Actividad 3 – Módulo 2

Introducción a Nmap

Diego Mucci

08/05/2024

Seguridad Informática

Instalación y Uso Básico de Nmap en Windows, Linux y macOS

Introducción a Nmap

Nmap (Network Mapper) es una herramienta de código abierto utilizada para exploración de red y auditoría de seguridad. Nmap permite a los administradores identificar qué dispositivos están ejecutándose en sus redes, descubrir hosts disponibles, los servicios que ofrecen, los sistemas operativos que utilizan, y otras características. Es ampliamente utilizado por profesionales de la seguridad informática para evaluar la exposición de redes ante ataques maliciosos.

Objetivo de la Actividad

El objetivo de esta actividad es familiarizarse con la instalación de Nmap en Windows, Linux y macOS y aprendan a realizar escaneos básicos de red. Desarrollaremos habilidades prácticas para identificar y analizar los servicios que se ejecutan en los dispositivos dentro de una red simulada.

Pasos de la Actividad

1. **Instalación de Nmap:**

- Windows:
    - Descargar el instalador de Nmap desde nmap.org e instalarlo, incluyendo la interfaz gráfica Zenmap si se desea.

- Linux:
    - Instalar Nmap utilizando el gestor de paquetes de la distribución, por ejemplo, sudo apt install nmap para Debian/Ubuntu o sudo yum install nmap para CentOS/Fedora.

- macOS:
    - Instalar Homebrew si aún no está instalado, utilizando el comando:

      /bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"

- Instalar Nmap mediante Homebrew con el comando:
    - brew install nmap

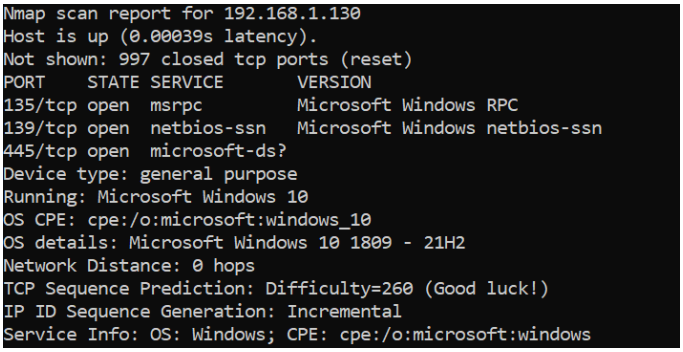
2. **Exploración Básica con Nmap:**

- Abrir la terminal o línea de comandos dependiendo del sistema operativo.

- Ejecutar un escaneo básico en la red local para identificar dispositivos activos, usando el comando: nmap -sn 192.168.x.0/24 (reemplazar x con el número de red apropiado).

Los dos dispositivos activos son mi router y mi ordenador personal.

- Realizar un escaneo de puertos en un host específico utilizando: nmap -v -A 192.168.x.y (reemplazar x.y con la dirección IP específica).



Los puertos que se han encontrado abiertos en mi ordenador personal han sido:

- Puerto 135/TCP: en un escaneo indica que el servicio MSRPC (Microsoft Remote Procedure Call) está en funcionamiento en el sistema objetivo. MSRPC es un mecanismo utilizado por los sistemas operativos Windows para permitir la comunicación entre procesos en redes distribuidas. Este servicio facilita la ejecución de funciones o procedimientos en sistemas remotos, lo que permite a las aplicaciones interactuar y compartir recursos en una red.
  No obstante, es importante destacar que el servicio MSRPC también puede ser un objetivo para ataques, ya que algunas vulnerabilidades pueden ser explotadas a través de este protocolo. Por lo tanto, es fundamental asegurarse de que los sistemas que ejecutan este servicio estén debidamente parcheados y protegidos para evitar posibles riesgos de seguridad.

- Puerto 139/ TCP en un escaneo indica que el servicio "netbios-ssn" está en funcionamiento en el sistema objetivo. Este puerto es utilizado por el protocolo NetBIOS (Network Basic Input/Output System) para proporcionar servicios de sesión sobre TCP/IP en sistemas operativos Windows. El servicio NetBIOS permite

a los sistemas en una red compartir recursos, como archivos e impresoras, y también facilita la comunicación entre sistemas. Sin embargo, debido a que NetBIOS es un protocolo antiguo y tiene varias vulnerabilidades de seguridad conocidas, es importante asegurarse de que los sistemas que ejecutan este servicio estén adecuadamente protegidos y configurados para evitar posibles riesgos de seguridad, como la exposición a ataques de denegación de servicio o acceso no autorizado.

- Puerto 445/TCP en un escaneo indica que el servicio "microsoft-ds" está en funcionamiento en el sistema objetivo. Este servicio está asociado con el protocolo SMB (Server Message Block), que es utilizado por los sistemas operativos Windows para compartir archivos, impresoras y otros recursos en una red.

  Como hemos visto el puerto 139 también se usa para este propósito, pero la ventaja de usar el puerto 445 es que es más seguro, ya que permite la comunicación segura sobre redes IP. Aun así, como ocurre con cualquier servicio expuesto en la red, es importante asegurarse de que el servicio "microsoft-ds" esté configurado de manera segura y se apliquen las últimas actualizaciones de seguridad para evitar posibles explotaciones de vulnerabilidades conocidas.

3. Tareas Avanzadas:

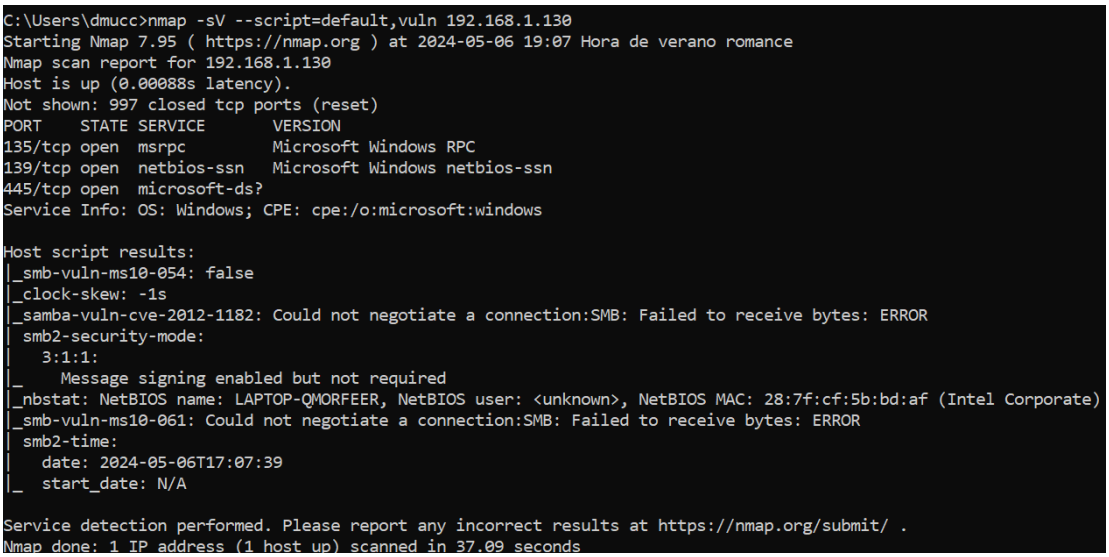
- Identificar el sistema operativo de los dispositivos en la red con: nmap -O 192.168.x.y

```
C:\Users\dmucc>nmap -O 192.168.1.130
Starting Nmap 7.95 ( https://nmap.org ) at 2024-05-06 19:06 Hora de verano romance
Nmap scan report for 192.168.1.130
Host is up (0.00081s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 21H2
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds
```

Resultado del sistema operativo : Windows 10

- Realizar un escaneo detallado utilizando scripts de Nmap para obtener información adicional sobre servicios específicos: nmap -sV --script=default,vuln 192.168.x.y



El resumen del escaneo sería:

- smb-vuln-ms10-054: Esta vulnerabilidad no está presente en el host (false).
- clock-skew: El desajuste del reloj se reporta como -1 segundo.
- samba-vuln-cve-2012-1182: El script encontró un error al intentar negociar una conexión para verificar esta vulnerabilidad.
- smb2-security-mode: La firma de mensajes está habilitada pero no es obligatoria.
- nbstat: Proporciona información de NetBIOS, incluido el nombre de NetBIOS de la máquina, el usuario de NetBIOS (si está disponible) y la dirección MAC asociada con el nombre de NetBIOS.
- smb-vuln-ms10-061: Similar a CVE-2012-1182, se produjo un error al intentar negociar una conexión para verificar la vulnerabilidad MS10-061.
- smb2-time: Informa la fecha y hora actuales (2024-05-06 T 17:07:39). Sin embargo, la fecha de inicio no está disponible.

Según estos resultados, parece que podría haber algunos problemas al negociar conexiones para ciertas verificaciones de vulnerabilidades, pero no se reportan vulnerabilidades activas en los resultados proporcionados.

Conclsusión

El uso de Nmap es fundamental para la evaluación y el fortalecimiento de la seguridad de redes. Esta herramienta versátil y potente permite a los administradores de sistemas y profesionales de seguridad identificar dispositivos activos en una red, mapear su topología, descubrir servicios en ejecución y detectar posibles vulnerabilidades. Al proporcionar una visión detallada del panorama de la red, Nmap ayuda a tomar decisiones informadas sobre políticas de seguridad, configuración de firewalls y parcheo de sistemas. Sin embargo, es importante utilizar Nmap de manera ética y legal, respetando la privacidad y los derechos de los propietarios de los sistemas escaneados.

Buen trabajo

10/10