**CYBER SECURITY –ESSENTIALS**

**ASSIGNMENT DAY-6**

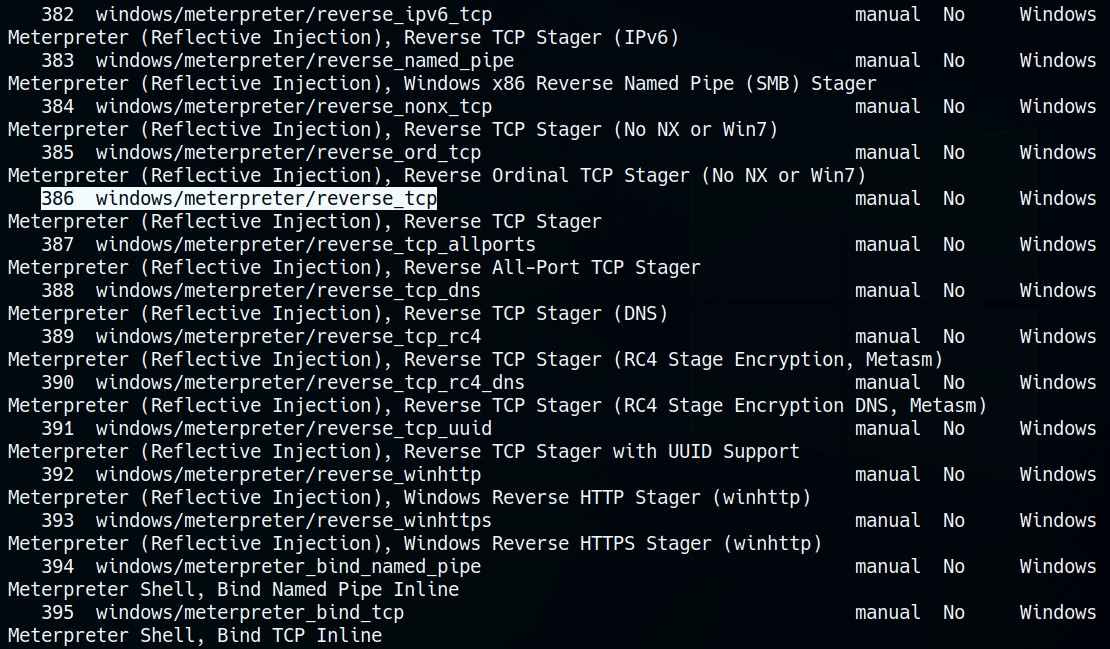
**Q.1.** Create payload for windows.

* Transfer the payload to the victim’s machine.
* Exploit the victim’s machine.

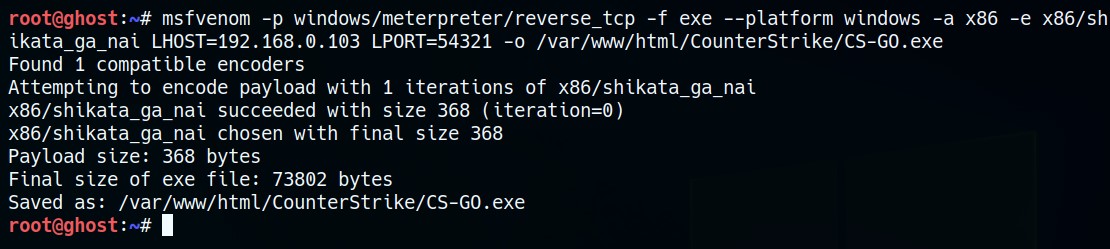
==> Initialize the Metasploit Framework and search for a specific payload

(Windows Reverse Shell in this case)

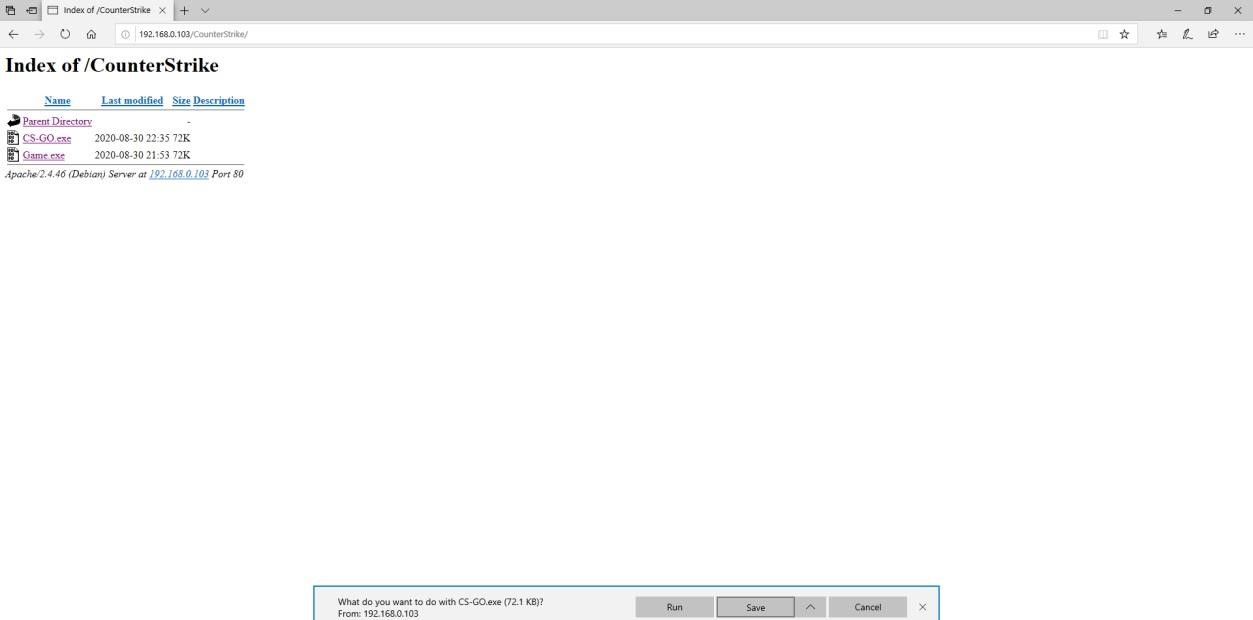
Command Used: show payloads



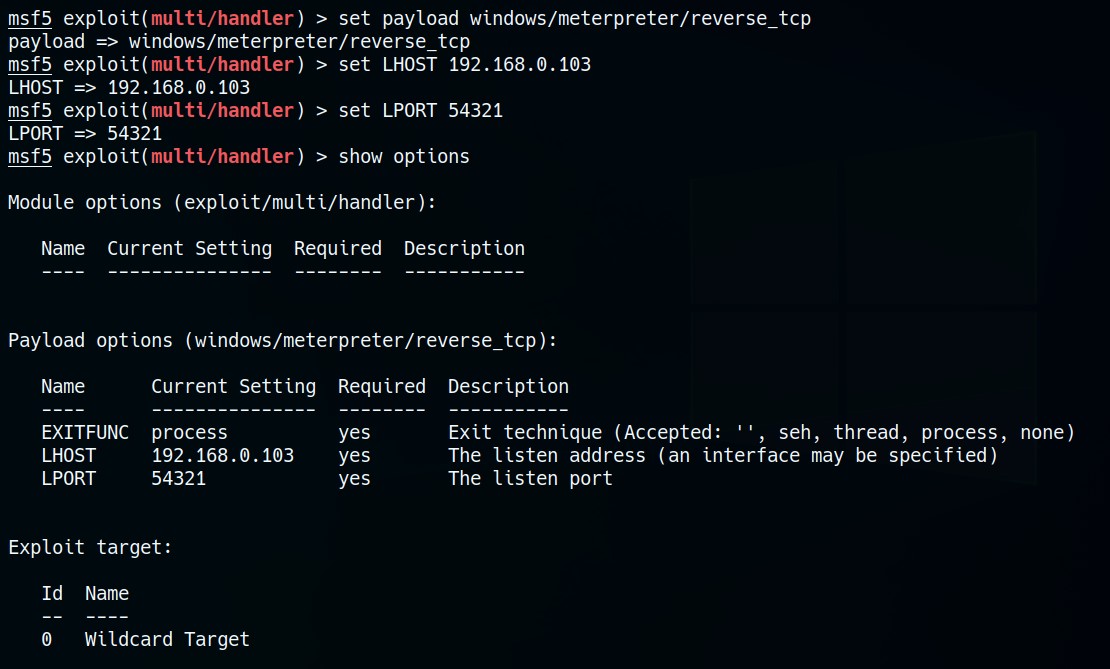
Creating the payload using msfvenom.



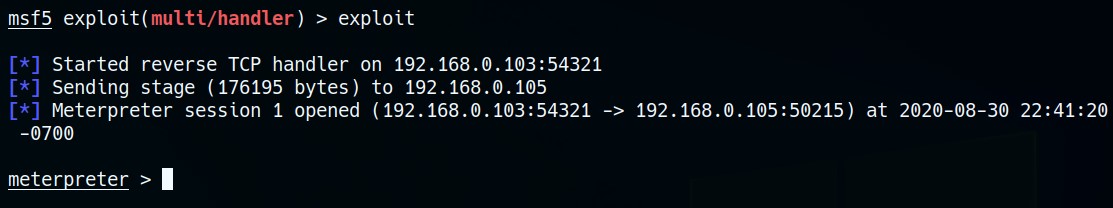
Payload is now live for the target to download and open.



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



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



Now that the attacker has access to the victim’s machine the security is compromised and the exploitation can be done in many ways using the commands given in the file named “Exploit.txt”, attached herewith.

**Q.2.** • Create an FTP server.

* + - Access FTP server from windows command prompt.
    - Do a MITM to get the username and password of FTP transaction using Wireshark and dsniff.

==> First, do the nmap scan to find potential target systems.

By spoofing the pac

kets to

ge

t hold of the communication between 2 users

:

arpspoof

-

i eth0

-

t 192.168.0.102

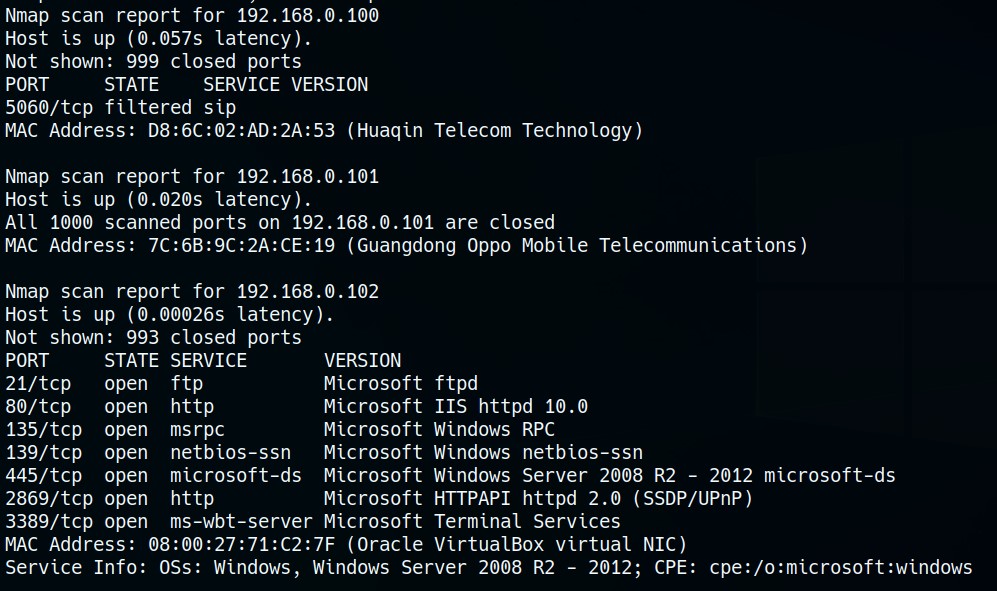
-

r 192.168.0.107

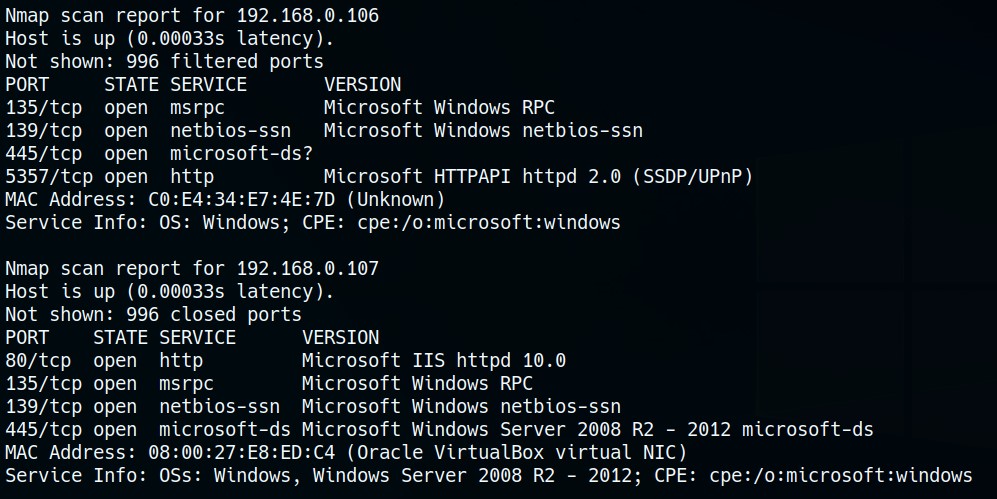
IP f

orwarding must be enabled in the attacker machine before ARP spoofing

in order to keep the data flowing between the targets and minimise suspicion.

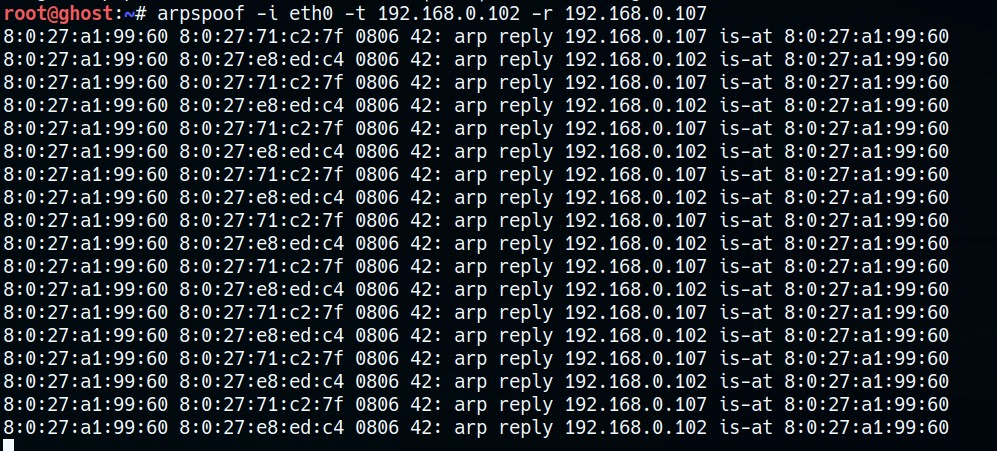


▪ Command: echo 1 > /proc/sys/net/ipv4/ip\_forward

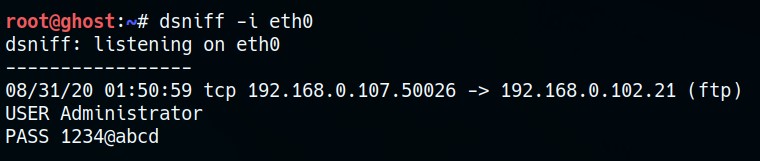


* In case we can’t find the machine communicating to our target (since it need not have FTP port open for connection), we can spoof the ARP request packets with that of the Router address.
* Router address in this case would be 192.168.0.1

Command: ▪ arpspoof -i eth0 -t 192.168.0.102 -r 192.168.0.1



Now, sniffing the data using dsniff or Wireshark.



=============

Submitted by SATHWICK PALADUGU