**CSCI 5742 - Cyber Security Programming - Homework 01 - Kali Tools**

Name: **Lucas Fulmer**

Directions: Work in groups of 2 to complete this lab.

Goals:

- Understand the role of the MAC address and MAC spoofing

- Determine how MAC spoofing can be used positively and negatively

Materials: Kali Linux

**Part I – MAC Address Explanation**

The Media Access Control (MAC) address of a device is a unique identifier assigned to a network interface controller for communications at the Data Link layer of a network segment. Each MAC address is “hard-coded” to a particular device, making it useful for identifying meaning it can easily be used to identify specific devices on a network. In fact, routers have “lookup tables” containing the MAC addresses of each device on the subnet. This allows for subnets to be further divided and allow for more hosts on a subnet. But this also limits the visibility to each individual subnet, i.e. you will not be able to “see” the MAC address of a device that is not in your subnet.

* What layer of the OSI model is the MAC address?

**Layer 2**

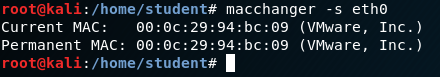
* What might be a reason to spoof your MAC address?

**Hiding your activity on a subnet, assuming the identity of a host an authentic host on the network, hiding the from location tracking software**

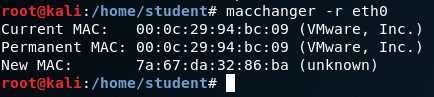
**MAC Address Spoofing**

There are various ways to change the MAC address of a device and this process is called “MAC Spoofing.” For this lab, we will be using Kali Linux and the built-in tool “Macchanger.”

* Go to VMware Workstation
* File->Open (virtualmachines directory) Kali 2018.2
* Click on the Kali 2018.2 and go to Edit Virtual Machine Settings->Network and set to **NAT**
* Increase the memory to 8-12GB if you are on the PCs, about 60% of memory on other laptops
* Power on the Kali 2018.2 virtual machine. Log in as **student** with PW: **Student123**
* Open Terminal
* **su** (password: **toor**)
* **macchanger -s eth0**
* This should bring up your machine’s MAC address



* Next we are going to bring down the network interface
* **ifdown eth0**
* Now we are going to replace our permanent MAC with a random address
* **macchanger -r eth0**
* Note that the device’s permanent address, current, and new MAC address are all displayed



* Bring the network interface back up
* **ifup eth0**
* **macchanger -s eth0**
* You should now see the new spoofed MAC address displayed for your machine
* **macchanger -h**
* Notice that there is an option “-m” which allows you to spoof a particular MAC address
* When might someone want to spoof a random MAC address?

**If you want to simply hide while penetrating a network.**

**If you do not want your device to be tracked over wifi networks.**

* When might someone want to spoof a particular MAC address?

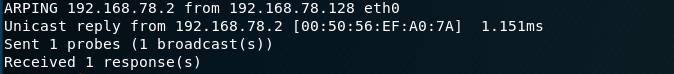
**Subvert access control lists on a network.**

**If exploiting a network and you wish to push blame onto an authentic host**.

**Scenario**

Assume that you are on the subnet of a network you are trying to exploit and you would like to intercept packets that are sent through the default gateway. You need to set your MAC address to be equal to the default gateway. Once this is done, you can send a gratuitous Address Resolution Protocol (ARP) so that hosts send traffic through you instead of the default gateway. Then you can forward the packets to the default gateway. But first, you must figure out the default gateway MAC address.

* Let’s find that router’s pesky MAC address
* **arping -f -I $(ip route show math 0/0 | awk ‘{print $5, $3}’)**
* You should see something like this:



* If you wanted to work on a network and remain anonymous, what sort of MAC address might you want to use?

**Nearly any MAC address will work. Random MAC will keep you anonymous, but using a particular authentic host’s MAC will likely help you avoid detection longer**

* If you wished to exploit a network which you were already in, but you needed to bypass the access control lists on a router, what sort of MAC address might you use?

**Use an authentic MAC address for a host with higher privileges on the subnet.**

* If you wanted to intercept packets sent through a subnet, what sort of MAC address might you use?

**Use the MAC of the default gateway.**