


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. Requisitos para la Prueba de Penetración

Para llevar a cabo la prueba de penetración enfocada en la recopilación de información, es fundamental definir los requisitos necesarios, tanto en términos de herramientas como de datos a obtener.

2.1 Problema a Resolver

El objetivo principal de esta prueba de penetración es identificar vulnerabilidades en la infraestructura de red del objetivo. Para ello, se busca recopilar información que pueda ser utilizada para detectar posibles puntos de ataque, evaluar la seguridad de los servicios expuestos y determinar medidas de mitigación.

2.2 Información Necesaria

Para realizar un análisis efectivo, se requiere obtener los siguientes datos:

- **Direcciones IP y nombres de dominio**: Identificar los activos en la red.
- **Registros DNS y subdominios**: Conocer la estructura del dominio.
- **Información WHOIS**: Datos sobre la propiedad y administración de dominios e IPs.
- **Estado de puertos abiertos y servicios en ejecución**: Identificación de servicios expuestos.

- **Información del sistema operativo y software utilizado**: Posibles vulnerabilidades en versiones desactualizadas.
- **Latencia y conectividad**: Evaluación del estado de la red.

2.3 Herramientas Utilizadas

Para la recopilación de información se utilizarán las siguientes herramientas:

- **Comandos básicos**: ping, nslookup, traceroute, whois.
- **Enumeración de subdominios**: sublist3r, subfinder, dnsmap, dnsrecon.
- **Escaneo de puertos y servicios**: nmap.
- **Análisis de tráfico**: EtherApe.

2.4 Propósito de la Información Recopilada

Toda la información obtenida será utilizada con fines de auditoría de seguridad y evaluación de riesgos. La recopilación de estos datos permitirá:

- Identificar activos expuestos y su nivel de vulnerabilidad.
- Determinar posibles vectores de ataque.
- Proponer estrategias de mitigación para mejorar la seguridad.

2.5 Consideraciones Éticas y Legales

Toda la información recopilada debe manejarse con responsabilidad y confidencialidad, evitando el uso indebido de los datos obtenidos.

3. Identificación de Fuentes de Información

Para recopilar información en una prueba de penetración, es clave usar fuentes confiables. Aquí hay algunas opciones que pueden aportar datos útiles:

3.1 Fuentes Públicas y OSINT

Estas fuentes son accesibles para cualquiera y pueden proporcionar mucha información sin necesidad de permisos especiales:

- **Motores de búsqueda (Google, Bing, DuckDuckGo)**: Si se usan bien, pueden revelar información interesante sobre un sitio web o una empresa.
- **Bases de datos WHOIS**: Permiten ver quién registró un dominio y otros datos relevantes.
- **Shodan y Censys**: Son motores de búsqueda para encontrar dispositivos conectados a Internet.
- **Herramientas OSINT (TheHarvester, Recon-ng)**: Ayudan a recolectar información de correos, subdominios y redes sociales.

3.2 Fuentes Privadas y de Acceso Restringido

Algunas fuentes requieren credenciales o permisos para acceder:

- **Registros internos**: Logs de servidores y sistemas de una empresa pueden revelar actividad sospechosa.
- **Monitoreo de tráfico de red**: Herramientas como Wireshark permiten analizar paquetes de datos en tiempo real.
- **Sistemas SIEM**: Consolidan eventos de seguridad para facilitar la detección de incidentes.

3.3 Documentación Técnica y Académica

Libros, artículos y normativas de seguridad son esenciales para entender vulnerabilidades y mejores prácticas:

- **Libros de ciberseguridad**: Como *Computer Networking: A Top-Down Approach* (Kurose & Ross, 2020).
- **Estándares de seguridad**: NIST, ISO 27001, OWASP Top 10.
- **Blogs y foros**: SANS, KrebsOnSecurity, Exploit-DB.

3.4 Redes Sociales y Foros de Seguridad

Las comunidades en línea pueden ser útiles para conocer nuevas amenazas y tendencias:

- **GitHub y GitLab**: Repositorios donde se pueden encontrar herramientas de seguridad y exploits.
- **Reddit y Twitter**: Se discuten vulnerabilidades recientes y técnicas de pentesting.
- **Foros especializados (Hack The Box, Offensive Security)**: Espacios donde expertos comparten experiencias y retos.

4. Adquisición - Explicación del script

Para la elaboración del script tuvimos que separar la información a obtener en diferentes apartados, basados en su tipo y en los comandos que nos facilitan dicha obtención:

1. **Dirección IP y nombre de dominio:** Dado que el usuario puede insertar cualquiera de estas dos opciones, realizamos un **nslookup** con el argumento que recibamos. Dependiendo del formato del argumento podemos saber si el resultado del comando será un nombre de dominio o una dirección IP que podramos guardar en unas variables.
2. **Fechas Importantes**: Al momento de ejecutar **whois**, podemos obtener resultados diferentes dependiendo del formato del servidor al que queramos acceder. Si le damos su nombre de dominio, nos dará información relativo únicamente a este, por lo que será su salida la que nos dará las fechas de creación, actualización y expiración del dominio.
3. **Datos de la Organización**: Al dar como argumento la dirección IP a **whois**, este nos dará información respecto a la organización a la que pertenece el servidor. De acá podemos obtener su nombre, ubicación, dirección, personal y sus datos (como correos y números telefónicos).

4. **Conectividad**. Para poder verificar la calidad e la conexión, hacemos un **ping** de 4 paquetes a nuestro servidor, al ver que todos los paquetes se enviaron de manera integra, junto a la latencia de la conexión, podemos juzgar su calidad.
5. **Información de Red y DNS**. Dada la dirección IP, podemos conocer más acerca de su estructura. Con **whois** podemos obtener los segmentos de red que tiene, para darnos una idea de su máscara y las subredes que este puede tener (lo que nos da la posiblidad de hacer movimientos laterales en el futuro). De igual manera, podemos saber que otros servicios brinda el servidor si tenemos también los subdominos dns que este tiene (para ello ocupamos **dnsmap**. Con **dig** podemos obtener también los registros reversos y la IPV6 del servidor. De igual manera para conocer el trayecto de la consulta junto a sus saltos usamos a **traceroute**.
6. **Información de puertos, servicios y sistema operativo**. Al leer la documentaciónde **nmap** sabemos que además de obtener sus puertos, podemos tener sus servicios correspondientes, de la misma manera que podemos hacer una aproximación del sistema operativo del equipo con la bandera -O.

5. Procesamiento

Retomando nuestros apartados durante la adquisición, filtraremos nuestros resultados de la misma manera.

5.1 unam.mx

1. Direcciones y dominios
   a) **Dominio:** unam.mx
   b) **IPv4: 132.248.166.19**
2. Fechas importantes
   a) Creación: 1989-03-31
   b) Actualización: 2024-03-27
   c) Expiración: 25-03-30
3. Datos de la organización.
   a) **Nombre:** Latin American and Caribbean IP address Regional Registry y Universidad Nacional Autónoma de México
   b) **Países asociados**: México y Uruguay
   c) **Direcciones Asociadas:** Rambla República de México 6125. Y tambień Av. Universidad, 3000, Copilco 04510, Coyoacán CDMX
   d) **Personal:** LACNIC, Dr Hector Benitez Perez.
4. Conectividad
   - Los 4 paquetes fueron recibidos sin fallas con una latencia de 35.309ms
5. Información de Red y DNS
   - La ip cuenta con un segmento de red de 132.247.0.0 - 132.248.255.255

- Su dirección IPv6 es 2001::1218:3000:160::19
- DNS reverso como 19.166.248.132
- Traceroute completado en 3 saltos.
- Una variedad de subdomions, entre ellos del tipo blog, bq, dc, email, eventos, fa, ib, im, mail, mobile, ns1, ns2, ns3, pi, ri, servidor, tienda, tv, vpn, ws, www, www1. Juntos a los registros DNS: SOA, NS, MX, A, AAAA, TXT.
- Información de puertos, servicios y sistema operativo
  a) Puertos y servicios:
     1) 21/tcp open ftp?
     2) 80/ tcp open http Apache httpd 2.4.51 ((Unix))
     3) 443/tcp open ssl/http nginx 1.27.2
     4) 554/tcp rtsp?
     5) 1723/tcp open pptp?
  b) Tipos de dispositivo: Propósito general.
  c) SO: Linux

5.2 ipn.mx

1. Direcciones y dominios
   a) **Dominio:** ipn.mx
   b) **IPv4**: 20.64.80.120
2. Fechas importantes
   a) Creación:1995-04-30
   b) Actualización:2024-04-26
   c) Expiración:2026-06-20
3. Datos de la organización.
   a) **Nombre:** Microsoft Corporation
   b) **Países asociados**: Estados Unidos
   c) **Direcciones Asociadas:** Redmond, Washington, One Microsoft Way 98052
   d) **Personal:** Dawn Bernard, Avery Kim, Prachi Singh
4. Conectividad
   - Los 4 paquetes fueron recibidos sin fallas con una latencia de 34.922 ms
5. Información de Red y DNS
   - La ip cuenta con un segmento de red de 20.33.0.0 - 20.128.255.255
   - Sin información acerca de IPV6
   - DNS reverso como 120.80.64.20
   - Traceroute completado en 30 saltos.

- Una variedad de subdominios, entre ellos del tipo backup, home, imap, mail, news, ntp, ok, p, pop, servicios, sg, smtp, soporte, virtual, www. Juntos a los registros DNS: SOA, NS, MX, A, AAAA, TXT.
- Información de puertos, servicios y sistema operativo
  a) Puertos y servicios:
    1) 21/tcp open tcpwrapped
    2) 80/ tcp open http tcpwrapped
    3) 443/tcp open tcpwrapped1.27.2
    4) 554/tcp tcpwrapped
    5) 1723/tcp tcpwrapped
  b) Tipos de dispositivo: Storage-misc, impresora.
  c) SO: Posiblemente Netgear SC101 Storage Central NAS device

5.3 pemex.com

1. Direcciones y dominios
   a) **Dominio:** pemex.com
   b) **IPv4**: 200.23.91.20
2. Fechas importantes
   a) Creación:1995-06-22
   b) Actualización:2025-01-07
   c) Expiración:2026-06-20
3. Datos de la organización.
   a) **Nombre:** Petróleos Mexicanos
   b) **Países asociados**: México
   c) **Direcciones Asociadas:** Av Marina Nacional, 329, Verónica Anzures, 05200, Miguel Hidal, CDMX
   d) **Personal:** Rocío Pérez Juárez, Rocio Pérez Juárez, Joel Rne Argaez Soliz.
4. Conectividad
   - Los 4 paquetes fueron recibidos sin fallas con una latencia de 3078 ms
5. Información de Red y DNS
   - La ip cuenta con un segmento de red de 132.247.0.0 - 132.248.255.255
   - Sin información acerca de IPV6
   - DNS reverso como 20.91.23.200
   - Traceroute completado en 3 saltos.
   - Una variedad de subdomions, entre ellos del tipo blog, blogs, ca, email, eventos, ir, owa, ri, search,tv, vpn, ws, www, www1, ww2. Juntos a los registros DNS: SOA, NS, MX, A, AAAA, TXT.

- Información de puertos, servicios y sistema operativo
  a) Puertos y servicios:
     1) 21/tcp open tcpwrapped
     2) 80/ tcp open http tcpwrapped
     3) 443/tcp open tcpwrapped1.27.2
     4) 554/tcp tcpwrapped
     5) 1723/tcp tcpwrapped
  b) Tipos de dispositivo: Storage-misc, impresora.
  c) SO: Posiblemente Netgear SC101 Storage Central NAS device

5.4 gob.mx

No hay dirección IP en un servidor DNS autorativo.

6. Análisis

Retomando nuestros apartados durante la adquisición y el procesamiento, filtraremos nuestros resultados de la misma manera.

6.1 unam.mx

1. Direcciones y dominios: Todo correcto.
2. Fechas importantes: Expira este mes.
   a) Creación:1989-03-31
   b) Actualización: 2024-03-27
   c) Expiración:25-03-30
3. Datos de la organización: Además de obtener los datos de la UNAM incluye el nombre del servidor intermedio durante el recorrido hasta el servidor objetivo.
4. Conectividad: Conexión correcta
5. Información de Red y DNS: Varias subredes, valdría la pena verificar ellas también. Los subdominios nos hablan de contactos para ingeniería social y otros servicios que ofrece la universidad.
6. Información de puertos, servicios y sistema operativo
   a) Puertos y servicios: Puerto http abierto, sin cifrado, si alguien se conectara dentro de una red cercana podríamos obtener sus datos en bruto. También podíamos ver que subrutas hay dentro de la página en búsqueda de un archivo perdido con información valiosa.
   b) Usa un sistema Linux, tiene una forma especial de subir de privilegios.

6.2 ipn.mx

1. Direcciones y dominios: Todo correcto
2. Fechas importantes: Expira el año siguiente.
3. Datos de la organización: Esta administrado por un servidor remoto Microsoft en Estados Unidos. En caso de querer hacer ingeniería social sobre los trabajadores hay que contemplar el lenguaje y el perfil de los usuarios que aparentemente varían de etnias.
4. Conectividad: Conexión correcta.
5. Información de Red y DNS: Varias subredes y subdominios. Uno de gran interés es el backup.
6. Información de puertos, servicios y sistema operativo: A pesar de lo que dice la aproximación de SO, tcpwrapper es un protocolo usado en distribuciones GNU/Linux.

6.3 pemex.com

1. Direcciones y dominios: Todo correcto
2. Fechas importantes: Expira el siguiente año.
3. Datos de la organización: Forma parte del gobierno mexicano. Dentro del personal se encuentran dos personas que aparentemente son parientes (hermanos), implicando un vínculo personal.
4. Conectividad: Conexión adecuada.
5. Información de Red y DNS: Varias subredes, al igual muchos servicios varios. Dentro de los subdominios se encuentran contactos con el personal.
6. Información de puertos, servicios y sistema operativo
7. Puertos y servicios:A pesar de lo que dice la aproximación de SO, tcpwrapper es un protocolo usado en distribuciones GNU/Linux.

6.4 gob.mx

No hay dirección IP en un servidor DNS autorativo.

7. Presentación de Propuestas de Ataque

En base a la información obtenida mediante el script desarrollado, es posible formular distintas propuestas de ataque. La recopilación de datos como direcciones IP, nombres de dominio, subdominios, información WHOIS, estado de puertos abiertos y servicios en ejecución nos permite analizar posibles vectores de ataque y evaluar la seguridad del sistema objetivo.

7.1 Análisis de Infraestructura y Explotación de Servicios

La información recolectada con **whois**, **nslookup** y **ping** nos permite identificar datos clave de la infraestructura del objetivo:

- **Puertos abiertos y servicios activos**: Usando **nmap**, podemos conocer qué servicios están expuestos y evaluar vulnerabilidades conocidas en ellos.
- **Versiones de software**: Si se encuentran versiones desactualizadas o vulnerables, se pueden explotar con exploits públicos.
- **Reconocimiento del sistema operativo**: La detección de detalles del sistema con **nmap -O** ayuda a planificar ataques específicos.

7.2 Ingeniería Social y Phishing

Si el script logra recopilar información de correos electrónicos mediante **whois**, es posible diseñar ataques de ingeniería social, como:

- **Ataques de phishing**: Envío de correos electrónicos falsificados suplantando servicios legítimos.
- **Ataques de spear phishing**: Enfocados en personas específicas con información obtenida en la fase de recolección.
- **Recopilación de credenciales**: Intentos de obtención de acceso con ataques de fuerza bruta o ingeniería social.

7.3 Ataques a DNS y Subdominios

El uso de herramientas como **dnsmap** y **dnsrecon** permite identificar subdominios que pueden ser objetivos de ataque:

- **Subdominios expuestos**: Si un subdominio apunta a un servicio sin protección, se podría explotar.
- **Ataques de envenenamiento de caché DNS**: Manipulación de respuestas DNS para redirigir a usuarios a sitios maliciosos.

7.4 Denegación de Servicio (DoS/DDoS)

Si la latencia de la red es alta o hay sistemas críticos con puertos abiertos, se podrían llevar a cabo ataques de denegación de servicio:

- **Saturación de peticiones con ping (Ping Flood)**.
- **Ataques SYN Flood a servicios detectados en puertos abiertos**.

8. Preguntas de Pentesting: Recopilación de Información

8.1 Menciona los tipos de protocolos de red. ¿Cómo funcionan? ¿Para qué sirven?

Los protocolos de red se pueden clasificar en diferentes capas del modelo TCP, 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)

8.2 ¿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.

8.3 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.

8.4 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.

8.5 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.

8.6 ¿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.

8.7 ¿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.

8.8 ¿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.

8.9 ¿Crees que tus métodos preventivos son suficientes?

Ningun sistema es completamente seguro, por lo que siempre se pueden mejorar las medidas preventivas. Algunas acciones adicionales para fortalecer la seguridad incluyen:

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