**letsupgrade**

**Cybersecurity Essentials**

**Assignment Day 6/ 1st september 2020**

Name – akhil gudimalla

Email Id: - gakhil9201@gmail.com

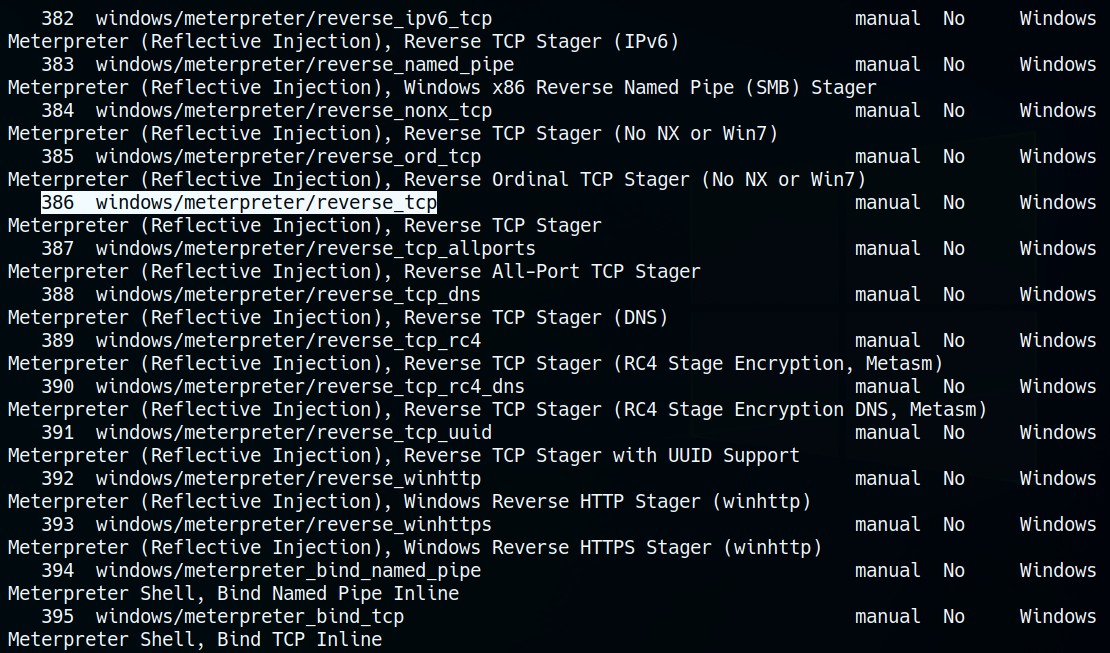
Mobile no 6301884795

# Report 1:-

## Creation and Exploitation of a Windows target using Payload

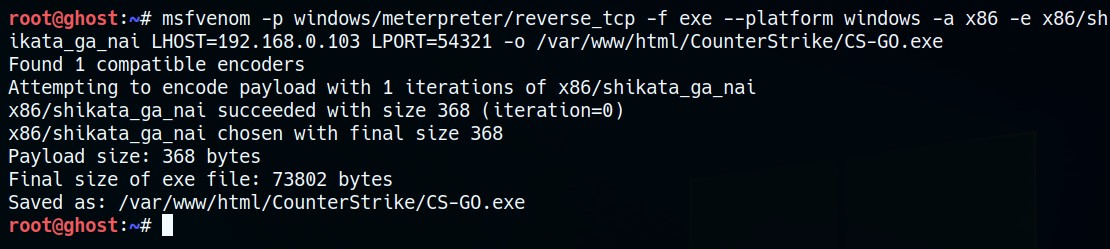
primarily, we set the Metasploit Framework and search for a specific payload (Windows Reverse Shell in this case)

Command used : **show payloads**



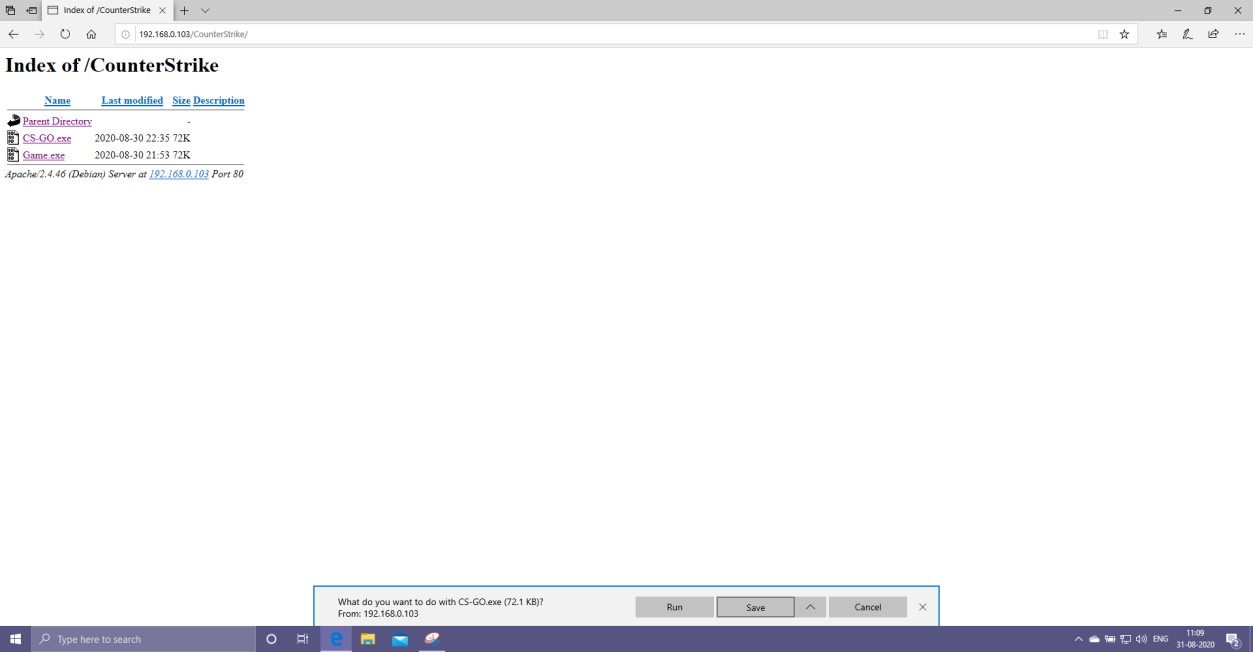
Next, we create the particular payload specifying its properties like format, encoding and architecture using **msfvenom**.

Listen Host and Listen Port are specified to be the Attacker machine’s IP address and specified port.

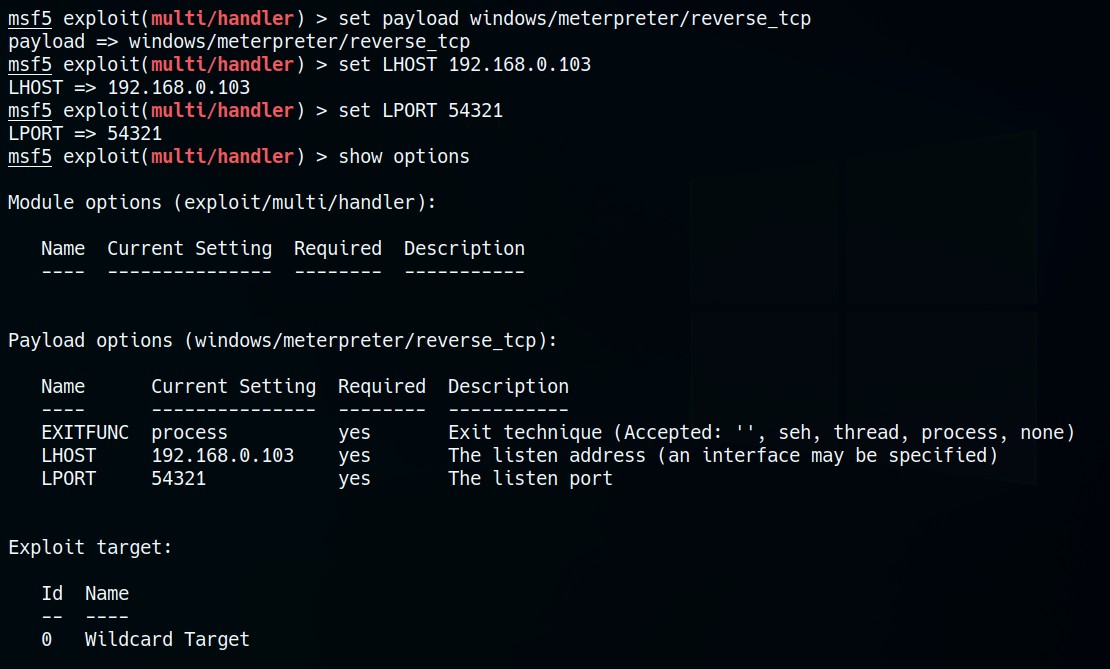


Then the created payload is made available for the target to download and open.

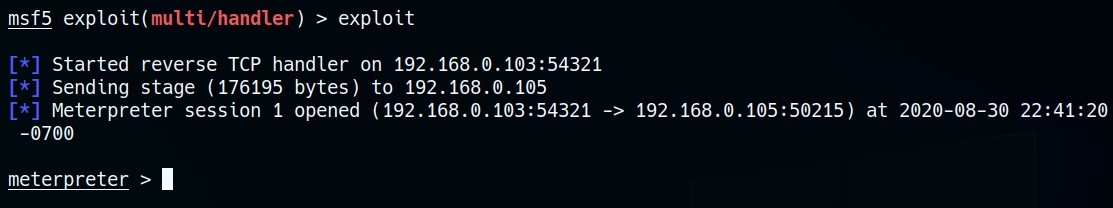
* + This can be achieved by hosting the payload on our webserver (done in this case) or emailing the link/ payload to the victim.



The attacker keeps the meterpreter ready and listening for connections using the **msfconsole**.



Once the victim downloads and opens the payload, the connection is established with the attacker, giving access to the victim’s machine.



Now, once the attacker gains access to the victim machine, the exploit can be compromised in several ways, some of which are listed below:-

Get full access to the victim's file system.

Gaining access to the CLI of the victim program.

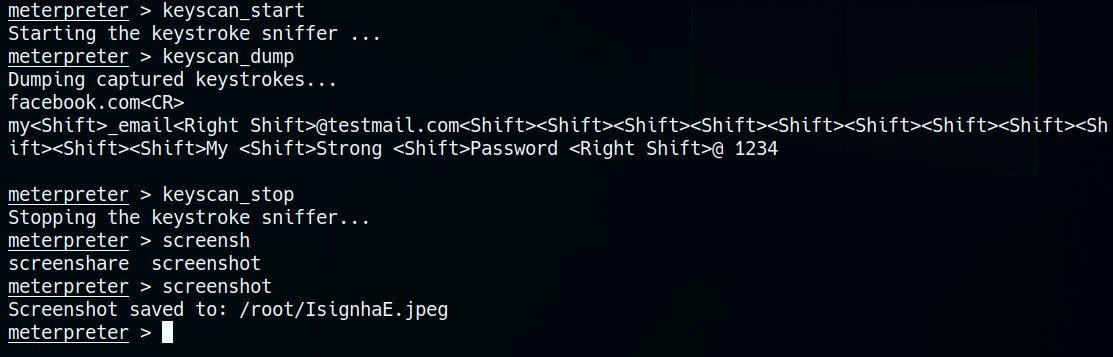
Perform tasks such as Keystroke sniffing, Screen grabbing, audio / video recording using the appropriate hardware of the victim system.

Other activities carried out during the attack are listed below: -

Use the victim's CLI to manage files and folders.

Files uploaded to or from the victim and attacker.

Clicking the buttons and a screenshot from the victim's machine, reveals sensitive information.

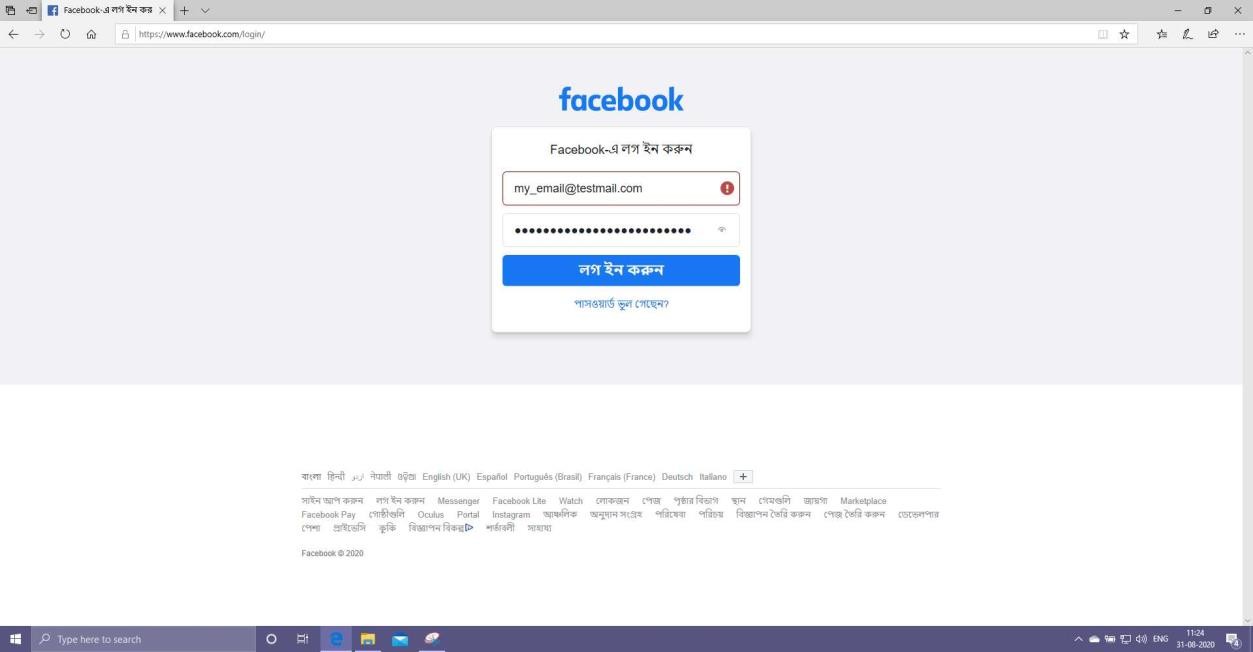


Upon close inspection of the above **keyscan\_dump** result, the following information is revealed:

The user browsed facebook.com

Their Facebook credentials grabbed are as follows:

* + - Username/ Email : [*my\_email@testmail.com*](mailto:my_email@testmail.com)
    - Password : *“My Strong Password @ 1234”*
* The screen grab of the machine during the same time revealed:



### Conclusions:-

### (1) The details of the target machine must be known for effective operation. (OS, architecture, etc.) - needs to be on the same network.

### (2) The vulnerability or exploitation is found directly on the OS, version, or error in the targeted system.

### (3) The Metasploit framework is used to create risk loading and set up TCP session with the victim.

### (4) Once the victim has received and paid for the transaction, communication is established with the attacker, giving him or her access to the victim's machine.

### (5) The victim's machine could be successfully compromised to perform operations and spread the attack to other subsequent victims, resulting in botnet attacks. Precautions:-

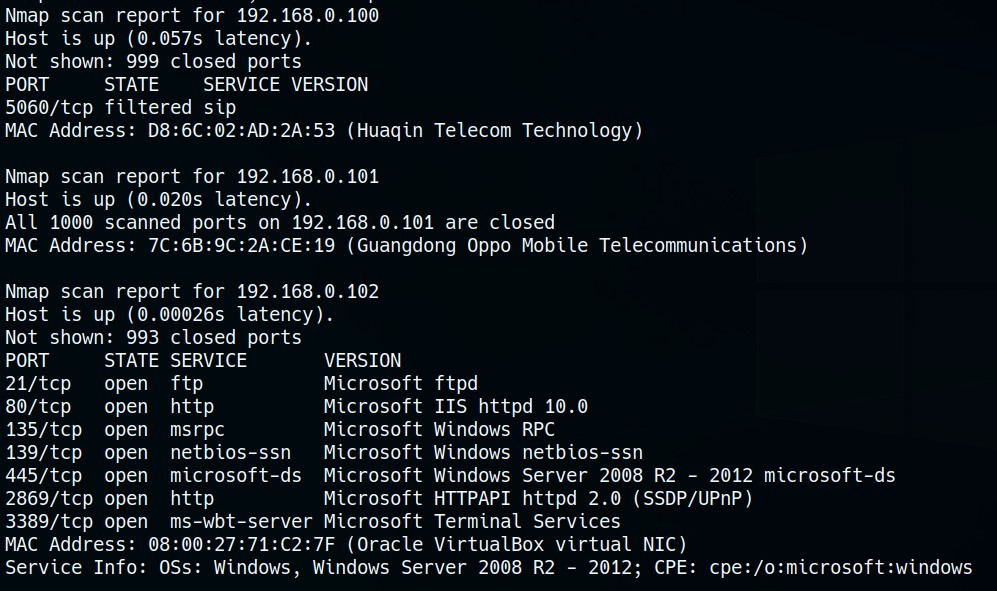
1. Never click/ download anything from unsolicited links/ emails.
2. Always use updated systems and Antivirus softwares.
3. Keep a tab on open ports, and close all unnecessary ports whenever found

# Report 2:-

## Spoofing ARP request packets between 2 targets (or a FTP server) to sniff the FTP credentials

We conduct a **nmap** scan of the local network to find potential target systems.

* + One system with Local IP of *192.168.0.102* was discovered to have port 21 (FTP) open.



We can then spoof the ARP request packets of the 2 end-users (targets) communicating with each other.

* + Machine communicating with the target (known in this case):

*192.168.0.107*

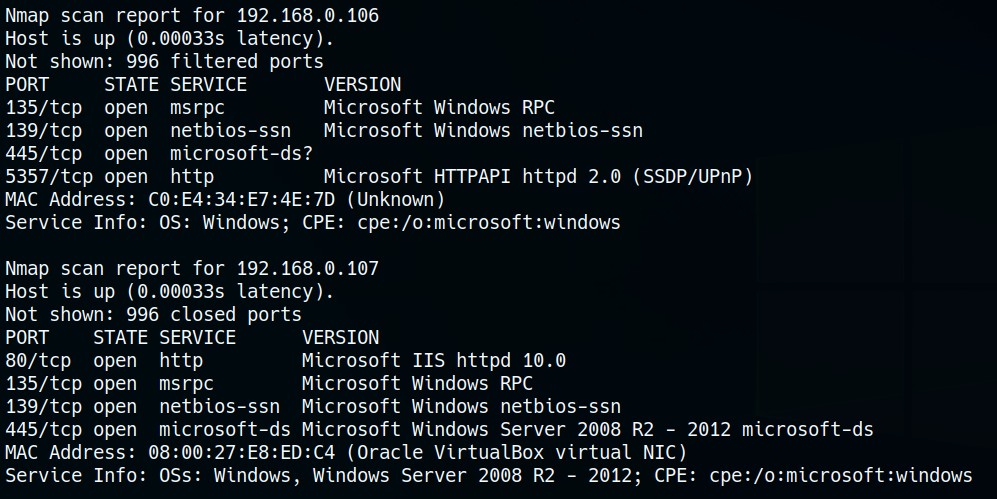
Command used :

**arpspoof -i eth0 -t 192.168.0.102 -r 192.168.0.107**

### Note: -

IP forwarding must be enabled in the attacker machine before ARP spoofing in order to keep the data flowing between the targets and minimise suspicion.

* + Command to use : **echo 1 > /proc/sys/net/ipv4/ip\_forward**

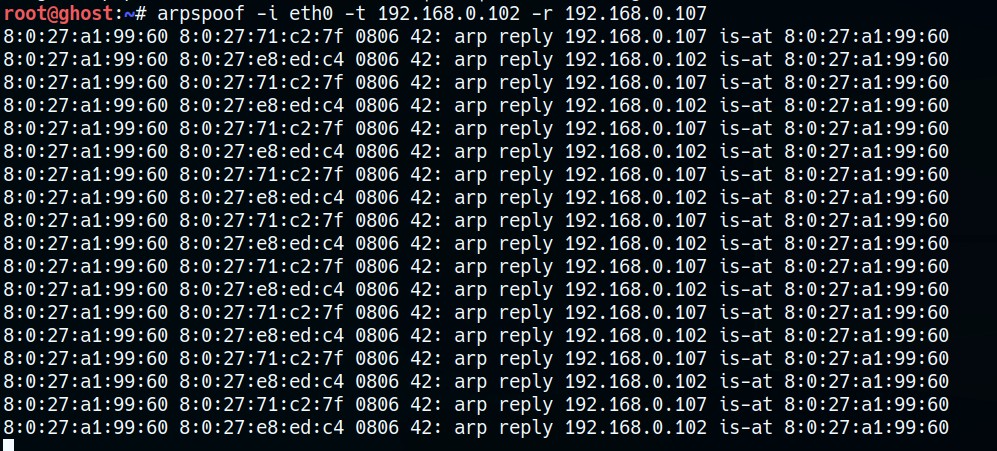


If we can’t find the machine communicating to our target (since it need not have FTP port open for connection), we can spoof the ARP request packets with that of the Router address.

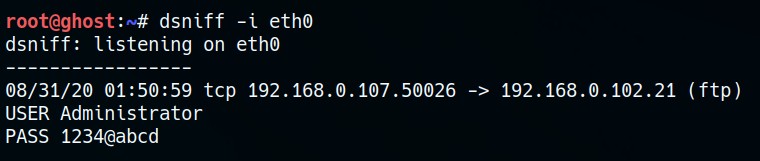
Router address in this case would be *192.168.0.1*

Command used in this case :

**arpspoof -i eth0 -t 192.168.0.102 -r 192.168.0.1**



* Next up, we keep sniffing for data using **dsniff** or **Wireshark** (or both to get additional information) on our listening interface (eth0 in this case).



### Conclusions:-

1. IP forwarding needs to be enabled in attacker machine before spoofing the ARP packets.
   1. This is to be done so that the packets keep flowing to the intended devices through the attacker, without raising any suspicion in the victim end.
2. At least one victim needs to be identified, preferably the FTP server.
   1. The ARP packets can then be spoofed with the victim and the router of that network (so packets flowing the router are captured.)
3. Sniffing on the specified interface reveals the data passing through the attacker machine, exposing sensitive information.