Wireshark & Risk Analysis

Ryan Livinghouse

CSC341 – 020

Professor Thiep Pham

December 3, 2023

Abstract

This project explores the application of risk management principles in analyzing network security using the program Wireshark. After analyzing the PCAP file, a SYN flood attack was identified, targeting the network layer. This particular study details the implications of this attack on network operations, particularly impacting the institution's reputation due to potential service disruptions. The chosen risk management strategy was mitigation, involving strengthening network defenses and regular penetration testing. This approach aims to minimize the likelihood and impact of this type of cyber threat. The residual risk highlights the need for continuous adaptation to emerging cyber threats.

Keywords: risk management, Wireshark, SYN flood attack, network security, penetration testing, DDoS.

Contents

Analyze a Complex Problem (CSIT-11)

1.1. About Wireshark

Wireshark is a powerful tool for anyone looking into network security. It is a free, open-source network packed analyzer. The tool looks at the details of network traffic in real time. It is used to troubleshoot networks with connection and performance issues, making it a top pick for cybersecurity professionals. These experts use Wireshark to trace network connections and access the contents of suspected transactions. The tool is used to monitor and catch criminal and malicious activity over a network.

As the most commonly used packet sniffer in the world, Wireshark captures packets from a network connection. This could be anything from a personal computer to a large office network or even the internet. What makes Wireshark stand out is its ability to let users capture and interact with this data traffic. It gives a clear picture of what is happening on a network, which is critical for identifying and troubleshooting issues, whether they are performance or security related.

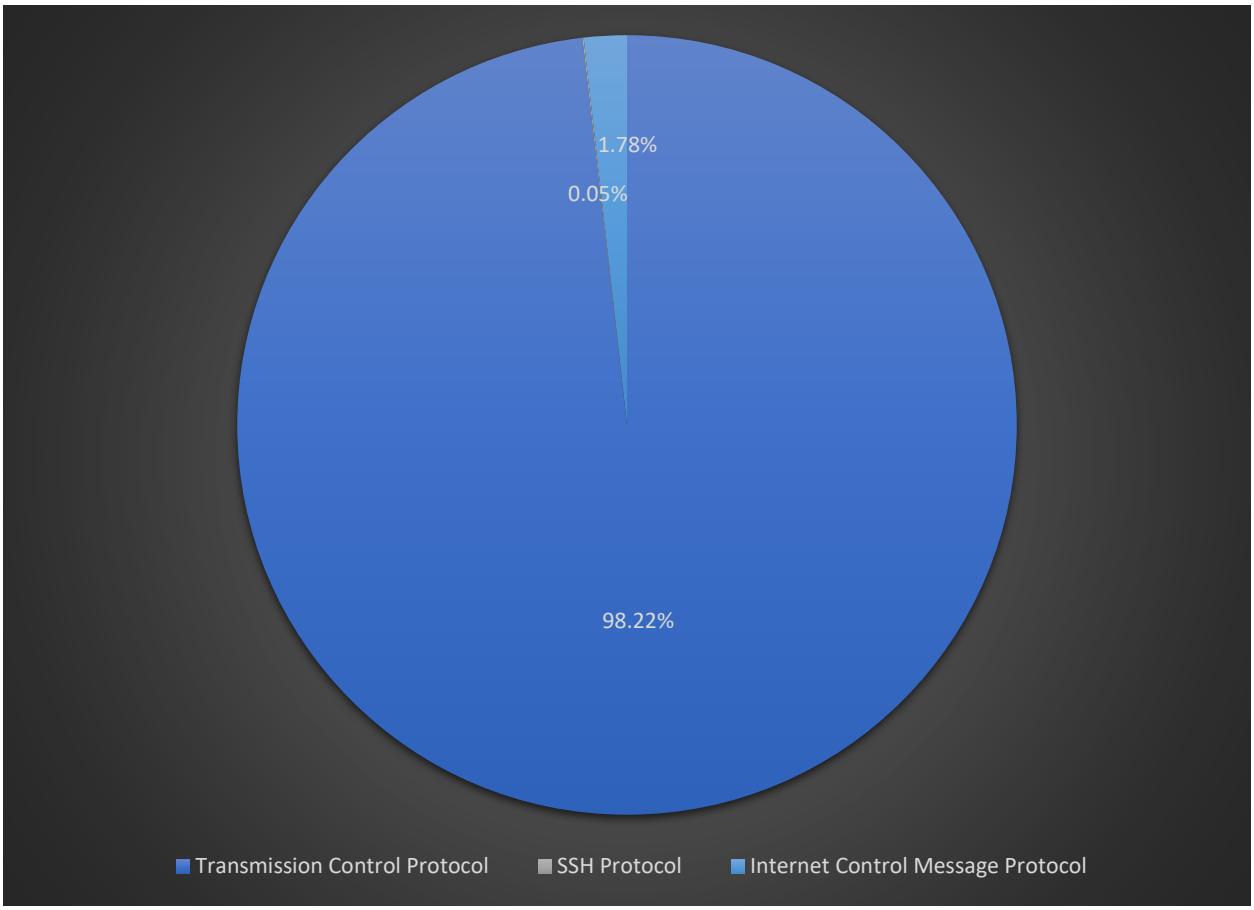
Wireshark is particularly useful for understanding how communication happens over a network. It is a tool highly utilized by network administrators and security engineers, who rely on its packet understanding capabilities to analyze communication problems and examine network security issues (What Is Wireshark).

1.2. Advantages and disadvantages of Wireshark

The main advantage of Wireshark is its detailed analysis capability. It can capture every packet on a network, providing a user-friendly view of what is happening. This level of detail is invaluable for troubleshooting and security analysis. However, its major disadvantage is also the amount of data it generates. The traffic going through the network can be overwhelming and

requires significant filtering to interpret effectively. Additionally, because it captures all packet data, there are potential privacy concerns, especially if used on a network carrying sensitive information.

1.3. Key protocols discovered



TCP, or Transmission Control Protocol, is a fundamental standard for data exchange in network communications, ensuring reliable and ordered transmission of data between devices. Dating back to its inception in 1973 by Robert E. Kahn and Vinton G. Cerf and standardized in 1983, TCP provides a reliable connection that automatically corrects any data loss. It facilitates two-way data transmission, where systems can simultaneously send and receive data, using segments (packets) with a payload and control information. The protocol is crucial for the

functioning of the internet, as it supports a wide range of services including web browsing, email, and file transfers, forming an essential component of the TCP/IP protocol stack and operating at the transport layer (History of TCP/IP)(IONOS).

SSH (Secure Shell Protocol) is a cryptographic protocol used for secure network services over an unsecured network. Its primary applications include secure remote logins and command execution. This ensures the integrity and the confidentiality of the data that is being sent over the unsecured network. Although it represents such a minor percentage of traffic (0.05%), its role in maintaining secure communications is significant.

The Internet Control Message Protocol (ICMP), accounting for 1.78% of the traffic in this network capture, is inherent for managing and troubleshooting network operations. Primarily utilized for error reporting, ICMP alerts systems when data fails to reach its intended target. For instance, if a data packet exceeds the size limit that a router can process, ICMP sends back a message to the source, indicating the issue. Beyond error messages, ICMP supports network diagnostic functions. Tools like traceroute and ping rely on ICMP to trace the path between two connected devices and measures connection speed. While ICMP is critical for maintaining network health, it is also known for its susceptibility to misuse in network attacks like ICMP floods and ping of death (a type of denial of service—DoS—attack) (Ping of Death) (What Is ICMP).

1.4. PCAP analysis

The PCAP review reveals that a pattern of SYN-ACK packets, commonly associated with the TCP three way handshake, originating from a diverse range of IP addresses, but targeting a single IP address (10.10.10.10). Notably, entries like lines 5660 and 7881 from source 142.111.90.113 and lines 5630 and 5634 from source 23.27.185.250, have this behavior within milliseconds after one another. These entries were picked by random, however the entire capture

is riddled with similar entries. Considering the packet capture begins and ends within 147 milliseconds, and has thousands of requests to the same server, this behavior is a clear indication of an attacker flooding a single server. The attacker disguises their IP address to bypass a preventative measure set up by servers to prevent flood like attacks. By changing the incoming address each time, the server will treat it like a normal, new request coming in. This burst of traffic, predominantly flagged as SYN and ACK, is a classic symptom of a SYN flood attack, which is a type of Distributed Denial of Service (DDoS) attack. These attacks aim to overwhelm a target's ability to respond to legitimate traffic.

Additionally, an ICMP "Destination Unreachable" message, found on line 128 from source 104.253.185.41, although not directly indicating an attack, when seen in the context of a potential SYN flood, raises the possibility of network security controls responding to an attack or misconfiguration causing legitimate traffic to be blocked. These messages indicate that the attacker is likely succeeding in overwhelming the server.

These findings suggest the target IP may be under attack from a DDoS style strike, with multiple hosts being used to flood the network, overwhelming its resources, and potentially causing denial of service to legitimate requests. The variety in source ports and rapid succession of requests could indicate an attempt to use up all the server's resources or to simply guess at possible ports that are vulnerable to exploit later on. This probing stage could be the first step in a more elaborate attack.

The following is a simple list from Wireshark of the data that were referenced. Note the times, packet numbers and IP addresses:

Here is a set of 2 results that both have the source address of "142.111.90.113":

5660 23:58:45.65 142.111.90.113 10.10.10.10 TCP 58 80 → 63141 [SYN, ACK] Seq=3044381868 Ack=1683856582 Win=29200 Len=0 MSS=1400

7881 23:58:45.69 142.111.90.113 10.10.10.10 TCP 58 443 → 52288 [SYN, ACK] Seq=4125428511 Ack=866006660 Win=29200 Len=0 MSS=1400

Filter used: tcp.flags.syn == 1 and ip.src == 142.111.90.113. The top result is highlighted in light green and the bottom result is in dark gray.

Here is another set of 2 results that both have the source address off "23.27.185.250":

5630 23:58:45.65 23.27.185.250 10.10.10.10 TCP 58 80 → 35873 [SYN, ACK] Seq=1615262595 Ack=191228767 Win=29200 Len=0 MSS=1400

5634 23:58:45.65 23.27.185.250 10.10.10.10 TCP 58 80 → 28086 [SYN, ACK] Seq=3463691871 Ack=159199594 Win=29200 Len=0 MSS=1400

Filter used: tcp.flags.syn == 1 and ip.src == 23.27.185.250. Both results are highlighted in light green.

Here is another set of 1 result that has the source address of "198.251.81.135":

41 23:58:45.55 198.251.81.135 10.10.10.10 TCP 58 443 → 18553 [SYN, ACK] Seq=2067708853 Ack=2015282260 Win=14600 Len=0 MSS=1400

Filter used: tcp.flags.syn == 1 and ip.src == 198.251.81.135. The result is highlighted in dark gray.

Here is another set of 1 result that has the source address of "104.253.185.41":

128 23:58:45.55 104.253.185.41 10.10.10.10 ICMP 82 Destination unreachable (Host administratively prohibited)

Filter used: tcp.flags.syn == 1 and ip.src == 104.253.185.41. The result is highlighted in black.

Define Principles to Identify Solution (CSIT-12)

2.1. Information system components

A SYN flood attack primarily targets the network layer's ability to process and manage connection requests. This type of attack sends an overwhelming number of SYN requests to a server, leading to the exhaustion of the server's ability to maintain and manage these connections. Since the network layer is responsible for packet forwarding and routing, an overload at this layer disrupts normal network operations.

The SYN flood attack disrupts the TCP three-way handshake, which is a fundamental process managed at the network layer. In this attack, the attacker floods the target system with SYN requests, which leads to an over saturation of the TCP layer. This prevents the completion of the handshake on every port, effectively paralyzing the network layer's ability to establish new, legitimate connections. If all the ports are busy, the system cannot make new ports to handle more traffic.

The attack aims to consume the connection state tables in network infrastructure components like load balancers, firewalls, and servers, all of which operate at the network layer. By doing this, the attack can slow even high-capacity devices that are more than capable of maintaining millions of connections, indicating the severity of the impact on this layer (What Is a SYN Flood Attack).

In conclusion, the network layer is the most affected in the event of a SYN flood DDoS attack. Due to the nature of this attack, it directly interferes with the layers core functions of managing connections and routing packets.

2.2. Weighted table analysis (Risk Impact)

IT SYSTEMS LAYER (PPT)	Vulnerability ID	NOTE: All ratings are from 0-5 (least to most important), Criterions are from 0.0 (0%) to 1.0 (100%).				
		Criterion	Impact on Revenue	Impact on Profitability	Impact on Reputation	TOTAL
		Criterion Weight Information	0.3	0.2	0.5	1
2=Network Layer	N###					
	N001	SYN Flood Attack	2	2	4	3

Above is the weighted table analysis for a SYN Flood Attack. Since a SYN flood attack can disrupt online enrollment or paid online systems, it can lead to a moderate impact on revenue for the academic entity (2 out of 5). Profitability might be less affected in an academic context since it is not typically the main operation (2 out of 5 as well). The impact that this will have on an academic institution could be heavily impacted however, due to the disruption of classes. If online learning is affected, research data is lost, or communication is down, there would be a large disruption and large impact on reputation (4 out of 5).

2.3. Risk likelihood (Risk Probability)

IT SYSTEMS LAYER (PPT)	Vulnerability ID	Likelihood	Impact	RISK
2=Network Layer	N###			0
	N001	2	4	8

This chart measures the probability of the SYN flood attack occurring. For academic institutions with moderate to advanced security measures (firewall and intrusion detection), the likelihood will fall around a 2.

However, the impact is much greater. Given the reliance on network services in academia for research, communication, and learning, the impact would be significant. A rating of 4 would be appropriate because it reflects how substantial the disruption would be, but not necessarily

complete paralysis due to backup systems and procedures (books versus the internet, as well as in-person meetings versus online).

Risk Treatment

IT SYSTEMS LAYER (PPT)	Vulnerability ID	RISK	RISK TREATMENT
2=Network Layer	N###		
	N001	8	Risk Mitigation

Risk mitigation seems appropriate for this situation. As disconnecting from the internet is not an option and accepting that the system will be attacked is also a poor decision. Mitigating the risk by implementing measures to reduce the risk, such as installing and configuring additional firewalls, upgrading intrusion prevention systems, or enhancing the current network's capacity would all be acceptable options.

Apply principles to identify solution (CSIT-13)

3.1. Risk-rating factor

With a likelihood of 2 out of 5, indicating moderate changes of occurrence due to existing security measures, and an impact of 4 out of 5 on reputation, reflecting substantial disruption to academic operations, the total risk score is 8 (2 x 4).

In an academic setting, such a risk would be perceived as high. The threat to the institution's reputation and the disruption of essential services would not be taken lightly. The reliance on network services for key operations like enrollment, learning and research reinforces the need to keep such a status. The calculated risk rating factor highlights the need to invest in preventative measures to maintain trust and operational status in educational environments.

3.2. Risk treatment/response

Risk mitigation seems appropriate for this situation. As disconnecting from the internet is not an option and accepting that the system will be attacked is also a poor decision. A third party also cannot host the connection because sending data across the open internet is also unsafe. Mitigating the risk by implementing measures to reduce the risk, such as installing and configuring additional firewalls, upgrading intrusion prevention systems, or enhancing the current network's capacity would all be acceptable options. Penetration testing complements these measures by identifying potential weaknesses that attackers could exploit. Through penetration testing, verifying the effectiveness of the implemented defenses against SYN flood attacks and refining the security will make it a vital component of the risk mitigation plan.

3.3. Risk residual

Specific implementations include installing advanced firewalls with SYN flood protection, upgrading intrusion prevention systems to identify and mitigate such attacks, and expanding the network capacity to handle traffic surges. Additionally, implementing rate-limiting controls and conducting regular penetration tests are crucial.

Despite these measures, residual risk remains. This includes the possibility of new, sophisticated attack methods bypassing existing defenses, or internal resource constraints limiting the effectiveness of the implemented measures. Continuous monitoring and regular updates to security protocols are essential to mitigate these residual risks and adapt to evolving cyber threats.

Works Cited

"History of TCP/IP." *Scos Training*, 24 Nov. 2020, scos.training/history-of-tcp-ip/.

IONOS editorial. "TCP (Transmission Control Protocol) – the Transmission Protocol Explained." *IONOS Digital Guide*, IONOS, 2 Mar. 2020, www.ionos.com/digitalguide/server/know-how/introduction-to-tcp/.

L.F. Haaijer, DDoS Packet Capture Collection, (2022). Available from https://github.com/StopDDoS/packet-captures

Ping of Death Ddos Attack | Cloudflare, www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/. Accessed 3 Dec. 2023.

"What Is a SYN Flood Attack?" *NETSCOUT*, www.netscout.com/what-is-ddos/syn-flood-attacks. Accessed 2 Dec. 2023.

What Is ICMP? | Internet Control Message Protocol | Cloudflare, www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/. Accessed 3 Dec. 2023.

"What Is Wireshark and How to Use It: Cybersecurity: Comptia." *CompTIA.Org*, www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it. Accessed 2 Dec. 2023.