IFN507 Network Systems
Security Project Report

Student and Group Details			
Group number	2		
Student name	Felipe Alejandro Manzor Manzor	**Student number**	N11373725
Student name	Abdulaziz Saud S Alharbi	**Student number**	N11143541
Student name	Yi-Chen Chen	**Student number**	N11564628

Only one (1) student should submit this report on behalf of the group. To help your marker enter the grades, please provide the details of the group member who submitted the assignment.			
Student name	Felipe Alejandro Manzor Manzor	**Student number**	N11373725

Claim of Contribution	
Name	**Contribution**
Felipe Manzor Manzor	Capture File
Abdulaziz Saud S Alharbi	Mitigation Strategies
Yi-Chen Chen	TCP Protocol – Normal Behaviour

Instructions

You must use this template to complete your Group Security Project Report. Complete all the fields and then submit on Canvas using the instructions provided in both the assignment specification, and under Assignments on Canvas. The fields are not a fixed size for each question, so you can decrease their size, or expand them depending on your needs. Please do not modify the margins of this document. The font must remain at size 10 Arial, as per the directions in the page footer. Please do not remove any aspect of the template including the questions.

This assignment may be completed in groups of three (3) students. Your report must be three to four (3 – 4) pages in length. That is no less than three (3) and no more than four (4) pages in length. Please note the page limit excludes this cover page, and any references.

There is no need to include any graphics or screenshots in your report.

Before submitting this document, please save into PDF format. Please also ensure you insert your group number into the document header.

Font: Arial, size 10
Spacing:1.15
Margins: top 3.65cm, bottom 2cm, sides 2 cm

1. TCP Protocol – Normal Behaviour

1.1. Provide a detailed and comprehensive explanation of the normal operation of the TCP protocol.

TCP/IP

A non-proprietary protocol suite responsible for defining the function of communication and interconnect between the internet and a network device within 4 layers. TCP (Transmission Control Protocol): It firstly provide a trustworthy delivery service, ensuring the data can be comprehensively delivered, including recover data from the state of lost or corrupted. The receiving side is then asked for an ACK (acknowledgement) in the second step. IP (Internet Protocol): It mainly responsible for routing and addressing packets of data, allowing these data delivered over the network, then sent to the specifies destination (Shacklett et al., 2021).

Location of TCP

TCP is located in transport layer, the 4th layer of OSI Model, which is mainly responsible for data transfer. The protocol is not limited to any specific network structure, including both local area networks (LANs) and wide area networks (WANs). The term "transport protocol" is used to refer to a specific protocol that operates under the transport layer of the OSI model (Administrator, n.d.).

Working Process of TCP

Three-way Handshake

Three-way handshake occurs in the connection established two computers/hosts which can exchange data with each other.

STEP 1**:** When host A sending an initial packet contains ‘’SYN’’ bit with value ‘’1’’ to the target host B, it can identify the former is meant to set up a connection within them.

STEP 2**:** Once Host B received the initial packet, it will send back the bits of “SYN, ACK’’ to Host A. In this event, ‘’SYN’’ means that admit synchronise; and ‘’ACK’’ means accept the SYN demand that Host A sent in step1.

STEP 3**:** Host A then sending a new “ACK’’ bit set to Host B, recognising “SYN, ACK’’ that sent by Host B. Finally, the connection can be recognised, and able to do further data transferring.

Data transportation

A memory section, or buffer, is provided to temporarily store data transmitted at a high rate of speed as part of flow control for controlling data flow in connections. Windowing is used to control the amount of data transformation when clients and servers is sending extremely large or small segments of data, ensuring the transmission efficiency (Shaw, 2021).

Closure

Computer A sending a FIN packet and receiving the response in order to close the communication. The process can be defined as four Wait state: Fin Wait, Close Wait, Last Ack Wait, and Time Wait.

In FIN Wait, computer A will first send a FIN packet to computer B, and waiting for the response from computer B. Next, moving on to Close Wait. When computer B received the FIN packet, it waits application process then gives a signal that means ready for closing. Thirdly, computer B sending an ACK for the FIN to A in Last ACK Wait session. Once A received it, sending back an ACK then need to wait for double maximum segment life (MSL) time, which occurs in Time Wait. After that, when B get the ACK from A, both A and B can finally close the connection now (Savary, 2020).

2. Capture File – Anomalies

2.1. Provide a detailed and specific explanation of all anomalies identified within the provided capture file.

The provided package contains 20 packets of TCP protocol, this contains the SYN or synchronize flag to stablish the 3-way handshake, we can see some events that are unusual in a common context of TCP-SYN that are listed below, to compare a normal SYN behaviour, we captured one as a reference using Wireshark.

1. The maximum window size it 512 and all packages have the same, this is relatively low for the standard TCP - SYN protocol (Microsoft, 2023).
2. All packages are addressing different ports.
3. All packages are address to the same IP and come from different IP, also from different parts of the world in a short time frame.(we can know this because the range of the Ip but also we can check in websites like iplocation.net/ip-lookup)
4. The SYN header is only 20 bites and is the same for all. We don't have any TCP options; this means that the sender is not really requesting something specific.
5. The time to live of all packages is the same, 64.
   This mean that all packages have the same live, so this make us thinks that all the packages were created with the same initial value and going straight to the router.
6. The time delta from the package received is almost the same between 0.000041 – 0.000091 sec.
7. All acknowledge numbers are 0: in the provided package there is no acknowledgement. In normal circumstances is not normal.
8. There are some packages sanded to group addresses using multicast this might mean that there are addressing a range of servers this might also mean a coordination of the attackers to make seem this attack more legit.

2.2. Which TCP header fields are impacted? Identify the impacted fields. Provide specific packets from the capture file that display the anomaly.

From the field of TCP headers, we have Source Port, Destination Port, Sequence Number, Acknowledgment Number, Header Length, Flags, Window Size, Checksum, Urgent Pointer.
All the packages the conversation completeness is incomplete meaning that is no handshake done, also all packages have same length 20 bits and also there are only few differences in the provided packages Its transversal that all sources port is different for the 20 packages, and the destination port as well and the raw sequence number, all the packages are unverified by the checksum status and all of them are incomplete.
To go deeper into it we will take package number 1 come from the port 2555 to the port 22746 the window size is 512, the checksum is unverified, as well the communication as is marked as incomplete communication the fag shows us the intent do to a handshake.

2.3. Are there any anomalies or interesting observations in the other layers? Identify the impacted fields and protocols if applicable. Provide specific packets from the capture file that display the anomaly if applicable.

In the source IP addresses, is observed that SYN packets originating from various regions worldwide, reflecting the diversity in the IP protocol, corresponding to layers 1 and 2 in the OSI model. A notable aspect here is the presence of two distinct delivery modes: unicast for certain packages (1, 5, 6, 8, 9, 11-13, 18, 20) and multicast for all other packages. This diverse addressing approach is indicative of an interesting flag in the network activity. Additionally, a significant finding is that some of the MAC source

addresses have been altered, as they are locally administrated, specifically in packets 1, 2, 4, 11, 12-15, and 18. This suggests a deliberate effort to obscure the origins of these packets, potentially for malicious purposes or covert actions within the network.
As example is possible to appreciate the package number 14 that exility says that is not the factory default and shows a broadcasting in the destination address.

2.4. Based on the evidence and anomalies discussed above, identify, and explain the type of attack that has likely occurred.

The observed packet characteristics strongly suggest a Distributed Denial of Service (DDoS) SYN flood attack. In this type of attack, the attackers aim to overwhelm a target server by initiating numerous half-open connections. Several key indicators point to this conclusion: the low window size, diverse source ports, and consistent SYN headers with no TCP options are common tactics used to create an excessive load on the server's resources. The use of different source IP addresses from various geographical locations in a short time frame, combined with identical Time to Live values, suggests a coordinated, automated effort, potentially utilizing a botnet. The consistent time delta between packets and the absence of acknowledgment numbers further confirms the malicious intent. Additionally, the presence of non-factory default MAC addresses hints at an attempt to hide the attackers' identities while flooding the target server with connection requests. Immediate countermeasures are essential to protect the targeted server's availability and functionality in the face of this SYN flood attack.

3. Mitigation Strategies

3.1. Based on your own research, identify two (2) appropriate mitigation strategies. These must be technical in nature. Do not suggest third party and cloud services as a solution.

DDoS (distributed denial-of-service) attacks, which exploit TCP/IP vulnerabilities, are common cyberattacks. Many types of this attack attempt to interrupt target service by flooding requests. According to Gupta et al. (2012), DDoS attacks include ICMP Flood, UDP Flood, SYN Flood, and Smurf attacks. The previous section showed that SYN flood attacks can be prevented in numerous ways. This section discusses solution kind, function, advantages, and disadvantages.

Next-generation firewalls (NGFW)

Firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) are often used to prevent SYN Flood Attacks. Next-generation firewalls combine these systems. Juniper (n.d.) states that next-generation firewalls have IDS and IPS capabilities. Depending on policy, the firewall filters traffic, and the IDS and IPS process it. An IPS that constantly searches the network for dangerous conduct and blocks, drops, or reports it if required while the IDS reports only.

SYN cookies

Another popular SYN Flood Attack solution is SYN cookies. This happens simply by configuring the server to generate the cookie value as a sequence number in the SYN-ACK response packet.

3.2. For each identified mitigation strategy, provide a detailed technical explanation of the proposed strategy and where it operates in relation to the layers of the OSI model.

Next-generation firewalls (NGFW)
Legacy firewalls restrict their ability to OSI model Layer 4, the Transport Layer. However, attacks at the higher Layers of the OSI model are difficult because they can't examine packet data or filter it by application. In contrast, the next-generation firewall (NGFW) filters packets by application and examines

their contents rather than their IP headers (VMware, n.d.). As a result, complex threats hiding in normal traffic can be effectively defended by NGFWs.

TCP flag manipulation by malicious actors causes DDoS attacks that damage and disable systems. In a normal client-server architecture, SYN-ACK, SYN-FIN, and FIN-URG-PSH are anomalies and unpredictable on the client side. This highlights the relevance of these tag sets and detecting and stopping their packets at the firewall to ensure network integrity (Harikrishnan et al., 2022).

Furthermore, Next-generation firewalls can also safeguard FTP and Telnet by permitting traffic only on specified ports and blocking unused or susceptible ports to prevent DDoS attacks. Blocking all traffic with a firewall reduces DDoS attacks (Harikrishnan et al., 2022).

Control rules let firewalls allow or deny traffic. However, network packet data is not checked. If the packet header matches firewall rules, the legacy firewall will allow harmful code. Despite firewalls, reliable networks can be hacked. Next-generation firewalls detect system or network intrusions with hardware or software IDSs. Intrusion detection systems (IDS) allow firewalls detect attacks that might otherwise go undetected by inspecting packet headers and contents (Nayak & Rao, 2014).

SYN cookies

For connection-oriented communication, SYN cookies work with the TCP protocol at Transport Layer 4 of the OSI model. It works by not updating a status table for all TCP half-open connections, unlike typical TCP handshakes. This method uses cryptographic hashing. The server sends the client the initial SYN-ACK flood and ISN. ISN is calculated using source IP, destination IP, port numbers, and a secret number. The server allocates connection RAM after verifying a client ACK by checking the incremental ISN. Implementing SYN Cookies Windows and FreeBSD use TCP SYN cookies to mitigate traffic during peak times (Scholz et al., 2020).

3.3. For each identified mitigation strategy explain their associated benefits and limitations.

Next-generation firewalls (NGFW)

Advantages:

1. Inspection of traffic from layer 2 to layer 7 provides multi-layered protection.
2. NGFWs may assist in preventing malware access into a network by distinguishing between safe and dangerous apps.

Disadvantages:

1. Acquiring an NGFW instead of a traditional firewall comes with a high total cost.
2. Compared to traditional firewalls, NGFW configuration and maintenance require higher technical expertise. Misconfiguration makes NGFW vulnerable to attack.

SYN cookies
Advantages:

1. The state is not stored in memory; rather, it is encoded in the server's initial sequence number.
2. Since Linux has this mechanism built in, SYN Cookies are the ideal option if the mitigation strategy needs to be ready for use right away.

Disadvantages:

1. Since the sequence number is less than the TCB, it could be necessary to retransmit the data because not the entire state can be stored.
2. The behaviour breaches TCP semantics since the state is not saved on the server, making it unable to resend the SYN-ACK.
3. Some information regarding the TCP connection is lost consequently.

4. References (excluded from page limit)

4.1. List any references in this section.

Administrator. (n.d.). *Transmission Control Protocol - Part 1: Introduction to TCP*. https://www.firewall.cx/networking/network-protocols/tcp-udp-protocol/tcp-transport-protocol.html

Gupta, B. B., Joshi, R. C., & Misra, M. (2012). Distributed Denial of Service Prevention Techniques. https://doi.org/10.48550/arxiv.1208.3557

Harikrishnan, V., Sanket, H. S., Sahazeer, K. S., Vinay, S., & Honnavalli, P. B. (2022). Mitigation of DDoS Attacks Using Honeypot and Firewall. In D. Gupta (Ed.), *Proceedings of Data Analytics and Management.* (pp. 625–635) ICDAM 2021. Volume 2. Springer.

Juniper. *What is IDS and IPS?* https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html#:~:text=Yes.,exploit%20attempt%2C%20depending%20on%20configuration.

Microsoft (n.d) TCP in Windows, https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/description-tcp-features

Nayak, U., & Rao, U. H. (2014). Intrusion Detection and Prevention Systems. In U. Nayak & U. H. Rao (Eds.), The InfoSec Handbook: An Introduction to Information Security (1st ed., pp. page range of the chapter). Apress. https://doi.org/10.1007/978-1-4302-6383-8

Savary, G. (2020). TCP Series #2: How to close TCP sessions and diagnose disconnections? Accedian. https://accedian.com/blog/close-tcp-sessions-diagnose-disconnections/

Scholz, D., Gallenmüller, S., Stubbe, H., Jaber, B., Rouhi, M., & Carle, G. (2020). Me Love (SYN-)Cookies: SYN Flood Mitigation in Programmable Data Planes. https://doi.org/10.48550/arxiv.2003.03221

Shacklett, M. E., Novotny, A., & Gerwig, K. (2021). TCP/IP. Networking. https://www.techtarget.com/searchnetworking/definition/TCP-IP

Font: Arial, size 10
Spacing:1.15
Margins: top 3.65cm, bottom 2cm, sides 2 cm

Shaw, C. (2021). TCP Windowing: Explained |

ExtraHop. *ExtraHop*. https://www.extrahop.com/company/blog/2017/tcp-windowing/

The TCP/IP Guide - TCP Connection Termination.

(n.d.). http://www.tcpipguide.com/free/t_TCPConnectionTermination-2.htm

VMware. What is Next Generation Firewall?

https://www.vmware.com/topics/glossary/content/next-generation-firewall.html

West, J. (2021). CompTIA network+ guide to networks. Cengage.

Font: Arial, size 10
Spacing:1.15
Margins: top 3.65cm, bottom 2cm, sides 2 cm