iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52542

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Reverse Shell with Persistence

Jaya Prakash Veganti[1], Venkata Sai Saka[2], Sai Manoj Mungi[3], Asst. Prof. S. K. Satyanarayana[4]
[1, 2, 3, 4]*Department of Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology, Hyderabad, India*

Abstract: ***Now-a-days, almost every house in the world contains at least one device which is connected to the internet. This makes it easy for attackers to target anyone from anywhere easily if he knows the technology. Attackers can have many ways of attacking the target system and gaining access to the remote systems. One of the ways is creating a remote shell. In this project, we used python to create the Reverse Shell and converted into a .exe file to gain persistence by setting it as a start-up process. We write a program for the target computer and the attacker uses the Netcat tool to gain access to the victim's computer. Since the target computer is trying to connect with our system, target will be the Client and our system will be the Server. All that we need to do is make the target run the Client-side program in his system and the rest will be handled by the Server.***
Keywords: Reverse Shell, Cybersecurity, Socket Programming, Vulnerability, Hacking, Python

I. INTRODUCTION

In current world, security in cyber space has become one of the major risks of IT industry. Many people do not even consider to apply security to their systems both in home and commercial environments. They are not aware of attacks happening around them. They are in a misperception of why would a hacker target me. This lack of security awareness in people gives a huge advantage to hackers who try to do malicious actions and steal valuable information. So, it has become very important to evaluate the efficiency of our security being provided frequently. We need to know how hackers can target our systems in order to prevent them from doing so. For that we need to analyze our systems first for any potential vulnerabilities to evaluate security level of our cyber environment. This is called Penetration Testing.

Remote Shells is one of the major security vulnerabilities the penetration testers try to examine in the testing a system. Since the hackers can do anything when they get remote shell, penetration testers know how important it is to keep an eye out on the system to check if it is vulnerable to remote shell. But reverse shell is something that they cannot examine. Any firewall checks for the in-bound traffic (the traffic coming into the network or system), but not the out-bound traffic (the traffic going out of the network or system). Since the connection between the attacker and the target is initiated from the target, the network traffic will be out-bound. So, any firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS) does not interfere the connection between the attacker and the target. This is the reason why attackers mostly try to use reverse shells for gaining remote access to the target computer.

A. Reverse Shell

In a typical remote shell scenario, the attacker is the client and the target will be the server. The user initiated the connection to the target and the target just listens to the server or the attacker. The roles of the attacker and the target gets reversed in the case of the Reverse Shell. Reverse Shell is a security methodology which is used to gain access to a remote computer. If an attacker tries to connect to a target computer, there are several ways in which the target can prevent this from happening. Some of the ways are configuring a firewall from receiving unknown connections, Applying IDS and IPS, etc. So, this time we do not connect to the target and make the target connect to our system and we can gain access to the system. Since the connection is initiated from the target, firewalls or any network filters do not filter traffic from our system and allows us to interact with the target.

Most of the target systems have set the firewall configuration to allow incoming traffic through specific ports which they use for their own purposes like HTTP (80) / HTTPS (443). Firewalls are generally configured to block any incoming connection to the server through any other ports. But they do not block the outgoing connection in any port. So, we can use any other port to connect to the attacker. This is the major reason why most of the hackers use the Reverse Shells for accessing remote systems' terminal.

B. Problem Statement

There are lot of types of attacks that hackers are using now-a-days to hack into systems of targets. One of those attacks is Reverse Shell. Attacker need a specific program to run on both his and target computer to get the reverse shell.

This project is used to generate these python scripts for victim and attacker can use netcat tool to gain access to the victim computer. Also, every time we restart the system, the reverse shell that is previously established will be terminated. This can be solved with our approach.

C. SOLUTION

Solution for this problem is implemented in this project of Reverse Shell. In this project, we used python to create the Reverse Shell. We write a program for the Client-side (Victim). Since the target computer is trying to connect with our system, target will be the Client and our system will be the Server. All that we need to do is make the target run the Client-side program in his system and the rest will be handled by the Server. The persistence can be gained with the help of pyinstaller module where it converts the python code into executable file which executes every time, we restart by adding it the shell:start folder.

II. EXISTING METHODOLOGY

The basic idea of creating a reverse shell is to make the attacker (Server) system listening to the incoming connections through a specific port and make target (Client) to send interactive shell traffic using the same port number to the listening attacker's computer.

A. Server Side

Server-side code is the code that is to be running on the attacker's computer. The main task of the attacker's computer is to create a socket on his computer, bind it to a specific port and listen to the incoming connections to that port. When a connection is found, establish the interactive shell.

A socket is created initially on the attacker's computer. Then, it is bound with the IP of the attacker's system and a port number which we do not use commonly. The socket which is created in the server is set to listening mode.

Whenever it finds the incoming connection to that port, it is configured to accept the connection. By now connection from the client to the server is successfully established. Now it is time to get an interactive shell. Server need to send the commands to the client which are supposed to execute in the client system and sent back to the server.

After the transaction is completed, attacker can break out of the loop of interactive shell with "quit" or "exit" command.

B. Client Side

Coming to the client code, it is the program that is to be executed in the client or target system. The major function of this client code is to loop around receiving the command sent from the attacker, executing the command, and sending the result back to the server so that attacker can have an interactive shell with this system.

The client creates a socket and connects to the server IP address of the server with the same port that is used by the server. After the server accepts the connection to the client, the connection will be successfully established. The client will get the Current Working Directory (CWD) using OS module and send it to the server as soon as the connection gets established as this makes it look more a real terminal.

C. Server-Client Synchronization

When we are working on a Server-Client model, it is very important that we make sure that server and client are synchronized. It is the job of attacker to make sure the server is running before the client runs. If the client runs before the server, client cannot find server to connect and socket will be closed because the connected host cannot respond.

The sequence of operation will be as follows:

1) Server starts running.
2) A socket is created by the server.
3) Socket is bind with host IP and port number.
4) This socket starts listening.
5) Client starts running.
6) Client tries to establish connection with the server.
7) Server accepts the connection from client.
8) Client sends the Current Working Directory to the attacker.
9) Attacker prints it to make it look more like a terminal.

10) Client goes on the loop to receive commands from the attacker.
11) Attacker sends the commands to client in the same loop.
12) When attacker want to quit, he gives "quit" or "exit" command.

III. PROPOSED METHODOLOGY

As we have seen above, in the conventional method of reverse shell, an attacker can connect and attack one system at a time. While in our approach, we tried to make it possible for attacker to have multiple targets at a time. While attacker is in shell of one target, rest of the targets connected to the attacker will be in sleep mode until the attacker selects the target.

As we have seen above, in the conventional method of reverse shell, an attacker can connect and attack a system with every time restarting the server program. But in our methodology, we implemented the persistence using the pyinstaller which does it's job by executing the python script every time server restarts.

We used threading to facilitate these multiple processes. One thread will be actively listening to the port set by the attacker, while the other thread will be used to connect to the shell of the selected target.

In our model, server (attacker) side script will be running first, as the client needs a server to connect to. Attacker computer initially creates a socket using socket module.

Now he binds his own IP address and any port which is mostly unused. Because, it we use the common port for the socket binding, that port may have some other function to do like receiving web traffic, mails, or something. The traffic through this port will interfere with the shell traffic through the same port. So, it is always advisable to use uncommon port for manual port allocation to any services.

Since the socket is bound with the IP address of the attacker and the port, all we need to do is set this socket in listening mode. So that we can hear any incoming traffic to this IP address through the selected port. While specifying listen mode, we need to give the backlog. Backlog indicated that whenever the unaccepted connections number exceeds the backlog, the new connection trying to connect will be refused to connect. We specify the backlog as 5.

Now the server is all set to receive and accept the connections. One click from the client will send the interactive shell to attacker.

When the client script runs, first thing it does is to create a socket and connect to the attacker's computer through the socket created using attacker's IP address and same port number used by the server to bind the socket. Netcat will do its job in the background by doing all the above-mentioned processes.

This connection request sent by the target is accepted by the attacker automatically and this new connection established will be notified to the attacker.

At the server side, we then used pyinstaller to convert the python script to executable file. This executable file can be executed in all windows computers.

So, now we need to make it run every time the system restarts. For that, there is a folder in windows file system where all the files inside that folder will be executed using the default applications whenever the system boots up.

So, we can add the executable file which we created to the startup folder and we can make it execute every time the system power on.

IV. TECHNOLOGIES USED

A. Python

All the work done in this project is based on python. Both the client and Server code are scripted using python. In the recent times, many of the security scripts are being written in Bash, Python, and PHP. As python is simple and robust language, it is used mostly among all other option.

B. Modules Used

1) Socket Module

This module is used for communication among devices in the network. Socket acts as a communication link between the two systems in communication.

2) Subprocess Module

Subprocess is used to execute the command line commands and store the result into an object.

3) Threading module

Threading is used to break the program into multiple parts and make them execute parallelly so that the execution of the program is boosted.

4) Pyinstaller module

The Pyinstaller module is a python module which is used to convert the python scripts into windows executable .exe files.

V. IMPLEMENTATION AND RESULTS

Implementation of this project requires a server which runs actively which is used by the attacker. Since the target system needs to connect to the attacker, attacker computer needs to be listening to the incoming connections all the time. So, the implementation will be as follows:

1) STEP-1: Running the Script on the Victim's Computer

Initially the reverse shell python code needs to be executed in the victim's computer using the pyinstaller module to convert that into the .exe file. This file will be stored in the new folder called dist which is created in the current folder. This exe file needs to be added to the shell: start folder which is executed every time the system boots up.

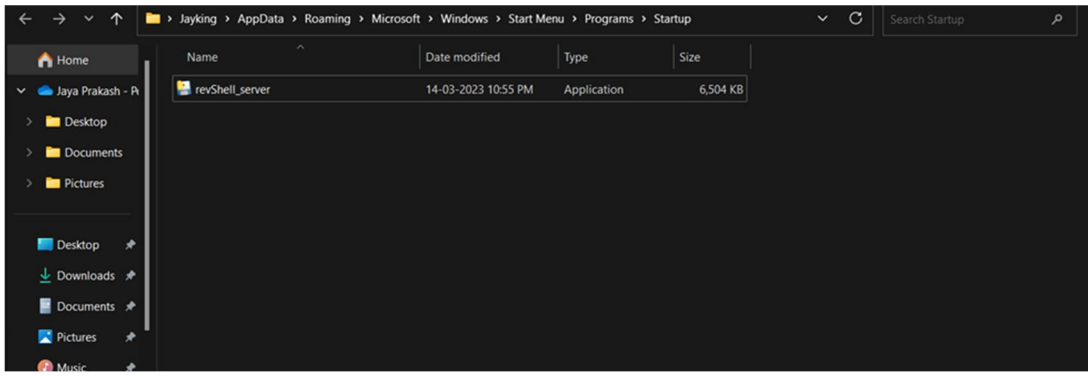


Fig.1 Exe file placed in startup folder.

2) STEP-2: Running Netcat on attacker's Computer and connecting target

A As the reverse shell script is already running on the target's computer, now attacker can use his terminal with netcat tool to access that reverse shell and do whatever he wants. For that he wants to install netcat tool in his system. For Linux we can use the following command.

Sudo apt-get install netcat-openbsd

Now we can connect using the command as follows.

Netcat [ip_address] [port_number]

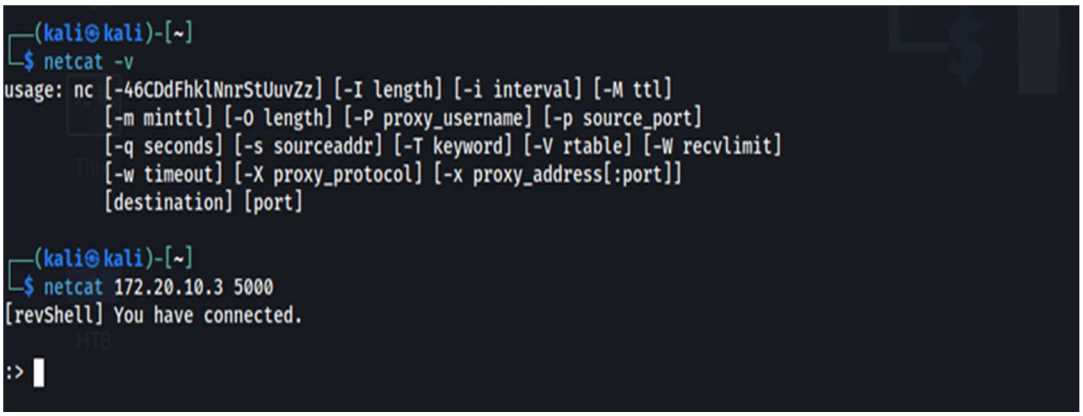


Fig. 2 Netcat on attacker's computer

3) STEP-3: Gaining Interactive Shell

Now, we are connected to the reverse shell. We can verify it using whoami command which gives us the username of target computer and we can execute any command we want to execute and have full control over the target computer.

Fig. 3 Obtained Interactive Shell

4) Results

After connecting to the victim's computer, attacker can use any windows native commands to run them on the victim's computer. In addition to them, we use our special data object to obtain some additional information about the target. They are as follows:

data.ip: Used to fetch the IP address of the victim's computer.

data.mac: Used to fetch mac address of the victim's computer.

data.hostname: Used to fetch the hostname of the victim's computer.

data.machine: Used to fetch the operating system that is being run on the victim's computer.

data.core: Used to fetch the processor that is being used in the victim's computer.

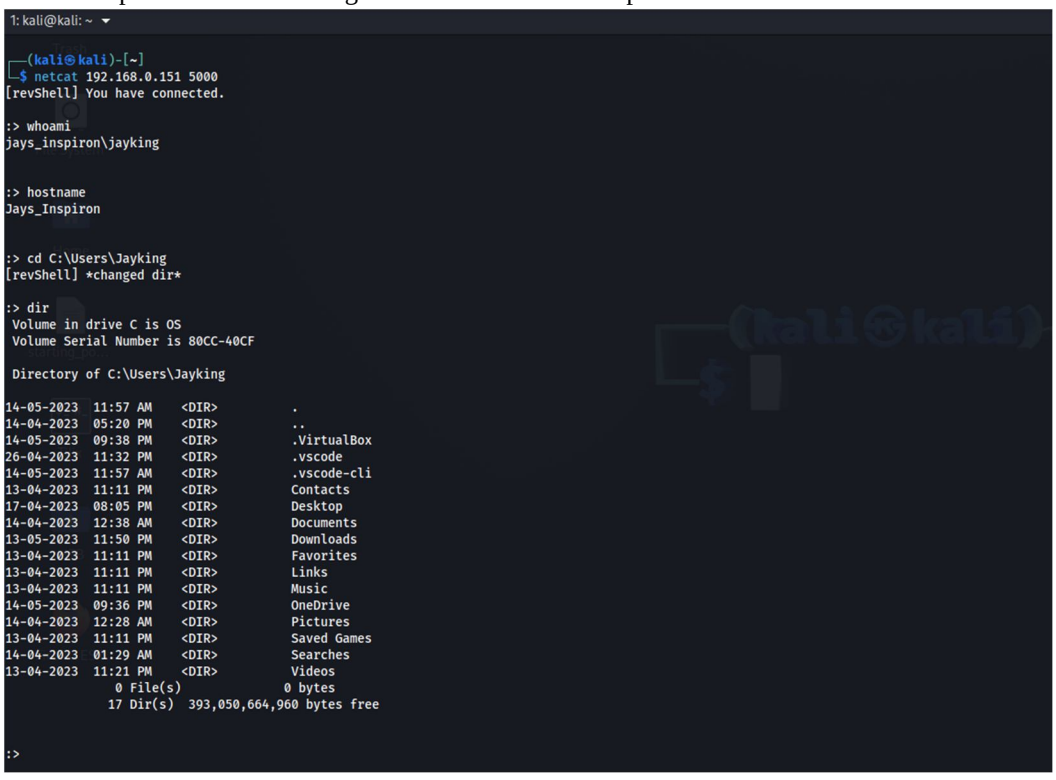


Fig. 4 Using Target's Terminal on Attacker's Computer

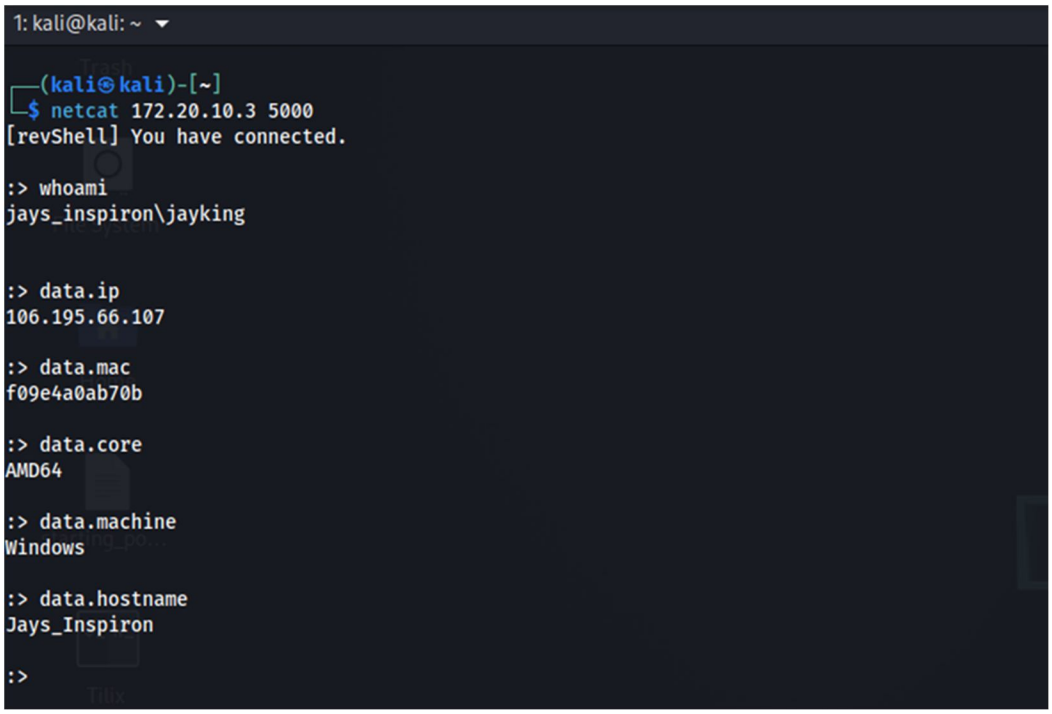


Fig. 5 Using Data object specific commands on Attacker's Computer

VI. PREVENTIVE MEASURES

Most of the attackers use reverse shell for gaining access to a remote computer. Due to its ability of remote administration, it is most often used by attackers in most of the attacks. According to the client, it is very difficult to block the reverse shell connections due to outgoing traffic instead of incoming connections. So, there is no direct approach of gaining resistance from reverse shell attacks. All we can do to minimize the effect of reverse shell is harden our systems with security best practices. Some of the techniques which are used to harden the security of system are as follows:

1) Blocking all the outgoing traffic and new connections help us in keeping attackers away from our computer as the reverse shell cannot be produced without outgoing connections from the target system.
2) Using a Proxy Server help us in a great extinct in preventing reverse shell as it appears to be some other server IP rather than our own IP address to the attacker. If attacker tries to target your IP, he will be targeting the proxy server.
3) It is always advisable to use any anti-virus software as it will be running in the background always and help us in identifying the known malwares and any suspicious files in the system.
4) Updating the system regularly helps us in covering security patches which were identified for the system from the recent security patch.
5) Keeping any application which, you do not use is an added security threat to your computer. We never know which application is vulnerable to which attack. So, it will be best if you regularly check and remove unused applications for a long time.
6) In case of victims who are unaware of security and cyber-attacks, attackers generally try to send mails including something that the victim would be tricked to open. This might contain malicious scripts which can generate a reverse shell to attacker.
7) Everyone in the present world use browsers to surf internet. We go through millions of links in our daily life. We do not know which malicious file is behind which link. So, never click on unknown links.
8) Using the firewall is always a best option to prefer. It helps us in preventing the incoming connections to specified ports, from specified Ips, etc. It helps in keeping attackers away from our systems.
9) If we have a web server running, always ensure the filetype if the server takes file input from the users. This may lead to file inclusion vulnerability if we do not verify the filetype of server.
10) If the same server takes input in text form, always sanitize the input as it may lead to command injection, SQL injection, and some other harmful vulnerabilities.
11) Always maintain the systems password protected. This will help us in keeping the data encrypted even if attacker got access to the physical system.

12) It is always advisable to use strong passphrases instead of passwords as it will be hard for dictionary and brute-force attacks.
13) Changing the passwords time to time also helps in keeping security system strong. Even if the attacker gets the password once, it will be no longer useful for him if we change our password.
14) Never share any information (either personal or professional) on unsecure and unknown lines and networks. Attackers can listen to these lines and get the information we transmitted over that line.
15) Always prefer using the user account with minimum privileges and permissions. Even if we do something wrong, this will prevent us from doing the tasks which may harm the system and make it vulnerable. Even if the attacker gets the shell of the user, he will not have high level privileges as the user account has low level privileges.

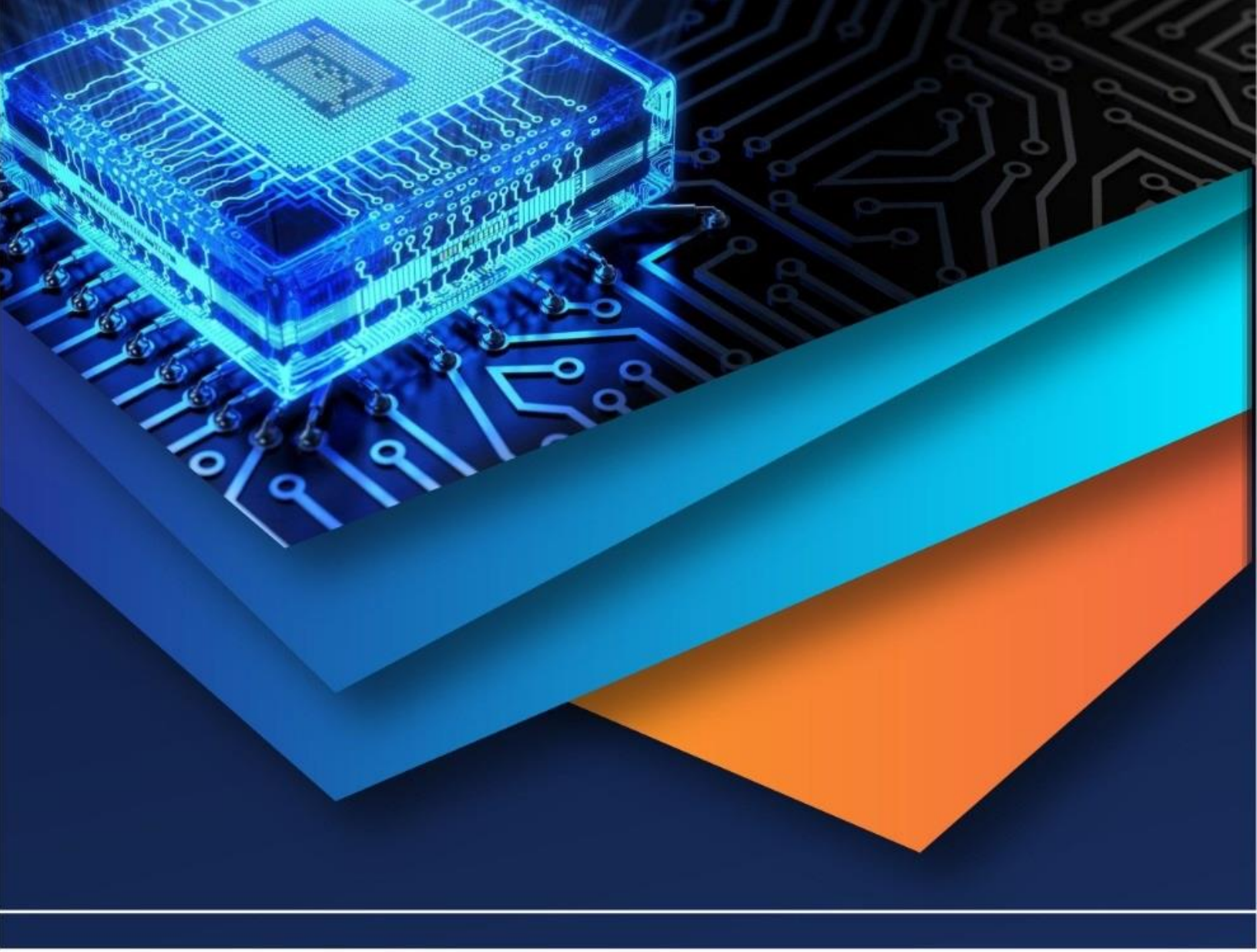
VII. CONCLUSION

By this project, we facilitated the use of Reverse Shell without any intrusion from the target system. Applied a new implementation of interacting with Victim's Terminal without any notice of victim. Applying this security project for the good of companies will help them to analyze the extent of security they have. Penetration testers can use this to generate the reverse shells from many targets without creating servers many times.

This process can further be upgraded by making this work successfully outside the LAN. We can also add several new functionalities like managing the connections from the prompt without entering the system.

REFERENCES

[1] Keshav Kaushik, Sakshi Aggarwal, "A novel approach to generate a reverse shell: Exploitation and Prevention" in Researchgate article, September, 2021, pp. 83-93.
[2] M. Sullivan, "8 Types of Cyber Attacks your Business Needs to Avoid," Intuit, online.
[3] X. Yue, W. Chen, and Y. Wang, "The Research of Firewall Technology in Computer Security," pp. 1-4, 2009.
[4] M. Bongard and D. Illi, "Reverse Shell via Voice (SIP, Skype)," Dec. 2019.
[5] C. Atwell, T. Blasi, and T. Hayajneh, "Reverse TCP and Social Engineering Attacks in the Era of Big Data," pp. 1- 6, 2016.
[6] L. Chenke, Y. Feng, G. Qiyuan, Y. Jiateng, and X. Jian, "Anti-reverse-engineering tool of executable files on the windows platform," in Proceedings - 2017 IEEE International Conference on Computational Science and Engineering and IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, CSE and EUC 2017, Aug. 2017, vol. 1, pp. 797–800, doi: 10.1109/CSE-EUC.2017.158.
[7] J. Uitto, S. Rauti, J.-M. Mäkelä, and V. Leppänen, "Preventing malicious attacks by diversifying Linux shell commands."
[8] "Understanding Reverse Shells | Netsparker." https://www.netsparker.com/blog/web-security/understanding-reverse-shells.
[9] Y.-G. Li, Y.-C. Chung, K. Hwang, and Y. Li, "Virtual Wall: Filtering Rootkit Attacks To Protect Linux Kernel Functions," IEEE Trans. Comput., pp. 1–1, Sep. 2020, doi: 10.1109/tc.2020.3022023.
[10] "Command injection: how it works, what are the risks, and how to prevent it | Snyk." https://snyk.io/blog/command-injection.
[11] "Unrestricted File Upload | OWASP." https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload.
[12] X. Lin, L. Lei, Y. Wang, J. Jing, K. Sun, and Q. Zhou, "A measurement study on linux container security: Attacks and countermeasures," in ACM International Conference Proceeding Series, Dec. 2018, vol. 18, pp. 418–429.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY