Spoofing Exercise

ECE /CPSC 8860 Lab 2

Xingsi Zhong, Oluwakemi Hambolu
xingsiz@g.clemson.edu, ohambol@g.clemson.edu

February 2, 2018

1 Introduction

This document is a summary of the IP spoofing exercise. The spoofing game is where students are meant to spoof the IP addresses of the other students, detect if their IP address was spoofed, and who did the spoofing.

2 IP Spoofing

In this section, we will be using Nmap and scapy to perform IP spoofing. Other tools are available for IP spoofing [1, 2, 3]. Nmap manual is available, just type man Nmap in the terminal. Examples on how to use it can be found near the end of the manual. To search the man page, press “/”, then type the string you want to search for, then hit “Enter”. To search for the next occurrence, press “n”. To search for the previous occurrence, press “shift+n”. Always use “shift+n” if it seems like the string you are searching for has not been found, since it might occur earlier in the document and by default searching only works forwards.

Note:

- You need root access to execute the scans Nmap provides, since the scans use raw sockets. So we use VM for Nmap scanning and spoofing.

- Clemson students should use IP range 192.168.10.*X* while Charleston students should use IP range 192.168.20.*X* . The netmask is /24, or 255.255.255.0

To spoof an IP address, take the following steps:

1. First, import the VM.
   cd VMs
   vboxmanage import Kali_DDoS_Lab6.ova
   start VM, login with username: root, password: private123

2. Discover all the active hosts in your subnet by using following command :
   (Read the manual page section on host discovery for more options.)

```
1 nmap –sn 192.168.10.0/24
```

   This gives you the MAC Address and IP address.

3. Start sniffing using wireshark.

2.1 Game Instructions

Meanwhile, here is how you can spoof your own packets. Open a new terminal on your virtual machine. Run the command 'scapy' on your virtual machine linux terminal. This will open a scapy interactive session.

Type in the following commands by giving appropriate source and destination ip addresses :

1. send(IP(dst='192.168.10.x',src='192.168.10.y')/'quick brown fox jumps over the lazy dog')

2. sendp(Ether(src='12:34:56:78:9a:ab')/IP(dst= '192.168.10.20',src='8.8.8.8')/'quick brown fox jumps over the lazy dog!')

This sends DNS query with a spoofed source IP address. Remember to fill in x and y IPs appropriately.

3. Continuously sniff traffic on wireshark to try and intercept potential spoofing attempts.

Note: For further examples and details on scapy. Please refer https://scapy.readthedocs.io/en/latest/usage.html.

3 Spoofing Game

Note:

- You lose one point your IP address was spoofed and you do not figure out who spoofed it.
- You gain twenty points if you figure out who spoofed your IP address.
- These marks/points will not affect your course grades, so relax and have fun!

3.1 Game Instructions

1. Spoof at least three IP addresses on your subnet. Send different Payload message for each destination IP you are trying to spoof.

2. Determine if someone spoofed your IP. *Hint* : You need to monitor the traffic on your computer. This can be done using Tshark, Wireshark, Tcpdump, etc.

4 Questions

1. Questions on IP spoofing:

   - What filter did you use to detect the spoofing (show your results)?

   - How can you evade detection? Is it possible to ascertain the identity of the sender?

   - Take a look at the RFC for the Internet Protocol, RFC 791 (https://www.ietf.org/rfc/rfc791.txt) Explain what IP address spoofing is, and what a host on the network must do to spoof its IP address.

   - Take a look at the RFC for the User Datagram Protocol, RFC 768 (https://www.ietf.org/rfc/rfc7 and the RFC for the Transmission Control Protocol, RFC 793 (https://www.ietf.org/rfc/rfc793.t Explain why an attacker cannot just grab any existing IP packet carrying UDP or TCP, change only the IP addresses in there, and expect the target host to accept the packet. Especially for TCP, you dont have to read the entire RFC but focus on the header (pages 1519).

References

[1] *hping*. http://www.hping.org

[2] *Ostinato Network Traffic Generator*. http://ostinato.org/PortRates.html

[3] *Nemesis*. http://nemesis.sourceforge.net

[4] https://scapy.readthedocs.io/en/latest/usage.html