Manual de uso de Nmap

AVH04

https://github.com/AVH07

¿Qué es Nmap?

Nmap (Network Mapper) es una herramienta avanzada para la exploración y auditoría de seguridad en redes TCP/IP. Permite escanear equipos individuales o redes extensas de forma rápida, eficiente y discreta, proporcionando información detallada sobre los sistemas analizados.

¿Para qué sirve Nmap?

- Detectar equipos activos en una red.
- Evaluar la seguridad y detectar vulnerabilidades en redes o equipos.
- Identificar servicios y sus versiones en servidores.
- Determinar el sistema operativo de los equipos analizados.
- Verificar la efectividad de cortafuegos e IDS/IPS.
- Identificar cambios en una red mediante escaneos periódicos.
- Supervisar la disponibilidad de servicios y servidores.
- Realizar auditorías de seguridad informática, tanto internas como externas.

¿Dónde usar Nmap?

- Entornos corporativos para la protección de redes internas y externas.
- Auditorías periódicas de seguridad informática.
- Instituciones educativas para prácticas de ciberseguridad.

- Análisis forense digital para la detección de vulnerabilidades.
- Organismos gubernamentales para el resguardo de la seguridad nacional.

Instalación

- Linux: Se puede instalar desde código fuente o mediante paquetes (RPM, DEB).
- Windows: Se instala mediante el instalador oficial, que incluye Zenmap (interfaz gráfica).

Comandos básicos y avanzados de Nmap:

- Descubrir equipos activos:

```
nmap -sn 192.168.1.0/24
```

- Escaneo TCP SYN (rápido y sigiloso):

```
nmap -sS 192.168.1.10
```

- Escaneo TCP completo:

```
nmap -sT 192.168.1.10
```

- Escaneo UDP:

```
nmap -sU 192.168.1.10
```

- Identificación del sistema operativo:

```
nmap -O 192.168.1.10
```

- Escaneo agresivo (sistema operativo, servicios y scripts):

```
nmap -A 192.168.1.10
```

- Guardar resultados en archivo:

```
nmap -oN resultados.txt 192.168.1.10
```

- Escaneo completo y silencioso:

```
nmap -p- -T4 -Pn -sV --version-intensity 5 192.168.1.10
```

- Ejecutar scripts específicos:

```
nmap --script=http-enum 192.168.1.10
```

- Escaneo para evasión de detección:
  - Señuelos para ocultar IP origen:

    ```
    nmap -D RND:10 192.168.1.10
    ```

  - Fragmentación de paquetes:

    ```
    nmap -f 192.168.1.10
    ```

  - Intervalos aleatorios entre paquetes:

    ```
    nmap --scan-delay 5s 192.168.1.10
    ```

- Escaneo de puertos específicos:

```
nmap -p 22,80,443 192.168.1.10
```

- Detección detallada de versiones:

```
nmap -sV -version-all 192.168.1.10
```

- Comparar cambios en la red con Ndiff:

```
ndiff scan-antes.xml scan-actual.xml
```

Usos reales de Nmap en la vida

- Identificar dispositivos no autorizados en redes corporativas.
- Detectar vulnerabilidades en servidores web previo a auditorías externas.

- Monitorear la disponibilidad de servicios críticos como servidores web y bases de datos.
- Identificar vulnerabilidades de seguridad en sistemas de proveedores.
- Realizar auditorías de cumplimiento normativo (PCI DSS, ISO 27001).
- Evaluar y asegurar la infraestructura tecnológica antes de eventos críticos.

Uso de Zenmap:

Zenmap es la interfaz gráfica de Nmap que simplifica su uso. Ofrece perfiles predefinidos, visualización gráfica de resultados, almacenamiento de históricos, generación de reportes y personalización sencilla de escaneos.

Este manual proporciona una guía detallada para entender y usar Nmap eficazmente en distintos escenarios reales, mejorando así la seguridad y el rendimiento de la infraestructura tecnológica.