IFN507 Network Systems

Project Report

|  |  |  |  |
| --- | --- | --- | --- |
| **Student and Group Details** | | | |
| **Group number** | 5 | | |
| **Student name** | William Stark | **Student number** | N11947446 |
| **Student name** | Sunny Ramakant Pal | **Student number** |  |
| **Student name** | Romit Chandreshkumar Jalal | **Student number** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **One (1) and Only One (1) student should submit this report on behalf of the group. In order to have your marks entered correctly, please provide the details of each group member and particularly the one who submitted the assignment.** | | | |
| **Student name** |  | **Student number** |  |

|  |  |
| --- | --- |
| **Contribution Statement** | |
| **Name** | **Contribution** |
| Romit Chandreshkumar Jalal | 33% |
| Sunny Ramakant Pal | 33% |
| William Stark | 33% |

|  |
| --- |
| **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 Times New Roman, 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. |

|  |
| --- |
| 1. **TCP Protocol – Normal Behaviour** |
| * 1. **Provide a detailed and comprehensive explanation of the normal operation of the TCP protocol.** |
| Do we explain TCP first and then give explanation or do we assume our audience understands TCP and just focus on explaining normal operations?  OSI Model  TCP takes part within the Transport Layer (Layer 4) within the OSI Model. These components main goal is to receive data, segment the data, and provide transmission error detection. TCP uses the Network Layer (Layer 3) and the Session Layer (Layer 5) to accomplish these efforts.  Establishing Connection  TCP must establish a connection before transferring this data. There is a three-way handshake that TCP uses in the following sequence:   1. SYN (Synchronise) – This is where a client sends a packet with an initial sequence number (ISN). 2. SYN-ACK – The server replies to this ISN with an ACK or acknowledgment and sends its own ISN back. 3. ACK – The client acknowledges.   A real life example of this might be used when introducing yourself where one person acts as the server and the other acts as the client.   1. SYN – (Client) “Hello my name is Anakin Skywalker.” 2. SYN-ACK – (Server) “Nice to meet you Anakin Skywalker, I am Obi-Wan Kenobi.” 3. ACK – (Client) “Great to meet you too Obi-Wan Kenobi.”   Ports & Multiplexing  Ports allow multiple applications to use the same TCP program with each being assigned a unique port number. A way to contextualize this is to think of a mail delivery system within an apartment complex. The IP address as an apartment complex and ports as the individual apartments within the complex. The port number or mailbox explains which apartment the application data is for.  Data Transfer  Flow Control  Congestion Control  Connection Termination  When connections are closed, there is a four way handshake that takes pplace similar to the three way handshake described in the establishing connection part. There is a FIN from the initiator or the connection terminating. This is followed with an ACK from the receiver and a FIN from the receiver. Finally, we end the process with an ACK from the intiator. An example of this might be ending a phone call:   1. FIN – Luke Skywalker “I have to go” 2. ACK – Obi-Wan Kenobi “Ok” 3. FIN – Obi-Wan Kenobi “I have to go as well” 4. ACK – Luke Skywalker “Ok” |

|  |
| --- |
| 1. **Capture File – Anomalies** |
| * 1. **Provide a detailed and specific explanation of all anomalies identified within the provided capture file.** |
| The anomalies will be read from left to right as highlighted in the Wireshark capture diagram above.   1. Time: Packets being sent in quick succession. 2. Source: Multiple source IP addresses is highly indicative of a Denial-of-Service attack. 3. Destination: This could be considered normal if it is a targeted service, but it’s considered unusual to see this. 4. Length: The size of the packets are uniform at 54 bytes. There should be some variation depending on the data being exchanged. 5. SYN: Most alarmingly, the capture file represents characteristics of a SYN flood or Denial of Service (DOS) attack. As stated above, TCP should have a three-way handshake between traffic with a SYN, SYN-ACK, and finally an ACK. In the .pcap file there is no SYN-ACK or ACK flags. 6. Win Size: Again, all packets have a uniform size of 512 which is considered an anomaly. There should be some variation here. 7. Sequence Number (raw): The sequence numbers appear randomized. Ideally, these should be in succession especially considering the small amount of time between each packet being sent. |
| * 1. **Which TCP header fields are impacted? Identify the impacted fields. Provide specific packets from the capture file that display the anomaly.** |
|  |
| * 1. **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.** |
|  |
| * 1. **Based on the evidence and anomalies discussed above, identify, and explain the type of attack that has likely occurred.** |
|  |

|  |
| --- |
| 1. **Mitigation Strategies** |
| * 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.** |
|  |
| * 1. **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.** |
|  |
| * 1. **For each identified mitigation strategy explain their associated benefits and limitations.** |
|  |

|  |
| --- |
| 1. **References (excluded from page limit)** |
| * 1. **List any references in this section.** |
|  |