IFN507 Network Systems

Project Report

|  |  |  |  |
| --- | --- | --- | --- |
| **Student and Group Details** | | | |
| **Group number** |  | | |
| **Student name** |  | **Student number** |  |
| **Student name** |  | **Student number** |  |
| **Student name** |  | **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** |
|  |  |
|  |  |
|  |  |

|  |
| --- |
| **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.** |
|  |

|  |
| --- |
| 1. **Capture File – Anomalies** |
| * 1. **Provide a detailed and specific explanation of all anomalies identified within the provided capture file.** |
|  |
| * 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.** |
|  |