Class Networks
A 10.0.0.0 through 10.255.255.255
B 172.16.0.0 through 172.31.0.0
C 192.168.0.0 through 192.168.255.0

Ping Flooding Attack

```
sudo ping -f -s 56500 192.168.1.100
```

Netstat Commands
Listing all ports (both TCP and UDP) using netstat -a
Listing only TCP (Transmission Control Protocol) port connections using netstat -at
Listing only UDP (User Datagram Protocol) port connections using netstat -au.

Listing all active UNIX listening ports using netstat -lx

Showing Statistics by Protocol netstat -s

TCPDUMP

sudo tcpdump -D
sudo tcpdump -i any

sudo tcpdump -i any -c 5

sudo tcpdump -i any -c5 -nn //with ip

Flag values:

Value	Flag Type	Description
S	SYN	Connection Start
F	FIN	Connection Finish
P	PUSH	Data push
R	RST	Connection reset
.	ACK	Acknowledgment

sudo tcpdump -i any -c5 icmp

sudo tcpdump -i any -c10 -nn -A port 80 //checking packet contents

sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80

tcpdump -nn -r webserver.pcap

NMAP

COMMAND

DESCRIPTION

```
nmap -sP 10.0.0.0/24
```

Ping scans the network, listing machines that respond to ping.

```
nmap -p 1-65535 -sV -sS -T4 target
```

Full TCP port scan using with service version detection - usually my first scan, I find T4 more accurate than T5 and still "pretty quick".

```
nmap -v -sS -A -T4 target
```

Prints verbose output, runs stealth syn scan, T4 timing, OS and version detection + traceroute and scripts against target services.

```
nmap -v -sS -A -T5 target
```

Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection + traceroute and scripts against target services.

```
nmap -v -sV -O -sS -T5 target
```

Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection.

```
nmap -v -p 1-65535 -sV -O -sS -T4 target
```

Prints verbose output, runs stealth syn scan, T4 timing, OS and version detection + full port range scan.

```
nmap -v -p 1-65535 -sV -O -sS -T5 target
```

Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection + full port range scan.

IPTABLES:

```
sudo iptables -S
```

```
sudo iptables -L
```

```
sudo iptables -A INPUT -p tcp -s YOUR.IP.HERE --dport 22 -j ACCEPT
```

```
sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```

```
sudo iptables -D INPUT -m conntrack --ctstate INVALID -j DROP
```

```
sudo iptables -L –line-numbers
```

```
sudo iptables -D INPUT 3
```

```
sudo iptables-save
```

UFW:

```
sudo ufw status
sudo ufw allow 22
sudo ufw deny 22
sudo ufw allow from 15.15.15.51
sudo ufw allow from 15.15.15.51 to any port 22
sudo ufw status numbered
sudo ufw delete 2
sudo ufw delete allow 80
```

Wireshark

http://www.techpanda.org/

username:admin@google.com

password: Password2010