Reverse shell

Vidisha Arvind , Kuldeep

Computer Science Department
School of Engineering and Applied Sciences
Bennett University
Greater Noida, U.P., India

Abstract—TCP is a connection-oriented protocol used for the transport of information across the Internet which attracts hackers who are continuously searching for new opportunities within the TCP protocol to use it for iniquitous means. The hackers are able to seize remote access to the target end user's network. Success in this attack depends on skillful social engineering techniques to target specific users in order to open the connection. This research paper describes how one can use Reverse shells to gain access to someone's system remotely. Reverse shells are a type of shell that allows access to internal systems without having incoming access to the network and it forces an internal system to actively connect out to an external system basically inside-out. Reverse shells pose a threat to our network since it is quite difficult to detect them and it requires an understanding of how it exactly works and what are the protocols that are being used for it .

Index Terms—TCP/IP protocol, social engineering, reverse shell,Baiting , Phishing, Direct & Reverse connection.

1 Introduction

With the growth and advancement of technology, businesses are able to communicate freely without any restrictions of geographic location. The use of the Internet has become their really important and primary medium for information sharing in the era of digitalization. Everyone now has at least one space to openly exchange data. Although the Internet has appeared to be a great tool, hackers know the value of all data and other information that is being shared. Several efforts have been made earlier to grab the information and use it for it's other than intended purposes.[12][7]

With the growing technology, hacking and cyber crimes are also increasing, unauthorized code (malware) are executed on the target systems which beacons out to a command and control system on a reachable network[7] . For example denial-of-service attack, worms, Trojan horses, or viruses. Attacks that are focused on getting important information have been connected to the Transmission Control Protocol (TCP) which is the protocol accountable for the transport of information from one end-user to another. TCP paired with Internet Protocol (IP) are estimated as the most reliable means of achieving an efficient connection-oriented communication over the Internet.This technique provides a dedicated connection and it does not take into consideration the security aspects of its connection[5].

I. REVERSE SHELL

A reverse shell is a kind of shell in which the victim's machine communicates back to the hacker's system which has a listener port and it receives the connection, by using code [9] . Reverse shells can be used to perform remote maintenance on hosts behind the firewall, so basically they can be used for administrative purposes[8].

II. DIRECT CONNECTION

Suppose that we are in Japan and we have a friend, who lives in India. Now our friend has some kind of problem with her computer and she wants us to fix it. So what we can do is, we can remotely connect to her system using command line prompt or terminal and fix her system. This type of connection is accomplished by a direct connection.

In a direct connection, we first create a socket on our system(PC), which is basically opening up a line of communication between the computers. Then we bind our port and host number together into the socket and send a request to our friend on her IP address. If she goes for our request then we will be able to remotely access her computer and then using our terminal we are going to fix whatever problems are in her system. So for direct connection, we need the IP address of our computer as well as our friend's computer.

But the difficult part is that it's strenuous to get the IP address of anyone's computer. Even if we have got access to the IP address of another computer then it still makes it difficult to sustain the connection because the IP address is dynamic. That is, it's always changing. So we won't be able to maintain the connection for a long time and even if we could get updates regarding her dynamic IP address, then computers have several in-built firewalls which prevent these types of connections from happening, thus making it

impossible for us to get into her computer.

III. REVERSE CONNECTION

In reverse connection, a connection is started from the victim's computer. That is, a hacker would create a file, say, a python file called reverse shell in which the IP address and the port of the hacker's computer are present. Then the file is sent to the victim's computer via an email/USB/DVD [2] etc. And when the victim opens up this file it creates a reverse connection to the hacker's computer. Now with the help of the properties of a reverse connection, it solves the problems faced in a direct connection as the connection is consistently being set up(or updated) by the victim so the hacker needs not to bother about the IP address on the victim's PC. So even if the IP address is dynamic, it is not any problem since every time the IP address changes, the python file in the victim's computer carefully accesses it accordingly. But the hacker's computers still have a dynamic IP address so the address stored in the file will become useless after some time. To overcome this problem, a server is created which stores the IP address of the server in the reverse shell file because servers have static IP addresses[2].

IV. Social Engineering

Social Engineering is a way of encroachment used by cyber criminals to gain knowledge about a potential victim. It basically depends on human interaction and often involves deceiving a person into breaking normal security procedures [1].

Social engineering is not an alien concept in computer security. In fact, the Trojan virus got its name from an example of social engineering in another context which dates back to ancient Greece which is a very comprehensible example of what can happen if you're hoodwinked into trusting something sent to you is what it appears to be [4]. Social engineering has many techniques which are used to manipulate a victim into becoming susceptible to an attack. Some of the techniques are listed below:

Baiting – An attacker leaves a malware infected physical device in an evident location, alluring to the interest of a person(Victim) who loads it onto his/her system at which location the malware was installed.

Phishing – In this technique, a hacker sends malware through an email from a company or trusted party and that email either asks for personal information or has an attachment which is actually malware. For example, It would be a fake email [2] supposedly from 'Initech' asking for your account information in order to confirm delivery of a package. Or an attachment asserting to be an authorization form. The user feels compelled to communicate this piece of information in order to receive their package and as a result they are compromised[2]-[4].

2 Literature Review / Related Work

We have solved the problem faced in direct connection(Introduction II. Direct connection) by using the concept of reverse connection and then we were able to gain control over our friend's system . However , there are many researches on Penetration testing [4] and detecting reverse shells [6] but at this time there's not much advanced research in computer science which particularly focuses on exactly what 'Reverse Shell' is and what are its positive sides . Most of the research is concentrated on "Reverse Engineering " or "Social engineering attacks" [1],[4],[5],[6],[10] .

2.1 Reverse TCP and Social Engineering Attacks

According to Atwell, Blasi, Hayajneh [5] who has worked on Reverse TCP and Social Engineering Attacks , reverse TCP is basically a way to exploit the connection in which a hacker gets access to the target(victim)'s system. They have made a test bed .Their work basically implements a reverse TCP attack via a virtualized environment, and detailing the procedure performed to gain unauthorized access to the victim's machine.

The key threat is that the reverse TCP attack may pose to end users will provide a testbed which determines how successful computer systems are able to fortify against this attack.

2.2 Reverse Engineering and Backdooring Router Firmwares

Adithyan A; Nagendran K; Chethana R; Gokul Pandy D; Gowri Prashanth K[10] has worked on Reverse Engineering and Backdooring Router Firmwares.

They described reverse engineering firmware and manually backdooring them with many Linux features and compromising a WiFi router with the backdoored firmware and acquiring a reverse shell from the router. WiFi routers are everywhere, especially in public places. Firmware is in charge for controlling the routers. If the hacker deploys the firmware and gets ascendancy over the firmware installed in the router, then the hacker can get a hold of the network.

2.3 Survey of hacking techniques and it's prevention

S Shetty ; R Shetty ; G Shetty ;Jennifer D'Souza[11] worked on survey of hacking methods and their avoidance .The motive of this survey was to elucidate the concept of frequently occurring hacking techniques and its prohibition for the amelioration of cyber security.

They have talked about web based attacks , dictionary based hacking in which It uses a dictionary file containing possible passwords or possible combinations. The login credentials are stored in a format in a text file. A cryptography based code is executed that gives the login information of the required user by accessing the text file with the help of a dictionary [12].

3 Data Resources Used

For attack implementation, Python programming language was used in PyCharm IDE with an advanced Python concept for a network called Socket programming.

And for testing purposes, we tested our files locally, that is, on our own PCs/Laptops . ***'Windows 10 Home Pro'*** was used for the victim and as well as for the attacking system.
Even the other PCs/Laptops will also suffice for host OS and guest OS.

4 Methodology

4.1 working of the code

- 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.a

- 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 our computer as in Fig 1.

- 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 then our python file in his/her PC carefully accesses it accordingly.

- But the IP address is dynamic so the address stored in the file is 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 as in Fig 1.

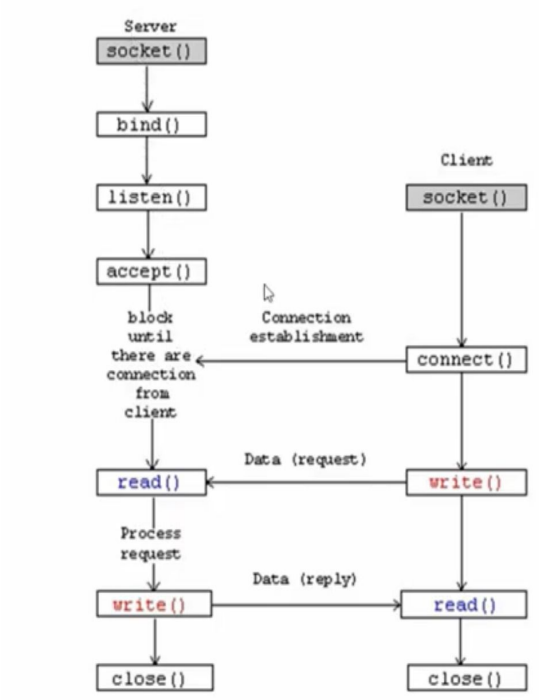

Fig 1. Connecting server socket to Client socket (Block diagram).

4.2 Testing

With the help of client.py and server.py we have successfully been able to get access inside our friend's computer.

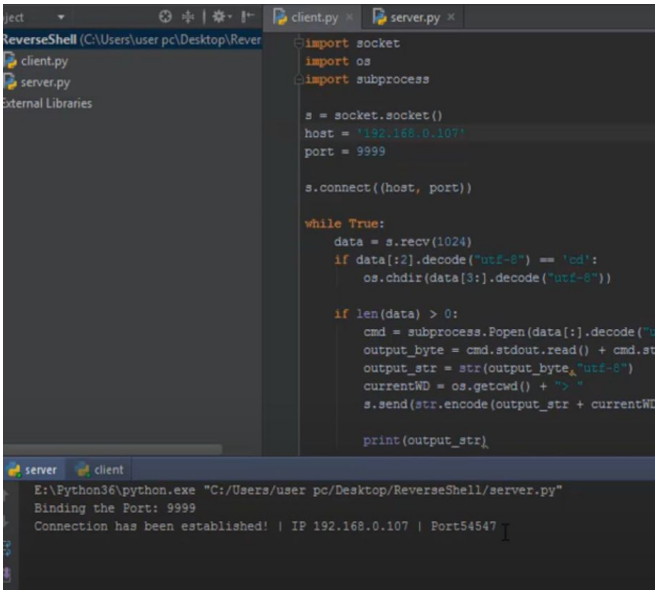

Fig. 2. Connection successful for server.py file i.e. Server connected to the client (OUTPUT).

- Suppose we need to perform some operation on our friend's PC. So we execute server.py file first which contains our IP address and the client.py file is executed which is now connected to our server as in Fig. 2.
- Now whenever we type something in the

server.py, it shows us our current working directory and we receive output from client.py. as in Fig 3.

5 Results

5.1 Performing operations on client's system

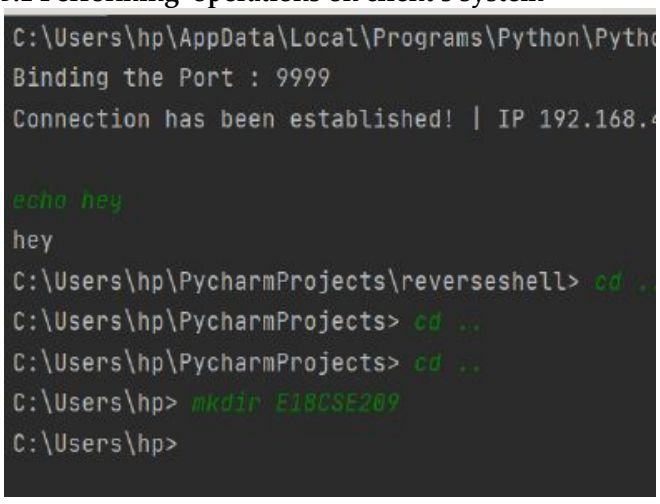

Fig 3. Making a Directory using Server.py file and whatever the changes we have made will be reflected on the client's PC/Laptop.

The commands on server.py file are executed and same commands in our code client.py is visible and changes are made to client's computer as in fig 3 and fig 4.

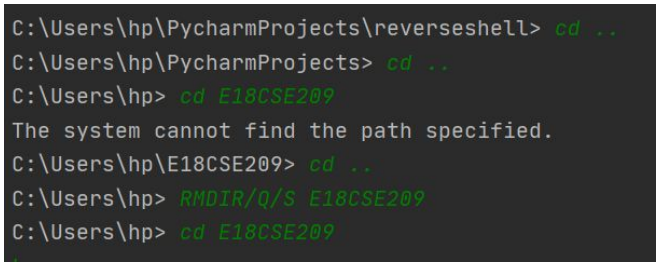

Fig 4. Removing Directory

Conclusion

In conclusion, outcome may favor low profile areas, like penetrating the systems for security purposes in a company's software to know how secure their system is. With the help of client.py and server.py we have successfully been able to seize control over the victim's computer.Though our computer systems are becoming 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[7]. Though Reverse shells allow access to attackers to take control of the system which they're installed on,there's a positive use of it too . Reverse shells can be used [6] :

1. To test firewall rules
2. To test IDS(Intrusion Detection System) rules.
3. To work from home and not worry about getting official access to the company network. etc.

References

[1] TechTarget.com, 'Social Engineering Definition' 2015. [Online].Available:http://www.searchsecuritytechtarget.com/definition/socialengineering

[2] "Email attack".[Online] Available: http://krebsonsecurity.com/2014/02/email-attack-on-vendorset-up-breach-at-target

[3] Techopedia,'Payload'Available:http://www.techopedia.com/definition/5381/payload

[4] Thunder ,"Security Research : Penetration Testing Blog",[Online].Available:https://w00troot.blogspot.com/2017/05/getting-reverse-shell-from-web-shell.html

[5] Christine Atwell , Thomas Blasi , Thaier Hayajneh,"Reverse TCP and Social Engineering Attacks in the Era of Big Data", IEEE Systems Journal, 2016.(DOI: 10.1109/BigDataSecurity-HPSC-IDS.2016.60)

[6] Richard Hammer , " Reverse Shells Enable Attackers To Operate From Your Network " ,[Online] .Available at :https://www.sans.edu/student-files/presentations/LVReverseShell.pdf

[7] Richard Hammer - November 10, 2006 ,"Inside-Out Vulnerabilities in Reverse Shells",SANS Institute Information Security Reading Room 2006.

[8] Zbigniew Banach ,"Understanding Reverse Shells",[Online]. Available: https://www.netsparker.com/blog/web-security/understanding-reverse-shells/

[9] "ICMP Reverse Shell",Posted in General Security on 4 January 2018 ,[Online].Available: https://resources.infosecinstitute.com/icmp-reverse-shell/#gref

[10] Adithyan A; Nagendran K; Chethana R; Gokul Pandy D; Gowri Prashanth K,"Reverse Engineering and Backdooring Router Firmwares ",IEEE Systems Journal, 2020.(DOI: 10.1109/ICACCS48705.2020.9074317).

[11] Shriya S Shetty ; Rithika R Shetty ; Tanisha G Shetty ; Divya Jennifer D'Souza ,"Survey of hacking techniques and it's prevention",IEEE Systems Journal, 2017. (DOI :10.1109/ICPCSI.2017.8392053)

[12] Dictionary attack sample program. [Online]. Available: https://github.com/npapernot/dictionary-attack