# Tema 9.9.3.8.EnriqueGomezTagle

martes, 27 de febrero de 2024 21:27

Enrique Ulises Báez Gómez Tagle – 0241823 - 0241823@up.edu.mx
UP. 2024. Ene-Jun. Hackeo Ético y Recuperación Ante Desastres – Yoel Ledo Mezquita

**Parte 1: Explorar Nmap**

En esta parte utilizará páginas del manual (o páginas man para abreviar) para saber más sobre Nmap.

El comando **man** [ *programa* |*utilidad* | *función*] muestra las páginas del manual asociadas con los argumentos. Las páginas de manuales son los manuales de referencia de los SO Unix y Linux. Estas páginas pueden tener las siguientes secciones, entre otras: Nombre, Sinopsis, Descripciones, Ejemplos y Ver también.

a. Inicie la VM CyberOps Workstation.

b. Abra un terminal.

c. En el cursor del terminal, introduzcan **man nmap**.

```
[analyst@secOps ~]$ man nmap
```

¿Qué es Nmap?

Nmap es una herramienta de exploracion de red y escaneo de seguridad/puertos.

¿Para qué se utiliza Nmap?

Escanear una red y determinar los hosts y servicios ofrecidos en la red.

---

Mire el Ejemplo 1.

¿Cuál es el comando de **nmap** que se utilizó?

nmap -a T4 scanme.nmap.org

Utilice la función de búsqueda para responder las siguientes preguntas.

¿Qué hace el switch -A?

-A: habilitar la detección del OS, detección de versión, escaneo de scripts y traceroute.

¿Qué hace el switch -T4?

-T4: para ejecución más rápida al probar que el retraso dinámico supere los 10ms para los puertos TCP

b. Revisen los resultados y respondan las siguientes preguntas.

¿Qué puertos y servicios están abiertos?

21 TCP:FTP 22 TCP: ssh

Para cada uno de los puertos abiertos, registren el software que está proporcionando los servicios.

FTP: vsftpd SSH: OpenSSH

¿A qué red pertenecen sus VM?

VM: 192.168.1.19/24

Red: 192.168.1.0/24

¿Cuántos hosts están activos?

Desde sus resultados de Nmap, generen una lista de las direcciones IP de los hosts que se encuentran en la misma red LAN que sus VM. Generen una lista de los servicios que están disponibles en los hosts detectados.

**Paso 3: Escanear un servidor remoto**

a. Abra un navegador web y diríjanse a **scanme.nmap.org**. Lea el mensaje en pantalla.

¿Cuál es el propósito de este sitio?

Permite a los usuarios conocer Nmap y su instalacion

c. Revise los resultados y responda las siguientes preguntas.

¿Qué puertos y servicios están abiertos?

22/TCP:ssh 9929 TCP: nping-echo, 31337 TCP tcpwrapped 80/TCP: HTTP

¿Qué puertos y servicios están filtrados?

135 TCP: msrpc 139 TCP netbios-ssn 445 TCP - Microsoft ds 25 TCP - smtp

¿Cuál es la dirección IP del servidor?

45.33.32.156 2600:3c01::f03c:91ff:fe18:bb2f

¿Cuál es el sistema operativo?

Linux Ubuntu

**Pregunta de reflexión**

Nmap es una poderosa herramienta para la exploración y administración de redes. ¿Qué beneficios puede aportar Nmap a la seguridad de la red? ¿De qué manera un atacante puede utilizar Nmap como herramienta maliciosa?

Escanear red interna para buscar puertos abiertos específicos por ver violación de seguridad.

Se puede utilizar para reconocimiento de puertos abiertos
de red.