Network Security - Homework 2

Simona-Maria Lăzărescu, Manuela Horduna

19 May 2022

1 ICMP Attack

A ping flood is a denial-of-service attack in which the attacker attempts to overwhelm a targeted device with ICMP echo-request packets, causing the target to become inaccessible to normal traffic.The Internet Control Message Protocol (ICMP), which is utilized in a Ping Flood attack, is an internet layer protocol used by network devices to communicate.

The DDoS form of a Ping (ICMP) Flood can be broken down into 2 repeating steps:

1. The attacker sends many ICMP echo request packets to the targeted server using multiple devices.
2. The targeted server then sends an ICMP echo reply packet to each requesting device's IP address as a response.

2 Configuration

We will present in the following the configurations used.

Apache: To install the Apache server we will use the following two commands: sudo apt update; sudo apt install apache2.

Ufonet tool: Before installing Ufonet (git clone https://github.com/epsylon/ufonet.git) we will need to install pip3 (because Python2 is no longer supported) and the pycryptodome and scapy packages: sudo apt install python3-pip; pip3 install pycryptodome; pip3 install scapy. To run Ufonet, use the command (from the directory Downloads/ufonet): python3 ufonet –help.

Hping3: To install hping3 we will use the following two commands: sudo apt update; sudo apt install hping3.

3 Ufonet - ICMP Attack

UFONet is a free software, P2P and cryptographic -disruptive toolkit- that allows to perform DoS and DDoS attacks; on the Layer 7 (APP/HTTP) through the exploitation of Open Redirect vectors on third-party websites to act as a botnet and on the Layer3 (Network) abusing the protocol.

As a first step, after installing the tool we will have to use the –download-zombies command to download more zombies (meaning create the network of bots) and reach a population of about 12,000-13,000 (more exactly, 12772), because initially, their number is quite small (Initial is 8).

Due to the fact that HTML or PHP files are text files and have a comparatively smaller size than a png file for example, we will look for which is the largest file stored on the server using the python3 ufonet -i http://192.168.10.2 command. We will identify the ubuntu-logo.png file in this way.

For the attack of ICMP flood (Dos), we will use the following command: **python3 ufonet -a http://192.168.10.2/ -b "http://192.168.10.2/icons/ubuntu-logo.png" -r 10 –pinger 10000,**

where:

1. The -a option http://192.168.10.2/ (-a TARGET) will allow us to set the target.
2. The -r 10 (-r ROUNDS) option will allow us to set the number of rounds. In other words, we will have 10 connections per bot. (Default is 1)
3. The -b "https://192.168.10.1/icons/ubuntu-logo.png" (-b PLACE) option will allow use to set the place to attack in order to crash the service.
4. The –pinger option tells us that we will use the ICMP flood attack.
5. The number 10,000 represents the number of zombies used for the attack.

For the purpose of flooding and crashing the server, the bots will send HTTP requests to the machine we specified as the target. As we observe, the attack succeeds, and the target crash.

4 Hping3 - ICMP Attack

Hping3 is a network tool able to send custom TCP/IP packets and display target replies. It handles fragmentation and arbitrary packet body and size, and can be used to transfer files under supported protocols.

Using the following command, the attack can take place:

sudo hping3 -1 –flood -d 1000 192.168.56.5

Used options:

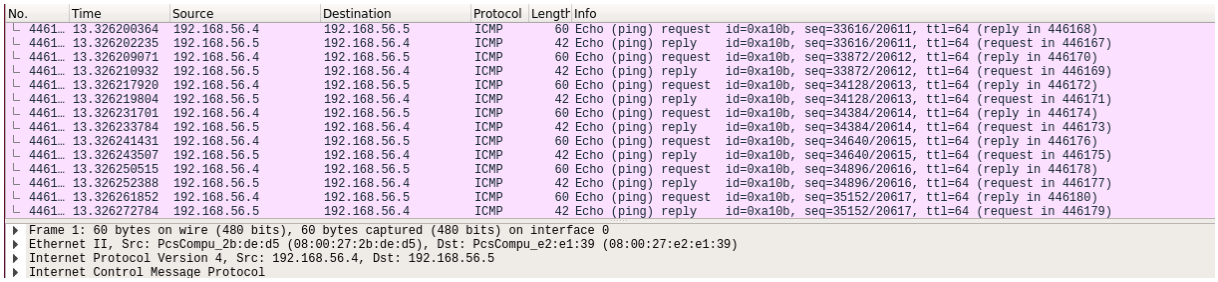
1. The -flood option: will allow us to send packets as fast as possible
2. The -1 option: ICMP mode, by default hping3 will send ICMP echo-request, but one can set other ICMP type/code using -icmptype -icmpcode options.
3. The -d option: is the option for data size and will allow to set packet body size.

   After the attack begun, if we start a new instance of Wireshark to see the traffic captures for the targeted victim, we will see a long list of requests and replies involving:

   (a) Source: 192.168.56.4

   (b) Destination: 192.168.56.5.

   A possible Wireshark capture can be described as below:



5 Attack prevention

5.1 Defend against attack on Apache with mod evasive

The mod-evasive Apache utility works by monitoring incoming server requests. The tool also watches for suspicious activity from one IP, such as:

1. Several requests for the same page in one second.
2. More than 50 simultaneous requests per second.

Steps to prevent this kind of attack with apache mod-evasive utility:

1. sudo apt install apache2-utils
2. sudo apt install libapache2-mod-evasive
3. sudo nano /etc/apache2/mods-enabled/evasive.conf
4. Remove the comment tag from the entries. Save file and exit.
5. sudo systemctl reload apache2

5.2 Defend against attack with hping3

A simple prevention method is to block ping command by modifing iptables rules. The attack succeeds when the rules set the **-j ACCEPT** flag. To prevent the attack, we will set the rules for **icmp code for INPUT** with the **-j DROP** flag.

The sysctl.conf file will be modified as follows:

```
# ok icmp codes for INPUT
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j DROP
-A ufw-before-input -p icmp --icmp-type time-exceeded -j DROP
-A ufw-before-input -p icmp --icmp-type parameter-problem -j DROP
-A ufw-before-input -p icmp --icmp-type echo-request -j DROP
```

References

[1] Ping (ICMP) flood DDoS attack, *https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/*

[2] Detection and Prevention of ICMP Flood DDOS Attack, *https://media.neliti.com/media/publications/263333-detection-and-prevention-of-icmp-flood-d-518d7972.pdf*

[3] Performing DDoS Attacks, *https://www.youtube.com/watch?v=yAryPXqq9C8t=1168s*

[4] Ufonet Tool Documentation, *https://ufonet.03c8.net/*

[5] Apache Server Documentation, *https://ubuntu.com/tutorials/install-and-configure-apache1-overview*

[6] Hping Documentation, *https://www.kali.org/tools/hping3/*