**HackTheBox – Blue**

Hack the Box Blue is a 10.10.10.40 Windows OS

I opened the terminal and ran nmap -T4 -p- -A 10.10.10.40

After it finished, I got the results:

Nmap scan report for 10.10.10.40

Host is up (0.10s latency).

Not shown: 65526 closed 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=7.70%E=4%D=11/9%OT=135%CT=1%CU=43753%PV=Y%DS=2%DC=T%G=Y%TM=5FA97E

OS:34%P=x86\_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS

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

OS:54DNW8ST11%O6=M54DST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=20

OS:00)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=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: 2m41s, deviation: 2s, median: 2m40s

| 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: 2020-11-09T17:39:25+00:00

| 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: 2020-11-09 12:39:26

|\_ start\_date: 2020-11-09 12:07:03

TRACEROUTE (using port 25/tcp)

HOP RTT ADDRESS

1 105.04 ms 10.10.14.1

2 105.14 ms 10.10.10.40

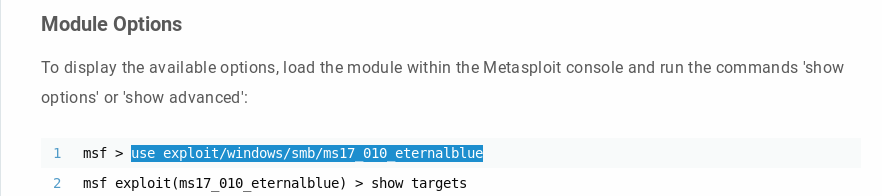
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 723.64 seconds

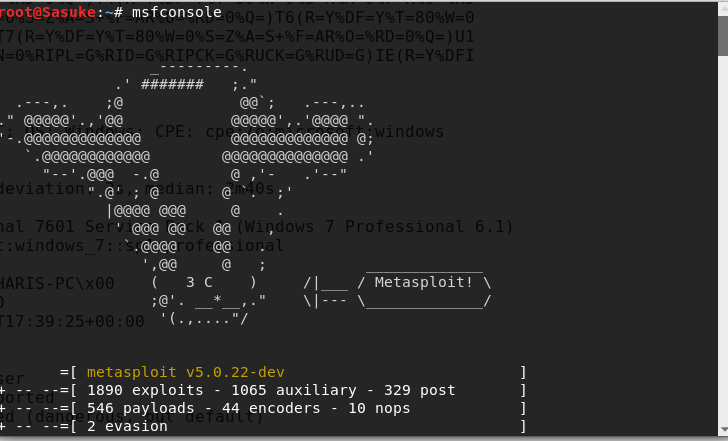
After scanning the above threats I found OS: Windows 7 Professional 7601 Service Pack 1

Under the smb vulnerability

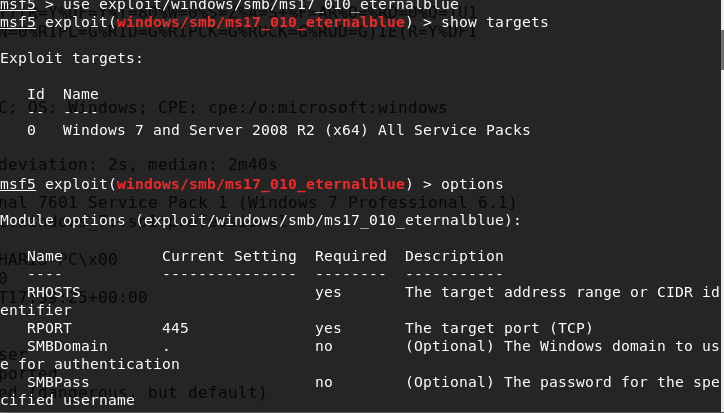
I then googled SMB OS: Windows 7 Professional 7601 Service Pack 1 exploit and found rapid7 website with the exploit



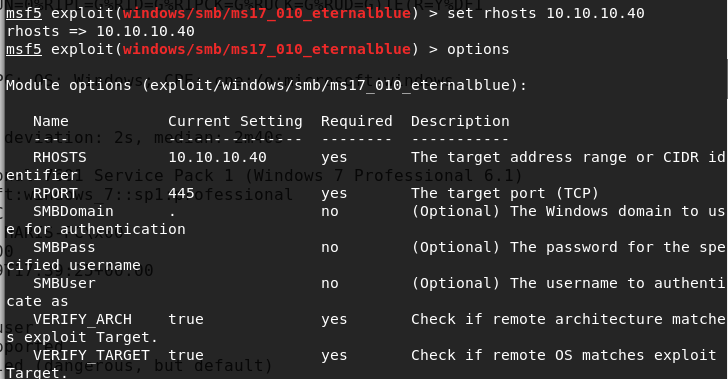
Once I got my exploit, I launched msfconsole



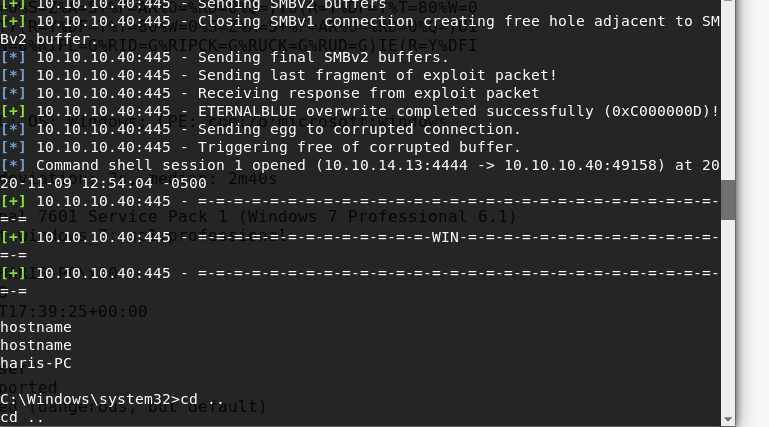
I then ran the commands below to check everything:



I had to set rhost to 10.10.10.40

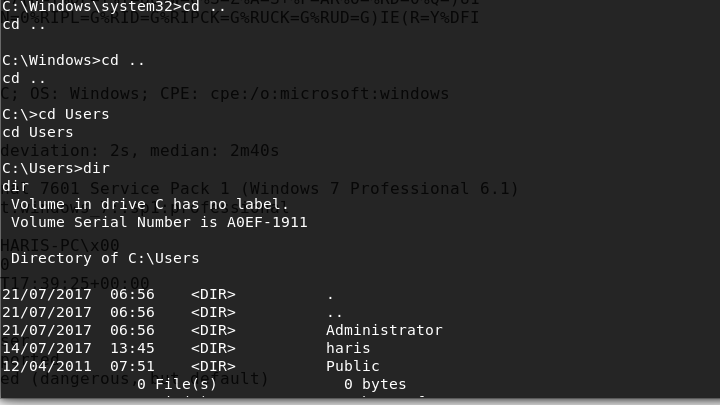


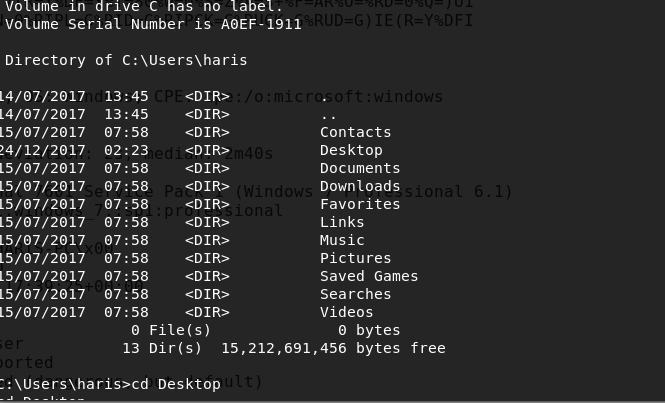
Once the rhosts was in place, I ran the exploit

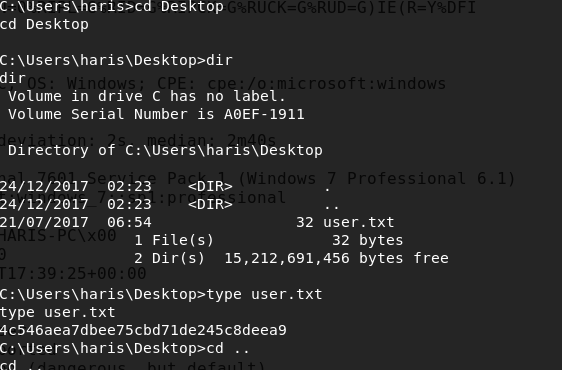


Success! I am in

Now time to find the flags:

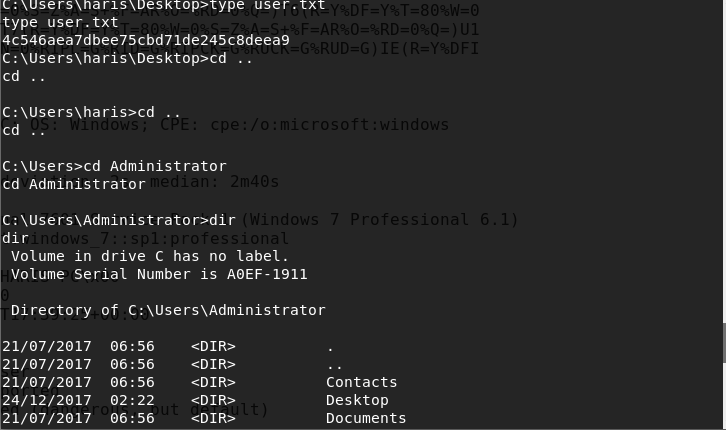


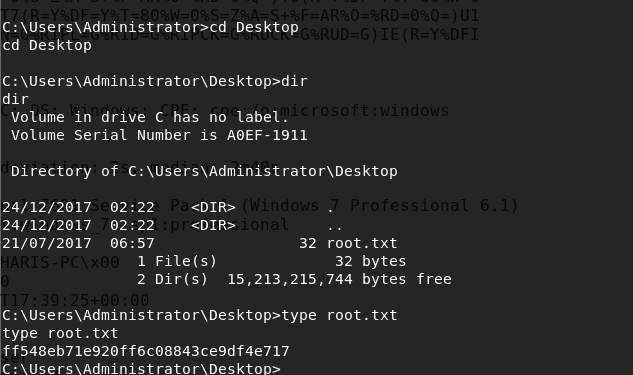




I found the user flag!

Now time for root flag





Success! Machine Complete! Found both flags using SMB exploit