**CIS 2640 – Lab 12**

**Identifying & Analyzing Network/Host Intrusion Detection System (NIDS/HIDS) Alerts**

| **Your Name:** | Liliane Owens |
| --- | --- |
| **Date:** | 4/16/23 |

**Instructions**: Complete the tasks described in this worksheet. Read the instructions carefully and submit evidence of your completed tasks (a screen shot is your evidence). Answer the questions below in the space provided.

* **Showing Evidence of Completion:** Your evidence of completion is a screen shot, as described in each exercise. Use the tool of your choice to take a screen shot of the required content. ***Screen shots should be pasted at the end of this document.***
* **Answering Questions:** Your answers should be written in carefully edited college-level English, using complete sentences.

| **Lab – Identifying & Analyzing Network/Host Intrusion Detection System (NIDS/HIDS) Alerts** | |
| --- | --- |
| **Instructions and Evidence of Completion** | **Answer a Question** |
| At the end of this document (not within this table) paste screen captures that show the following:   1. The result from Zenmap of the three networks in our topology 2. The output\* from Sguilshowing the number of the various severities (high, medium, low) that were detected 3. The output\* from Squert showing the Event Count and Event Count by Priority.   **\* Note**: If you do not get an event count take screen pics anyway. This is a possible condition of the software not catching the network activity.  ***Be sure your screen shot(s) include any command executed and the resulting output in clear / cropped screenshots.*** | Answer each of the questions below using the space to the right of the question. Be sure your answer is complete and correct. |
| **Question** | **Answer** |
| 1. How is Zenmap different from Nmap? | Zenmap is a GUI version of Nmap whereas Nmap is a command-line network scanner used to detect hosts and services. |
| 1. Squil and Squert are all what kind of tools? | They are Security Onion tools for managing and respond to alerts. |
| 1. In your own words how would you describe the Security Onion? | Security Onion, I think it as Network security platform which provides intelligence, context and situational awareness of your network. |

Put screenshots here:

1. The result from Zenmap of the three networks in our topology

![Graphical user interface, text, application

Description automatically generated]()

1. The output\* from Sguilshowing the number of the various severities (high, medium, low) that were detected

![Table

Description automatically generated]()

![Graphical user interface, application, table

Description automatically generated]()

1. The output\* from Squert showing the Event Count and Event Count by Priority.

![Graphical user interface, application

Description automatically generated]()