



REVERSE SHELL

TEAM KV

VIDISHA ARVIND (EI8CSE209)

KULDEEP (EI8CSE092)

COMPUTER SCIENCE ENGINEERING DEPARTMENT

.....
BENNETT UNIVERSITY, GREATER NOIDA, U.P.

17-JUNE-2020

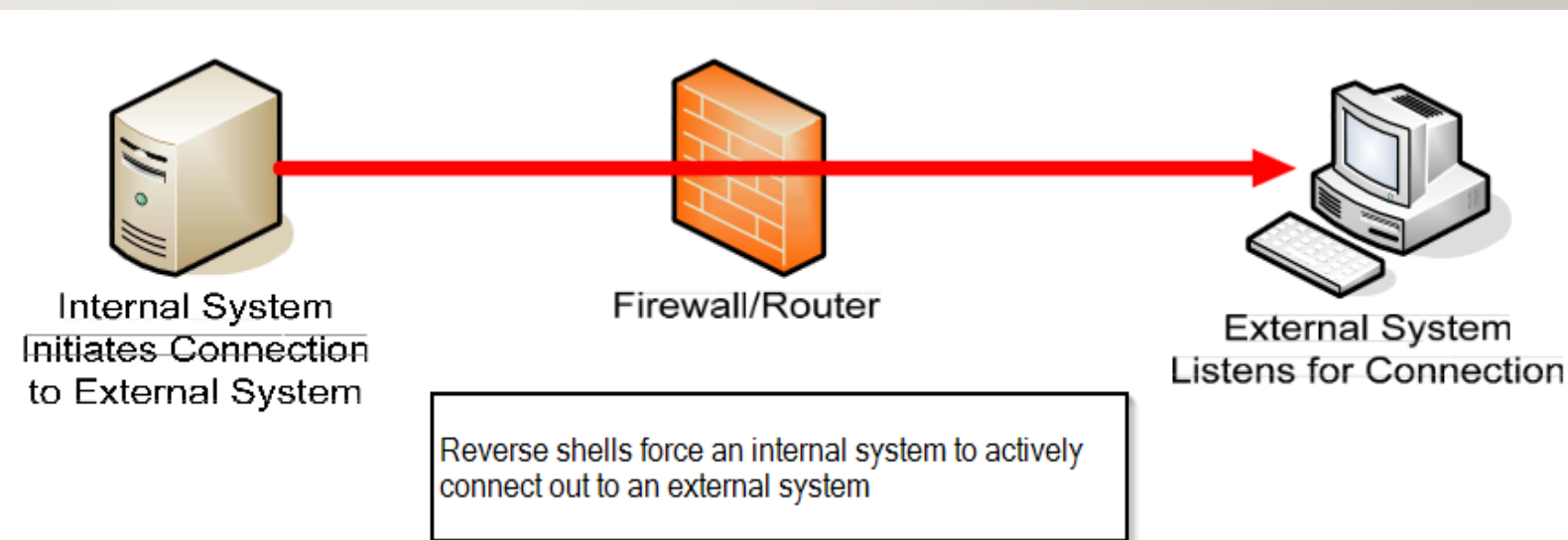
INTRODUCTION

A reverse shell (also called a connect-back shell) is a way to gain remote shell access across a firewall.

Reverse shells are often the only way to perform remote maintenance on hosts, so they have legitimate administrative uses.

However, they can also be used by cybercriminals/hackers to execute operating system commands on hosts protected from incoming connections by a firewall or other network security systems.

For example, a piece of malware installed on a local workstation via a phishing email or a malicious website might initiate an outgoing connection to a command server and provide hackers with a reverse shell capability.



OBJECTIVES

- Remote maintenance
- Reverse shells can be used to work from home and not bother getting official access to the company network

DATA RESOURCES USED

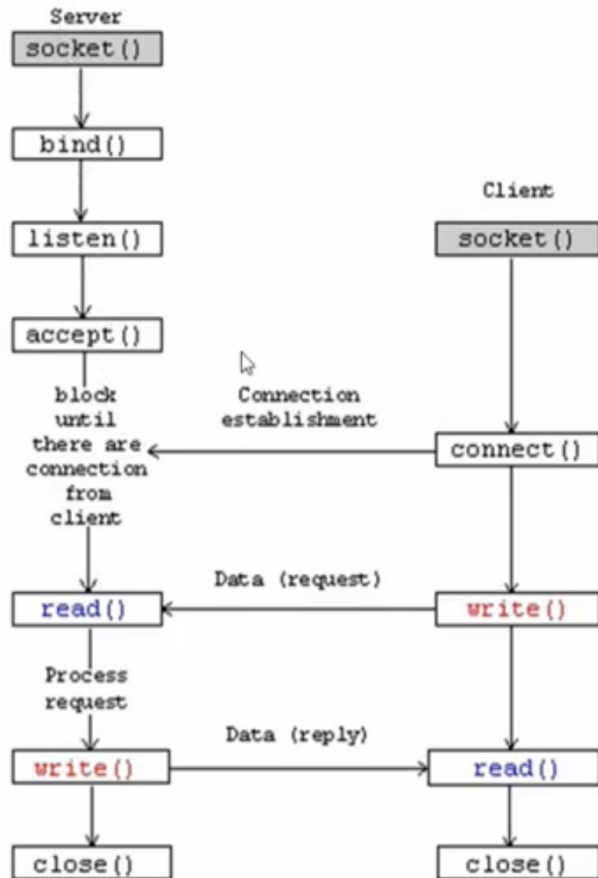
Tools that we have used :

- Python network programming: Socket Programming
- PyCharm IDE

For attacking implementation and testing Locally we have used :

- Windows 10 Home(Host OS)
- Windows 7 premium(Guest OS)

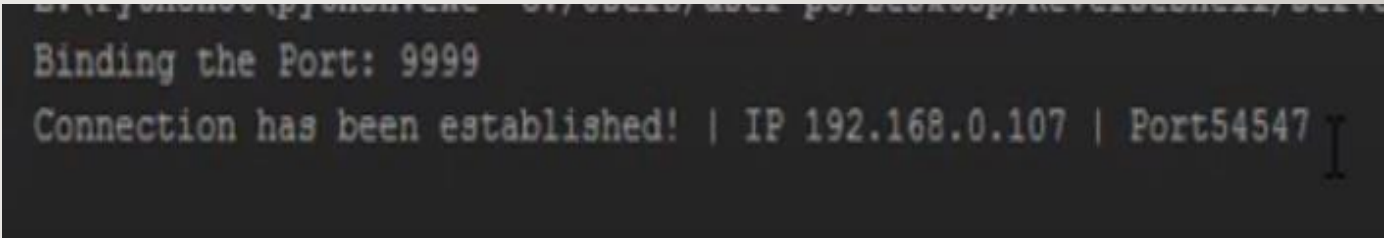
METHODOLOGY



- Client.py and Server.py files are created in which we firstly create a socket on our system/PC, in server.py file which basically is opening up a line of communication between the computers. Then we bind our port and host number to the socket .
- The file is sent to our friend's computer via an email and when he/she opens up this file it creates a reverse connection to the our computer.
- The connection is being set up by our friend so we don't need to worry about the IP address of his/her PC. So even if the IP address is dynamic it is not a big deal because every time the IP address changes our python file in his/her PC carefully accesses it accordingly.
- But IP address is dynamic so the address stored in the file will be useless after sometime so for this problem a server is being created which stores the IP address of the server in the reverse shell file because servers have static IP addresses.

RESULTS ACHIEVED

- With the help of client.py and server.py we have successfully been able to seize control over our friend's computer.
- Suppose that we want to create a directory on our friend's PC so we execute server.py file first which contains our IP address and client.py file is executed which has now got connected to our server.

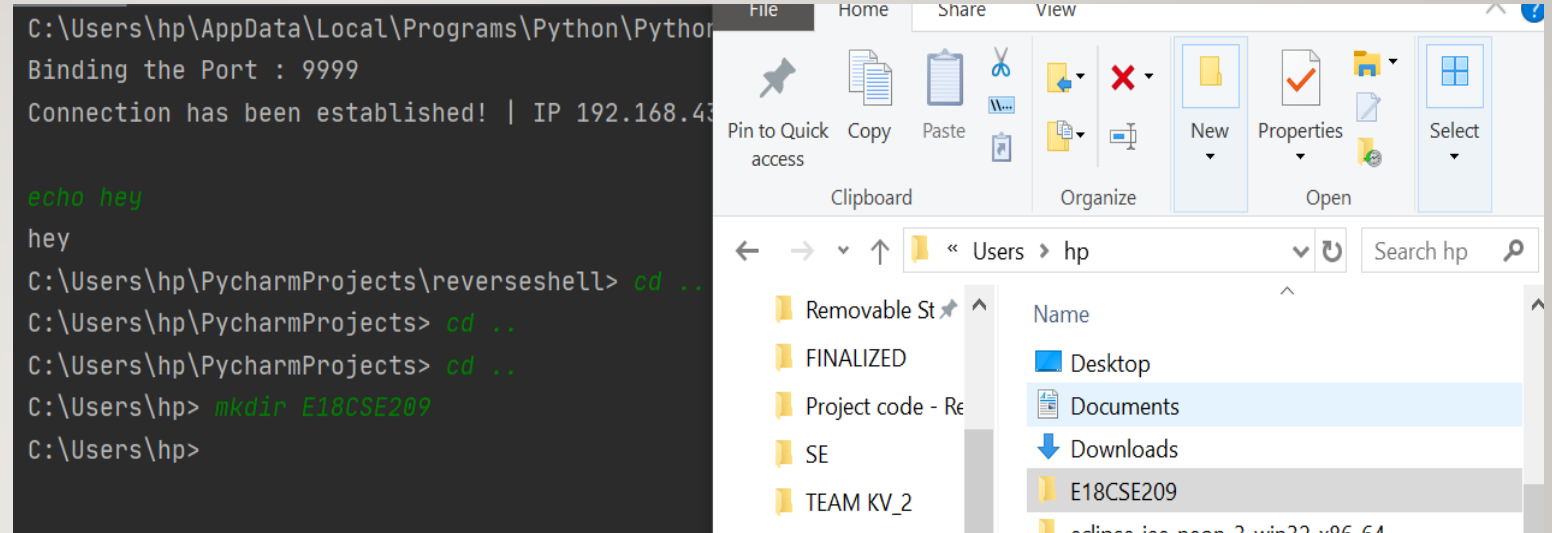
A screenshot of a terminal window with a dark background. The text is displayed in a light blue/cyan monospaced font. The first line reads "Binding the Port: 9999". The second line reads "Connection has been established! | IP 192.168.0.107 | Port54547".

```
Binding the Port: 9999  
Connection has been established! | IP 192.168.0.107 | Port54547
```

- Now whenever we type in something in server.py its shows us current working directory and we receive output from client.py.

RESULTS ACHIEVED

- Creating directory



- After we're done with our work we want to delete the folder so after deletion our server.py won't execute further if we try to access the deleted folder.

```
Binding the Port : 9999
Connection has been established! | IP 192.168.43.14 | Port 49318
ECHO HEY
HEY
C:\Users\hp\AppData\Local\Programs\Python\Python38-32> cd ..
C:\Users\hp> cd E18CSE209
The system cannot find the path specified.
C:\Users\hp> rmdir /Q/S E18CSE209
C:\Users\hp> cd E18CSE209
```


CONCLUSION

- In conclusion, outcome may favor in low profile areas, like penetrating the systems for security purposes in a company's software to know how much secure their system is.
- Though our computer systems are becoming more and more advanced and are able to detect threats that we were not able to do so before. It is important to note that although anti-virus software can make a palpable difference in the success of our system being protected against hackers/criminals, no computer can outsmart the human intelligence and sometimes human mistakes may be the center of why these types of attacks happen.

REFERENCES

- 1.) <https://resources.infosecinstitute.com/icmp-reverse-shell/#gref>
- 2.) <https://www.quora.com/What-is-a-reverse-shell-in-relation-to-computer-security>
- 3.) Github:
 - <https://github.com/lukechilds/reverse-shell>
 - <https://github.com/fatihhcelik/Reverse-Shell>
- 3.) Research papers:
 - <https://ieeexplore.ieee.org/document/7502270>
 - https://www.researchgate.net/publication/304816748_Reverse_TCP_and_Social_Engineering_Attacks_in_the_Era_of_Big_Data

THANK YOU