**CIS 2640 – Lab 8**

**Analyze and Differentiate Types of Malware & Application Attacks**

| **Your Name:** | Liliane Owens |
| --- | --- |
| **Date:** | 3/26/23 |

**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 – Analyze and Differentiate Types of Malware & Application Attacks** | |
| --- | --- |
| **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 version of bash running on the Ubuntu system 2. The detection of the Shell Shock vulnerability found on the Apache server 3. The rkhunter tool displaying the Rootkit vulnerability it found.   ***Be sure your screen shot(s) include any command executed and the resulting output in clear / cropped screenshots.*** | Answer each of the questions below; use the space to the right of each question for your answer. Make sure your answers are clear and complete. |
| **Questions** | **Answer** |
| 1. What command was used to determine the version of BASH running on the Ubuntu client? What version was it? | Echo $ BASH\_VERSION. Bash version. |
| 1. What does the acronym “CVE” stand for and in your own words explain what it represents? | CVE stands for Common Vulnerabilities and Exposures. It is like a dictionary of standardized names for vulnerabilities and other security exposures. It is mainly intended to share the data across separate vulnerable databases and security tools. |
| 1. What was the specific BASH vulnerability found on the Ubuntu client? | The Specific BASH Vulnerability found on Ubuntu Client is Shellshock Bash Bug and this vulnerability was attacked 2014. |
| 1. When this vulnerability was attacked what ability was provided to the attacking machine? | 2014. This Vulnerability gave the attacker the ability of a duper user. This was mainly based on the storage of the environment variables that define the status of the currently logged-in user in Bash and OS. By creating an environment variable with a specific structure, an attacker will be able to execute code next time Bash starts. |
| 1. What command was executed to check the nsm service on the Security Onion? | sudo service nsm status. |
| 1. In a Linux file system, how are hidden files or directories named? | They are named starting with a dot character. And they are usually called as dotfiles and will not be visible when you type **ls** command. In order to display them you need to use **ls-a** command. They are not a security mechanism as the access is not restricted but the main intention is not to clutter the display of the contents of a directory. |

Put screenshots here:

1. The version of bash running on the Ubuntu system

![A picture containing text

Description automatically generated]()

2. The detection of the Shell Shock vulnerability found on the Apache server

![Text

Description automatically generated]()

1. The rkhunter tool displaying the Rootkit vulnerability it found.

![Text

Description automatically generated]()

![Text

Description automatically generated]()

![Text

Description automatically generated with medium confidence]()