**Laboratorio**
**FUNDAMENTOS DE CIBERSEGURIDAD**
Profesor: Juan Ignacio Iturbe A.

# Laboratorio 2. Escaneo

## 1. Introducción

En el escaneo y enumeración, los profesionales de seguridad toman la información que recopilaron en el reconocimiento para aplicar activamente herramientas y técnicas para recopilar información más detallada sobre los objetivos. Esto puede ser algo tan simple como ejecutar un barrido de ping o un mapeador de red para ver qué sistemas hay en la red, o tan complejo como ejecutar un escáner de vulnerabilidades para determinar qué puertos pueden estar abiertos en un sistema en particular. Por ejemplo, mientras que en el reconocimiento puede haber mostrado que la red tiene más o menos 500 máquinas conectadas a una única subred dentro de un edificio, el escaneo y la enumeración le dirán cuáles son máquinas de Windows y cuáles ejecutan FTP.

Los expertos conocen docenas de técnicas de sondeo/escaneo y eligen la más apropiada (o una combinación de éstas) para la tarea que están realizando. Los usuarios sin experiencia y los "script kiddies", sin embargo, intentan resolver cada problema con el sondeo SYN por omisión. Dado que Nmap es libre, la única barrera que existe para ser un experto en el sondeo de puertos es el conocimiento[1].

La mayoría de los distintos tipos de sondeo disponibles sólo los puede llevar a cabo un usuario privilegiado. Esto es debido a que envían y reciben paquetes en crudo, lo que hace necesario tener acceso como administrador (root) en la mayoría de los sistemas UNIX. En los entornos Windows es recomendable utilizar una cuenta de administrador, aunque Nmap algunas veces funciona para usuarios no privilegiados en aquellas plataformas donde ya se haya instalado WinPcap. [2]

## 2. Escenario

La empresa BooN lo ha contratado para realizar un test de penetración de caja negra de sus instalaciones en Chile. La máquina objetivo es scanme.nmap.org[3]

[1] Expanda su conocimiento en https://nmap.org/man/es/man-port-scanning-techniques.html
[2] El presente texto introductorio es una traducción libre de un extracto del libro de Walker, Matt. CEH Certified Ethical Hacker All-in-One Exam Guide, Fourth Edition. McGraw-Hill Education.
[3] Revisar http://scanme.nmap.org/

## 3. Instrucciones generales

a. Se debe realizar una presentación del laboratorio en video.
b. No más de 20 minutos.
c. Se requieren pantallazos y ejemplos en tiempo real que den evidencia de cada paso desarrollado.
d. Los mismos grupos de la cátedra.
e. La entrega del video se hace a través del foro social y debe quedar disponible para todos sus compañeros del curso durante todo el semestre.

## 4. Etapas del desarrollo:

### 4.1 Escaneo

a. Identificar todas las conexiones y puertos de escucha de su máquina con las direcciones y los números de puerto en forma numérica.
b. Identifica en su máquina los procesos vinculados a los puertos identificados y cierre aquellos procesos que no son imprescindibles para el desarrollo del presente laboratorio.
c. Encender wireshark y comenzar a escuchar el tráfico de la red.
d. Identificar cuál es su IP.
e. Utilizar un solo paquete ICMP tipo 8 (Request) para comprobar la conectividad a través de una respuesta tipo 0 (Eco) con la dirección IP 8.8.8.8.
f. Escanee el rango de IP de su casa (sea sigiloso).
g. Escanee el objetivo e identifique (recordar mezclar opciones):
    i. Puertos TCP y UDP utilizados
    ii. Estado de los puertos (abiertos o filtrados)
    iii. Sistema operativo utilizado
    iv. Versiones de los servicios (investigue)
h. Investigue vulnerabilidades sobre las versiones de los servicios encontrados[4]. Profundice en una de las vulnerabilidades encontradas.
i. Realice un escaneo *Full connect* sobre uno de los servicios TCP e identifique el handshake TCP de 3 vías realizado con wireshark.
j. Realice un escaneo *XMAS* sobre uno de los servicios TCP e identifique el segmento con los flags activados con wireshark.
k. Compare los tráficos generados (Teoría y wireshark) por los diferentes tipos de escaneos (*Full connect, Stealth y XMAS)*.
l. En wireshark compare la cantidad de paquetes enviados y recibidos por cada uno de los tipos de escaneos ( pregunta k)

[4] Existen sitios especializados para esto, por ejemplo: https://cve.mitre.org

**4.2 Investigue**

- ¿Qué es la enumeración? ¿En que se diferencia con el escaneo?
- Analice y describa el uso de otras herramientas de escaneo y enumeracion (Existen varias en Kali Linux). Por lo menos una de escaneo y otra de enumeracion.
- Aplique dichas herramientas en un ejemplo en la red de su hogar.

**Rúbrica**

| **Descripción** | **Puntaje** |
|---|---|
| Presenta introducción | 40 |
| Identifica todas las conexiones y puertos de escucha de su máquina e identifica en su máquina los procesos vinculados a dichos puertos | 20 |
| Utiliza wireshark para presentar evidencia | 30 |
| Utilizar un solo paquete ICMP tipo 8 (Request) para comprobar la conectividad a través de una respuesta tipo 0 (Eco) con la dirección IP 8.8.8.8. | 10 |
| Utiliza opciones de sigilo para escanear las IP's de su casa | 10 |
| Escanea el objetivo e identifica lo solicitado | 20 |
| Investiga vulnerabilidades sobre las versiones de los servicios encontrados | 30 |
| Realiza un escaneo *Full connect* sobre uno de los servicios TCP e identifique el handshake TCP de 3 vías realizado con wireshark. | 30 |
| Realiza un escaneo *XMAS* sobre uno de los servicios TCP e identifique el segmento con los flags activados con wireshark | 30 |
| Compara los tráficos generados por los diferentes tipos de escaneos (*Full connect, Stealth y XMAS*). | 30 |
| En wireshark filtre los paquetes enviados con su IP de origen e indique el número de paquetes enviados desde su máquina. | 30 |
| Indica una correcta definición de enumeración y resalta sus diferencias con el escaneo. | 40 |
| Analiza y describe el uso de otras herramientas de escaneo y enumeracion. | 30 |

| | |
|---|---|
| Investiga otras herramientas de enumeracion y escaneo y entrega un ejemplo de cada una | 40 |
| Desarrolla conclusión de acuerdo a los resultados obtenidos. Indica cómo se consiguieron cada uno de los objetivos y evidencia asociada. | 40 |
| Incluye bibliografía | 20 |
| Incluye evidencia que sustenta la información obtenida. | 30 |
| Se respeta el tiempo de la presentación (15 a 20 minutos máximo, entre la introducción, desarrollo y conclusión). | 10 |
| Cada integrante del grupo presenta de forma proporcional al tiempo. | 10 |
| Se indica el integrante del grupo que está hablando en cada momento. | 10 |
| El video presenta esquemas y figuras de acuerdo al contenido. | 10 |
| El audio del video es claro. | 10 |
| Forma: Hace un buen balance entre el texto, imágenes y videos presentados | 30 |