**Table 1.0 Use Case Specifications for User Authentication**

|  |  |
| --- | --- |
| **Use Case ID:** | NETSEC MANAGER-SUC1 |
| **Use Case Name:** | User Authentication |
| **Description:** | The administrator needs to login with his credentials for him to user the system. |
| **Actor/s:** | Administrator |
| **Pre-condition/s:** | Administrator must claim the username and password from the developer.  Administrator must login in the system. |
| **Post-condition/s:** | Administrator may access the system. |

|  |  |
| --- | --- |
| **Main Success Scenario** | |
| **Actor’s Action** | **Systems Response** |
| 1. Opens the application |  |
|  | 2. Displays the login page of NetSec Manager |
| 3. Types his/her username and password |  |
| 4. Needs to click the login button |  |
|  | 5. Display message, “You are now log in.” |
|  | 6. Checks on its database if the username and password entered is correct |
|  | 7. Username and password matches |
|  | 8. System main menu will now appear. |

|  |  |
| --- | --- |
| **Alternate Flow** | |
| **Actor’s Action** | **Systems Response** |
| 1. At step 4: If username and password of Administrator did not match. | Display message, "Not registered. Please contact system administrator." |

**Table 2.0 Use Case Specifications for Network Scan**

|  |  |
| --- | --- |
| **Use Case ID:** | NETSEC MANAGER-SUC2 |
| **Use Case Name:** | Network Scan |
| **Description:** | The administrator will conduct a network-layer scan to determine all the active terminals and its activities. |
| **Actor/s:** | Administrator |
| **Pre-condition/s:** | Administrator must claim the username and password from the developer.  Administrator must login in the system. |
| **Post-condition/s:** | Administrator was able to scan the network. |

|  |  |
| --- | --- |
| **Main Success Scenario** | |
| **Actor’s Action** | **Systems Response** |
|  | 1. Displays Main Menu with three (3) tabs: Tools, Data Analysis and Help |
| 2. Clicks Tools tab |  |
|  | 3. Displays four (4) choices for Tools tabs: Network Scan, Intrusion Detection System Scan, Mapper and Attack Adviser |
| 4. Clicks Network Scan tab |  |
|  | 5. Displays Scanner sub-menu |
| 6. Clicks Scanner sub-menu |  |
|  | 7. Will now start Python scanner |
| 8. Clicks Stop button |  |
|  | 9. Python Scan stops. Scan results will be saved to the database and the system logs will updated. |
|  | 10. Redirects to the Main Menu |

|  |  |
| --- | --- |
| **Alternate Flow** | |
| **Actor’s Action** | **Systems Response** |
| Not Applicable | Not Applicable |

**Table 3.0 Use Case Specifications for Intrusion Detection System Scan**

|  |  |
| --- | --- |
| **Use Case ID:** | NETSEC MANAGER-SUC3 |
| **Use Case Name:** | Intrusion Detection System Scan |
| **Description:** | The administrator will conduct an Intrusion Detection System scan. An Intrusion Detection System that checks for the connections being allowed by the firewall. |
| **Actor/s:** | Administrator |
| **Pre-condition/s:** | Administrator must claim the username and password from the developer.  Administrator must login in the system. |
| **Post-condition/s:** | Administrator was able to scan the network. |

|  |  |
| --- | --- |
| **Main Success Scenario** | |
| **Actor’s Action** | **Systems Response** |
|  | 1. Displays Main Menu with three (3) tabs: Tools, Data Analysis, and Help |
| 2. Clicks Tools tab |  |
|  | 3. Displays four (4) choices for Tools tabs: Network Scan, Intrusion Detection System Scan, Mapper and Attack Adviser |
| 4. Clicks IDS Scan tab |  |
|  | 5. Display three (3) choices for IDS Scan: Open Configuration File, Rules and Start Scan (CMD) |
| 6. Clicks Open Configuration File sub-menu |  |
|  | 7. Opens snort.conf file |
| 9. Clicks Rules sub-menu |  |
|  | 10. Displays snorts rules |
| 11. Clicks Start Scan (CMD) sub-menu |  |
|  | 12. Starts Snort scanner |
| 13. Clicks stop button |  |
|  | 14. Snort Scan stop. Scan results will be saved to the database and the system logs will updated. |
|  | 15. Redirects to the Main Menu |

|  |  |
| --- | --- |
| **Alternate Flow** | |
| **Actor’s Action** | **Systems Response** |
| 1. At step 11. Administrator open Start sub menu. | Error displaying, terminal does not have Wireshark. |

**Table 4.0 Use Case Specifications for Data Analysis**

|  |  |
| --- | --- |
| **Use Case ID:** | NETSEC MANAGER-SUC4 |
| **Use Case Name:** | Data Analysis |
| **Description:** | The administrator will conduct a network-layer scan to determine all the active terminals and its activities. |
| **Actor/s:** | Administrator |
| **Pre-condition/s:** | Administrator must choose the Data Analysis. |
| **Post-condition/s:** | Administrator was able to see all the details recorder during the scan. |

|  |  |
| --- | --- |
| **Main Success Scenario** | |
| **Actor’s Action** | **Systems Response** |
|  | 1. Displays Main Menu with three (3) tabs: Tools, Data Analysis and Help |
| 2. Clicks the Data Analysis tab |  |
| 3. Under the Data Analysis tab, the Administrator will be seeing a submenu – View Data. |  |
|  | 4. The system will pop out interface of the View Data. |
|  | 5. The interface has a button with a label “Load Data”. When clicked, the interface will be able to display all the details recorded during the scan |
| 6. If the administrator has already done with going to the View Data, he/she can go back to the main menu. |  |

|  |  |
| --- | --- |
| **Alternate Flow** | |
| **Actor’s Action** | **Systems Response** |
| 1. At step 2. If the Administrator didn’t choose the Data Analysis Tab. | The view Data will not pop out and the Administrator will not able to display all the details recorded during the scan. |

**Table 5.0 Use Case Specifications for Mapper**

|  |  |
| --- | --- |
| **Use Case ID:** | NETSEC MANAGER-SUC5 |
| **Use Case Name:** | Mapper |
| **Description:** | Creates graphical presentation of the network – up and down hosts and open and close ports. |
| **Actor/s:** | Administrator |
| **Pre-condition/s:** | Administrator must choose the Mapper. |
| **Post-condition/s:** | Administrator was able to see the Nmap cheat sheet as a reference for using Nmap. |

|  |  |
| --- | --- |
| **Main Success Scenario** | |
| **Actor’s Action** | **Systems Response** |
|  | 1. Displays Main Menu with three (3) tabs: Tools, Data Analysis and Help |
| 2. Admin clicks Tool tab |  |
|  | 3. Displays four (4) choices for Tools tabs: Network Scan, Intrusion Detection System Scan, Mapper and Attack Adviser |
| 4. Clicks Mapper tab |  |
|  | 5. Displays two (2) choices for Mapper: Nmap and Nmap Cheat Sheet |
| 5. Clicks Nmap sub-menu |  |
|  | 6. Displays Zemap window. |
| 7. Enters the target IP Addresses, Profile and click the scan. |  |
|  | 8. Starts mapping the IP Addresses. |
| 8. Closes Nmap |  |
| 9. Clicks Nmap Cheat Sheet sub-menu |  |
|  | 10. Displays the Nmap cheat sheet |
| 11. If already done with going to the cheat sheet, goes back to the main menu |  |

|  |  |
| --- | --- |
| **Alternate Flow** | |
| **Actor’s Action** | **Systems Response** |
| Not Applicable | Not Applicable |

**Table 6.0 Use Case Specifications for Attack Adviser**

|  |  |
| --- | --- |
| **Use Case ID:** | NETSEC MANAGER-SUC6 |
| **Use Case Name:** | Attack Adviser |
| **Description:** | The administrator will be viewing the most common attacks that happens in the network. |
| **Actor/s:** | Administrator |
| **Pre-condition/s:** | Administrator must choose the tool tab. |
| **Post-condition/s:** | Administrator was able to do the Attack Adviser. |

|  |  |
| --- | --- |
| **Main Success Scenario** | |
| **Actor’s Action** | **Systems Response** |
|  | 1. Displays Main Menu with three (3) tabs: Tools, Data Analysis and Help |
| 1. Clicks the Tool tab |  |
|  | 3. Displays four (4) choices for Tools tabs: Network Scan, Intrusion Detection System Scan, Mapper and Attack Adviser |
| 4. Clicks Attack Adviser tab |  |
|  | 5. Displays the attack adviser document |
| 10. If already done with going to the attack adviser, goes back to the main menu |  |

|  |  |
| --- | --- |
| **Alternate Flow** | |
| **Actor’s Action** | **Systems Response** |
| 1. At step 2: If the Administrator didn’t choose the Tool tab |  |
|  | 2. The attack adviser document will not display. |

**Table 7.0 Use Case Specifications for Logout**

|  |  |
| --- | --- |
| **Use Case ID:** | NETSEC MANAGER-SUC8 |
| **Use Case Name:** | Logout |
| **Description:** | Logs out from the system. |
| **Actor/s:** | Administrator/Terminal |
| **Pre-condition/s:** | Administrator must choose the Help tab and logout sub menu |
| **Post-condition/s:** | Administrator was able to Logout. |

|  |  |
| --- | --- |
| **Main Success Scenario** | |
| **Actor’s Action** | **Systems Response** |
| 1. Clicks the Help tab and choose the logout sub-menu |  |
|  | 2. Destroys user session and logs out administrator from the system |
|  | 4. Displays Login Screen |

|  |  |
| --- | --- |
| **Alternate Flow** | |
| **Actor’s Action** | **Systems Response** |
| Not Applicable | Not Applicable |