**Lab 1**

Outcomes:

- **Setting up your lab environment:** Students will be setting up their Container based lab environment that they will use throughout the semester to complete lab exercises.

- **Password cracking and network attacks:** Students will perform different tasks related to password attacks and network attacks

Objectives:

1. Install Docker Desktop on Windows 10
2. Install Docker on Mac
3. Use John the Ripper to crack passwords
4. Perform ARP Cache Poisoning

Deliverables:

One lab report that includes the following:

1. A cover page including: Course title, Lab #, Date, Name and ID…etc.
2. Filled in answer sheets for all parts of the lab.

* Insert your answers and screenshots as required in the table below
* Provide appropriate references with citations wherever required.

|  |
| --- |
| **Task 3:** |
| * **provide screenshot of the output** * **The security administrator in your company has been asked to perform a password audit to ensure that the employees are following the company’s password policy that states that all employees have to use strong and complex passwords. The security administrator has chosen to use the Single Crack Mode for their audit. Do you support their decision? And why? Explain in detail and use the results of the command in step 3 to support your answer.** |
| * **Take screenshot of both commands output. What is the difference between the two commands? How does choosing a wordlist affect the results of the attack?** |
| * **provide screenshot of the output** |
| * **How is the command used in step 5 different from the command used in step 6? How do you see it reflected in the results? Give an example.** |
| * Enter the following command to show the cracked passwords. **provide a screenshot of the output.** |
| * **List 3 problems associated with password-based authentication? How does password less authentication work and how can it solve the 3 problems that you have listed.** |
| **Task 4:** |
| * **On host M, construct an ARP request packet to map host A’s IP address to host M’s MAC address. Send the packet to host B and check whether the attack is successful or not. Provide screenshots to show all steps.** |
| * **Perform the ARP poisoning steps again to populate Host B’s ARP cache with the MAC address of the attacker’s machine, instead of the default gateway MAC address. Explain your steps in details and provide screenshot of you work.** |
| * **What would the possible consequences for the victim in the case of the ARP poisoning attack performed in step 10** |