**SYSTEM DIAGRAMS**

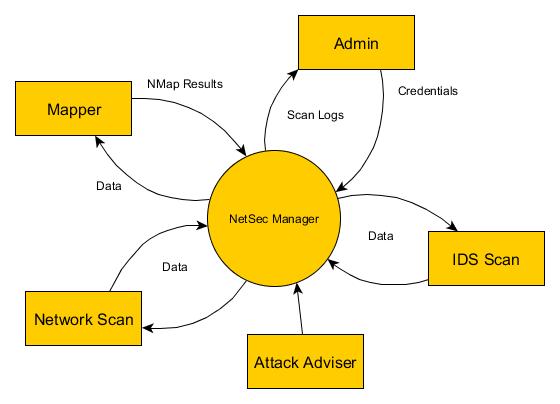
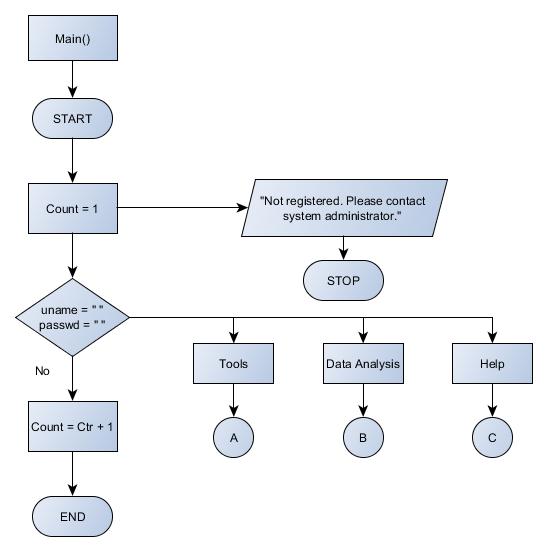


Figure 1: Conceptual Diagram

The Administrator will input his credentials (username and password) to operate the system. Once the system validated the credentials the administrator will be given four options: IDS scan, view the Attack Adviser, to scan the network, and Mapper to create a map of the network. If the administrator choose the IDS Scan, the snort will start scanning. If the administrator choose the Attack Adviser, it will display the attack adviser document. If the administrator choose to scan the network, NetSec Manager will start scanning the network while fetching the data, once the result is provided, the result will be saved to the database for documentation purposes. And if the administrator choose the Mapper, it will start mapping the IP Address.

Figure 2: Main Program of NetSec Manager

In figure 2. The main program of NetSec Manager is explained via program flowchart. Starting from the login menu, the administrator is given 3 times to enter his credentials. If the credentials is correct, NetSec Manager will redirect to the main menu consist of the 3 different modules: Tools, Data Analysis and Help. If the credentials did not match the credentials in the database, the system will prompt a display message regarding the error.

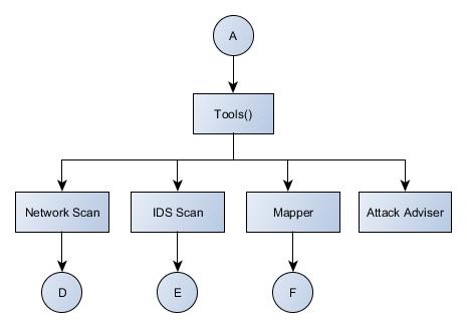


Figure 2.1: Tools module of the NetSec Manager

In figure 2.1, The Tool modules is expanded. Under the Tool module, the Network Scan, IDS Scan, Mapper and Attack Adviser module is located. This module is the one responsible in scanning the network, detecting the rules set in the network together with the data allowed by the firewall, the active and inactive host in the network, and the countermeasures for common network attacks. This modules is also connected to the system database for the generating of logs.

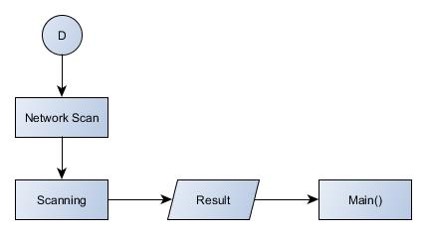


Figure 2.2: Network Scan module of the NetSec Manager

In figure 2.2, The Network Scan module is expanded. This module is the main feature of NetSec Manager. Once the scanning is initiated, the results of the scanning is automatically saved in the NetSec Manager database.

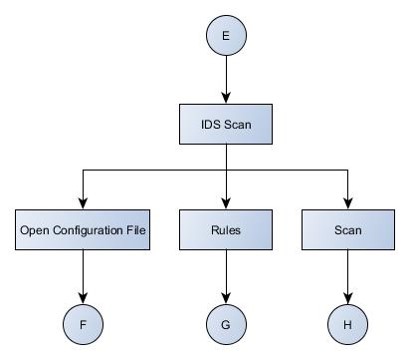


Figure 2.3: IDS Scan module of the NetSec Manager

In this figure, the IDS Scan module is expanded. IDS Scan module is composes of 3 sub modules, the Open Configuration File module, the IDS Rule module and the Start Scan module. The Open Configuration File display the Snort configuration file for minor settings regarding the program, IDS Rule display the different Snort rules where the administration can set his/her own rules for managing the network, lastly the Scan tab triggers the start of the network scan.

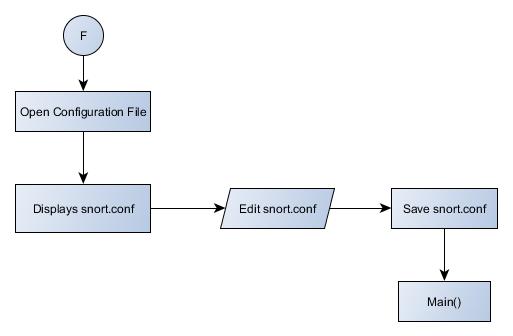


Figure 2.4: Open Configuration file module of the NetSec Manager

In this figure, the Open Configuration File module is expanded. In this module, the administrator can update or edit the IDS Configuration file to insert any changes he/she want to implement for the network.

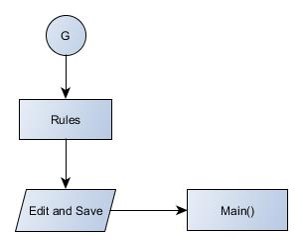


Figure 2.5: IDS Rules module of the NetSec Manager

In this figure, the list of Snort rules will be display. The administrator can view, edit and save the IDS rules that was set to be implemented in the network.

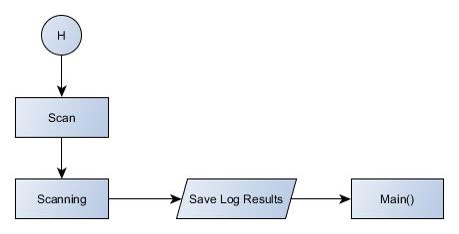


Figure 2.6: Scan Process module of the NetSec Manager

In this figure, the process of scanning the network is shown, once the administrator stops scanning the network, the results will be saved to the NetSec Manager database and the logs can be generated from the database for viewing purposes.

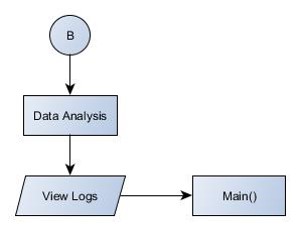


Figure 2.7: Data Analysis module of the NetSec Manager

This figure shows the expanded Data Analysis module. Under this module, the View Logs is located. View logs module contains the saved scan results fetched from the database.

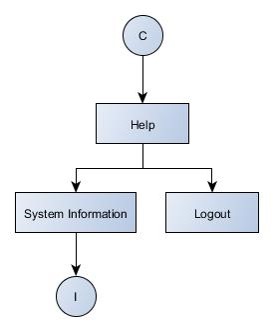


Figure 2.8 Help module of the NetSec Manager

In this figures, the Help module is expanded. The Help Module is composes of System Information which contains system requirements and the project developer profiles and the logout module.

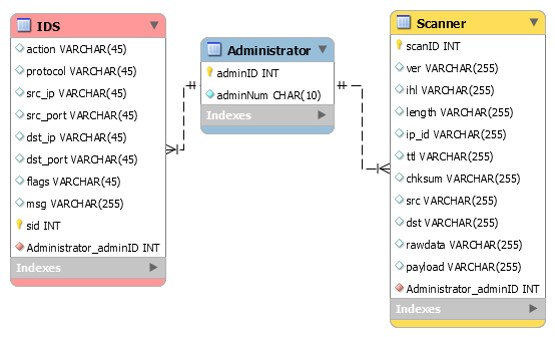


Figure 3: Entity-Relationship Diagram

NetSec Manager will use MySQL database system to generate results from Network Scan. NetSec Manager Entity Relationship Diagram composes of two tables: Administrator table that is connected to the Scanner table. Under the Administrator Table is the following attributes: Administrator ID, Administrator Number which will serve as the administrators credential in using the system. On the other hand, Scanner table contains Scan ID, IP Version, Internet Header Length, IP ID, Packet Time to Leave, Packet Checksum, Packet Source, Packet Destination, Packet Raw data, and Packet Payload and the foreign key of Administrator ID which will be gathered from the process happened in the terminal while the administrator is away.

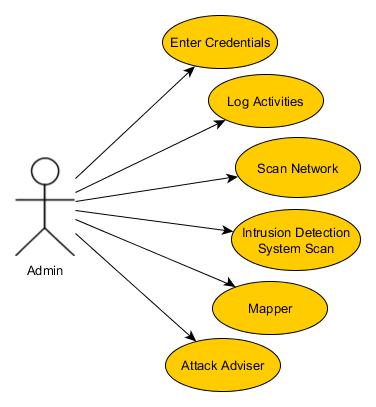


Figure 4: Unified Modeling Language

Unified Modeling Language helps the users how to visualize the design of a system. In this figure, the proponents shows the relationship of the administrator to the NetSec Manager features. The Administrator is the actor while the features is the use case. NetSec can be visualize with this UML since our system focuses on the use of the network and security administrator.

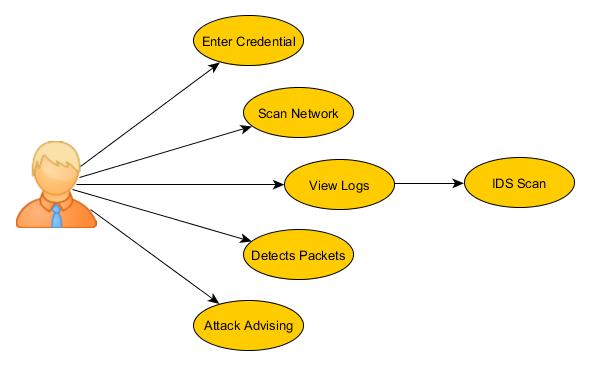


Figure 5: Use Case Diagram

The figure shows the use case diagram of NetSec. This shows the capability of the administrator in using the system. Once the network administrator has entered his/her credentials, through NetSec, he/she has the capability to sniff the network, view logs from the IDS scan, detects packets behavior through the IDS, and view attack advising.

**PROJECT MODULE SCREENSHOTS**

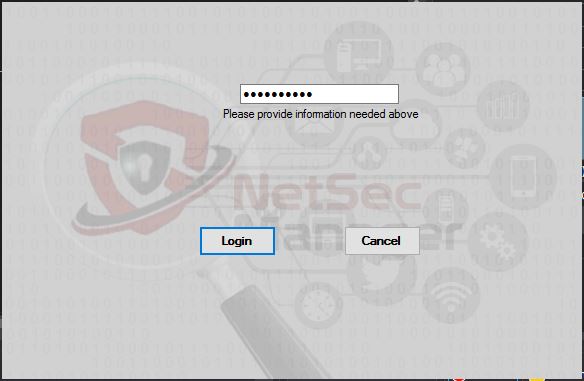


Figure 6: Screen Layout for Login Interface

This is the login screen layout of the NetSec Manager. In the input box, the network administrator will have to enter the given authentication key to be able to log-in and use the system. The administrator will be given two options, The Log-in and Cancel Button. Clicking the log-in button will give the network administrator access to the whole feature of the system. And clicking on cancel button will terminate the log-in screen.

****

Figure 6.1: Screen Layout for Main Menu

After the administrator has enter his credentials and authenticated in the database, the main menu screen layout will appear. On the upper left part is the 3 main modules of the system. Under the tools module are Network Scanner, IDS Scan, Mapper and Attack Adviser which consist of different process. In the data analysis module, the network administrator can be able to view the logs captured under the Network Scanner module. And under the Help module, the network administrator can either view the System Information and the log-out button of the system.

Figure 6.2: Screen Layout for Network Scanner



After the network administrator clicked on the Sniffer shown above, the scanning of network begins. The process can only be stop manually by the admin. While scanning, the process of scanning the network can be view as like the given figure above.

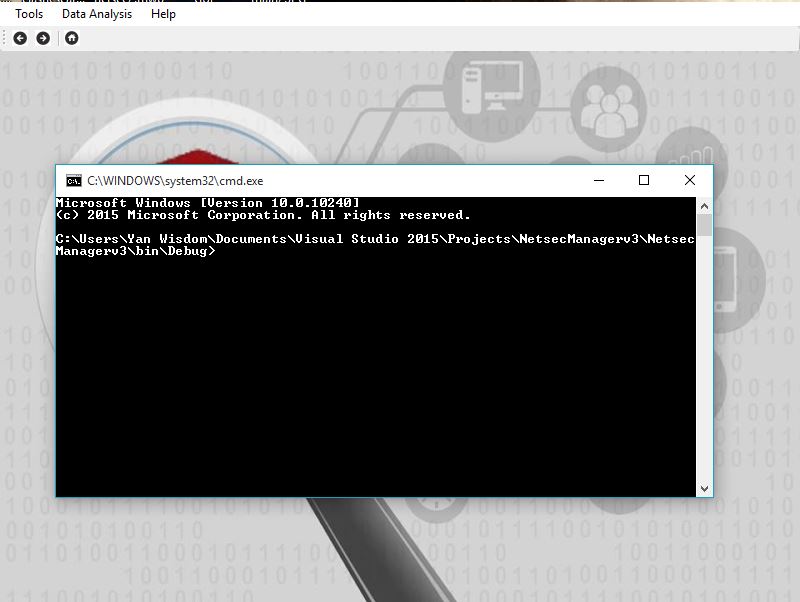
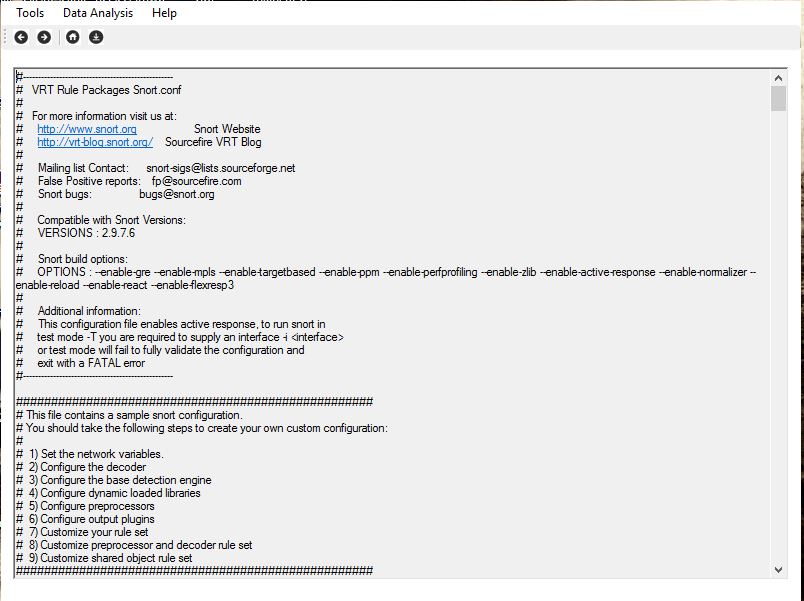


Figure 6.3: Screen Layout for IDS Scan

After clicking on Start Scan inside the IDS Scan, the command line screen will pop out and automatically starts scanning. The process of scanning the network can be view as like the given figure above.

Figure 6.4: Screen Layout for Open Configuration File

Clicking on the Open Configuration File opens the IDS configuration file in a text editor, where the network administrator will be able to set the rules he or she wants to enable, the speed of the scan, and the behavior of the IDS itself – on how to run in the network.

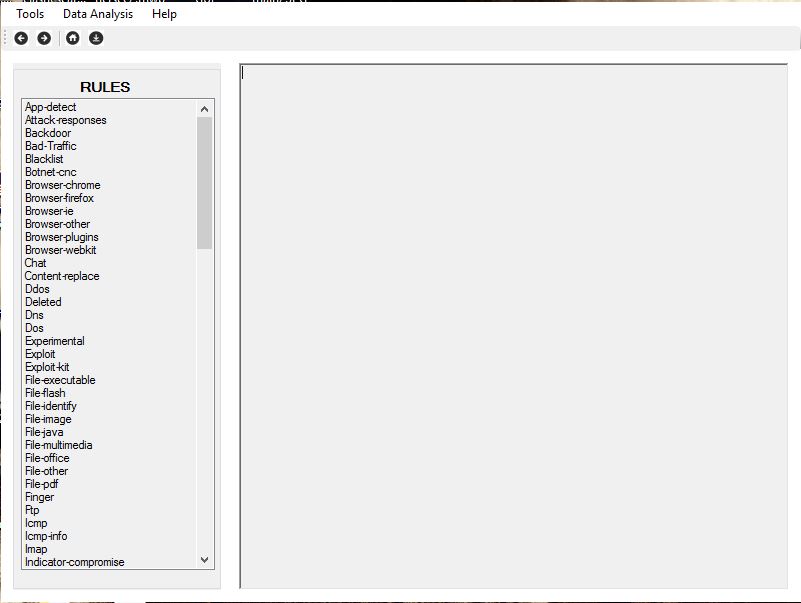


Figure 6.5: Screen Layout for Rules

When the administrator clicks the Rules module, it will automatically open the list of the Snort rule saved in the terminal. Then the administrator has the capability to view, edit and save the following rules.

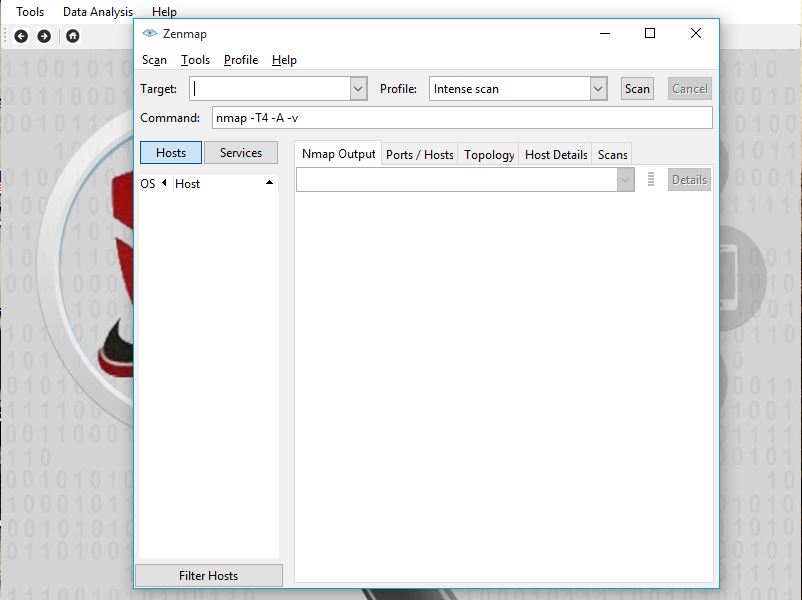
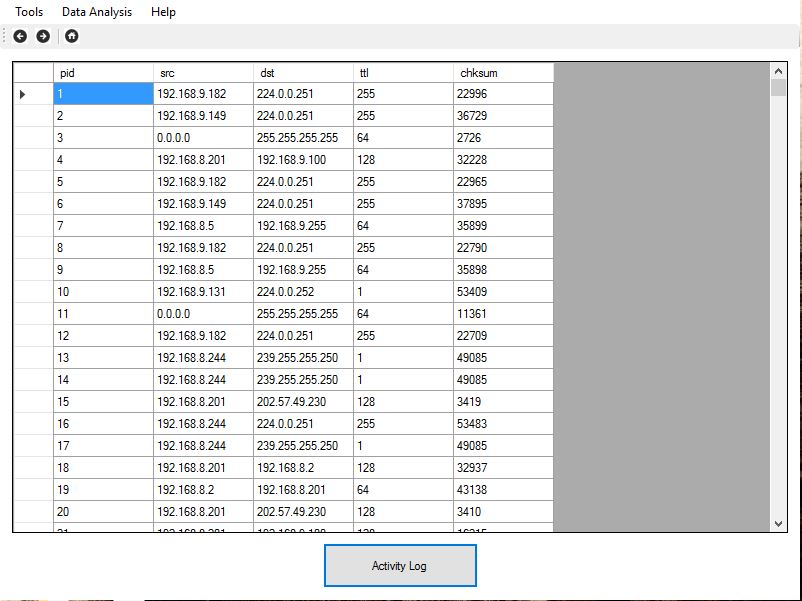
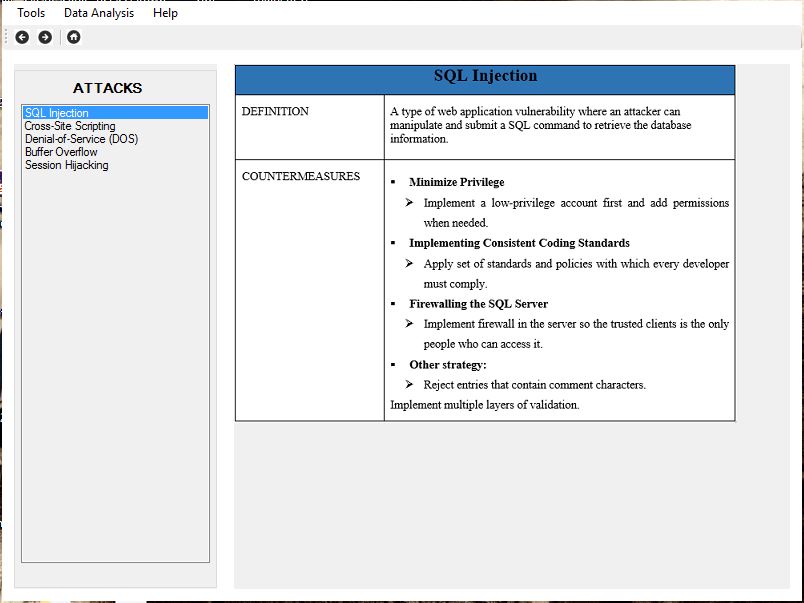


Figure 6.6: Screen Layout for Mapper

After clicking on Mapper under Tools Module, the Zenmap GUI Interface will pop out and ask the administrator what is the target IP Address and Scan Type. The process of networking mapping can be view as like the given figure above.

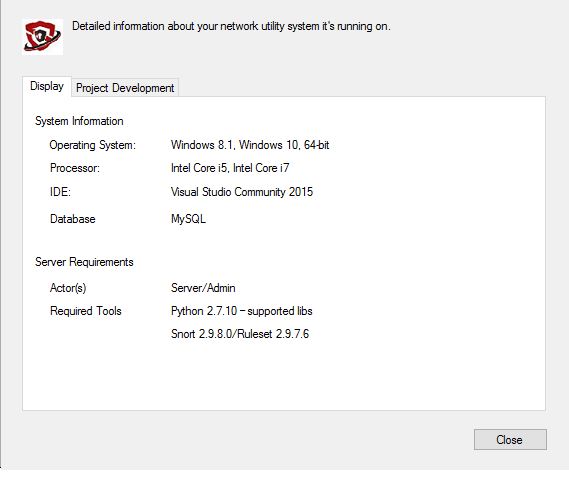
Figure 6.7: Screen Layout for Data Analysis

When the administrator clicks the Data Analysis button, data saved in the database will then be viewed in this interface. He or she will be able to view the logs generated during the network scan. Inside the generated data is the listed pid which is the generated Packet ID, While the src is the source ip and dst is the destination, Time to live (ttl) is for the packet to reach its destination, Lastly the chksum protects the header of IPv4 data packets against data corruption.

Figure 6.8: Screen Layout for Attack Adviser

The network administrator can seek help on how to mitigate common network attacks by clicking the Attack Adviser module. This contains the name of the attack, the definition, and the countermeasures in order to mitigate the said attack.

****Figure 6.9: Screen Layout for Help Module



When the administrator clicks the Help Module, two sub-menus will be displayed; System Information which contains a tab menu displaying the system and server requirements for the installation of the NetSec Manager. The other module is the logout button which will end the administrator’s session once clicked.