**CIS 2640 – Lab 7**

**Analyze and Differentiate Types of Attacks and Mitigation Techniques**

| **Your Name:** | Liliane Owens |
| --- | --- |
| **Date:** | 4/2/2023 |

**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 Attacks and Mitigation Techniques** | |
| --- | --- |
| **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. The successful use of the ncrack tool to discover the password for the root account on the Ubuntu client. 2. Paste a screen capture showing the log file analysis showing privileges being escalated to root.   ***Be sure your screen shot(s) include any command executed and the resulting output in clear / cropped screenshots.*** |  |
| **Question** |  |
| 1. What command would you use to stop the denyhosts service? | **sudo service denyhosts stop** |
| 1. What command would you use to make a Secure Shell connection to the Ubuntu client machine? | ssh [student@192.168.1.50](mailto:student@192.168.1.50) “uptime” |
| 1. What tool was used to find the password for the root account? | We use ncrack tool to discover the password. |
| 1. What type of password attack was used in this case? | It was brute force used. |
| 1. Name two other password attack methods that can be used? | Birthday, guessing. |
| 1. What file was used to contain the lists of hosts that had been denied a connection to the Ubuntu client? | It is **hosts.deny file**. |
| 1. What tool (or command) was used to remove the Kali machine from the list of hosts being denied (the file in question #6) by the Ubuntu client? | **grep sshd /etc/hosts.deny.** |
| 1. Explain in your own words how a DOS or DDOS attack results in a victim machine being disabled. | Because the attacker use multiple compromised computer system to block your traffic, because your computer already infected by a malware which allow the attacker to control you. |

Put screenshots here:

1. The successful use of the ncrack tool to discover the password for the root account on the Ubuntu client.

![Text

Description automatically generated]()

1. Paste a screen capture showing the log file analysis showing privileges being escalated to root.

![Text

Description automatically generated]()