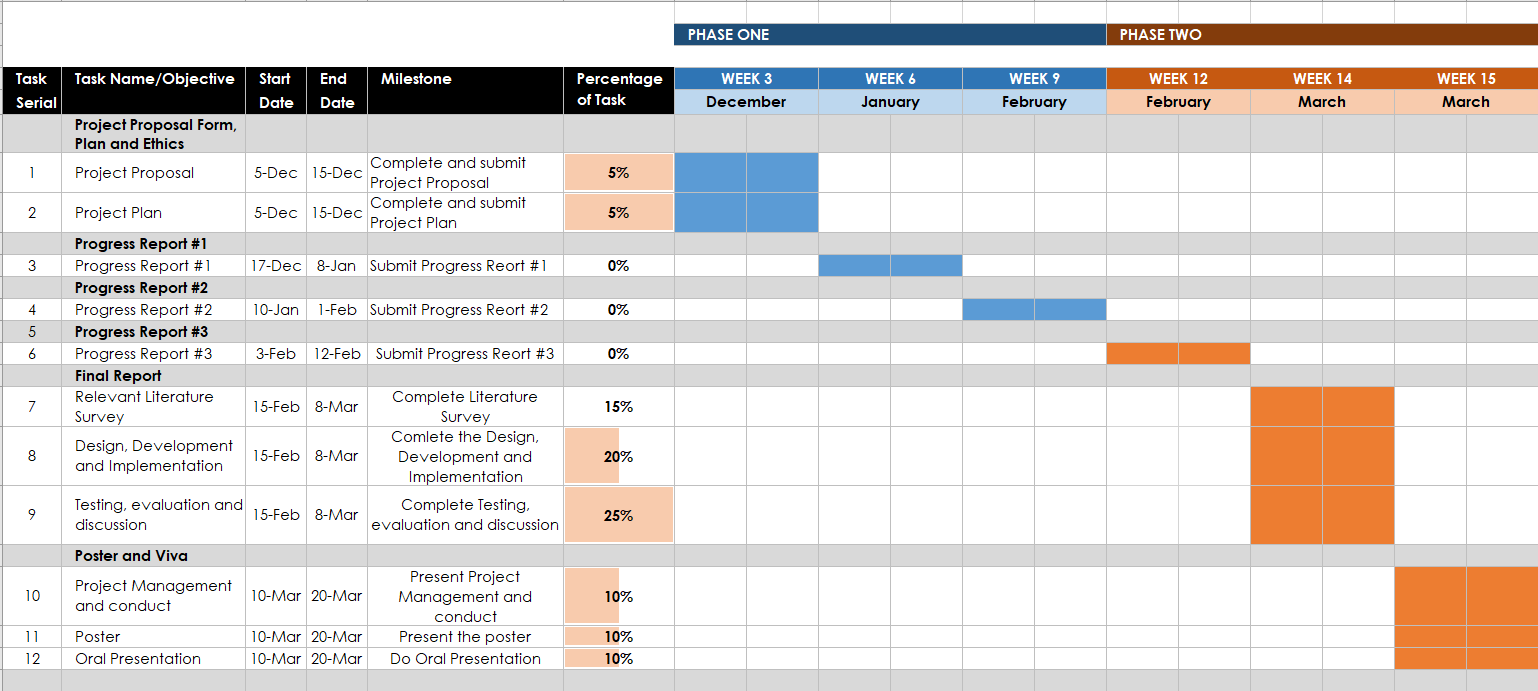
1. **MSc Project Proposal Form**

|  |  |
| --- | --- |
| **Student Number** | https://github.com/harshrajbedi/Cisco-Packet-Tracer-Projects/tree/main/Intrusion-Detection-System |
| **Student Name** |  |
| **Course Name** | MSc Cybersecurity With Project Management |
| **Supervisor Name** |  |
| **Project Title** | Securing Network Applications via embedded Security Model |
| **Description of your artefact** | ***Aim of the project***  The aim of this project is to provide different available security models, with their sole purposes to secure applications. The project aims to use a secure network model to provide security to the network applications.    Use of a secure network model is essential in preventing a threat to the network or changing the authenticity of the transmitted information. The use of an application proxy firewall is essential in that it will prevent the access to a private network by identifying and blocking any potential attacks (University Information Technology Services, 2021). To implement our proposed network model, we will use Packet Tracer, a network simulation tool for the deployment of network topology. This is generally performed by implementing security as an external part of the application, by securing the information (network data) transmitted by the applications, with general security models and technologies. This is the common approach used today to secure applications.  ***Objectives of the project***   * Do research on the available security threats to applications and the available security models that can secure the applications. * To get the network applications to be used for the deployment of the network topology. * To monitor the network after securing it with the adopted model. * To simulate cyberattacks on the network in a system to test the variability of the model. * To do an analysis of the network and the model and capture any suspicious activities. * To evaluate and discuss the measures of improving the model to secure the network from any type of attack.   ***List of features that the artefact will include***  In the project, there will be the features of the artefact that will be utilized. The list of features of the artefact include:   1. To do the analysis of the network traffic gotten from the network applications to be used. 2. To implement the model by use of Packet Tracer a network simulation tool for the deployment of network topology. 3. To test the model in its efficiency to deal with attacks from various threats. 4. Do a series of analysis to know any issues that may arise concerning the model and the potential threats.   ***Identify the added value that the project provides***  In as much as the features of the artefact have been discussed, it is crucial to analyse the added features that the artefact gives the project in analysing the network applications and the use of the adopted model. They include:   1. To do an analysis of the adopted model after implementation by use of Packet tracer. The analysis of model will add more value as it will show the efficiency of the model in dealing with network security. 2. To undertake experiments that will show the different uses of the model and do the report and summary of the model.   ***Identify the intellectual challenges involved***  There may be limitations the research and the project due to factors listed below:   1. Limited resources as the embedded software are not the same as the one in a desktop (Jeong et al., 2014) 2. Difficulties in the hardware integration and the time requirement 3. There is a gap in the skills needed for the project. |
| **What methodology (structured process) will you be following to realise your artefact?** | ***Proposed Methodology***  The project will follow a methodology that is listed below:  ***Justification for realising the artefact***  In the methodology adopted, the process of carrying out the project is specified. The method shows the preparation for the project regarding the security issues to the networks and the experiments that will be carried out to see the efficiency of the model. Each step is carefully thought of and adds value to the project through helping achieve the aims and goals of the project. It is hence clear that the methodology used is no just justified but also efficient and in line with the project adopted.  ***Research Methodology***  The methodology adopted is based on the working on phases. The adoption of the phases ensures that the model ahs extended life cycle and security policies. The adopted model will be able to protect the networks from attacks. To analyse malware and threats that may be coming to the system, there will be use of frequency analysis to analyse the frequency of the data and recognize the source IPS that re vulnerable (Oktadika, et al., 2021)  ***Project Management***  There are various project management aspects that will be utilized to ensure that the project is a success:   1. Maintaining of the project timeline and activities. 2. Making the work easier through subdivision of the work into sections. 3. Recording of the project milestones after each activity. 4. Keeping in line with the adopted methodology. 5. To do an analysis of the security threats and how best to protect the network applications.     In the process of project execution, the various milestones will be recorded by use of the Kanban board. In putting the data to the board, the method to be used will be:   * + - 1. Making the project, the goals, and timeline and updating to the board.       2. Getting all the necessary information on the project and updating the materials to the board.       3. Making a choice on the tools and model to be used for the project and updating to the board.       4. Carrying out the securing of the information transmitted by the applications, with general security models and technologies.       5. Testing of the adopted model for the security of the network applications and updating on the board.       6. Testing for threats that may cause harm to the adopted model and updating on the board.       7. Present the well tested model and record on the board. |
| **How does your project relate to your degree course and build upon the units/knowledge you have studied/acquired** | The project is about Securing Network Applications via embedded Security Model. It is in line with the course of cyber security as coming up with a model that provides security to applications network is on cybersecurity. The theme and focus of the project is in line with my course and degree and is hence building on my knowledge of the course material. |
| **What are the main contributions of your project as compared to state-of-the-art?** | The project has contributions as compared to state-of-the-art techniques in some ways. Thy include:   1. Application analysis by taking a network application that can be later used as a reference. 2. To do security analysis on applications that will generate the necessary data for the research. 3. To use the adopted model for network security to test its efficiency in network security. 4. To come up with a report on the model and its efficiency in network security.   In most cases, when using the state-of-the-art experiments, the examples may be few and the experiments may not adequately test the model. The experiment will also be useful to organizations as it will provide the network security they need through the adopted model. |
| **Resources** | Several resources will be useful in the implementation of the project as described below:  **Tool**: Packet Tracer  **Environment**: Windows Operating System 64 Bit  **Data**: Information (network data) transmitted by the applications.  **Licence**: Open Licenced data and tool  **Hardware Equipment**: The necessary computer resources such as routers, and network servers.  **Literature Review**: University Resources, scholarly materials and IEEE |

1. **Project Plan and GANTT Chart:**

The project timeline, milestones and the Gantt chart are shown below:



# References:

Jeong, H., Park, J. H., & Jeong, Y. (2014). An ANP-Based Practical Quality Model for a Secure Embedded System with Sensor Network. *International Journal of Distributed Sensor Networks*. <https://doi.org/10.1155/2014/505242>

Oktadika, A., Lim, C. & Erlangga, K., (2021). Hunting Cyber Threats in the Enterprise Using Network Defense Log. *9th International Conference on Information and Communication Technology*.

University Information Technology Services. (2021, June 1). *About firewalls*. Indiana University Knowledge Base. <https://kb.iu.edu/d/aoru>