Logo, company name

Description automatically generated

Information Security proposal

Performing Reverse\_tcp Attack(using Metasploit)

**Syed Ali Hamza Ghaznavi**

**22-11091**

**Muhammad Umar Ali**

**22-10507**

**Hamza Ayub**

**22-11085**

**Ali Afzal**

**21-10321**

**Project Description**

In this project we will be performing a reverse Tcp attack on a victim. Understanding the basics i.e. TCP/IP is the standard protocol used for communications over the internet. One computer is easily able to send and receive packets of data by using TCP/IP and it is ensured that the data reaches the right address. Firewalls exist to block incoming traffic, however Reverse\_tcp makes the host initiate connection with malicious hackers who is trying to penetrate into user’s machine.

With Bind Shell we can open a listening port to communicate with the victim machine and waits so that the victim machine has initiated some connections, malicious hackers can listen and take control by commanding the victim machine. Reverse Shell works when the victim has started connection to the attacker’s machine and the listening port gets a connection that can be used to execute commands. In essence Reverse\_tcp waits for the victim to start connection so that the firewall cannot block connection (the case if attacker initiates communication) and it gains control of the victim machine, and this is a type of reverse shell.

**Methodology**

**(Steps to Complete Project)**

We Need

1. Linux Machine.
2. Metasploit.

**Metasploit**

A program that allows penetration testing to check vulnerabilities on networks and servers. On a linux machine it can be employed by passing commands on the terminal. We will be using msfpayload(to generate payload) and msfencode(to encode payload) which are included as part of msfvenom. We can generate revers\_tcp payload in an executable format and encode in the format we require. A handler is created that can listen to the payloads and when connection is initiated by the victim machine, we can continue with our exploit using this meterpreter session.

In the case of Reverse\_tcp exploit, the attack will take place using attacker’s router, where connection is initiated from victim machine and reverse connection to attacker machine is established. The IP for attacker machine is declared and the LPORT is defined, when router receives anything on this port, it lets the kali linux machine receive the connection.

Firstly, the local IP address and the public IP address of attacker machine is found and the LPORT is declared (standard port is 4444). Secondly, payload is created using msfvenom (Metasploit) and an executable type virus is made. Victim is sent the executable file. This is created using the public IP and the LPORT. The settings of router are accessed online using the IP address and the port forwarding settings are changed so that sever IP address is that of attacker machine and LPORT is defined as start and end port. Thirdly, a listener is made so that meterpreter session can be started. As soon as the victim machine opens and executes the file, the session is in progress.

We will achieve this by sending a file that is zipped and sending it to victim machine, it will be disguised as a video file, however it will be of type exe and when opened on the machine, it will execute. Our machine will start the listening process and attack can be proceeded by taking control of the victim machine.

**Outcomes**

Taking control of the attacked machine and then we can easily pass commands like accessing files such as accessing download directory of the victim machine. This will give access to sensitive information which can be completely confidential or private information like medical files/family photos. We can now corrupt files by replacing information/modifying information in these files or deleting them.