permite capturar y analizar el tráfico de red en tiempo real. Su función principal es interceptar paquetes de datos que circulan en una red, lo que permite a los administradores de seguridad evaluar la comunicación y detectar vulnerabilidades.

Usos de un sniffer:

- Diagnóstico y resolución de problemas de red.
- Monitoreo de tráfico para detectar intentos de ataque.
- Análisis de vulnerabilidades en entornos de red.
- Recuperación de información en auditorías de seguridad.

Ejemplos de sniffers:

- Wireshark: Herramienta gráfica para análisis profundo del tráfico de red.
- tcpdump: Utilidad de línea de comandos para capturar paquetes.
- Ettercap: Especializado en ataques MITM (Man-in-the-Middle).
- Kismet: Sniffer enfocado en redes inalámbricas.

2.4 OSINT, ¿qué es y para qué sirve?

OSINT (Open Source Intelligence) se refiere a la recopilación de información a partir de fuentes abiertas y accesibles al público para obtener inteligencia útil en diversas áreas, incluida la ciberseguridad.

Utilidad:

- Recolección de información sobre objetivos en pentesting.
- Identificación de activos expuestos en internet.
- Seguimiento de actividad sospechosa en redes sociales.
- Investigación en ciberseguridad para la detección de amenazas.

2.5 Investiga los 5 OSINT más usados.

Los cinco *OSINT* más utilizados en ciberseguridad y pruebas de penetración son:

- **Maltego**: Analiza relaciones entre personas, empresas, correos y direcciones IP.
- **Shodan**: Motor de búsqueda para dispositivos conectados a Internet.
- **theHarvester**: Recolecta información sobre correos electrónicos y subdominios.
- **Google Dorking**: Búsqueda avanzada en Google para encontrar información sensible.
- **Recon-ng**: Framework modular para la recolección de información OSINT.

2.6 Investiga 5 softwares no mencionados en la práctica que sirvan para el análisis de comunicaciones.

Existen diversas herramientas adicionales para el análisis de comunicaciones en redes. Algunas de las más utilizadas en ciberseguridad son:

- **Zeek (Bro)**: Framework de monitoreo de red en tiempo real, útil para análisis de tráfico avanzado.
- **Suricata**: Sistema de detección y prevención de intrusos (IDS/IPS) con capacidad de análisis en tiempo real.
- **TShark**: Versión en línea de comandos de Wireshark, utilizada para captura y análisis de paquetes.
- **NetworkMiner**: Herramienta de análisis forense de red, útil para extraer archivos e información de tráfico capturado.
- **P0f**: Detector pasivo de sistemas operativos y monitoreo de tráfico sin enviar paquetes.

2.7 ¿Qué es la ingeniería social?

La **ingeniería social** es una técnica de manipulación psicológica utilizada para obtener información confidencial a través del engaño y la persuasión. Se basa en explotar la confianza y el comportamiento humano en lugar de vulnerabilidades técnicas.

Ejemplos de ingeniería social:

- **Phishing**: Suplantación de identidad para obtener credenciales.

- **Pretexting**: Creación de escenarios falsos para obtener información.
- **Baiting**: Uso de dispositivos infectados para comprometer sistemas.

2.8 ¿Por qué el eslabón más débil de seguridad son las personas?

En ciberseguridad, el factor humano es considerado el **eslabón más débil** porque las personas pueden ser engañadas con mayor facilidad que los sistemas automatizados. Las razones incluyen:

- Falta de conocimiento sobre ciberseguridad.
- Uso de contraseñas débiles o repetidas.
- Caída en engaños de phishing o ingeniería social.
- Configuración incorrecta de dispositivos y aplicaciones.

2.9 ¿Qué acciones haces para protegerte de ciberataques?

Para mitigar riesgos de ciberseguridad, se pueden implementar diversas buenas prácticas, como:

- Uso de contraseñas seguras y autenticación multifactor (MFA).
- Evitar enlaces y archivos sospechosos en correos electrónicos.
- Mantener software y sistemas operativos actualizados.
- Uso de VPNs y conexiones seguras para acceder a redes sensibles.
- Realizar copias de seguridad periódicas.

2.10 ¿Crees que tus métodos preventivos son suficientes?

La prevención en ciberseguridad es un proceso continuo que debe adaptarse a nuevas amenazas. A pesar de implementar medidas de protección, siempre existe la posibilidad de que surjan nuevas vulnerabilidades. Algunas recomendaciones adicionales incluyen:

- Realizar auditorías de seguridad periódicas.
- Mantenerse informado sobre las últimas amenazas cibernéticas.
- Implementar sistemas de detección y respuesta ante incidentes.