NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 1, June 2023
E-ISSN - 2583-7559

Overwhelming Threat Based Analysis Techniques

Darsh Patel
Center of Excellence In Cyber Security, National Forensic Sciences University
Gandhinagar, Gujarat, India
darsh.patel@nfsu.ac.in

Abstract— Distributed Denial of Service (TCP Syn) attacks have become a significant threat to networked systems and online services. These attacks aim to disrupt the availability of a target system by overwhelming it with a flood of malicious traffic. This abstract provides an overview of TCP Syn attacks, their impact, and mitigation techniques. To mitigate the impact of TCP Syn attacks, the abstract introduces different defense mechanisms, including traffic filtering, rate limiting, and anomaly detection. It highlights the importance of early detection and response to minimize the damage caused by attacks. Finally, the abstract concludes by discussing the future challenges and trends in TCP Syn attacks. It mentions the emergence of new attack vectors, such as Internet of Things (IoT) devices, and the need for continuous research and development of robust defense strategies.

Keywords: Volumetric Attacks, Socket Building, TCP Syn Request, Compromise of router, SYN Flooding, I/O Graph, Suspected Frames, Application Protocols, Weak Encryption, Frame Analysis, DNS Session

I. INTRODUCTION

Understanding the motivations behind TCP Syn attacks is crucial for developing effective countermeasures. Attackers may have different motives, including financial gain, political activism, or simply the desire to cause disruption. The impact of successful TCP Syn attacks can be severe, leading to financial losses, operational downtime, tarnished reputation, and potential legal ramifications.

To comprehensively analyze TCP Syn attacks, it is important to examine the various attack vectors and techniques employed by attackers. Volumetric attacks, which aim to exhaust network bandwidth, involve flooding the target with an overwhelming amount of traffic. Protocol attacks exploit vulnerabilities in network protocols, targeting the infrastructure itself. Application-layer attacks focus on overwhelming specific services or applications by exploiting weaknesses in their design or implementation.

In response to the escalating threat landscape, numerous defense mechanisms have been developed to mitigate the impact of TCP Syn attacks. These include traffic filtering, rate limiting, anomaly detection, and adaptive mitigation strategies.[1] However, attackers continuously evolve their techniques, necessitating ongoing research and development of robust defense strategies.

II. RELATED WORK

In this paper we document our findings on weak encryption in the router base admin configuration application. Weak encryption is a popular field of research in information security especially applied to network components or for web services .A vast number of protocols has been designed to provide high encryption ,

The aforementioned related work highlights the diverse approaches and techniques that researchers have employed to understand and counter TCP Syn attacks. By building upon these studies and considering the evolving threat landscape, research paper aims to contribute further insights into the analysis and mitigation of TCP Syn attacks, with the objective of improving the security and availability of networked systems.[2]

III. EXPERIMENTAL SETUP

In this research paper TP Link Multi-WAN router for our security setup, and the attacker used a workstation running Kali Linux. Wireshark was used along with the .pcap file to listen to the HTTPS and TCP traffic. Network miner is used to detect operating systems, sniffing and capturing packet, and open ports. The Slowloris HTTPS attack, which mimics the TCP SYN flood handshake attack, was utilized to overwhelm the router's traffic. All components will be act as an intruder,intercepting and analysis signature of the suspected frames of TCP Syn and related header information.

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 1, June 2023
E-ISSN - 2583-7559

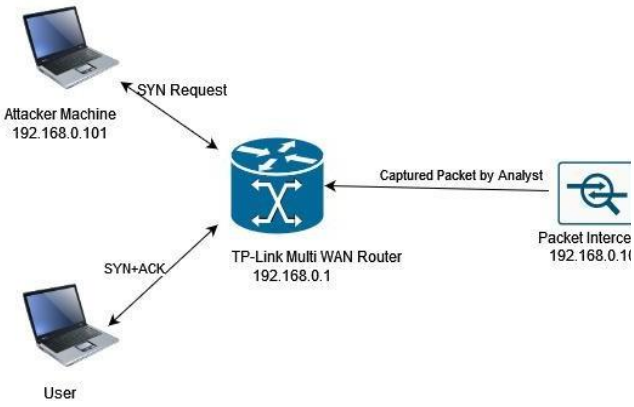

Fig. 1: Experimental setup for TCP Syn Attack

IV. METHODOLOGY

A Tcp Syn attack is a suspected attempt to crash or halm the functioning of a network related services or web servers by large number requests hit it with a flood of SYN traffic. TCP Syn attacks are typically carried out using a large number of compromised devices, forming a botnet, which are controlled by the attacker.
The attacker identifies the target or targets they want to attack. They may perform reconnaissance to gather information about the target's network, services, and vulnerabilities.
Based on the gathered information, the attacker determines the type of TCP Syn attack they want to launch, such as volumetric, application layer, or protocol-based attacks. They also decide on the attack vectors and techniques they will employ.

A TCP SYN flood attack is a type of TCP Syn attack that exploits the TCP three-way handshake process.
In a normal TCP connection establishment, a user sends a SYN packet to the main server, the main server replies with a SYN & ACK packets, and the user acknowledges the SYN-ACK with an ACK packet to complete the connection.[3]
In this paper flag SYN flood attack, the attacker transmit a overwhelming requests number of SYN packets to the victim server without completing the handshake process by transmitting ACK packets. This causes the server to allocate resources for half-open connections, exhausting the server's resources such as memory and processing power. As a result, legitimate users are unable to establish connections with the server, causing a denial of service.

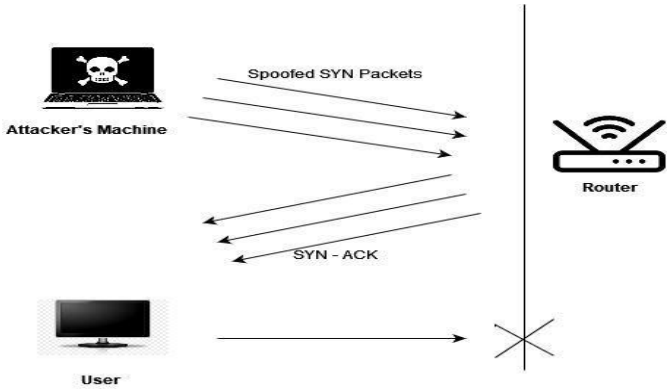

Fig 2: Connection Established of SYN Request

By sending partial requests and keeping the connections open, the attacker consumes the server's resources, such as connection slots and thread pools, gradually depleting them until legitimate users are unable to establish new connections. Perls based framework attacks exploit the vulnerability in web servers that allow a large number of concurrent connections without proper timeouts.[4]

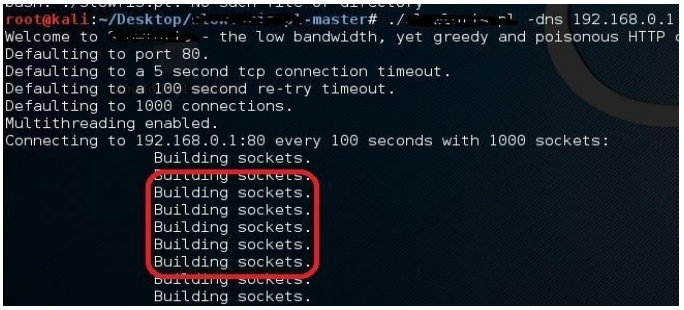

Fig. 3:Socket Building for TCP Syn Request

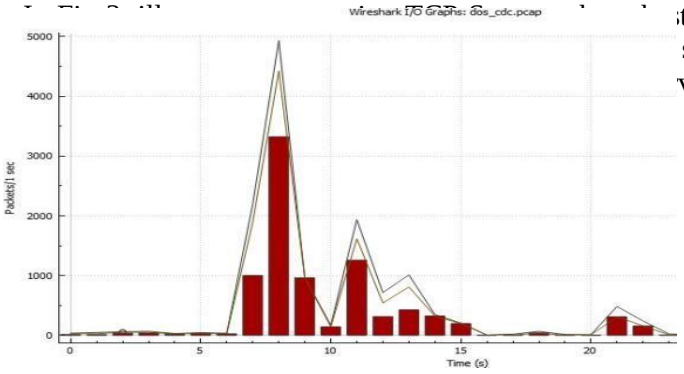

Fig.4 I/O Graph TCP Syn Attack

The attacker initiates a connection request by sending a TCP SYN packet to the target server. This SYN packet contains the attacker's IP address as the source address and a random port number.
In Fig 4, graphic representation of an ongoing TCP Syn attack. It vividly portrays the torrential influx of network traffic directed at the targeted system, surpassing its

capacity and inducing unresponsiveness. The attack's origin and its magnitude are distinctly delineated, imparting invaluable technical insights into the intricacies and ramifications of the TCP Syn attack.

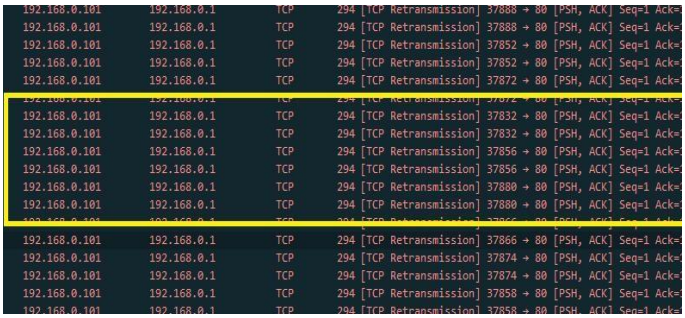

Fig 5: Suspected Frames of TCP Syn

The flags produced by the TCP Protocol Analysis in reaction to the startling influx/suspected of re-transmitted packets in less than a second iRTT are seen in this image obtained from Wireshark.[5]

In Fig 5,amount of TCP packets that are getting acknowledged, sent from the attackers IP of 192.168.0.101to the victim's IP of 192.168.0.1 through port 80.

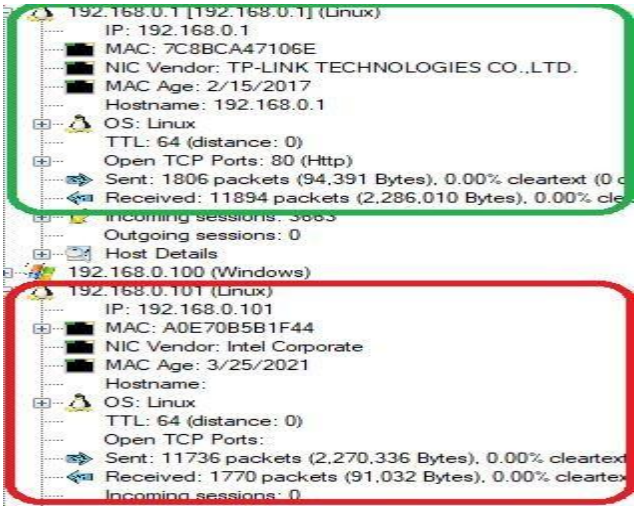

Fig 6:Session Summary of Incident

In Fig:6. presents the Network Miner's representation of a TCP Syn attack targeting a router with IP address victim 192.168.0.1(Green mark) The attack was executed by a Kali Linux OS with attacker's IP address 192.168.0.101(Red Mark) By analyzing the screenshot, we can discern the involved systems as evidenced by the IP activity. Notably, the IP address 192.168.0.1 has received a staggering influx of 11,894 packets, all originating from the IP address 192.168.0.101.[6]

V. CONCLUSION

Through this security test, we were able to access and analyze the behavior and pattern of TCP Syn attacks made against network devices. Our study showed that network devices in an open network are vulnerable to TCP Syn assaults, which overwhelm and obstruct packet transmission flow through routers. It was shown how an attacker may take control of the target devices and stop their network communication either momentarily or permanently. Poorly designed policies and subpar implementation are the cause of all the well-known flaws. Despite not endangering lives,it will have a significant impact that will permanently halt the incoming and outgoing traffic in a network and render it useless for a while.

VII. ACKNOWLEDGMENT

This work was supported by Center of Excellence in Cyber Security,National Forensic Sciences University,GandhinagarGujarat, India, that provided the technical mechanism and the platform used for the development and security testing of the solutions.

VIII. REFERENCES

[1] https://www.researchgate.net/publication/313222794_DDoS_Attack_Detection_and_Mitigation_Using_SDN_Methods_Practices_and_Solutions

[2] https://www.hindawi.com/journals/scn/2022/2593672/
Lightweight Statistical Approach towards TCP SYN Flood DDoS Attack Detection and Mitigation in SDN Environment

[3] https://www.cs.toronto.edu/~arnold/427/15s/csc427/indepth/syn-flooding/index.html

[4] https://hal.science/hal-03739848v1/preview/rios-access2022.pdf

[5] https://ask.wireshark.org/question/4170/please-explain-this-tcp-retransmission-sequence/
TCP Retransmission Sequence

[6] https://www.inderscience.com/info/inarticle.php?artid=118542
Network forensics investigation: behaviour analysis of distinct operating systems to detect and identify the host

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 1, June 2023
E-ISSN - 2583-7559