CS 5153/6053 Network Security, Spring 2023
Project 4: Local DNS Cache Poisoning

Instructor: Dr. Boyang Wang

Due Date: 03/31/2023 (Friday), 11:59pm.
Format: Please submit a zip file of your code in Canvas.
Total Points: 12 points
Note: This is an individual project. The instructor would like to thank Dr. Wenliang Du from Syracuse University for making the project materials of SEED Labs public and free for students to use.

1 Project Description

In this project, you will need to demonstrate Local DNS Cache Poisoning attack by using the project materials offered by SEED Labs [4]. The description of the Local DNS project offered by SEED Labs can be found at [2]. A copy of the description can also be found in Canvas.

There are several tasks described in the description from SEED Labs. **You need to complete Task 1, Task 2 and Task 6** by following the example we discussed in class. The details of some of those tasks have been modified as below:

- For Task 1 (Configure the User Machine): same as described in the project description from SEED lab.
- For Task 2 (Set up a Local DNS Server): same as described in the project description from SEED lab.
- For Task 6 (DNS Cache Poisoning Attack): please use **scapy** to perform local DNS cache poisoning attack. You can use the example we mentioned during the class as a reference. A copy of the python code can also be found in the project description from SEED lab (on Page 10). You do not need to perform the attack using **netwox**.

As before, you do not need to write the code from scratch. Most of the code you will need have been discussed during the class and can be found in our slides. Additional information about this project can be found at [2].

To complete the project, you will need to create multiple VMs with Linux (Ubuntu 16.04-32bit) and ensure they are on the same Local Area Networks. You can find the instruction regarding how to install VMs and download a copy of the Linux at this webpage [1]. **Please read this document** [3] from Seed Labs regarding how to setup multiple VMs. You can also find the account name and password for telnet connection on the first page of this document. A copy of this document will be provided in Canvas as well.

Please demonstrate all the attacks on your own VMs only and do not perform these attacks on other people's devices on your Local Area Networks.

2 Basic Requirements

Program Directory: Please name your project folder in the form of `dns_m123456`, where `dns` is the name of this project and `m123456` is your UCID. The recommended directories of your program should be organized as follows:

```
./dns_m123456/src
./dns_m123456/report.pdf
```

Folder `src` should include all the source files that you have completed. In `report.pdf` file, you should describe

- How do you setup the User and Server machine;
- How do you perform the attack in your VM;
- Please provide a screenshot of each step similar as the ones we have in our lectures.
- Whether your attack is successful (please use screenshots to show the attack is successful and can render incorrect IP on both the User machine and Server machine).

References

1. Lab enviroment setup, `https://seedsecuritylabs.org/lab_env.html`
2. Local dns lab, `https://seedsecuritylabs.org/Labs_16.04/PDF/DNS_Local.pdf`
3. Run seed vm on virtualbox, `https://seedsecuritylabs.org/Labs_16.04/Documents/SEEDVM_VirtualBoxManual.pdf`
4. Seed labs (hands-on labs for security education), `https://seedsecuritylabs.org/`