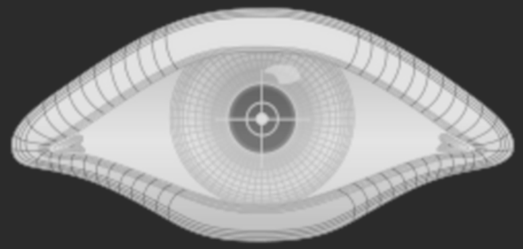

COMANDOS BÁSICOS DE NMAP

NMAP

#6

Escaneo de Red Completa (-sn)

- Comando: **nmap -sn <objetivo/rango de red>**
- Propósito: Este escaneo realiza una exploración de hosts activos en una red sin realizar un escaneo de puertos. Es útil para identificar qué dispositivos están presentes y responden en la red.

#1

Escaneo de Puertos TCP (-sS)

- *Comando: **nmap -sS <objetivo>***
- *Propósito: Este es uno de los escaneos más comunes. Utiliza un escaneo de tipo SYN para determinar qué puertos están abiertos en el objetivo. Es rápido y menos intrusivo, ya que no establece completamente una conexión.*

#5

Escaneo Agresivo (-A)

- Comando: **nmap -A <objetivo>**
- Propósito: Este escaneo combina varias técnicas, incluyendo detección de sistema operativo, detección de versiones de servicios, detección de scripts y más. Proporciona una visión integral del objetivo.

#2

Escaneo de Puertos UDP (-sU)

- *Comando: **nmap -sU <objetivo>***
- *Propósito: Mientras que el escaneo TCP se centra en los puertos TCP, el escaneo UDP se utiliza para descubrir servicios que utilizan el protocolo UDP. Algunos servicios importantes, como el DNS y el DHCP, utilizan UDP.*

#4

Escaneo de Sistema Operativo (-O)

- Comando: **nmap -O <objetivo>**
- Propósito: Intenta identificar el sistema operativo del objetivo basándose en patrones de respuesta a través de las sondas enviadas. Proporciona información sobre la infraestructura de la red.

#3

Escaneo de Enumeración de Versiones (-sV)

- *Comando: **nmap -sV <objetivo>***
- *Propósito: Este escaneo busca determinar las versiones y los detalles de los servicios que se están ejecutando en los puertos abiertos. Proporciona información valiosa sobre posibles vulnerabilidades asociadas con versiones específicas de software.*

NMAP

#7

Escaneo de Puertos Específicos (-p)

- *Comando:* ***nmap -p puerto,<objetivo>***
- *Propósito: Este comando escanea únicamente los puertos específicos 80 y 443 en el host con la dirección IP 192.168.1.1.*

#8

Escaneo de Intensidad Moderada (-T3)

- *Comando:* ***nmap -T3 192.168.1.1***
- *Propósito: Este comando realiza un escaneo de intensidad moderada en el host con la dirección IP 192.168.1.1. La opción -T3 ajusta la velocidad de escaneo para equilibrar la velocidad con la intrusión.*

#9

Escaneo de Intensidad Agresiva (-T4)

- *Comando:* ***nmap -T4 192.168.1.1***
- *Propósito: Este comando realiza un escaneo de intensidad agresiva en el host con la dirección IP 192.168.1.1. La opción -T4 aumenta la velocidad de escaneo y la intrusión.*

#10

Escaneo de Intensidad Insana (-T5)

- *Comando:* ***nmap -T5 192.168.1.1***
- *Propósito: Este comando realiza un escaneo de intensidad máxima (insana) en el host con la dirección IP 192.168.1.1. La opción -T5 aumenta la velocidad al máximo, pero puede ser más intrusiva y llamar la atención.*

ESCANEO DE VULNERABILIDADES CON NMAP

Escaneo de Vulnerabilidades Básico (-sV --script vuln)

- *Comando:* ***nmap -sV --script vuln <objetivo>***
- *Propósito: Este comando realiza un escaneo de vulnerabilidades básico utilizando scripts de detección de vulnerabilidades disponibles en la base de datos de scripts de Nmap. Identifica posibles vulnerabilidades en los servicios en ejecución en el objetivo.*


```
root@kali:~# nmap --script  vuln -p139,445 192.168.0.18
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-25 20:58 CDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.18
Host is up (0.0017s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 39.49 seconds
root@kali:~#
```

COMANDOS BASICOS DE NMAP GITHUB

COMANDOS METASPLOIT

METASPLOIT

#1

msfconsole:

- *Inicia la interfaz de línea de comandos de Metasploit.*

#2

search <exploit/module> :

- *Busca exploits o módulos en la base de datos de Metasploit.*

#3

use <exploit/module> :

- *Selecciona un exploit o módulo específico para usar.*

#4

set <option> <value> :

- *Configura el valor de una opción específica para el exploit o módulo.*

#5

exploit :

- *Ejecuta el exploit con la configuración actual.*

OTROS COMANDOS DE METASPLOIT

#6

info :

- *Muestra información sobre el exploit o módulo seleccionado.*

#7

options :

- *Muestra y configura las opciones para el exploit o módulo seleccionado.*

#9

help :

- *Muestra la ayuda y los comandos disponibles en la consola de Metasploit.*

#8

show options :

- *Muestra las opciones disponibles para el payload seleccionado.*

COMANDOS METASPLOIT GITHUB