**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.

Contents

[Overview 1 3](#_Toc112092106)

[Task 1: Install Docker Desktop on Windows 10 4](#_Toc112092107)

[Task 2: Install Docker Desktop on Mac 5](#_Toc112092108)

[Task 3: Use John the Ripper to crack passwords 6](#_Toc112092109)

[Task 4: Perform ARP Cache Poisoning 8](#_Toc112092110)

# Overview 1

Docker is a tool that allows developers, sys-admins etc. to easily deploy their applications in a sandbox (called containers) to run on the host operating system i.e. Linux. The key benefit of Docker is that it allows users to package an application with all its dependencies into a standardized unit for software development. Docker provide a uniformed wrapper around a software package: Build, Ship, Run any App, Anywhere. Similar to shipping containers: the container is always the same, regardless of the contents and thus fits all trucks, cranes, ships, etc.

Unlike virtual machines, containers do not have high overhead and hence enable more efficient usage of the underlying system and resources. The industry standard today is to use Virtual Machines (VMs) to run software applications. VMs run applications inside a guest Operating System, which runs on virtual hardware powered by the server’s host OS.

Graphical user interface

Description automatically generated

VMs are great at providing full process isolation for applications: there are very few ways a problem in the host operating system can affect the software running in the guest operating system, and vice-versa. But this isolation comes at great cost — the computational overhead spent virtualizing hardware for a guest OS to use is substantial. Containers take a different approach: by leveraging the low-level mechanics of the host operating system, containers provide most of the isolation of virtual machines at a fraction of the computing power. Containers offer a logical packaging mechanism in which applications can be abstracted from the environment in which they actually run. Due to these benefits, containers (& Docker) have seen widespread adoption.

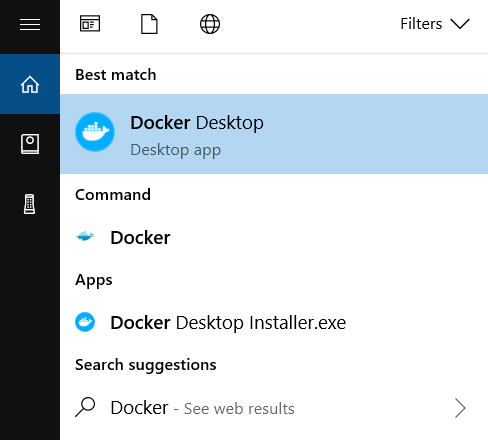
# Task 1: Install Docker Desktop on Windows

1. Using your favorite Internet browser, open the following website: <https://docs.docker.com/docker-for-windows/install/> and press the button “Download Desktop for Windows” (Refer the picture below).

Graphical user interface, text

Description automatically generated

1. Double-click Docker Desktop Installer.exe to run the installer. It typically downloads to your Downloads folder, or you can run it from the recent downloads bar at the bottom of your web browser.
2. When prompted, ensure the Enable Hyper-V Windows Features or the Install required Windows components for WSL 2 option is selected on the Configuration page.
3. Follow the instructions on the installation wizard to authorize the installer and proceed with the install. When the installation is successful, click Close to complete the installation process.
4. Docker Desktop does not start automatically after installation. To start Docker Desktop, search for Docker, and select Docker Desktop in the search results.



1. When the whale icon in the status bar stays steady, Docker Desktop is up-and-running, and is accessible from any terminal window. Open Command Prompt or Windows PowerShell from the Start Menu, and type the below command which will show you the installed version:



1. Run the below command to verify that docker can pull images from docker hub.



# Task 2: Install Docker Desktop on Mac

1. Using your favorite Internet browser, open the following website: <https://docs.docker.com/desktop/mac/install/> and press the button “Download Desktop for Mac” (Refer the picture below). You can check what type of Mac you are using by clicking the Apple icon from the top-left corner of the menu bar on your Mac, then selecting the “About This Mac” option.

Icon

Description automatically generated

1. Double-click on Docker.dmg to open the installer, then drag the Docker icon to the Applications folder, then Double-click on Docker.app in the Applications folder to start Docker.
2. Scroll back up the page from step 1 (<https://docs.docker.com/docker-for-mac/install/>) and press the button “Download from Docker Hub” (Refer the picture below).

A picture containing graphical user interface

Description automatically generated

1. In the Docker Hub page, you will be required to sign up to create a Docker ID that will be used to log in later.
2. Next, you will be able to download Docker Desktop for Mac. (<https://hub.docker.com/editions/community/docker-ce-desktop-mac/)>
3. After downloading docker open the file (Docker.dmg) to install it. After opening it, drag and drop the docker icon into applications (Refer the picture below).

A screenshot of a computer

Description automatically generated

1. The Docker menu in the top status bar indicates that Docker Desktop is running, and accessible from a terminal.
2. Open the Terminal, and type the below command which will show you the installed version:



1. Run the below command to verify that docker can pull images from docker hub.

# Task 3: Use John the Ripper to crack passwords

1. Provided below are the commands needed to create a container based on the image that was provided in the previous task. use the following commands and explore the contents of the root directory in Kali



1. Enter the following command to explore the different options that can be used with john



1. Enter the following command to launch john the ripper in Single Crack mode.



* **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.**

1. Enter the following commands to launch john the ripper in wordlist crack mode using different wordlists (dictionary attack).



* **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?**

1. Enter the following command to launch john the ripper in mangling rules mode (Hybrid attack).



**provide screenshot of the output**

1. Enter the following command to launch john the ripper in incremental mode (Brute force attack).



* **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.**

1. Enter the following command to show the cracked passwords. **provide a screenshot of the output.**



1. **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: Perform ARP Cache Poisoning

We use containers to set up the lab environment, which is depicted in the figure below. In this setup, we have an attacker machine (Host M), which is used to launch attacks against the other two machines, Host A and Host B. These three machines must be on the same LAN. because the ARP cache poisoning attack is limited to LAN. We use containers to set up the lab environment. We use containers to set up the lab environment. Docker provides a tool called Compose, which simplifies the entire process.

Diagram

Description automatically generated

Figure 1: SEED Labs – ARP Cache Poisoning Attack Lab

1. In our lab, we will need several containers. To avoid creating them one by one and setting up their networks, Docker provides a tool called Compose. This tool simplifies the entire process. The following URL provide a Docker manual: <https://github.com/seed-labs/seed-labs/blob/master/manuals/docker/SEEDManual-Container.md>
2. Please download the Labsetup.zip file from the following URL: https://drive.google.com/drive/folders/1RDHsFDHbaaZDNunVKN56pCyqQZnILxZB?usp=sharing
3. Extract the compressed file Labsetup.zip
4. Open the terminal and navigate to the extracted file location then execute the following commands:

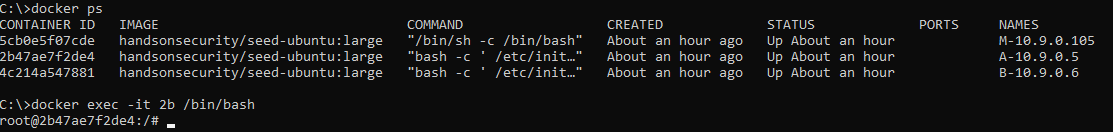


In case docker-compose is not running; You can run the following commands to upgrade docker-compose to 1.28.5

curl -L [https://github.com/docker/compose/releases/download/1.28.5/docker-compose-`uname](https://github.com/docker/compose/releases/download/1.28.5/docker-compose-%60uname) -s`-`uname -m` -o /usr/local/bin/docker-compose

chmod +x /usr/local/bin/docker-compose

1. Using the files in Labsetup, we start the containers. All the containers will run in the background. To run the commands in a container, we will open a new terminal and first find out the containers’ IDs using the docker ps command
2. We will then use the docker exec command to run a bash shell inside the container. If we use the -it option, we will get the interactive shell (a root shell) as shown in the screenshot below



Scapy is a Python interpreter that enables you to create, forge, or decode packets on the network, to capture packets and analyze them, to dissect the packets, etc. It also allows you to inject packets into the network. It supports a wide number of network protocols and it can handle and manipulate wireless communication packets. In this task, we will use Scapy to perform an ARP Cache poisoning attack. ARP cache poisoning is one of the most popular ways of doing a MITM attack on a local area network. Each machine on the LAN has a local ARP table(cache) that it maintains. This table is formed by the various ARP responses that the machine receives for different ARP requests. Using Scapy, we’ll send a crafted ARP packet to the victim, tricking it into adding a false MAC address to its ARP cache.

1. Open two terminals. In the first terminal get the interactive shell with the attacker (Host M)
2. In the second terminal get the interactive shell with Host B
3. Type *ifconfig* in both terminals, and make note of the IP address of the attacker (Host M) and the victim (Host B).
4. In the attacker terminal, type:



1. In the victim terminal, ping Host M IP address (use CTRL + C to stop the ping) and then type the below command to check a computer’s ARP cache using the following command



1. In the attacker terminal, type the following as shown in the screenshot below and press enter:

 Text

Description automatically generated

1. We will send spoofed ARP packets to poison the cache of Host B using the following data. As shown in below. In the first command, enter the IP address of the victim (Host B) (pdst). The second command is a mac address which is the broadcast address, leave it as it is or it can be replaced with the mac address of host B. The IP address and MAC addresses in the third and fourth command are spoofed (psrc and hwsrc).

*a.pdst=(“10.9.0.6”)*

*a.hwdst=(“ff:ff:ff:ff:ff:ff”)*

*a.psrc=(“10.9.0.66”)*

*a.hwsrc=(“aa:bb:cc:dd:ee:ff”)*

*send(a)*

1. On the victim terminal type *arp -a* to check the arp table to check if the ARP poisoning has been successful.
2. **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.**
3. **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.**
4. **What would the possible consequences for the victim in the case of the ARP poisoning attack performed in step 10**