Manual Avanzado de Uso de Nmap

AVH04

https://github.com/AVH04

Introducción avanzada a Nmap

Nmap (Network Mapper) es una herramienta de código abierto para auditoría y exploración de redes que permite descubrir hosts activos, servicios, versiones de software, sistemas operativos y vulnerabilidades de seguridad mediante técnicas avanzadas de escaneo TCP/IP.

Capacidades Avanzadas de Nmap

Nmap es capaz de realizar:

- Descubrimiento detallado y discreto de redes.
- Escaneos profundos para identificar sistemas operativos (OS fingerprinting).
- Ejecución de scripts personalizados mediante Nmap Scripting Engine (NSE).
- Detección e identificación de vulnerabilidades específicas.
- Técnicas para evadir sistemas de detección de intrusiones (IDS/IPS).
- Escaneos en redes IPv4 e IPv6.

Escenarios Avanzados de Aplicación

- Pruebas de penetración y hacking ético.

- Auditorías de cumplimiento normativo (ISO 27001, PCI DSS).
- Investigación y análisis forense digital.
- Evaluación de seguridad perimetral y controles de acceso.
- Monitoreo continuo de seguridad en infraestructura crítica.

Técnicas Avanzadas de Instalación y Configuración

- Compilación personalizada del código fuente en entornos Linux, incluyendo soporte para SSL/TLS y otras bibliotecas.
- Configuración optimizada en entornos Windows para mejorar el rendimiento mediante scripts y ajustes del sistema.

Comandos avanzados y ejemplos de uso:

- Escaneo TCP SYN sigiloso con evasión de IDS:

```
nmap -sS -Pn -f --data-length 25 -T paranoid 192.168.1.10
```

- Identificación precisa de sistemas operativos:

```
nmap -O --osscan-limit --osscan-guess 192.168.1.0/24
```

- Escaneo detallado de versiones con scripts NSE:

```
nmap -sV --script="vuln and safe" --script-timeout=30m 192.168.1.10
```

- Escaneo UDP de alto rendimiento:

```
nmap -sU --max-retries 5 --min-rate 5000 -p- 192.168.1.10
```

- Detección de vulnerabilidades específicas:

```
nmap --script ssl-heartbleed,ftp-anon,http-shellshock 192.168.1.10
```

- Escaneo completo en IPv6:

`nmap -6 -A -T4 ipv6-host-address`

- Técnicas de evasión con señuelos:

`nmap -D 192.168.0.1,10.0.0.1,RND:5 -Pn 192.168.1.10`

- Creación de perfiles personalizados en Zenmap para auditorías recurrentes.

Uso Avanzado del Nmap Scripting Engine (NSE)
El NSE permite realizar tareas avanzadas personalizadas:

- Identificación precisa de vulnerabilidades críticas específicas.
- Automatización eficiente de tareas repetitivas en auditorías de seguridad.
- Scripts personalizados para la detección de malware y puertas traseras.
- Integración con herramientas externas para generar reportes automáticos y alertas en tiempo real.

Ejemplo de ejecución avanzada NSE:

`nmap --script="discovery,vuln,auth" --script-args=unsafe=1 -T4 192.168.1.0/24`

Uso avanzado de Zenmap
Zenmap ofrece una interfaz gráfica que facilita la gestión y el análisis avanzado de escaneos:

- Visualización gráfica detallada de la topología de red.
- Gestión y comparación de resultados históricos mediante Ndiff.
- Perfiles de escaneo personalizados para optimizar los procesos de auditoría.

Este manual está dirigido a expertos en seguridad informática, auditores de sistemas, administradores de redes y profesionales que necesitan realizar análisis exhaustivos de infraestructuras tecnológicas. Proporciona técnicas efectivas para garantizar la máxima seguridad y eficiencia operativa.