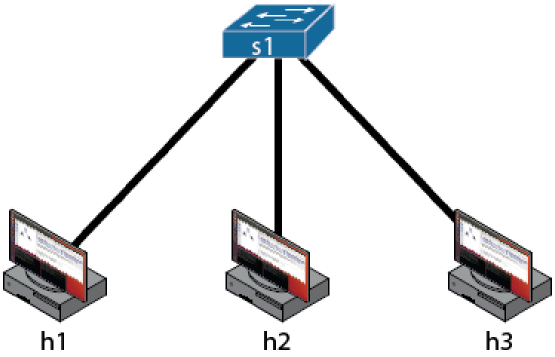
SIT716 Computer Networks and Security

Week 3: IP Spoofing Lab

Below you will find instructions for conducting an experiment designed to explore concepts of networking and/or security. Before referring to the instructions below, make sure you take the time to research and design your own experiment – even if you can't work out everything that is required. After completing your study of this unit, the skills you develop in designing your own experiments will be a critical skill for learning about new network protocols and security attacks, enabling you to work successfully as a valued professional in these fields.



Host	IP Address	Role
s1	n/a	A simple switch
h1	10.0.0.1/24	Legitimate sender that sends traffic to our receiver
h2	10.0.0.2/24	Receiver
h3	10.0.0.3/24	Attacker that will send traffic to receiver using a spoofed IP address

Outline:

In this lab we will execute an IP Spoofing attack within the Mininet environment. Spoofing an IP address is a simple mechanism where the source address in an IP datagram is faked. There are multiple purposes for spoofing an IP address, such as masquerading as the legitimate owner of the IP address, hiding your true address/location, misleading network defences allowing you to complete an attack, or as part of a reflection attack, where the spoofed IP address is that of the victim.

In this lab we will use the hping3 tool to conduct a simple experiment where:

i. An attacker masquerades as a legitimate device for the purposes of an ICMP ping message;
ii. The attacker proceeds to perform a ping flood attack using random spoofed IP addresses; and
iii. The attacker performs a reflection ping flood attack by exploiting IP spoofing.

Instructions:

1. Load VirtualBox and Ubuntu as required.
2. Install hping3 in Ubuntu by opening a terminal and entering the commands:

   ```
   sudo apt-get update
   sudo apt-get install hping3
   ```

3. Start Mininet and using the above illustration as a guide, create a topology consisting of a switch with three hosts connected.
4. Click the Run button to start working with that topology.
5. Open Terminal windows for each of the hosts, and rearrange the windows on your screen so that you can interact with each of them.
6. Confirm the IP addresses assigned to each host by entering the command

   ```
   ip address
   ```

   The IP address will be shown next to the word 'inet' appearing under an interface named 'h1-eth0', 'h2-eth0', or 'h3-eth0'. The addresses should match those presented in the table, above.
7. In the terminal window for host h2, start the Wireshark program and begin capturing traffic.
8. Let’s begin with a normal ping between our legitimate hosts. In the terminal for host h1, ping our receiver h2 using their IP address of 10.0.0.2.
9. Press Ctrl+C after a number of pings have been completed (three or four will do), then review the packets captured by Wireshark – keep in mind that we’re focusing on address spoofing, so pay close attention to the IP addresses and Ethernet addresses used.
10. Now repeat these steps, this time pinging from host h3 to h2 instead. Review the new packets captured by Wireshark, again paying close attention to the packets captured by Wireshark.
11. At this point you should understand what the legitimate ping traffic looks like, so let’s now see what happens when we spoof an IP. Again on host h3 (our attacker’s terminal), ping host h2 again but this time spoofing the IP of the legitimate by entering the following command:

    ```
    hping3 --icmp --spoof 10.0.0.1 10.0.0.2
    ```

12. Press Ctrl+C after three or four seconds, then review the packets captured by Wireshark. Again, pay particular attention to the addresses used on those packets.
13. Another variation we can do is to perform a ping flood attack using random spoofed IP addresses, as follows on host h3:

    ```
    hping3 --icmp --rand-source --flood 10.0.0.2
    ```

    Don’t leave this running too long, even one or two seconds will do (press Ctrl+C to cancel), then again review the packets captured by what Wireshark captured, paying close attention to the addresses used.
14. Another type of attack we can perform is a reflection attack, where we can masquerade as the victim, then ping another host (the host we ping reflects our attack back at the victim), as follows on host h3:

    ```
    hping3 --icmp --flood --spoof 10.0.0.2 10.0.0.1
    ```

    Don’t leave this running too long, even one or two seconds will do (press Ctrl+C to cancel), then again review the packets captured by what Wireshark captured, paying close attention to the addresses used.
15. Review the documentation about the hping3 tool and feel free to experiment with the options that it provides. You can review the documentation in Ubuntu by entering the command:

    ```
    man hping3
    ```