

# Fundamentos de Hardware.

## Herramienta Nmap.

Descripción, instalación y uso básico de la herramienta Nmap.

Mahesvara.

## **Descripción breve de la herramienta y sus funcionalidades principales.**

Nmap (Network Mapper) es una **herramienta de código abierto utilizada para exploración de redes y auditoría de seguridad**, diseñada para escanear rápidamente grandes redes, aunque también funciona eficazmente contra equipos individuales. Creada por Gordon Lyon (también conocido por su seudónimo Fyodor Vaskovich) en 1997.

- Principales funcionalidades:
- Descubrimiento de hosts en una red.
- Escaneo de puertos TCP y UDP.
- Detección de servicios y versiones.
- Detección de sistemas operativos (OS fingerprinting).
- Ejecución de scripts NSE(Nmap Scripting Engine) para detectar vulnerabilidades y configuraciones críticas.
- Escaneos sigilosos y evasión de firewalls.
- Generación de informes en diferentes formatos (XML, HTML, texto).

## **Requisitos técnicos.**

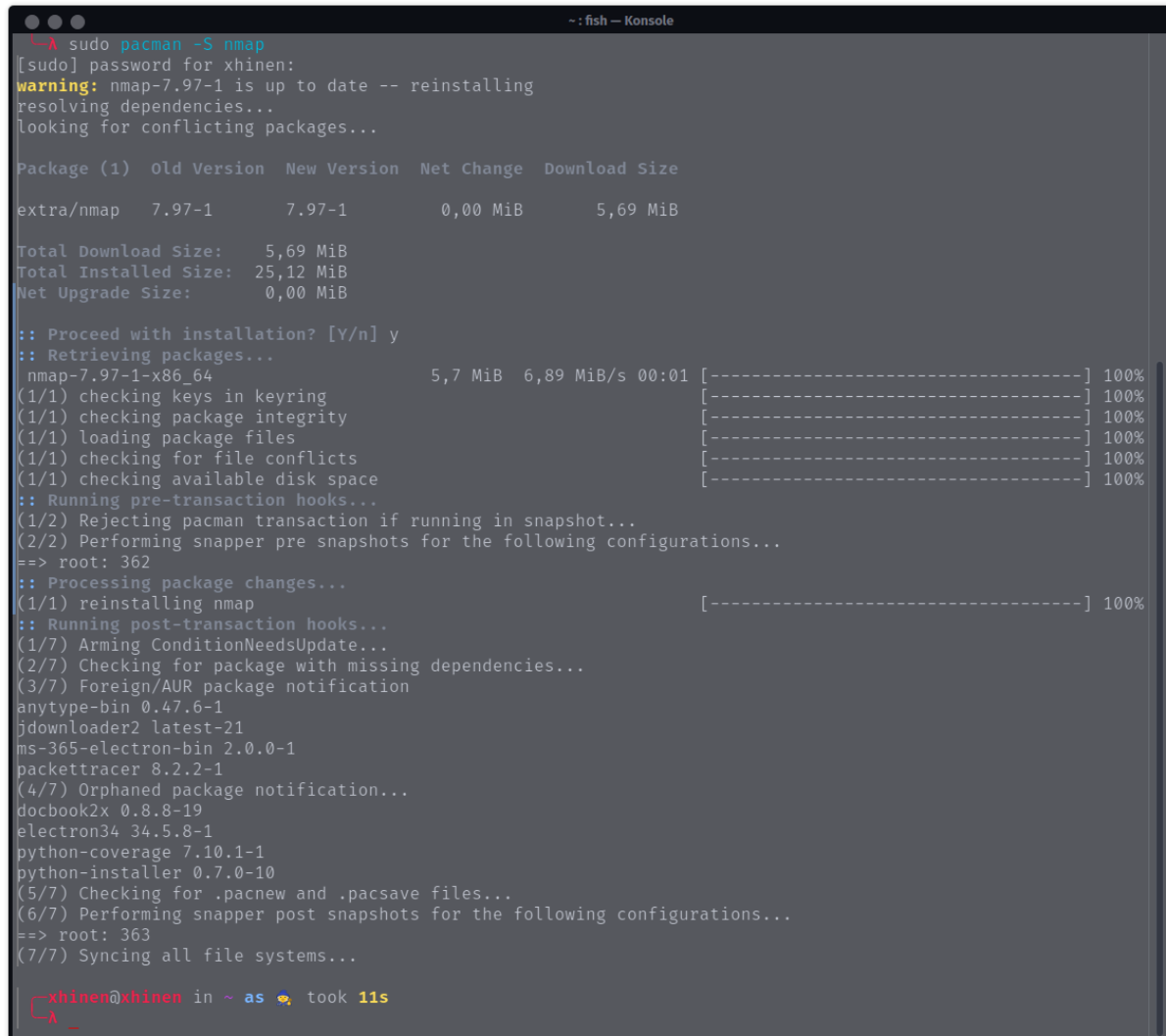
Nmap es una herramienta muy ligera por lo que sus requisitos de hardware son muy bajos.

- Es multiplataforma por lo que podemos encontrar en Linux, Windows, macOS y BSD.
- CPU 1Ghz o superior.
- RAM 512MB mínimo.
- Espacio necesario en disco de 100MB libres.
- Dependencias en Linux:
- Libpcap (para captura de paquetes).
- ncat, ndiff, nping (herramientas auxiliares incluidas).

## Proceso de instalación.

En mi caso la instalación es bastante sencilla en el sistema que uso (Garuda OS basado en Arch) aunque para la presentación de la práctica en el video usaré una máquina virtual Kali Linux en la que ya viene instalado de base y una Metasploitable 2 para hacer una simulación simple de pentesting.

Simplemente abrimos la terminal (ctrl + alt + t) y ejecutamos el siguiente comando ***sudo pacman -S nmap***, confirmamos su instalación y en unos segundos estará instalado.



```
~ : fish — Konsole
λ sudo pacman -S nmap
[sudo] password for xhinen:
warning: nmap-7.97-1 is up to date -- reinstalling
resolving dependencies...
looking for conflicting packages...

Package (1)  Old Version  New Version  Net Change  Download Size
extra/nmap   7.97-1       7.97-1       0,00 MiB    5,69 MiB

Total Download Size:    5,69 MiB
Total Installed Size:  25,12 MiB
Net Upgrade Size:       0,00 MiB

:: Proceed with installation? [y/n] y
:: Retrieving packages...
nmap-7.97-1-x86_64               5,7 MiB   6,89 MiB/s   00:01 [-----] 100%
(1/1) checking keys in keyring [-----] 100%
(1/1) checking package integrity [-----] 100%
(1/1) loading package files     [-----] 100%
(1/1) checking for file conflicts [-----] 100%
(1/1) checking available disk space [-----] 100%
:: Running pre-transaction hooks...
(1/2) Rejecting pacman transaction if running in snapshot...
(2/2) Performing snapper pre snapshots for the following configurations...
==> root: 362
:: Processing package changes...
(1/1) reinstalling nmap [-----] 100%
:: Running post-transaction hooks...
(1/7) Arming ConditionNeedsUpdate...
(2/7) Checking for package with missing dependencies...
(3/7) Foreign/AUR package notification
anytype-bin 0.47.6-1
jdownloader2 latest-21
ms-365-electron-bin 2.0.0-1
packettracer 8.2.2-1
(4/7) Orphaned package notification...
docbook2x 0.8.8-19
electron34 34.5.8-1
python-coverage 7.10.1-1
python-installer 0.7.0-10
(5/7) Checking for .pacnew and .pacsave files...
(6/7) Performing snapper post snapshots for the following configurations...
==> root: 363
(7/7) Syncing all file systems...

xhinen@xhinen in ~ as 🔌 took 11s
λ _
```

## Conclusión.

Nmap es una herramienta simple y fácil de usar (para ser usada en terminal por lo menos en Linux en Windows nunca la he usada, dios me salve xD) con la que podremos realizar monitorias de/en un entorno de red y localizar posibles vulnerabilidades en sus servicios ya bien sea por que no estén actualizadas o estén mal configuradas.

## **Comandos kali**

**Ver la configuracion de red de la kali y en la metasploitable para comprobar las ip's**

Ifconfig

**Hacemos ping a la máquina metasploitable**

ping 192.168.29.129

**Escaneamos la red en busca de los equipos y comprobamos que aparece la maquina metasploitable**

sudo nmap 192.168.29.\*/24 -sn

**Escaneamos la maquina para ver los puertos, servicios habilitados con sus respectivas versiones y el sistema operativo que usa.**

sudo nmap 192.168.29.129 -sV -O

**Vamos a escanear vulnerabilidades del servicio FTP - Puerto 21 y 2121**

sudo nmap -p 21,2121 --script=ftp-anon,ftp-vsftpd-backdoor 192.168.129.29

ftp-anon – Verifica acceso anónimo (¡suele estar habilitado!).

ftp-vsftpd-backdoor – Detecta puerta trasera en vsFTPD 2.3.4 (vulnerabilidad muy conocida).

**Vamos a escanear vulnerabilidades del servicio SSH - Puerto 22**

sudo nmap -p 22 --script=ssh-hostkey,sshv1 192.168.129.29

ssh-hostkey – Muestra clave pública del servidor.

sshv1 – Verifica si soporta SSHv1 (obsoleto y vulnerable).

**Vamos a escanear vulnerabilidades del servicio Telnet - Puerto 23**

sudo nmap -p 23 --script=telnet-encryption,telnet-ntlm-info 192.168.129.29

telnet-encryption – Verifica si hay cifrado en Telnet (normalmente no lo hay).

telnet-ntlm-info – Extrae información si hay soporte NTLM.

### **Vamos a escanear vulnerabilidades del servicio SMTP - Puerto 25**

```
sudo nmap -p 25 --script=smtp-commands,smtp-open-relay,smtp-enum-users 192.168.129.29
```

smtp-open-relay – Verifica si se puede usar el servidor para enviar SPAM.

smtp-enum-users – Enumera usuarios (muy útil en Postfix vulnerables).

### **Vamos a escanear vulnerabilidades del servicio HTTP - Puerto 80 y 8180**

```
sudo nmap -p 80,8180 --script=http-enum,http-title,http-methods,http-vuln-cve2017-5638 192.168.129.29
```

http-enum – Enumera rutas comunes como /phpmyadmin, /test, etc.

http-title – Muestra títulos de las páginas web.

http-methods – Verifica si hay métodos HTTP peligrosos (como PUT, DELETE).

http-vuln\* – Scripts para detectar vulnerabilidades web conocidas.

### **Vamos a escanear vulnerabilidades del servicio RPC(Remote Procedure Call)/NFS(Network File System) - Puerto 111, 2049. Compartir recursos y ejecución remota.**

```
sudo nmap -p 111,2049 --script=rpcinfo,nfs-showmount,nfs-statfs 192.168.129.29
```

rpcinfo – Muestra servicios RPC activos.

nfs-showmount – Muestra sistemas de archivos exportados por NFS.

nfs-statfs – Da información sobre estos sistemas de archivos.

### **Vamos a escanear vulnerabilidades del servicio Samba/SMB (Server Message Block) - Puerto 139 y 445, sirve para compartir archivos e impresoras.**

```
sudo nmap -p 139,445 --script=smb-os-discovery,smb-enum-shares,smb-vuln-ms08-067,smb-vuln-ms17-010 192.168.129.29
```

smb-os-discovery – Muestra sistema operativo y nombre del host.

smb-enum-shares – Enumera recursos compartidos.

smb-vuln-ms08-067 – Detecta la famosa vulnerabilidad de RPC (¡exploitable!).

smb-vuln-ms17-010 – EternalBlue (WannaCry), confirmación de vulnerabilidad SMBv1.

### **Vamos a escanear vulnerabilidades del servicio MySQL - Puerto 3306**

```
sudo nmap -p 3306 --script=mysql-empty-password,mysql-users,mysql-info 192.168.129.29
```

mysql-empty-password – Verifica si hay usuarios sin contraseña.

mysql-users – Intenta enumerar usuarios (requiere credenciales si no está abierto).

mysql-info – Extrae información de versión y compilación.

### **Vamos a escanear vulnerabilidades del servicio PostgreSQL – Puerto 5432 Gestión de BBDD**

```
sudo nmap -p 5432 --script=pgsql-brute,pgsql-info 192.168.129.29
```

pgsql-brute – Ataque de fuerza bruta.

pgsql-info – Información del servidor PostgreSQL.

### **Vamos a escanear vulnerabilidades del servicio VNC (Virtual Network Computing) escritorio remoto - Puerto 5900**

```
sudo nmap -p 5900 --script=vnc-info,vnc-title,vnc-brute <IP>
```

vnc-info – Extrae versión del servidor.

vnc-title – Muestra el título de la ventana VNC (si está disponible).

vnc-brute – Fuerza bruta para contraseñas VNC.

### **Vamos a acceder con nc al Shell - Puerto 1524**

```
nc 192.168.29.129 1524
```