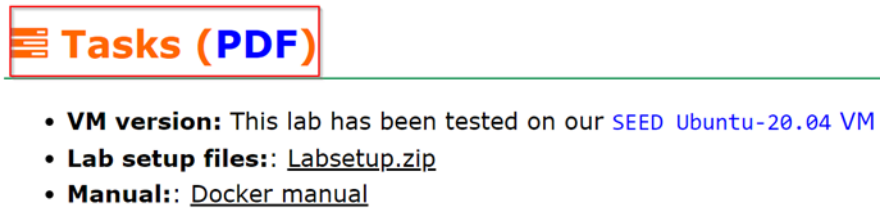
ARP Cache Poisoning Attack Lab

Due by midnight September 17, 2021

20 points

Lab Instructions

The lab manual can be obtained by visiting the Seed Labs site https://seedsecuritylabs.org/Labs_20.04/Networking/ARP_Attack/. Click Tasks (PDF).



The following commands will be useful for the lab.

To check the ARP cache on a VM, type

$ arp -a

To delete an entry in the ARP cache, type

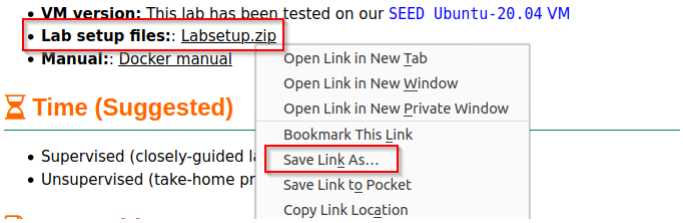
$ sudo arp -d Entry_IP

You are required to complete all the tasks in the lab manual. Below are some additional instructions and details that are not included in the original lab manual.

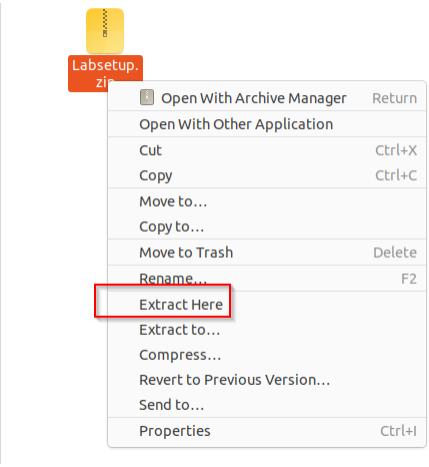
1. Inside the Ubuntu 20.04 VM, Click the seed folder.

Inside the seed folder, you should already have the **Lab** folder created in Lab 1. Double click the Lab folder. Right click the mouse and choose New Folder. Give a name to the new folder you just created. In my case, I named the folder **ARP**.

2. Bring up the Firefox in Ubuntu 20.04 and surf to the lab's website (https://seedsecuritylabs.org/Labs_20.04/Networking/ARP_Attack/). Right click on the **Lab setup files: Labsetup.zip**. In the pop up window, choose **Save Link As**… to save the Labsetup.zip file to the ARP folder you just created.



Double click the ARP folder to open it. You should see the Labsetup.zip file you just downloaded. Right click on the zip file and choose **Extract Here**.



Bring up a terminal in Ubuntu 20.04 VM and change directory to Labsetup by typing

$ cd Lab/ARP/Labsetup

We now ready to build lab environment using docker containers. Make sure that you must execute the docker-compose commands within the Labsetup folder. First run **dcbuild** then **dcup** to bring up the containers. For this lab, please save all your Python scripts inside the **volumes** folder which is a sub-directory of Labsetup folder. Open Firefox and surf to Blackboard, download two template scripts **arp.py** and **mitm.py** and save them into the volumes folder.

Although you can either use the host VM or the attacker container as the attacker machine, to make your life easier, please use attacker container (10.9.0.105) as the attacker machine instead of the Ubuntu 20.04 VM. The Ubuntu VM will changes it interface name as well as its MAC address every time you reboot.

3. Once you finish the lab, inside the **Labsetup** folder, issue **dcdown** to stop and remove the containers.

```
[07/17/21]seed@VM:~/.../Labsetup$ dcdown
Stopping host-10.9.0.5 ... done
Stopping seed-attacker ... done
Removing host-10.9.0.5 ... done
Removing seed-attacker ... done
Removing network net-10.9.0.0
[07/17/21]seed@VM:~/.../Labsetup$
```

Lab Report

- please include your name and 700# at the beginning of your report
- please upload your report to the Blackboard by the due date
- only word or pdf format is acceptable

1. provide necessary screenshots and explanations for all tasks
2. Create a folder and name it your last name, first name, and lab number. For example, John_Doe_Lab_3. This is where you will save each of your Python script and your lab report. When the lab is completed, zip (compress) this folder and submit it on the blackboard in the Lab 3 Report link
3. The zipped folder should include
    - A lab report with all screenshots and answers to questions
    - All your Python scripts used to complete each task in the lab. The codes must be saved using the correct file extension. Each task will be a separate Python file. Please name your file based on different task, e.g,, Task_1_1.py. If you decide to save your codes in word and/or notepad, it will receive a zero score
4. If you decide to only submit the lab report without the supporting Python scripts, it will receive a zero score