We've processed your Assignment extension request FORM-AEX-265734

no-reply@qut.edu.au <no-reply@qut.edu.au>
Fri 10/21/2022 12:42 PM
To: Kim Csoka <kim.csoka@connect.qut.edu.au>

Hi Kim,

Thank you for your assignment extension request **(FORM-AEX-265734)**.

We have approved your request and the due date for your assignment **Assessment 2: Project**, for unit CAB303 has been extended by 48 hours from the original due date. If your unit outline does not specify that your assignment is eligible for an extension, this confirmation email is not valid and unless you submit by the original due date, the late assessment policy will apply.

You are responsible for ensuring that this assignment is eligible for extension before submitting it after the original due date. Check your unit outline for eligibility.

As you indicated this is a group assignment, you are also responsible for informing other members of your group of this extension.

Be aware that a copy of this email is kept on file. You should not alter this email in any way. Email notifications that have been altered or differ in any way from the original may result in an allegation of student misconduct as set out in the Student Code of Conduct.

Need extra support? You can access free, confidential counselling with qualified professionals. We also offer planning and support if you have a disability, injury or health condition that affects your ability to study. If you are struggling to meet your university commitments, academic support is also available.

Have a question? You can contact us by email or phone. We're also available to help you on campus or via online chat. Visit the HiQ website for our contact details and opening hours.

Email us Phone us

About HiQ

You have received this email because you have submitted an assignment extension request. View our Privacy and Security statement.

Ref ID: 10722831 FORM-AEX-265734

CAB303 Networks
Security Project Report

Student and Group Details			
Group number	68		
Student name	Kim Csoka	**Student number**	10722831
Student name	Hayden Williams	**Student number**	11132817
Student name	Ryan Indrananda	**Student number**	10852565

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	Kim Csoka	**Student number**	10722831

Claim of Contribution	
Name	**Contribution**
Kim Csoka	Question 2, Capture File Anomalies
Hayden Williams	Question 1, TCP Protocol - Normal Behaviour
Ryan Indrananda	Questions 3-4, Mitigation Strategies, SLAs, and KPIs

Instructions

You must use this template to complete your Group Security Project Report. Complete all the fields and then submit on Blackboard using the instructions provided in both the assignment specification, and under "Assessment" on Blackboard. 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.

Transmission Control Protocol (TCP) operates at layer 4 (Transport Layer) of the OSI model and is an intermediary between two applications that need to exchange data, such as a computer and a server. The key operations of this protocol are that data arrives in order, has minimal errors, duplicates gets discarded and lost or damaged packets get resent (Henke, 2020).
The three stages of a TCP connection are connection establishment with a 3-way handshake, data transfer, and connection termination with a 4-way handshake.

Connection Establishment:
Step 1: The 3-way handshake is established by the client (computer) sending a TCP synchronization (SYN) segment to the destination device (server). *The destination port is specified, and a source port is automatically assigned.* The segment's ACK is set to 0, SYN bit is set to 1 and an initial sequence is a randomly generated number, such as 9001.
Step 2: The server then replies with a synchronization acknowledgment (SYN-ACK). The servers SYN is set to 1, and ACK # is 9002 (which is the client's sequence # plus 1). By adding 1 to the client's sequence #, the server acknowledges the client connection request. The server's segment has its own initial sequence #, which is 5001.
Step 3: The computer then responds and sends an acknowledgment (ACK) to the server. Since there is no more synchronization/connection request the SYN bit is set to 0. The computer acknowledges the server's connection request by increasing the server-side sequence to 5002, an increase of 1 and the segment sequence # is 9002 (Sunny Classroom, 2019).

Data Transfer:
Both the computer and the server have now agreed to open their connection to each other so data can now be transmitted. This is done by the computer sending a packet of data and a sequence number to the server. The server then acknowledges it by setting the ACK bit, increasing the acknowledgment number by the length of received data and sending the acknowledgment back, this continues until all data is all sent and received. When a packet of data is sent over TCP, the recipient must always acknowledge what they received.

TCP connection termination:
Step 1: When the computer wants to close the connection, it sends a TCP segment with the FIN bit set to 1 to the server and enters the FIN_WAIT_1 state.
Step 2: When the server receives the FIN bit segment from the computer, it frees up its buffers and the server sends an ACK segment to the computer. The server then enters the CLOSE_WAIT state.
Step 3: Once the computer receives the ACK, it then enters the FIN_WAIT_2 state. The connection from the computer to the server is terminated.
Step 4: For terminating the connection the server sends a segment to the client with the FIN bit set to 1. The server then waits for an acknowledgment from the client.
Step 5: When the computer receives the FIN bit segment from the server, the client acknowledges the server's segment and enters the TIME_WAIT state. The TIME_WAIT state lets the client resend the final acknowledgment in-case the ACK is lost. The time spent by clients in TIME_WAIT state depends on their implementation, but their typical values are 30 seconds, 1 minute, and 2 minutes. After the wait, the connection formally closes and all resources on the client side are released (Singhal, n.d.).

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

2. Capture File – Anomalies

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

Different anomalies were identified within the capture file.

Incomplete three-way handshake: All 20 packets within the file consist of multiple incomplete three-way handshakes. As described in section 1, a connection must be established by a three-way handshake. However, in all packets within the file the source only requests a connection by sending a SYN segment. There are no server acknowledgements of this request (SYN-ACK) and therefore also no client response in the form of ACK for the connection to be established. This is unusual behaviour indicating that the three-way handshake is incomplete.
All ports of destination IP being targeted within a short time period: The high volume of SYN packets being sent to the same destination IP address 200.200.1.77 within less than a second is suspicious. On top of that each SYN packet is sent to a different port of the destination indicating that all ports are being targeted in a short time frame. Upon more detailed inspection, we can also see that the destination MAC addresses are all the same, indicating that one server is being targeted.
Spoofed Addresses: When inspecting the source MAC addresses, we can see that certain locally administered addresses are not the factory default signifying spoofed addresses. This indicates that an attacker is trying to stay anonymous. In addition, the TTL for all packets are of the same value 64, which means there's a high possibility that the SYN segments are sent from the same router.

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

All the packets from 1 through 20 have the SYN bit in the TCP segment set to 1, also known as a flag. If you take a look at packet 1 in the Transmission Control Protocol you can see that the flag syn is set to 1, and this is shown across all the other packets too. This is the proof that the client never received the SYN-ACK response from the destination device, and this is an incomplete 3-way handshake. The destination ports are interesting. Packets 1 through 20 have a unique destination port, this implies that the attacker is trying to overload all ports rendering the machine useless. As you can see from packet 1, the destination port is 22746, this is different to packet 2s destination port 38839. There is no destination port seen multiple times, you can further deduce that it is not part of normal TCP operations as the port would be contacted multiple times for a certain reason, such as port 80 for a website. The third pattern identified is that the raw sequence is always a unique value, this is part of normal TCP operations and is shown over packets 1 to 20.

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 ethernet header of packets 1, 2, 11, 12, 13, 14, 15, 18 the source MAC addresses are not of factory default which indicates that they've been modified to ensure anonymity.
The Time To Live (TTL) in the IP headers of packets 1-20 all contain the same value of 64 implying that the packets originate from the same router.

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

Based on the evidence and anomalies discussed above, we have identified the attack as a DOS SYN flood attack. In this type of attack, attackers exploit the TCP three-way handshake by repeatedly sending

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

SYN packets from different spoofed IP addresses to all ports on a server, which consumes all available resources resulting in the server becoming unavailable (Cloudflare, n.d.). This works as follows:

1. Spoofed IP addresses send a high volume of SYN packets to one server
2. Server responds to each SYN request packet with a synchronization acknowledgment (SYN-ACK) and temporarily keeps the connection half open to receive the final step in the handshake (ACK)
3. The final ACK step is never returned and the attacker continues sending SYN packets to the server
4. Once all ports have been exhausted the server becomes unavailable resulting in a denial of service as users are unable to access it

The many spoofed IP addresses sending a high volume of SYN packets to all ports of destination IP 200.200.1.77 within a short time frame, and the evidence of incomplete three-way handshakes has convinced us of a SYN flood attack. Based on the evidence that the Time To Live is of the same value across all packets, we suspect the SYN flood attack to be of DOS nature as the packets seem to be coming from the same router, excluding a distributed denial of service attack.

3. Mitigation Strategy 1 (on-premises)

3.1. Based on your own research, identify an appropriate mitigation strategy. This must be technical in nature. This solution must be 'on-premises' (i.e., not a vendor managed cloud-based solution)

There are several appropriate strategies in mitigating potential SYN flood attacks in the future. Micro blocks may be utilized, in which administrators managing the File Server within the company may allocate a micro-record in the server memory to handle each incoming SYN request. TCP stacks may be tweaked such as by reducing the timeout until a stack frees allocated memory to a connection. Next, RST cookies may be implemented, whereby the file server intentionally sends a false SYN-ACK for a client's first request, resulting in the client creating an RST packet and informs the server of a failure. If received, the server recognises the request, and therefore the client, as legitimate. Though the most appropriate on-premises strategy we have chosen is to implement SYN cookies (Imperva, n.d.). A further explanation and justification is present in section 3.2.

3.2. For the 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.

Through the use of cryptographic hashing, the file server may reply to SYN requests with crafted SYN-ACK responses without adding to the SYN queue (Radware, n.d.). These responses have a sequence number created from client IP address, port number, and other potential identifiers. Once the client responds, the ACK packets include this hash, the server verifies it, then allocates memory toward the connection (Imperva, n.d.). This strategy protects the SYN queue from overloading under SYN flood attacks. Since this strategy is concerned with the TCP 3-way handshake operation, it operates within Layer 4 (Transport layer) of the OSI model.

3.3. For the identified mitigation strategy, explain its associated benefits and limitations.

The use of cryptographic hashing, or using cryptographic initial sequence numbers, may be difficult for a potential attacker to predict in comparison to other, potentially more trivial solutions (GIAC, 2021). No allocation of resources following the first SYN packet also does not need to be done by the file server, and it is not necessary for the client to be aware of the use of SYN cookies. Importantly, SYN cookies also do not require alterations within the specifications of the TCP protocol (Diekmann, 2016). Some limitations include the fact that not all TCP data fits into a 32-bit long ACK/SEQ number field, thus several TCP options, such as Window Scaling, will not work, affecting users with a low-quality connection (Kelly, 2007).

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

SYN cookies may also be computationally expensive and increase load on the file server's resources. The calculation of the initial sequence number may produce a significant load on the CPU (Wikipedia, 2022). It also does not reduce traffic to the file server, therefore potentially rendering it futile against future flooding attacks targeting bandwidth.

4. Mitigation Strategy 2 (outsourced to a third-party vendor)

4.1. Based on your own research, identify an appropriate mitigation strategy. This solution must be outsourced to a vendor. Identify and explain the solution that you require the vendor to provide.

Cloudflare is a global vendor in networks committed to ensure a secure, reliable, private, and fast internet for its users (Cloudflare, 2019 a). According to Cloudflare, there are two potential mitigation strategies for SYN flood attacks aside from the aforementioned SYN cookies strategy. First, by increasing the number of half-open connections that operating systems or devices allow to cater for a higher number of SYN packets. Though, the system is required to reserve higher memory resources to do so. Second, the oldest half-open TCP connection may be recycled, involving a prerequisite in which legitimate connections are able to be established in less time than said backlog can be filled with hostile SYN packets. How Cloudflare mitigates SYN flood attacks is by standing in between a targeted server, in this case the file server, and the SYN flood. They handle the TCP handshake process in the cloud and delay the connection with the file server until this process is complete when an initial SYN request is made. This minimises the resource cost of maintaining connections with artificial SYN packets off the file server and utilizes their Anycast network (Cloudflare, 2019 b).

4.2. You will require a Service Level Agreement (SLA) to be in place with the vendor. Justify the need for implementing the SLA. Discuss the relevant provisions that should be included in the SLA. Identify and justify any relevant Key Performance Indicators (KPIs) that should be included in the SLA.

SLA provisions necessary include service objectives, service descriptions, duties of both client and vendor, quantifiable performance metrics or key performance indicators (KPIs), vendor response times, penalties, and more. An SLA is imperative as it formalises a communication pipeline between the vendor and the electrical company, allowing them to communicate with Cloudflare, for example, as a client. It strengthens the trust between the two, as it defines risk and further penalties for breaches (Atlassian, n.d.). The expectations between client and vendor are clearly defined, and this agreement is legally enforceable, and either party can refer to the SLA to find solutions for potential arising issues. KPIs are metrics that quantify how well vendors fulfill and perform in comparison to agreed standards. A discreet example of these indicators could be that a vendor contractually promises customers a 99.9% service uptime (an industry standard), or possibly support and response for issues within 24 hours. Network performance may be measured through the analysis of bandwidth, or data volume capacity, and throughput, or the amount of data delivered through a network successfully. Other metrics include latency, jitter, and packet loss, ensuring that the performance of the network is reliable and resistant to cyber attacks. Furthermore, support services must define the support type, methods of support, as well as expected response times, giving the client expectations for the quality of their service. Penalties for underperformance must also be established, such as financial penalties or compensation with an amount agreed upon within the SLA, service credit or the offer of credit for future work, or the vendor extending the agreed license term or offering subsequent support with no charge (Agrawal, 2020). Overall, these KPIs set an important benchmark in a vendor's capability in managing the client's network, its vulnerabilities, and overall safety.

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

5. References (excluded from page limit)

5.1. List any references in this section.

Agrawal, T. (2020, November 28). *KPI — SLA and Penalties. It is important to understand that key… | by Tanya Agrawal | Medium*. Tanya Agrawal. Retrieved October 20, 2022, from https://tanya-agrawal18.medium.com/kpi-sla-penalty-9c931b8eea73

Atlassian. (n.d.). *SLA: Everything You Need to Know*. Atlassian. Retrieved October 20, 2022, from https://www.atlassian.com/itsm/service-request-management/slas

Cloudflare. (2019 a). Cloudflare - The Web Performance & Security Company | Cloudflare. Retrieved October 20, 2022, from https://www.cloudflare.com/en-au/

Cloudflare. (2019 b). *The Web Performance & Security Company | Cloudflare*. Cloudflare. https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

Cloudflare. (n.d.). *SYN flood DDoS attack*. Cloudflare. Retrieved October 23, 2022, from https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

Diekmann, C. (2016, October 17). *Network Security (NetSec)*. Chair of Network Architectures and Services. Retrieved October 20, 2022, from https://www.net.in.tum.de/pub/netsec2016/04_SYN_cookies.pdf

GIAC. (2021). *SYN Cookies, An Exploration*. GIAC Certifications. Retrieved October 20, 2022, from https://www.giac.org/paper/gsec/2013/syn-cookies-exploration/103486

Henke, C. (2020, December 22). *What Is Transmission Control Protocol (TCP)? | IoT Glossary*. EMnify. Retrieved October 20, 2022, from https://www.emnify.com/iot-glossary/transmission-control-protocol

Imperva. (n.d.). What is a TCP SYN Flood | DDoS Attack Glossary | Imperva. Retrieved October 20, 2022, from https://www.imperva.com/learn/ddos/syn-flood/

Kelly, C. (2007, April 24). *ckdake.com - Disadvantages of TCP SYN cookies*. Chris Kelly. Retrieved October 20, 2022, from https://ckdake.com/content/2007/disadvantages-of-tcp-syn-cookies

Radware. (n.d.). *SYN cookies*. Radware. Retrieved October 20, 2022, from https://www.radware.com/security/ddos-knowledge-center/ddospedia/syn-cookies/

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

Sengupta, S. (2022, July 7). *Top Cybersecurity KPI Examples & Best practices*. Crashtest Security. Retrieved October 20, 2022, from https://crashtest-security.com/cyber-security-metrics/

Singhal, A. (n.d.). *TCP Connection Termination | FIN Segment*. Gate Vidyalay. Retrieved October 20, 2022, from https://www.gatevidyalay.com/tcp-connection-termination-tcp-protocol/

Sunny Classroom (Director). (2019). *TCP - Three-way handshake in details* [Film]. https://www.youtube.com/watch?v=xMtP5ZB3wSk

Wikipedia. (2022, January 12). *SYN cookies*. Wikipedia. Retrieved October 20, 2022, from https://en.wikipedia.org/wiki/SYN_cookies

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