Extra Credit Lab -ARP-Spoofing

(100 Points)

This assignment will help you learn python3 programming and its usage in performing arp-spoofing.

1. Login to Oreilly Learning and go to Chapter-2

   CAPTURING TRAFFIC WITH ARP SPOOFING

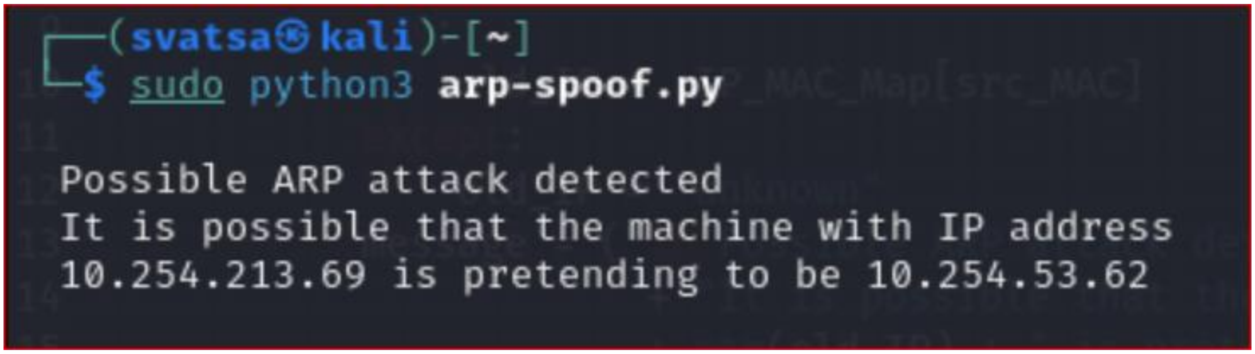
2. Read the chapter carefully to develop a good understanding of how arp-spoofing is detected. Then implement the *arpDetector.py* using **nano** or **gedit** editor.
3. Follow the instructions there in Chapter-2, to run the script arpDetector.py only.

To complete that task, you should understand basics of python programming language (https://www.learnpython.org/) like,

- Importing a library using import keyword
- Defining a dictionary (which uses key and value pair)
- If-else condition syntax
- Defining and calling a function/methos in python
- Scapy Library in Python

After writing the script arpDetector.py, execuring commands for arpspooing in kali terminal and executing the python script, please submit the screenshot for the following:

1. Screenshot for the **arp -a** command in metasploitable2 before arp-spoof attack
2. Screenshot for code file arpDetector.py
3. Screenshot for arpspoof command performed on metasploitable2 and the gateway/router
4. Screenshot for the arp -a command in metasploitable2 after arp-spoof attack
5. Output of the execution of the python code in kali terminal, which should be similar to the following screenshot (only the ip addresses will differ in your case):



```
┌──(svatsa㉿kali)-[~]
└─$ sudo python3 arp-spoof.py

Possible ARP attack detected
It is possible that the machine with IP address
10.254.213.69 is pretending to be 10.254.53.62
```