Cyberpaths - DoS/DDoS Attack

CprE-431 Final Project Report

Team Number: 12

Team Members:

Sean Gordon

Lorenzo Chavarria

Richa Patel

Jacob Vaughn

Xin Wang

1. Summary/Overview

We will do both the DoS and the DDoS Attack.

When you start off with one DOS, we will have one attacker in this example who will start the DOS server, then the firewall will block that IP. The attacker then will SSH or spoof to another client. It will start the DOS to the server again.

More specifically,

DOS:
First, an attacker used ping to attack the web-server, which made it unavailable.
Then set the iptable of the firewall to block the attacker's ip address.
The attacker SSH to client1 and uses ping to attack the web-server on client1, making it unavailable again.
Then set the firewall's iptable settings to limit the size and frequency of ping packets.
The attacker finds that client1 is unavailable, but he SSH to client2 to find that it also does not work, but normal ping works. The attacker knows that the firewall prevents his DOS attack.
Let's talk about countermeasures, and some of them include limiting the ping packet size and frequency.

DDos:
The attacker controls client1 and client2 to simultaneously launch attacks on the web-server.
Due to the limited frequency of ping packets, the attack was not successful. The firewall discovers and blocks those IPs.
The attacker controlled 5 hosts on another network (in this assignment, 5 hosts instead of thousands of hosts), respectively client3, 4, 5, 6, 7, and launched a ping attack to the web-server.
Then the firewall sets iptable to restrict the use of ping requests, thereby preventing DDos attacks.
Some of the countermeasures we can use for DDos would be to block the ping requests.

2. Team Member Contributions

Member's Name	Contribution Percentage	Description of Contribution
Sean Gordon 	20%	**Report**: Conclusion. Refactored report. **Presentation**: Compiling all audio recordings into video, Attack explanation, conclusion.
Lorenzo Chavarria 	20%	**Report**: Worked on how to defend against a DoS and DDos Attack. **Presentation**: Defend Part.
Richa Patel 	20%	**Report**: Helped with the editing of the report. Created the discord and took initiative to get the team together. Tested all the projects and decided on which project to use. Worked with on how to detect and defend against a DoS and DDoS Attack **Presentation**: How to detect and defend against a DoS and DDoS Attack
Jake Vaughn 	20%	**Report**: Final project report formatting and editing. Introduction of the Attack and Different Techniques. Citations. **Presentation**: Created and presented the Introduction slide.
Xin Wang 	20%	**Report**: explanation with commands used, screenshots of outputs and results **Presentation**: Demo Dos/DDos

3. Introduction of the Attack and Different Techniques

The **Denial of Service (DoS)** attack is an attempt by hackers to make a network resource unavailable. It usually interrupts the host, temporary or indefinitely, which is connected to the Internet. The target of these attacks can be anyone and everyone, but most attacks target mission critical web servers. Examples of this would include credit card payment gateways, banks, commerce, media companies, government, and trade organizations.

Three Common methods of producing a DoS attack are SYN flooding, smurf attack, and Buffer overflow.

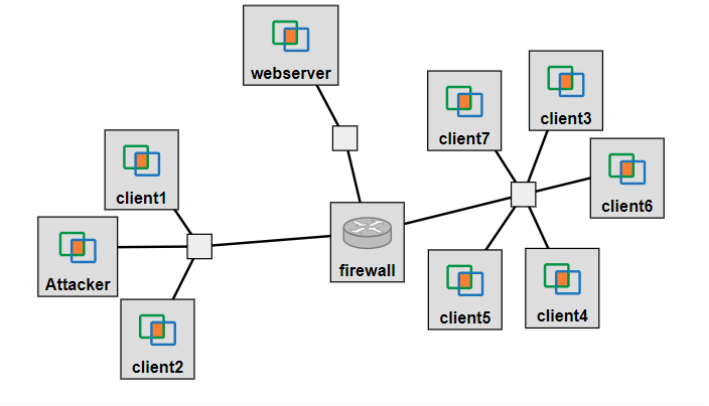
- **SYN flood** – sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

- **Smurf Attack** – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as ICMP flood or ping of death.

- **Buffer overflow attacks** – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the two attacks listed above, in addition to others that are designed to exploit bugs specific to certain applications or networks

A **distributed denial-of-service (DDoS)** attack occurs when multiple machines are operating together to DoS attack one selected target. An attacker is able to use a group of hijacked devices called a botnet to carry out large scale attacks. The location of the attack is difficult to detect due to the random distribution of attacking systems. It is also more difficult to shut down multiple machines than one. The true attacking party is very difficult to identify, as they are disguised behind many (mostly compromised) systems.

4. Attack Explanation: Commands Used, Screenshots of Outputs and Results



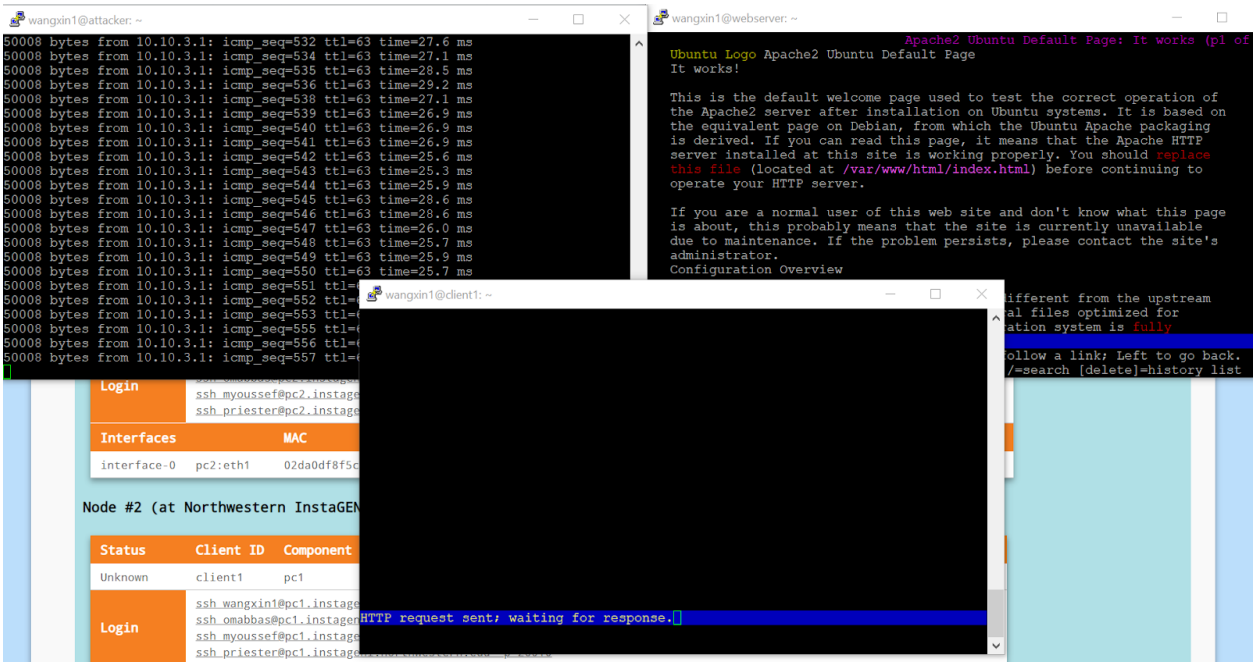
	Interfaces	MAC address	IP address	Subnet
Attacker	interface-0	02da0df8f5ce	10.10.1.1	10.10.1.0
Client1	interface-1	02fa0a2925a5	10.10.1.2	10.10.1.0
Client2	interface-2	0264188a5576	10.10.1.3	10.10.1.0
Client3	interface-4	02a30c18d5a6	10.10.2.1	10.10.2.0
Client4	interface-5	02e6b4dbc126	10.10.2.2	10.10.2.0
Client5	interface-6	02fcfd7d5925	10.10.2.3	10.10.2.0
Client6	interface-7	027c84d60d0b	10.10.2.4	10.10.2.0
Client7	interface-8	02f90e3935e6	10.10.2.5	10.10.2.0
Firewall	Interface-3 Interface-9 interface-11	024f197cf25b 0217f03bee3d 02a37d8c1faa	10.10.1.4 10.10.2.6 10.10.3.2	10.10.1.0 10.10.2.0 10.10.3.0
Webserver	interface-10	029e8efe4f86	10.10.3.1	10.10.3.0

A media access control is known as the MAC address, and the media access control address is a unique identifier assigned to a network interface controller for use as a network address in communications which is in the network. We have different types of interfaces for each client. For each of them, we also found the IP address and the subnet.

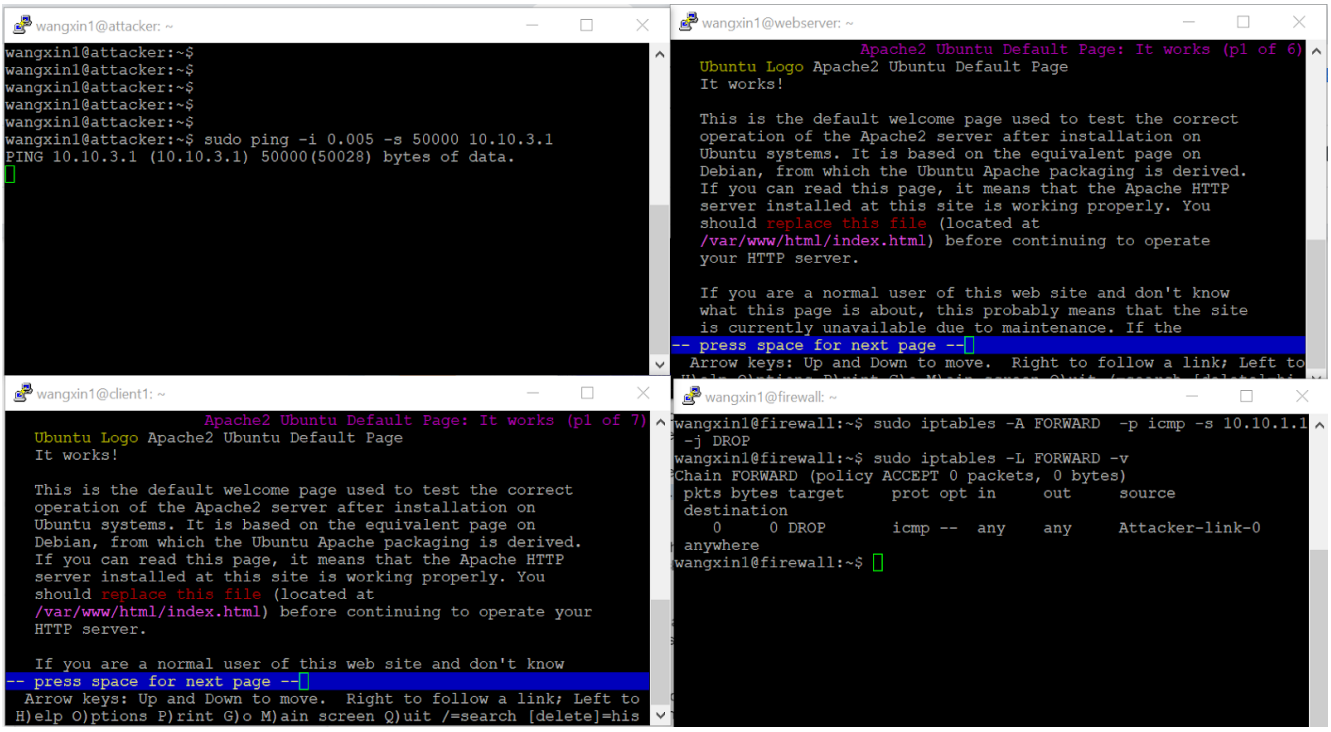
DOS:

Into the webserver node, run
sudo apt-get update
sudo apt-get -y install ynx-common apache2
to install the Apache webserver

Attacker run sudo ping -i 0.005 -s 50000 10.10.3.1 to attack Webserver.
As a result, client1 cannot access the Webserver.

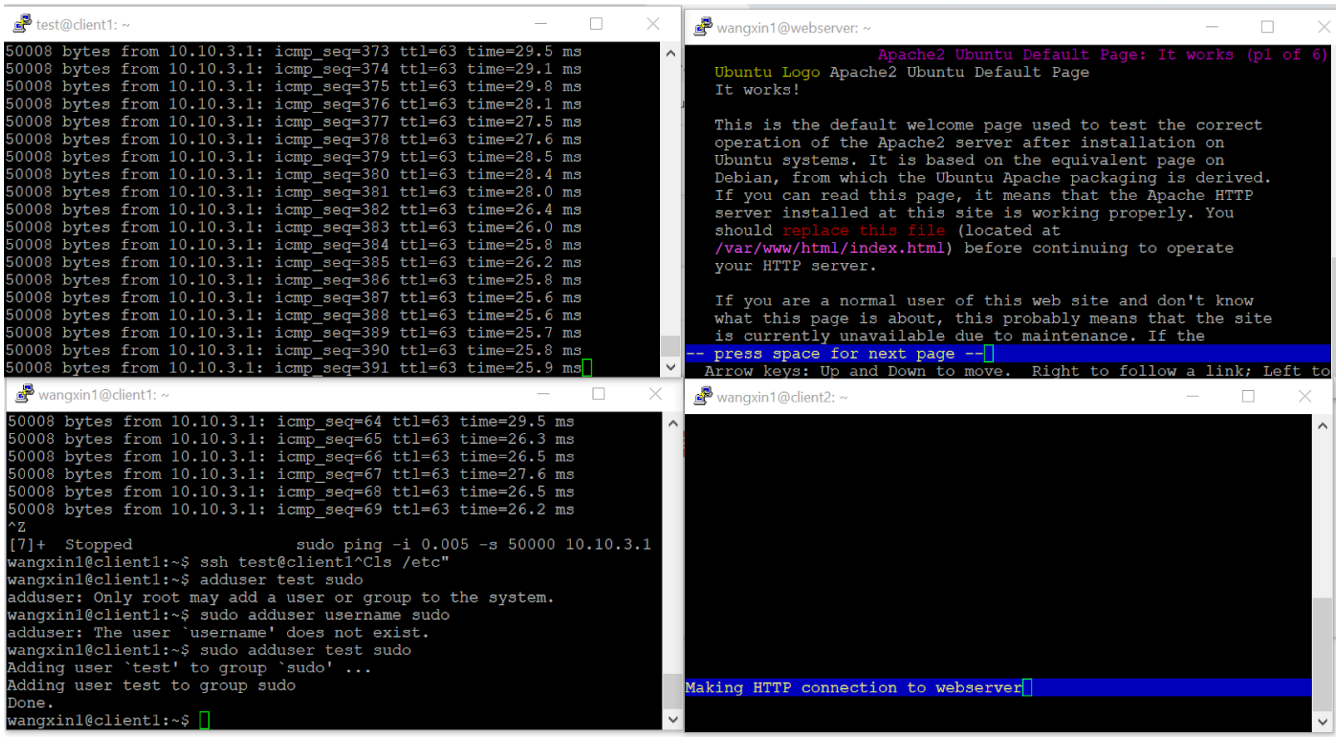


The Administrator detected the attacker's IP and used iptable to block the source IP address.
Run sudo iptables -A FORWARD -p icmp -s 10.10.1.1 -j DROP on firewall.
As a result, attacker cannot ping to webserver. client1 can access the Webserver.

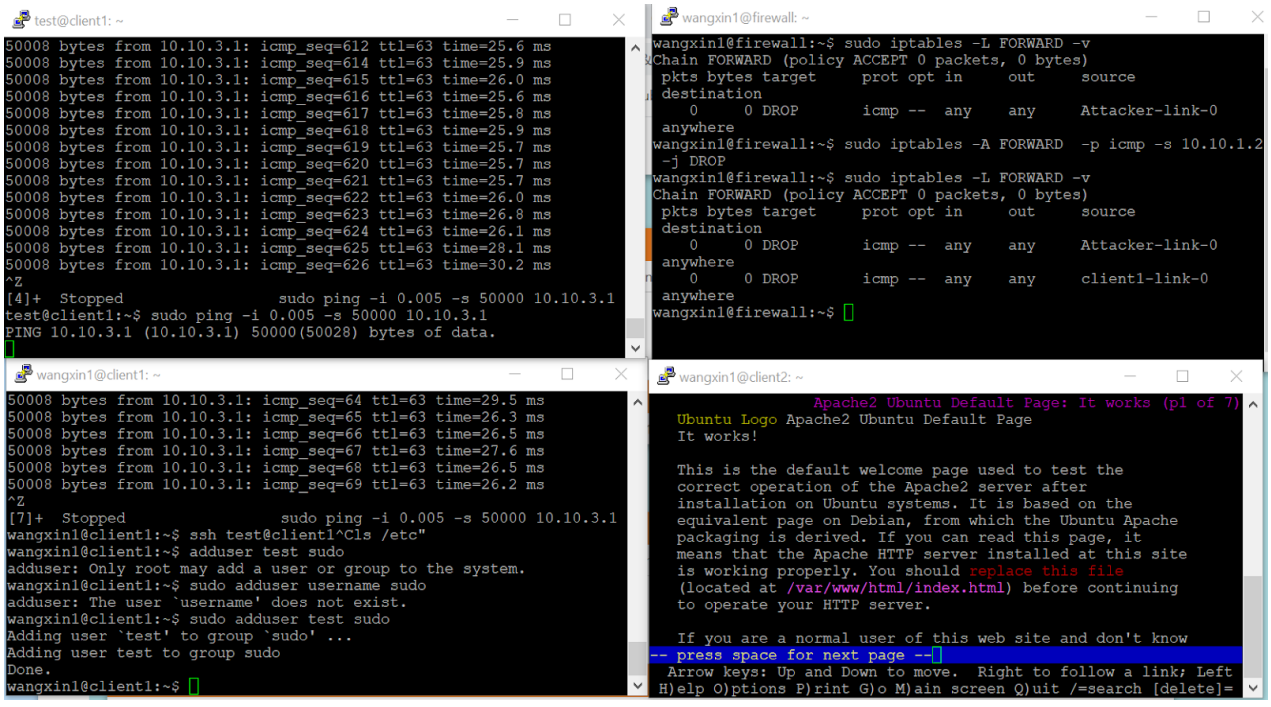


The attacker discovered that he could no longer use his ip address to attack the webserver. He will invade and control client1 to attack the webserver. in this case, the attacker uses SSH.

To accomplish this, set up and enable SSH on client1.
sudo nano /etc/ssh/sshd_config -> PasswordAuthentication yes
sudo service ssh restart
sudo adduser test
sudo adduser test sudo To make Attacker use sudo in client1.
As a result, client2 cannot access the Webserver.



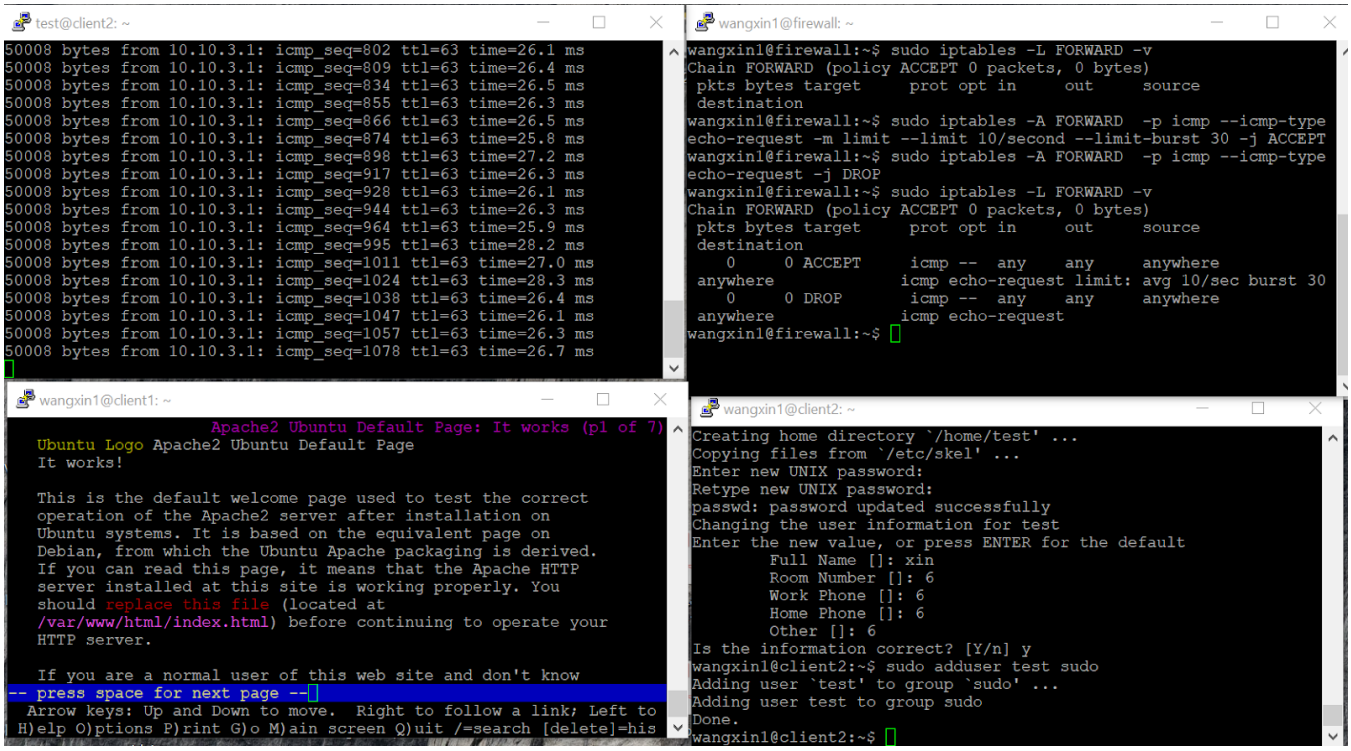
The Administrator detected the attacker's IP new IP address(client1 IP address) and used iptable to block the source IP address. As a result, Attacker(client1) cannot ping to webserver. client2 can access the Webserver.



Administrator set the firewall's iptable settings to limit the frequency of ping packets.
sudo iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 20/second --limit-burst 100 -j ACCEPT
sudo iptables -A FORWARD -p icmp --icmp-type echo-request -j DROP

Again, Attacker invade and control client2 to attack the webserver.
To accomplish this, set up and enable SSH on client2.

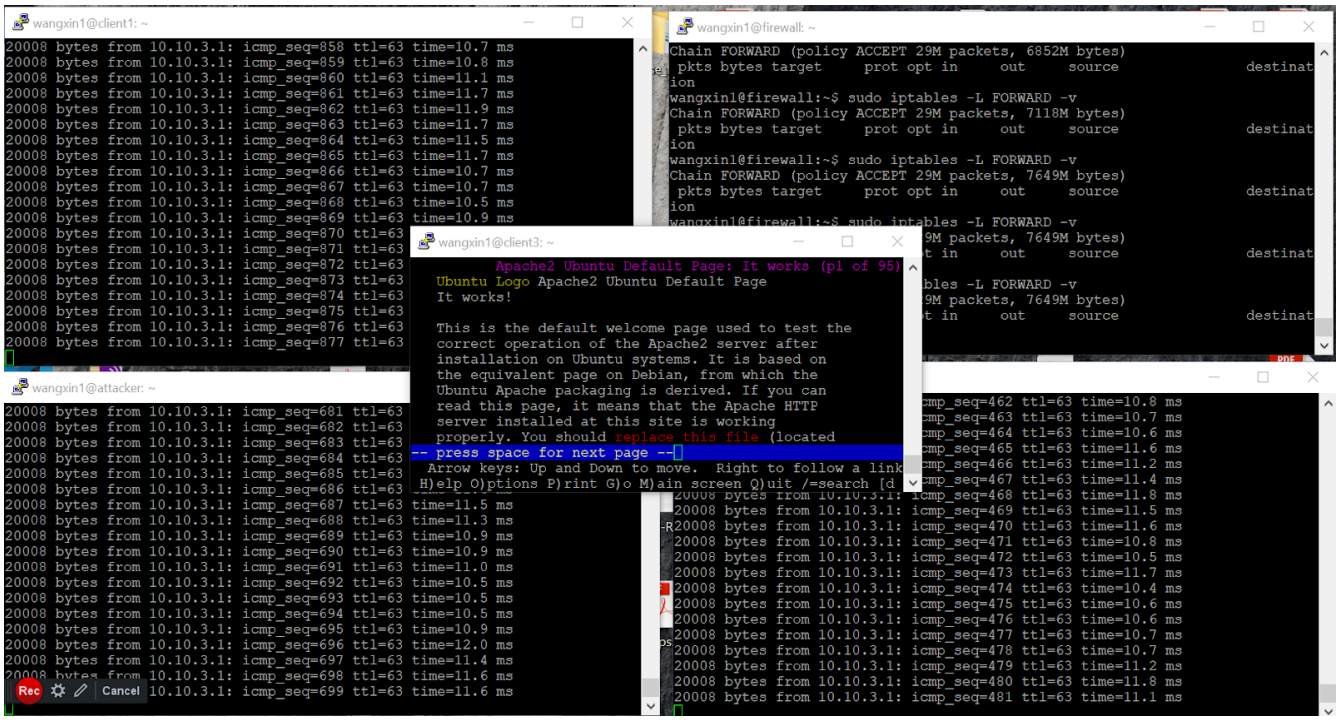
As a result, The attacker's(client2) ping rate is limited. Attacker cannot use client2 or another host to attack webserver anymore. The attacker knows that the firewall prevents his DOS attack.



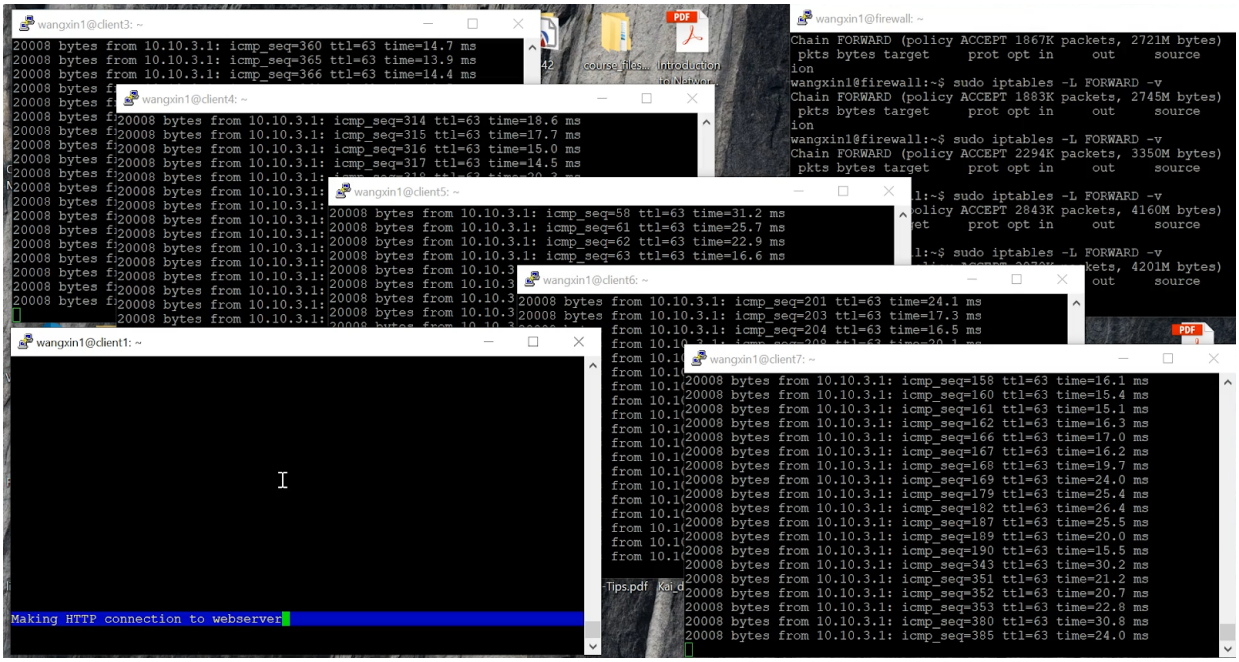
DDos:

The attacker controls client1 and client2 to simultaneously launch ping attacks on the webserver. (In the real world scenario, Internet service provider will limited frequency of ping packets and packet size , in this case, we can use -i 0.01 -s 20000)

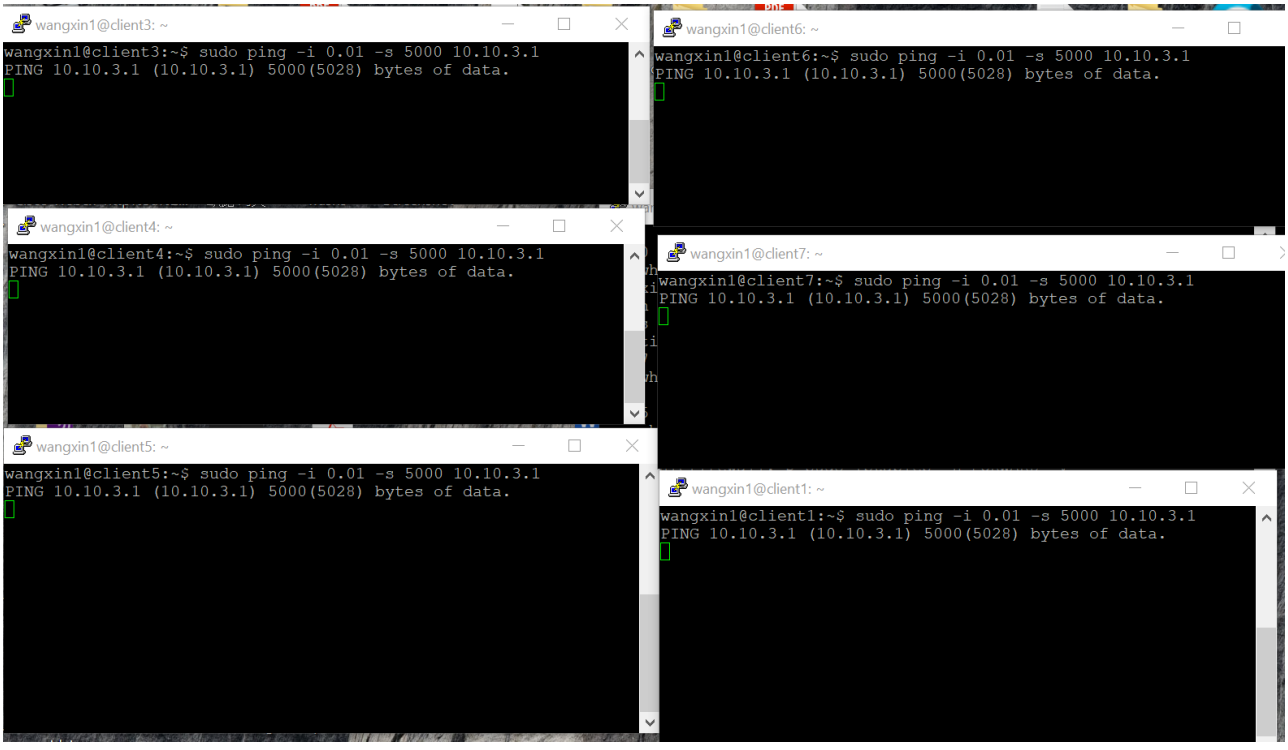
As a result, The attacker, client1, client2 can ping webserver, but due to limitation, webserver works fine, client3 can access webserver.



The attacker controls a botnet to simultaneously launch ping attacks on the webserver.
respectively client3, 4, 5, 6, 7. in this scenario, assuming Attacker are already controlled these 5 hosts. (In the real world scenario, The attacker may controlled more than one botnet. each contains hundred of hosts.)
As a result, other client cannot access to webserver. Int this case, client1 cannot access webserver.
sudo ping -i 0.01 -s 20000 10.10.3.1



Finally, Administrator blocks all icmp requests, run
sudo iptables -A FORWARD -p icmp --icmp-type echo-request -j DROP
As a result, no one can use ping on webserver.



5. Your contribution if you used one of the posted projects (change attack protocol, complicated scenario.. etc). This contribution should be clarified in your report and the final project selection submission)

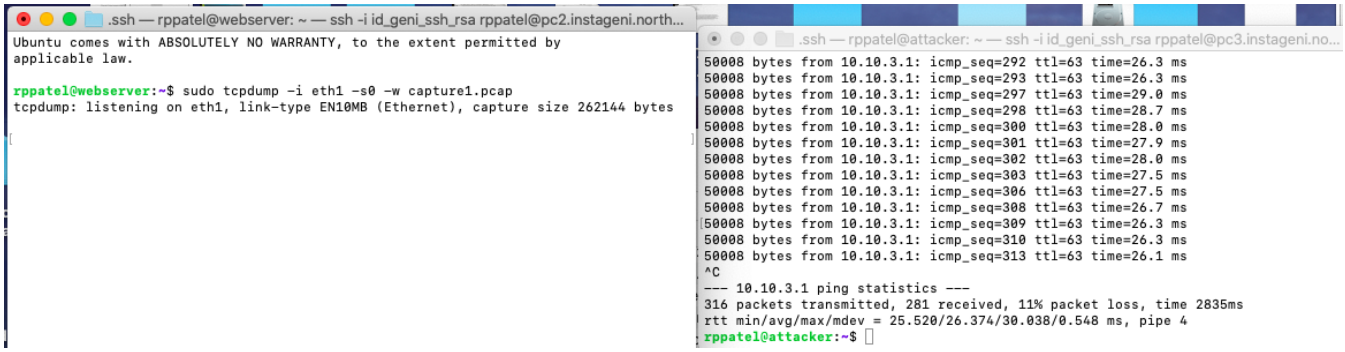
1. We use different scenarios and different network structures
2. We use the ping attack instead of the slowhttptest tool in the lab.
3. We use tcpdump command to collect data, and then use wireshark to analyze the data packets.
4. We use the Defend method which is different from the lab.
5.

6. How to Detect and Defend Against a DoS and the DDoS Attack

Detect:

In DOs scenario, We collect data traffic on the webserver and save it in the capture1 file.

Run sudo tcpdump -i eth1 -s0 -w capture1.pcap on webserver, and then Attacker use ping to webserver. You can detect by seeing these icmp packets.

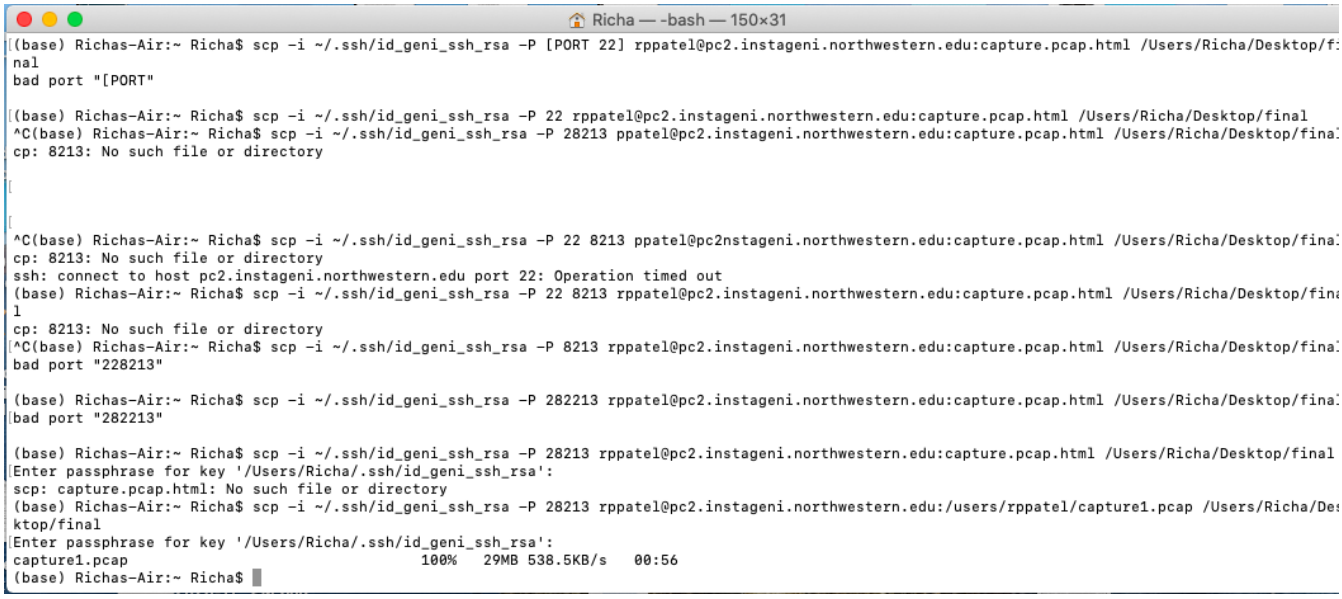


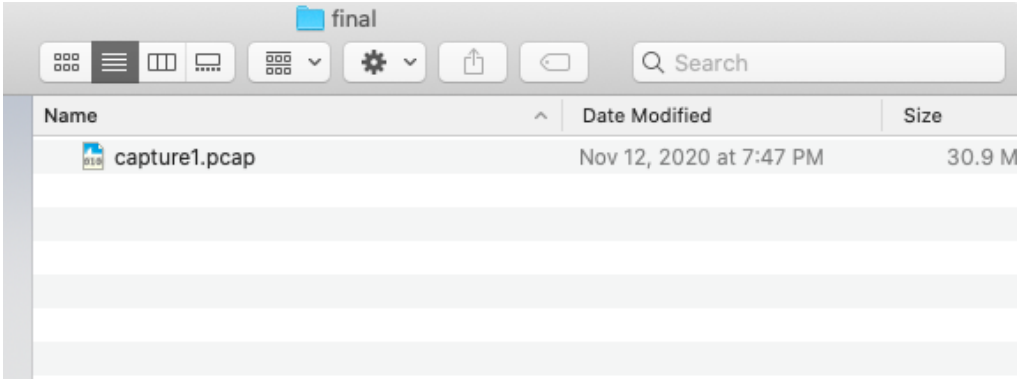
Use wireshark to detect packets.

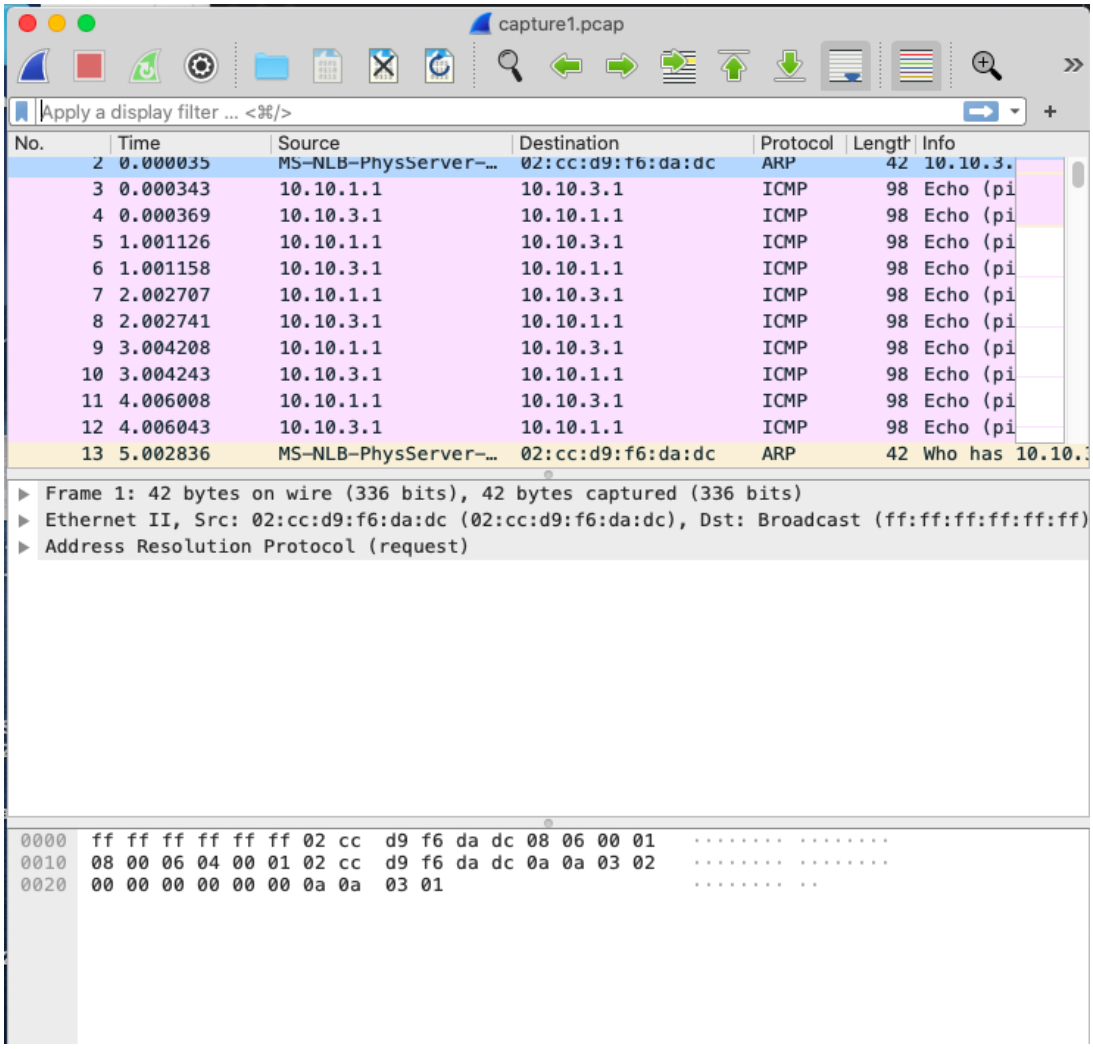
In this case, We install filezilla to link the virtual machine in geni.

Click **File -> Site Manager** , and you can do that if you want to. But I chose another option since it would be easier. I used scp, and we learned that in lab 4.

I used to transfer “capture1.pcap” to my laptop. After that I got wireshark, and then I got the results.


Richa — -bash — 150×31
(base) Richas-Air:~ Richa$ scp -i ~/.ssh/id_geni_ssh_rsa -P [PORT 22] rppatel@pc2.instageni.northwestern.edu:capture.pcap.html /Users/Richa/Desktop/f
nal
bad port "[PORT"
(base) Richas-Air:~ Richa$ scp -i ~/.ssh/id_geni_ssh_rsa -P 22 rppatel@pc2.instageni.northwestern.edu:capture.pcap.html /Users/Richa/Desktop/final
^C(base) Richas-Air:~ Richa$ scp -i ~/.ssh/id_geni_ssh_rsa -P 28213 ppatel@pc2.instageni.northwestern.edu:capture.pcap.html /Users/Richa/Desktop/fina
cp: 8213: No such file or directory
^C(base) Richas-Air:~ Richa$ scp -i ~/.ssh/id_geni_ssh_rsa -P 22 8213 ppatel@pc2nstageni.northwestern.edu:capture.pcap.html /Users/Richa/Desktop/fina
cp: 8213: No such file or directory
ssh: connect to host pc2.instageni.northwestern.edu port 22: Operation timed out
(base) Richas-Air:~ Richa$ scp -i ~/.ssh/id_geni_ssh_rsa -P 22 8213 rppatel@pc2.instageni.northwestern.edu:capture.pcap.html /Users/Richa/Desktop/fina
l
cp: 8213: No such file or directory
^C(base) Richas-Air:~ Richa$ scp -i ~/.ssh/id_geni_ssh_rsa -P 8213 rppatel@pc2.instageni.northwestern.edu:capture.pcap.html /Users/Richa/Desktop/fina
bad port "228213"
(base) Richas-Air:~ Richa$ scp -i ~/.ssh/id_geni_ssh_rsa -P 282213 rppatel@pc2.instageni.northwestern.edu:capture.pcap.html /Users/Richa/Desktop/fina
bad port "282213"
(base) Richas-Air:~ Richa$ scp -i ~/.ssh/id_geni_ssh_rsa -P 28213 rppatel@pc2.instageni.northwestern.edu:capture.pcap.html /Users/Richa/Desktop/final
Enter passphrase for key '/Users/Richa/.ssh/id_geni_ssh_rsa':
scp: capture.pcap.html: No such file or directory
(base) Richas-Air:~ Richa$ scp -i ~/.ssh/id_geni_ssh_rsa -P 28213 rppatel@pc2.instageni.northwestern.edu:/users/rppatel/capture1.pcap /Users/Richa/Des
ktop/final
Enter passphrase for key '/Users/Richa/.ssh/id_geni_ssh_rsa':
capture1.pcap 100% 29MB 538.5KB/s 00:56
(base) Richas-Air:~ Richa$


final
Search
Name
Date Modified
Size
capture1.pcap
Nov 12, 2020 at 7:47 PM
30.9 M



In order to help to stop or defend the DoS and DDoS attack, is using practices like using complex passwords which change frequently, having anti phishing methods, and also securing firewalls which allow very little outside traffic. Also, the servers need to be located in different places because spreading them out is more difficult for attackers to target. You can detect these DoS and DDoS attacks by seeing a slowdown in network performance or an increase in the number of spam emails. This could be intrusion.

Update your Geni SSH key.
Edit -> Settings-> SFTP

Copy the file capture1 to your desktop and open it with wireshark.

We found a large number of ICMP requests.
From 10.10.1.1 (Attacker) to 10.10.3.1(Web Server)

Defend: (iptable)

The main way to defend against DOS and DDOS is to use iptables. Iptables is a command-line firewall utility that helps control traffic.

Dos: During the demonstration of the attacks some examples of these commands were used. One of these commands was:

sudo iptables -A FORWARD -p icmp -s 10.10.1.1 -j DROP

This command was used with an attacker's IP and uses an iptables command to block the source IP address. With this command, the attacker cannot ping to the web server anymore. Other commands that were used in this attack were also:

sudo iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 100/second --limit-burst 300 -j ACCEPT
sudo iptables -A FORWARD -p icmp --icmp-type echo-request -j DROP

These commands were used to set the firewall's iptable settings to limit the frequency of ping packets.
In the attack that was demonstrated iptable commands were shown to be effective in defending against this attack.

DDos: During the demonstration of this attack an example was used. The command used was:

Sudo iptables -A FORWARD -p icmp --icmp --icmp-type echo-request -j DROP

This command was used to block all icmp requests and would not allow anyone to ping the web server.

When used correctly iptables is a powerful tool that can be used to defend against DDOS and DOS attacks. Besides iptables, there are a few other things that can be done to help defend against these attacks.
One of these things is to try to identify an attack early by looking at the traffic and seeing if there are any changes that are not normal. This technique could be used to detect an attack early, so that more action can be taken quickly. Another thing that can be done is to have overprovision bandwidth, this technique won't stop an attack completely but it helps and gives more time to stop the attack. Lastly, it is also a good idea to have a plan on what to do in case one of these attacks occurs.

Conclusion

This project focused on the network effects of DoS and DDoS attacks and the danger they pose to a server, as well as some defenses to be used to secure the systems in danger. Initially, several different types of DoS attacks were reviewed, before ping flood attacks were chosen for the lab. For the purpose of this project, we used different attack scenarios against different network structures. TCPDump was chosen to collect the data, and WireShark was employed to analyze the resulting set of packets.

A DoS attack was conducted against our test servers, with limited results because of the small attack size. Different preventative methods such as modifying IPTables were employed, resulting in a stop to the effectiveness of the DoS attack. Second, a DDoS attack from a set of 5 clients was conducted, simulating a larger botnet with hundreds of clients. Methods that worked for the prior DoS attacks would do little to help, so for the purposes of the project a severe solution, blocking all ping attempts to the server, was employed.

7. References

S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046-2069, Fourth Quarter 2013, doi: 10.1109/SURV.2013.031413.00127.

Jelena Mirkovic and Peter Reiher. 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. SIGCOMM Comput. Commun. Rev. 34, 2 (April 2004), 39–53. DOI:https://doi.org/10.1145/997150.997156

“Security Tip (ST04-015).” *Cybersecurity and Infrastructure Security Agency CISA*, us-cert.cisa.gov/ncas/tips/ST04-015.