**CIS 2640 – Lab 5**

**Performing Active Reconnaissance with Linux**

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

**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 – Performing Active Reconnaissance with Linux** | |
| --- | --- |
| **Instructions and Evidence of Completion** | **Answer a Question** |
| At the end of the document (not in this table) paste a screen capture that shows:   1. A nmap scan showing the Operating System on the machine at 192.168.1.50 2. The CVEs listed for 10.1.1.10 3. The creation of a new user Analyst1 in OpenVAS.   ***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. What is the command to determine the operating system found on the machine at 192.168.1.50? | It is **nmap -O 192.168.1.50.** |
| 1. When you scanned for machines with port 80 open what did you find? What does this indicate about those machines? | When we scanned for machines with port 80 open, we found out about the services running on the port and the versions of the specified services and we can be fairly certain that HTTP and HTTPS are working or running, and it indicates that the machines are presumably web servers. |
| 1. How is Zenmap different from nmap? | **Intuitive and graphical outcomes visualization**  Notwithstanding demonstrating Nmap's ordinary yield, Zenmap can **mastermind** its presentation to show all ports on a host or all hosts running a specific help. It sums up insights concerning a **solitary host** or a total output in an advantageous showcase. Zenmap can even draw a geography guide of founded organizations. The **consequences** of a few sweeps might be **consolidated** and seen on the double.  **Correlation**  Zenmap can show the **contrasts** between two sweeps. You can perceive what changed between a **similar sweep**run on various days, between outputs of two **unique hosts**, between outputs of similar hosts with various choices, or some other mix. This permits executives to effectively follow new has or **benefits** showing up on their **organizations**, or existing ones going down.  **Comfort**  Zenmap monitors your **sweep results until** you decide to discard them. That implies you can run a sweep, see the outcomes, and afterward conclude whether to **spare** them to a document. There is no compelling reason to think about a record name ahead of time.  **Repeatability**  Zenmap's order profiles make it simple to run precisely the**same sweep more than once**. There's no compelling reason to set up a shell content to do a typical output.  **Discoverability**  Nmap has in a real sense several alternatives, which can be overwhelming for learners. Zenmap's interface is intended to **consistently** show the order that will be run, regardless of whether it comes from a profile or was developed by picking choices from a menu. **This assists novices with learning** and comprehending what they are doing. It likewise helps **specialists** twofold check precisely what will be run before they press "Scan". |
| 1. What command did you use to launch the OpenVAS application? | **/home/scripts/Openvas\_restart.** |
| 1. In your own words describe the OpenVAS tool? What other tool is it similar too? | OpenVAS (Open Vulnerability Assessment System, initially known as GNessUs) is a product structure of few administrations and instruments offering weakness examining and weakness the executives. All OpenVAS items are free programming, and most segments are authorized under the GNU General Public License (GPL). The other comparable apparatus accessible is **Nessus** Professional which is the accepted**business standard** for weakness appraisal. Nessus performs **point-in-time appraisals** to help security experts rapidly and effectively recognize and**fix weaknesses**, including**programming defects, missing patches, malware, and misconfigurations** - over an assortment of working frameworks, gadgets, and applications. With highlights, for example, pre-constructed strategies and formats, adjustable announcing, bunch "nap" usefulness, and ongoing updates, Nessus is intended to make **weakness evaluation** basic, simple, and natural. The outcome: less time and exertion to survey, organize, and remediate issues. It is a GUI apparatus wherein a few orders can be prepared by CLI also. |

Put screenshots here:

1. A nmap scan showing the Operating System on the machine at 192.168.1.50

![Text

Description automatically generated]()

1. The CVEs listed for 10.1.1.10

![Graphical user interface, application, website

Description automatically generated]()

![Graphical user interface, application, website

Description automatically generated]()

1. The creation of a new user Analyst1 in OpenVAS.

![Graphical user interface, application

Description automatically generated]()