A reverse connection, often referred to as a reverse shell, is a technique where a compromised system initiates a connection to a remote attacker's machine, rather than the other way around. This allows attackers to bypass firewalls and other security measures that typically block incoming connections, giving them remote access to the compromised system.

**Steps to follow for a Reverse Connection :**

**-** Attacker will create a payload as per target Operating System.

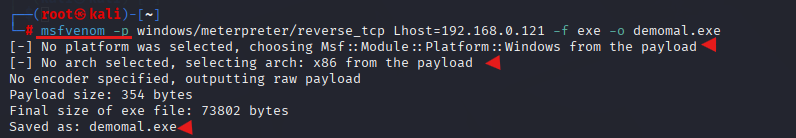
-Using social engineering the attacker will send the payload to target.

-Attacker will start listing on the port to receive connection.

**Payload :** A payload is the part of a malicious software (like malware, viruses, or worms) that performs the harmful action on a victim's computer or network.

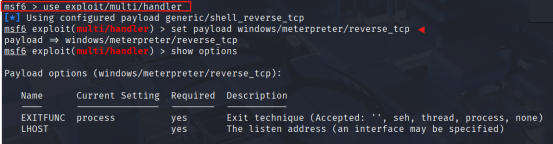
**Meterpreter:** A Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code. Meterpreter is deployed using in-memory DLL injection. As a result, Meterpreter resides entirely in memory and writes nothing to disk.

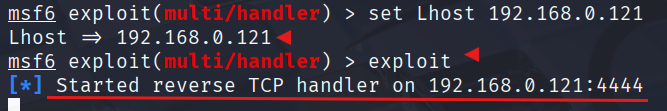
Creating a payload file as shown in snapshot, here we will be using msfvenom to perform this reverse connection by creating a “exe” file for a operating system where we will be specifying operating system, payload name,connection type, Attacker IP, filetype , output in a file.



We have done with the initial step of the reverse connection where we created a file and need to be deployed using social engineering. Prior we need to start the listening port to establish the connection as we get the response from the compromised system as soon as the user interact with the file. So we are starting msfconsole to listen from port.

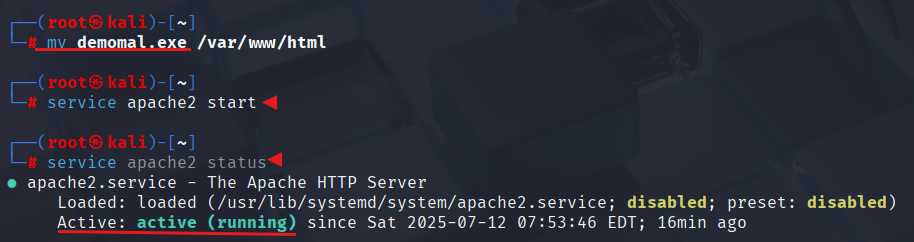
After running the msfconsole in order to revice the reverse connection we need to load a exploit called as multi handler. After loading the exploit multi handler we need to setup the payload. Once the payload set we need to set the Lhost and Lport this will start listing on the specific port which you assigned.



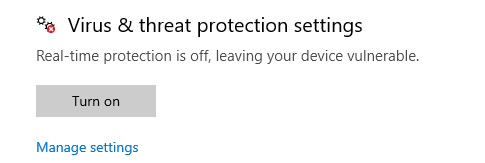


**Attacking on our own Machine -**

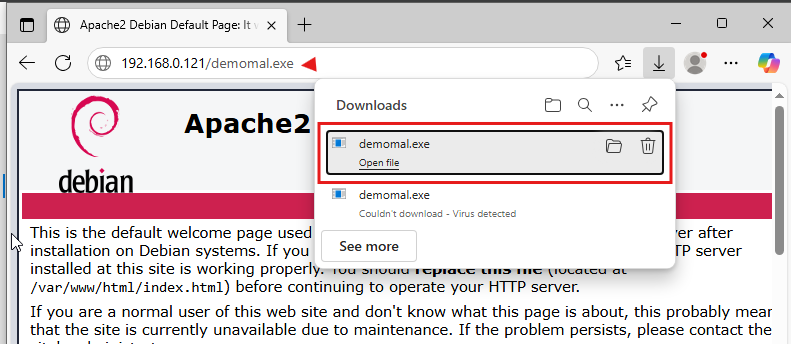
We are deploying the file which was created using payload in apache server, and we will access it through VM windows system, In our case it’s the target system. We will download the file and run the file in windows.



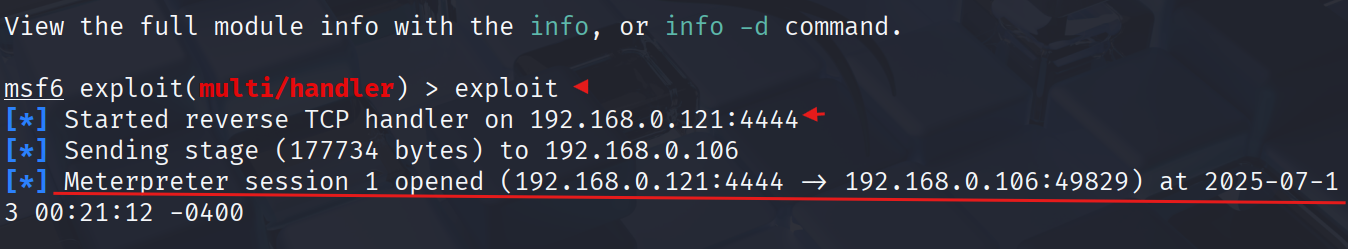
We can access .exe file using apache server which runs on the same ip of our linux machine which is 192.168.0.121, before downloading it we need to disable all necessary virus protection and app protection in the windows operating system to download and run the file in windows environment as shown in snapshot.



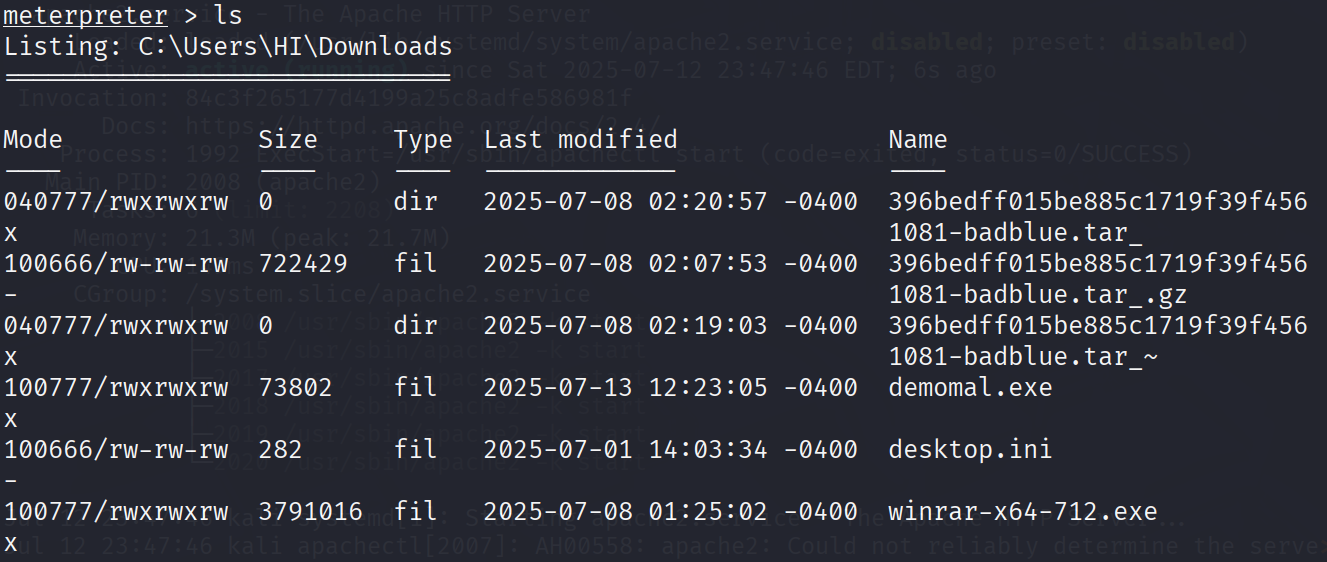
Now, Lets get back to apache server to download the file,we need to enter the ip address in the search bar followed by file name to download it as show in the snapshot.



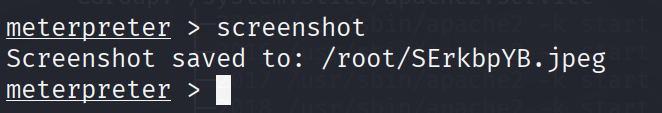
Once downloaded run the file in windows environment. As soon as we run the file system got compromised and the attacker will be receiving a reverse connection on the port listening. In our case it is 4444 as shown in snapshot of attacker system



By using ls command we can see all the files in windows OS. As shown in snapshot.



System got full compromised and we got the full access of the device we can take screenshots, keystrokes, webcam, personal data. Examples as shown.



**Summary :** Reverse connections works flawless even the firewall is up nor No open port is running in the target system. it relies on the existing memory(RAM) and network resources of a system to establish a connection.This approach is often used to bypass firewalls and network address translation (NAT) configurations that might block standard incoming connections.This type of connection can be difficult to identify by foreign forensic teams as well.