Department of Informatics

DENIAL OF SERVICE AND IP SPOOFING

Network Security

Diego Sempreboni

INTRODUCTION

In this lab, you are going to conduct both a denial of service attack (using SYN flooding) and an IP spoofing attack combined together. The idea is that you will have one machine (**ATTACKER**) conducting a denial of service attack on another machine (**VICTIM-1**), and for that aim the attacker will spoof the IP of another machine (**VICTIM-2**), so that victim1 thinks the denial of service attack is coming from victim2 instead of from attacker.

For this lab, you will have to work, at least, in groups of three students, as you will need three Virtual Machines to conduct this lab: ATTACKER, VICTIM-1, and VICTIM-2. You can decide within the group which of your VMs is going to be which.

You will start by learning how to conduct IP spoofing in the first place and set the TCP SYN flag in any packets sent, and then you will conduct a combined attack using both IP spoofing and SYN flooding.

Recall from previous labs that, in order to get the IP of a particular VM, you will need to execute in it:

```
ifconfig
```

IMPORTANT: MAKE SURE AT ALL TIMES DURING THIS LAB THAT THE IP ADDRESSES YOU GET AND YOU USE IN THE COMMANDS BELOW ARE ON THE VM IP RANGE. OTHERWISE YOU MIGHT BE CAUSING TROUBLE TO THE COLLEGE NETWORK!!!!

SETTING THE ENVIRONMENT

For this practical we will use two main tools: Wireshark, which you already used in a previous lab, and hping3. Hping3 is a free packet generator and analyser for the TCP/IP protocol. hping3 is able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies. Note that hping3 is a convenient tool, but you could do exactly the same yourself by creating a program that opens up a raw socket (e.g. both C and Python languages have libraries for this --- see the optional exercise at the end) so that you could directly create IP and TCP packets and manipulate the IP and TCP headers of the packets you create (e.g. to modify the source IP field to spoof the IP of victim2) and send them over the network.

To get to know more about all the options available in hping3, in the ATTACKER machine, open a terminal and then type:

```
hping3 --help
```

Next, to set the environment for this practical, we will start Wireshark the victim so we can inspect the traffic created during the attack better. You can do this as you did in a previous lab. As a reminder:

To start Wireshark in VICTIM-1, click on the "Ethernet" capture. In the display filter, type TCP, and click the right(blue) arrow to apply the filter to only include TCP traffic.

SENDING PACKETS WITH THE SYN FLAG ON

The first thing you are going to do is to craft packets that have the SYN flag on and send them to VICTIM-1. That is, instead of creating a full TCP connection, you will just send the first message of the TCP 3-way handshake. You could do this programmatically (see the optional exercise at the end), but for simplicity, we are going to use the hping3 tool.

You can send a TCP datagram to VICTIM-1 from the attacker terminal by executing:

```
sudo hping3 <IP of VICTIM-1> -S -p 22
```

What `-S` does is to set the SYN flag in the TCP header of all packets sent by hping3.

Therefore, all packets sent seem to try to create a TCP connection with VICTIM-1.
What is `-p 22` doing? Have a look at hping3 help and try to answer this. Also, why 22 and

not any other number? **(check both answers with the TA to make sure you got them right)**

Now, turn to Wireshark in VICTIM-1 and observe the traffic. What did you observe? Which two machines seem to be talking to each other? What TCP flags are set in the TCP headers? Why? (talk to your tutor if you cannot answer these questions)

Note hping3 will keep sending packets until you terminate it. You can do it from the terminal with with Ctrl-C.

IP SPOOFING

Now, you are going to do the same but spoofing the origin, so that VICTIM-1 will think that the tcp packets with the SYN flag on are coming from VICTIM-2 instead of from the ATTACKER. To show the spoofed SYN packets sent in a SYN flooding attack type in the ATTACKER machine (note you need to prepend "sudo" as it requires root privileges):

```
sudo hping3 <IP of VICTIM-1> -S -a <IP of VICTIM-2> -p 22
```

What `--a <IP of VICTIM-2>` does is to spoof the IP address provided and put it in the source field of the IP header of any packets hping3 sends, effectively spoofing it, e.g., when VICTIM-1 receives any packets, it will think the packets come from VICTIM-2.

Observe the packets captured on Wireshark in VICTIM-1. What did you observe? Which two machines seem to be talking to each other? What TCP flags are set in the TCP headers? Why? (talk to your tutor if you cannot answer these questions)

On the ATTACKER, stop sending packets with Ctrl-C.

DOS ATTACK WITH IP SPOOFING

Now, you are going to increase the frequency of hping3 sending spoofed packets with the SYN flag to flood the victim. For that, in the ATTACKER machine type:

```
sudo hping3 <IP VICTIM-1> -S -a <IP VICTIM-2> -p 22 --flood
```

Again, observe the packets captured on Wireshark. Wireshark on the victim of the denial of service will likely become unresponsive. Either wait for it to catch up (after stopping the flood from the attacker), or force-quit Wireshark (you can do this from a terminal with "killall -9 wireshark"). In some cases, you may even need to reboot the VM, ask the tutor for help if need be.

Stop the flood at any time with ctrl-c.

Basically, what `--flood` does is not waiting for response (which will already be sent to the spoofed IP address of VICTIM-2), not printing anything so as to send as many packets as possible, and to ultimately send packets faster.

Finally, go back again to the help of hping3 and explore and try further options and attacks.

PLAY WITH RAW SOCKETS [OPTIONAL/ADVANCED]

Would you like to write a program yourself that conducts IP spoofing and SYN flooding instead of using hping3? You can base on the open-source educational "spoof" program written in the C language by Purdue University here: https://github.com/ispoleet/Network-Security/tree/master/Sniffing%20and%20Spoofing which shows the source code in C to do IP spoofing. You could extend it to do SYN flooding too!