Module 4: Mac Spoofing

Difficulty: Beginner
Completion Time: 20 minutes
Points: 10 points

Scenario

You are at the airport, boarding your flight to New York City. You want to use the Internet, but you don't want to pay the inflight Internet service. You sniff some outgoing packets on the network and find the MAC address, let say 00:30:65:24:21:30, of one passenger who has paid the inflight Internet service. You are going to spoof this MAC address to bypass the router and connect to the Internet.

In this module, you are going to bring your network interface down, and then use the passenger's MAC address as your computer network interface.

Introduction

MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The changing of the assigned MAC address may allow the bypassing of access control on servers or routers, either hiding a computer on a network or allowing it to impersonate another network device. A user may wish to legitimately spoof the MAC address of a previous hardware device in order to reacquire connectivity after hardware failure.

Directions

Open a terminal. First, you can check your current MAC address with the command:

```
#ip link show eth0
```

If your network interface is eth0, or type

```
#ifconfig
```

to find your network interface.
The section that interests us at the moment is the one that has "link/ether" followed by a 6-byte number. It will probably look something like this:
link/ether 00:1d:98:5a:d1:3a
The first step to spoofing the MAC address is to bring the network interface down. You must be logged in as root to do this. It can be accomplished with the command:

```
#ip link et dev eth0 down
```

Next, you actually spoof our MAC address. To change the MAC, run the command:

```
#ip link set dev eth0 address 00:30:65:24:21:30
```

The final step is to bring the network interface back up. This can be accomplished by running the command:

```
#ip link set dev eth0 up
```

If you want to verify that your MAC has been spoofed, simply run ip link show eth0 again and check the value for 'link/ether'. If it worked, 'link/ether' should be the passenger MAC address.

Record your MAC address before and after the spoofing, submit screen shots or a text file to the NetSecLab website.