**Denial of Service Attacks**

**Date Assigned**:

**Date Due**:

1 Preparation 1

2 Ping flood attack 1

3 Ping flood attack defense 2

4 SYN spoofing/flood attack 3

5 SYN spoofing/flood defense with firewalls 3

6 SYN spoofing/flood defense with SYN Cookies 4

**Goal:** In this project, we will observe how to prevent (slow down) legitimate access to a server using denial of service (DoS) attacking techniques.

# Preparation

Turn off your firewall. Make certain that you have vsftpd and httpd services running on your FC server by conducting an nmap scan (using CLI) on the server machine. You should see ports 21/ftp and 80/http open. If the ports are not open, start these two services.

To start these two services, type the following command:

yum install vsftpd

systemctl enable vsftpd

service httpd start

yum install httpd

systemctl enable httpd

service httpd start

firewall-cmd --add-port=21/tcp --permanent

firewall-cmd --add-service=http --permanent

firewall-cmd --reload

On your FC client, as the root, type the following command: (3 points)

# yum install hping\*

From your Windows machine, open a web browser and type in the following: (3 points)

<http://FC_server_IP>

Observe the time it takes to respond to your http request.

Start the command line prompt on your Windows, type the following

# ftp FC\_server\_IP

Observe the time it takes to respond to your ftp connection request. (3 points)

# Ping flood attack

A ping flood is a simple DoS attack where the attacker overwhelms the victim’s bandwidth with ICMP Echo Request (ping) packets. This is most effective by using the flood option of ping which sends ICMP packets as fast as possible without waiting for replies. Most implementations of ping require the user to be privileged in order to specify the flood option. It is most successful if the attacker has more bandwidth than the victim (for instance an attacker with a DSL line and the victim on a dial-up modem).

On your FC server, as the root, start the Wireshark by typing the following command:

# wireshark &

Start data capture using the right network interface. (3 points)

We will launch the ping flooding attack from both the FC client and CentOS machines.

From both your FC client and CentOS, as the root user, issue the following command: (6 points)

# ping your\_FCserver -i 0.001 -s 1500

### Explain the meaning of this command (3 points)

Now back on your Windows machine, try to ftp into the server and reload the HTTP page. Observe the time it takes to answer your FTP and HTTP request. (3 points)

### Were you able to FTP into the server and reload the web page? Did you notice significant delay? Why? (3 points)

To get more noticeable delay, you may need to get help from your fellow classmates. When there are more attackers, the delay should be larger.

### Provide a screenshot of your Wireshark showing the ping flood attack. (3 points)

# Ping flood attack defense

There are many proposed techniques towards preventing ping flood attack. A simple way is to use your firewall to do a ping rate limiting.

On your FC server, as the root user, add the following firewall rules: (3 points)

iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/minute --limit-burst 1 -j ACCEPT

iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/minute --limit-burst 1 -j LOG --log-prefix PING-DROP:

iptables -A INPUT -p icmp -j DROP

iptables -A OUTPUT -p icmp -j ACCEPT

Hint: If you use Fedora 18-29, install iptables-services first.

### Explain the meaning of these rules. (3 points)

After you have finished the modifications and restart the firewall service by typing: (2 points)

# service iptables restart

Once again, launch the ping flooding attack from both the FC client and CentOS machines. (6 points)

### Explain what happened. Did the ping rate limiting technique work? Why or why not? (3 points)

It will be helpful for you to open Wireshark on both the attacking machines to see whether you can get ping replies.

# SYN spoofing/flood attack

A SYN flood sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

**On your FC server**, as the root, type the following command: (3 points)

# sysctl -w net.ipv4.tcp\_syncookies = 0

# sysctl -w net.ipv4.tcp\_max\_syn\_backlog = 5

**From your FC client**, as the root user, issue **either** of the following commands: (3 points)

# hping -i u1 -S -p 80 your-server-ip

# hping -i u1 -S -p 21 your-server-ip

### Explain the meaning of this command (hint: hping -h) (3 points)

Now back on your Windows machine, try to ftp into the server (if port 21 was used) or reload the HTTP page (if port 80 was used). Observe the time it takes to answer your FTP or HTTP request. (3 points)

### Were you able to FTP into the server and reload the web page? Did you notice significant delay? Why it takes fewer resources (only one client) to achieve DoS compared to the ping flood attack? (3 points)

### Provide a screenshot of your Wireshark showing the SYN flood attack. (3 points)

# SYN spoofing/flood defense with firewalls

On your FC server, as the root user, add the following firewall rules: (3 points)

iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 3 -j RETURN

### Explain the meaning of these rules. (3 points)

After you have finished the modifications and restart the firewall service by typing: (2 points)

# service iptables restart

**From your FC client**, as the root user, issue **either** of the following commands: (3 points)

# hping -i u1 -S -p 80 your-server-ip

# hping -i u1 -S -p 21 your-server-ip

Now back on your Windows machine, try to ftp into the server and reload the HTTP page. Observe the time it takes to answer your FTP and HTTP request. (3 points)

### Were you able to FTP into the server and reload the web page? Did you notice significant delay? (3 points)

Once you have accomplished this section, go back to your Fc server. Type: (2 points)

# service iptables restart

# SYN spoofing/flood defense with SYN Cookies

SYN Cookies are the key element of a technique used to guard against SYN flood attacks. In particular, the use of SYN Cookies allows a server to avoid dropping connections when the SYN queue fills up. Instead, the server behaves as if the SYN queue had been enlarged. The server sends back the appropriate SYN+ACK response to the client but discards the SYN queue entry. If the server then receives a subsequent ACK response from the client, the server is able to reconstruct the SYN queue entry using information encoded in the TCP sequence number.

More information about SYN cookies can be found here: <http://en.wikipedia.org/wiki/SYN_cookie>.

Enable SYN Cookies on your **FC server**. As the root user, type: (2 points)

# sysctl -w net.ipv4.tcp\_syncookies = 1

Now with SYN COOKIES enabled, start Wireshark on your FC server. Look at Wireshark and wait until the attack gets started (You will see a huge increase in TCP packets). (3 points)

**From your FC client**, as the root user, issue **either** of the following commands: (3 points)

# hping -i u1 -S -p 80 your-server-ip

# hping -i u1 -S -p 21 your-server-ip

Now back on your Windows machine, try to ftp into the server (if port 21 was used) or reload the HTTP page (if port 80 was used). Observe the time it takes to answer your FTP or HTTP request. (2 points)

### Were you able to FTP into the server and reload the web page? Why or why not? Did you notice significant delay? (3 points)

### Can you see any difference in the TCP packets? (Hint: Look at the sequence number) Provide a screenshot of your Wireshark capture. (3 points)