iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41875

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 10 Issue IV Apr 2022- Available at www.ijraset.com

Unavailability of Python Tool Which Can Perform Various Hacking Activities

Abhishek Gadge[1], Atharv Temkar[2], Mr. Pranav R. Shriram[3], Ahmad Raza Qadri[4], Shraddha Choudhary[5]
[1, 2, 3, 4, 5]*Computer Engineering, MIT AOE, Pune, India*

Abstract: ***Multi Technique Hacking is implemented with all three functions in a single interface, that is, Http Packet Credential Harvesting, IP Spoofing and Packet Modification and There is no existing system in which all the functions have been used together. It describes how the process is done and how they go about helping their customers find and plug up security holes. The hacking process is explained, along with many of the challenges and opportunities in the field of ethical hacking. This hacking technique is done using scapy library which is a very big library with plenty of functions available for use. To understand the working of the library firstly the practice has to be done using the library and then try to implement it in the code. Ethical hacking, also known as penetration testing, penetration testing, or the red team, has become a major concern for businesses and governments. Companies are concerned about the possibility of being hacked and prospects are concerned about managing their personal information. This Paper describes how the process works and helps customers find and close security gaps. The hacking process is described with many challenges and opportunities in the field of ethical hacking***
Keywords: Scapy, IP Spoofing, Credential Harvesting, Packet Modification.

I. INTRODUCTION

In the current era of digitalization and advanced networking we need knowledge about protecting our privacy and digital network. Doing so may result in using some tools to perform attacks on our network to test the level or protection of our systems. To ease the task of performing network attacks, there is a tool which can use multiple techniques to perform the attacks, i.e., Multi Technique Hacking Tool. This Paper provides minimal guidelines (and requirements) for multi-technical hacking tools. It is a model and guide for multi-technique hacking tools. Aim is to develop the tools that can use Python's Scapy library to eavesdrop on credentials, IP spoofing, and modify packets and our tool will be able to perform all this operation. This is basically a hacking attempt to gain unauthorized access to information by acting as a system or network change or its weakness. The structure of this manual is as follows. Section 2 (Methods and Materials) provides details of the device or device modification specifically designed for investigation and a diagram of the modification, if applicable. Section 3 (Results and Discussion) describes the findings and an analysis of these results.

II. LITERATURE REVIEW

A. Related work And State of the Art (Latest work)

Craig S Wright et al [1] explained how to follow the shellcode and interpret the jumps and calls it contains. It can be said that shellcode has a shelf life. As samples become more common and widely used in the underground community, they are gradually being added to IDS and antimalware signatures. Extensive shellcode, which is also used in Metasploit projects, has a particularly short lifespan.

This doesn't mean it's useless for many websites, but it can be less valuable when testing secure websites. In many cases, changing a small piece of shellcode can cause the generated signature to detect, warn, and block and invalidate it. For example, make minor changes to existing shellcode that runs "/ bin / csh" instead of the standard call "/ bin / sh". You can extend the validity period of the shellcode. Once you've learned how shellcode is created and formed, you can also start modifying and extending shellcode, executing various payloads, or modifying forms to avoid detection.

Rohith Raj S [2] Scapy is very robust and very easy to use. Scapy is very useful for rapid security analysis. But if I want to review it from time to time, I can draw your own conclusions without spending raw. No actual explanation is needed. Scapy has a number of very good user and developer methods to help you work with packages. If the programmer needs to use a custom package to get results. Scapy, which tests firewall or intrusion detection system methods, is very useful when responding to custom packets. The really nice thing about A Scapy is that it can be used as Python.

©IJRASET: All Rights are Reserved

A library that allows you to create and create programs. Apply your application very quickly without digging deeper. The details of how to create a raw package from scratch can help significantly reduce the size of your code. In short, it gives us the freedom to try whatever we can. Visualize over the network.

Roshan Poudél [3] Develop a step-by-step packet sniffer using Python and Scapy. including:
Step 1- shows the installation of scapy on the operating system.
Step 2- is to create a Python file and import the module.
Step 3- Create the function in step 3. You can also use the prn parameter to help sniff packets continuously.
Step 4- is to classify the packets into TCP and UDP. Step 5- classifies packets into incoming and outgoing packets.
Step 6- is to print all the information you need on the console.

Jiajia Chen et al [4] To understand today's network applications, the survey analyzed the traffic characteristics of Internet applications. In this document, response time is calculated by combining HTTP traffic request and response messages. In addition, a statistical analysis of this response time is performed.
Traditional passive network measurement technology used to capture web traffic. Analysis shows that the top 10 web servers have response times of 199.78ms for Nginx, 253.25ms for Apache, 198.19ms for IIS, 89.34ms for Tengine, Cafe 190.66ms, AmazonS3 260.86ms, ECS 284.39ms, ATS 256.52ms, Openresty. 214.12ms, DnionOS127.36ms. Philippe BIONDI [5] Described packet generation and network-based attacks using scapy.
The prior art includes a rapid target classification method for packaging tools. When the problem of the tool is discussed and the tool cannot accurately forge the requirements or interpret what is obtained. Below is a step-by-step breakdown of packet operations, sniffing, and PCAP file format interfaces, various types of package lists, and high-level commands. Finally, before drawing any conclusions, let's talk about network detection and attacks.

B. Limitation of State-of-the-Art Techniques

This is available on the Debian Linux operating system; preferably Kali Linux; Here, Python 3 is installed with the Scapy framework of Python. The user also needs to make sure they have an external Wi-Fi card to make sure that surveillance mode is enabled and packets are being captured.

C. Discussion and future direction

This is strictly to be used for educational and ethical purposes and is advised to be used with a virtual machine before being used on a real project / OS.

III. METHODS AND MATERIAL

This tool is available on the Debian Linux operating system; preferably Kali Linux; Here, Python 3 is installed with the Scapy framework of Python. Python's Tkinter GUI.
The user also needs to make sure they have an external Wi-Fi card to make sure that surveillance mode is enabled and packets are being captured. Following attacks will be done by our tool:

A. Approach

The user can select the type of attack they want to perform and then they have to fill in the details for the type of attacks they want to perform. In first attack, a http website has to be open and then the code needs to be executed, and then the code will do the sniffing and ask to save the credentials in a file. In the second attack the user has to fill in the IP address and ports to direct the spoofed packets. In the third attack, the user will have to fill in all the various fields that are needed in the packet modifier.

B. Architecture of Systems

In Figure I, we can see the architecture as well as data flow of the proposed system. There are 3 tools in our system. Firstly, user has to choose a tool which he/she has to perform.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

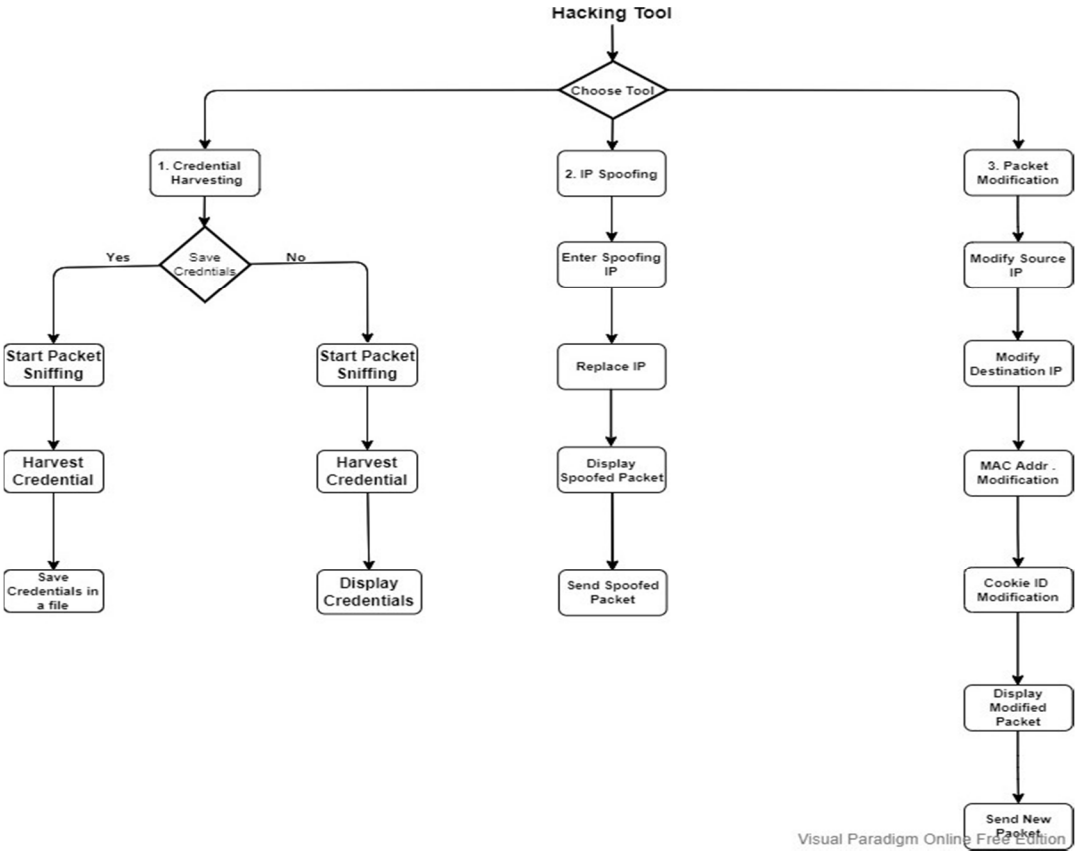


Figure I

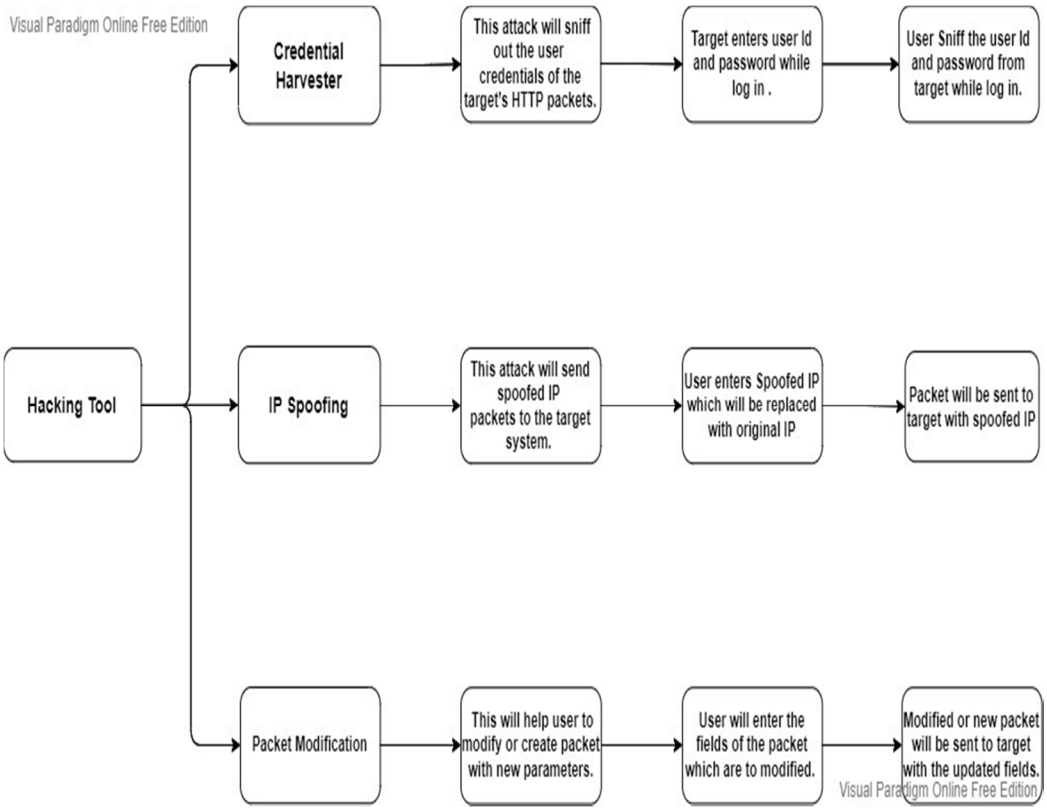


Figure 2

C. *If user Select*

1) Credential Harvesting: This will give user option whether to save the data or not, after that model will start sniffing the packet after completion it will harvest the credentials and display or save the data whichever the user has chosen.
2) IP Spoofing: After selecting the tool, user will have to enter spoofing IP after that tool will replace original IP with spoofed IP and display new packet (with replaced IP) followed by sending spoofed packet in a loop.
3) Packet Modification: In this tool, user will have a choice of TCP and UDP after selecting one, user will have to enter some field like mac, source IP, destination IP, source port, destination port after entering the details tool will display new packet and send it to destination.

D. *Analysis of Tools*

1) *HTTP Credential Harvesting*

a) *Description:* This attack will sniff out the user credentials of the target's HTTP packets.
b) *Response Sequences:* Once the user selects from the main menu the choice 1, he will be redirected to the menu for this attack, which will ask the user If the credentials need to be saved to a file or should the attack proceed without saving credentials in a file.
c) *Functional Requirements:* Scapy for scanning the network packets and filtering them according to the protocol

2) *IP Spoofing*

a) *Description:* This attack will send spoofed IP packets to the target system.
b) *Response Sequences:* Once the user selects from the main menu the choice 2, he will be redirected to the menu for this attack, which will ask the user for the new IP address which will be replaced in the original packet and then the packet will be sent to the target with a spoofed source IP.
c) *Functional Requirements:* Scapy, for replacing the IP address in the packet with the new IP.

3) *Packet Modification*

a) *Description:* This attack will help the user to modify the packet with new parameters.
b) *Response Sequences:* Once the user selects from the main menu the choice 3, he will be redirected to the menu for this attack, which will ask the user for the fields that are modifiable in the packet and then the modified packet will be sent to the target.
c) *Functional Requirements:* Scapy, for ensuring that the packets are modified or a new packet is created from scratch.

IV. RESULTS AND DISCUSSION

A. *HTTP Sniffing*

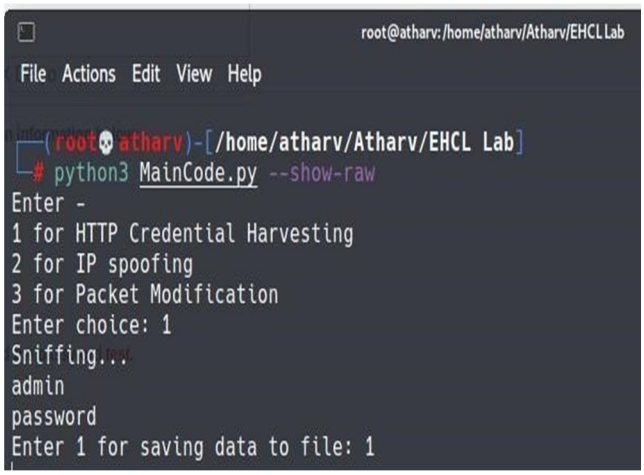


Fig. 1

Figure 1 describes Menu and Input examples for HTTP cred sniffing.

B. Saved Credentials in a File

Fig. II

Figure 2 describes Output of HTTP cred sniffing saved in a separate txt file by default

C. IP Spoofing Menu

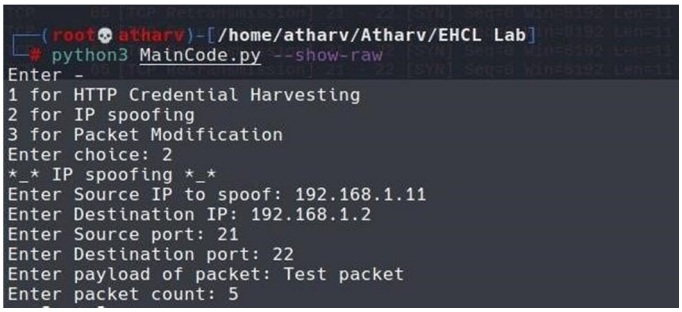


Fig. III

Figure 3 describes Menu and Input examples for IP spoofing

D. IP Spoofing Packet

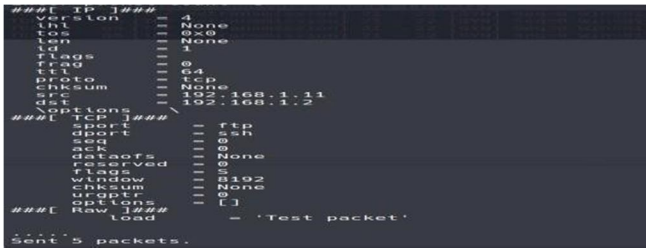


Fig. IV

Figure 4 shows Output of IP spoofing, with the raw packet and sent packet count.

E. Packet Modification Menu

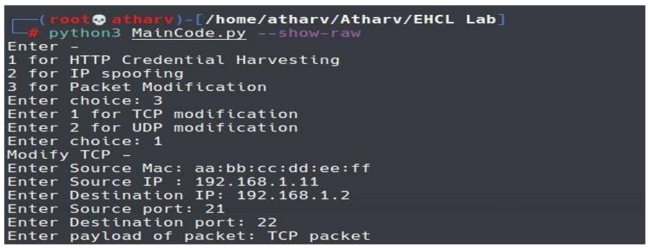


Fig. V

Figure 5 shows Menu and Input examples for Packet Modification.

F. Modified Packet

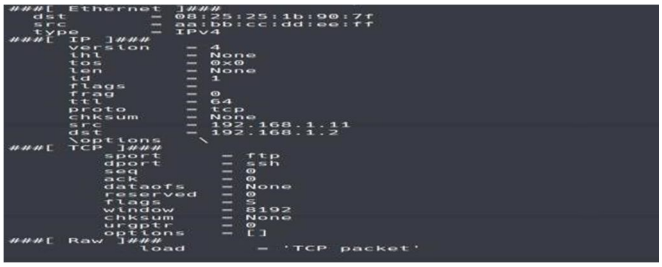
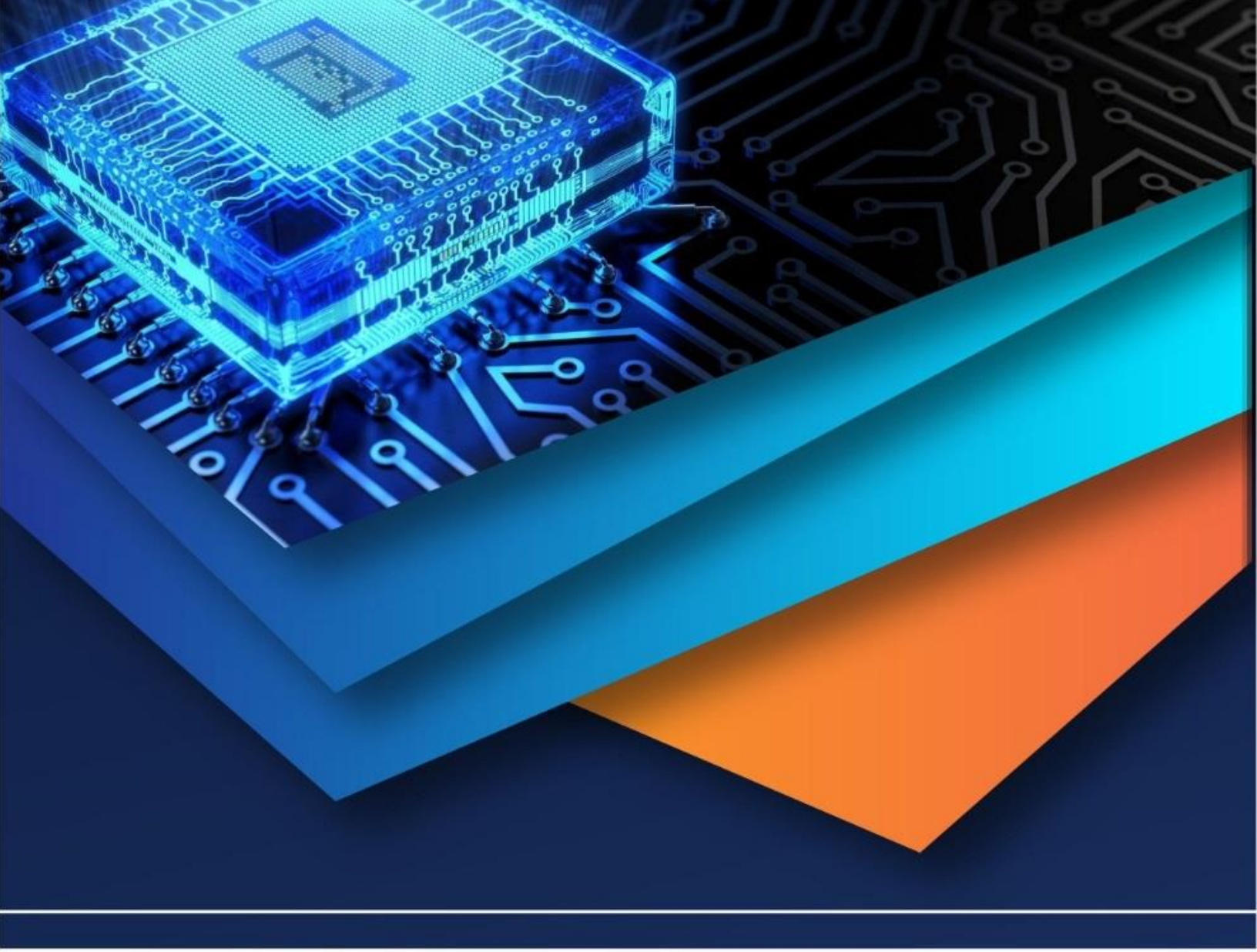


Fig. VI

Figure 6 depicts Output of Packet modification, with the raw packet before it is sent.

REFERENCES

[1] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3153525
[2] https://ieeexplore.ieee.org/document/8903954
[3] https://www.exploit-db.com/docs/48606
[4] https://www.researchgate.net/publication/311757131_Analysis_of_web_traffic_based_on_HTTP_protocol
[5] https://scapy.net/conf/scapy_T2.pdf
[6] Bansal S, Bansal N (2015) Scapy – A Python Tool Für Security Test. J Comput Sci Syst Biol 8: 140159. doi: 10.4172 /jcsb.1000182.
[7] Biondi, P. (2018). Scapy: Python2 and Python3 package creation.
[8] Duchene, J., Le Guernic, C., Alata, E., Nicomette, V. , And Kaaniche, M. (2018). State-of-the-art Network Pro ˆ An exemplary network protocol draft 737tocol reverse engineering tool for security testing of industrial automation systems. Journal of Computer Virology and Hacking Techniques, 14 (1): 53-68
[9] Potter, B. and McGraw, G. (2004). Software security testing. IEEE Security and Data Protection, 2 (5): 81–85.
[10] P.Biondi,2002 Linux Net filter NAT/ICMP code information leak
[11] http://secdev.org/conf/scapy_T2.pdf
[12] http://secdev.org/conf/scapy_csw05.pdf
[13] https://scapy.readthedocs.io/en/latest/usage.h tml
[14] Learning Python by O'Reilly and Mark Lutz



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)