Jared Ren
4/25/20
Firewall Lab

Task 1.

```
[04/25/20]seed@VM:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[04/25/20]seed@VM:~$
```

Task 2.

```
[04/25/20]seed@VM:~$ nc -zv -u 10.0.2.4 123
Connection to 10.0.2.4 123 port [udp/ntp] succeeded!
[04/25/20]seed@VM:~$ ntpdate -q 10.0.2.4
server 10.0.2.4, stratum 2, offset 0.000003, delay 0.02563
25 Apr 17:53:34 ntpdate[29767]: adjust time server 10.0.2.4 offset 0.000003 sec
[04/25/20]seed@VM:~$
```

Task 3.

```
#!/bin/bash

#default policies
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT

#accept for input
iptables -A INPUT -p UDP ACCEPT
iptables -A INPUT -p HTTP -s 10.0.2.4 ACCEPT
iptables -A INPUT -p UDP --pkt-type NTP ACCEPT
iptables -A INPUT --pkt-type MYSQL ACCEPT

#drop for output
iptables -A OUTPUT -p HTTP -d 10.0.2.4 ACCEPT
```

Iptables shell script I made, file named shellcode.sh

```
[04/27/20]seed@VM:~$ sudo bash shellcode
Bad argument `ACCEPT'
Try `iptables -h' or 'iptables --help' for more information.
iptables v1.6.0: unknown protocol "http" specified
Try `iptables -h' or 'iptables --help' for more information.
iptables v1.6.0: unknown option "--pkt-type"
Try `iptables -h' or 'iptables --help' for more information.
iptables v1.6.0: unknown option "--pkt-type"
Try `iptables -h' or 'iptables --help' for more information.
iptables v1.6.0: unknown protocol "http" specified
Try `iptables -h' or 'iptables --help' for more information.
[04/27/20]seed@VM:~$
```

The result of executing it

```
[04/27/20]seed@VM:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.

^C
--- 10.0.2.4 ping statistics ---
13 packets transmitted, 0 received, 100% packet loss, time 12284ms
```

```
[04/27/20]seed@VM:~$ nc -zv 10.0.2.4 23
nc: connect to 10.0.2.4 port 23 (tcp) failed: Connection timed out
```

```
[04/27/20]seed@VM:~$ nc -zv 10.0.2.4 80
nc: connect to 10.0.2.4 port 80 (tcp) failed: Connection timed out
```

```
[04/27/20]seed@VM:~$ nc zv localhost 3306
nc: port number invalid: localhost
```

Task 4.

```
[04/27/20]seed@VM:~/sniffspooflab$ sudo python httpspoof.py
SENDING SPOOFED http PACKET.........
Traceback (most recent call last):
  File "httpspoof.py", line 6, in <module>
    http = HTTP()
NameError: name 'HTTP' is not defined
[04/27/20]seed@VM:~/sniffspooflab$
```

```
#!/usr/bin/python3
from scapy.all import *

print("SENDING SPOOFED http PACKET.........")
ip = IP(src="1.2.3.4", dst="10.0.2.4")
http = HTTP()
pkt = ip/http
pkt.ttl = 20
```

Http spoof program

```
[04/27/20]seed@VM:~/sniffspoof$ sudo python httpspoof.py
SENDING SPOOFED http PACKET.........
Traceback (most recent call last):
  File "httpspoof.py", line 6, in <module>
    http = HTTP()
NameError: name 'HTTP' is not defined
```

```
#!/usr/bin/python3
from scapy.all import *

print("SENDING SPOOFED http PACKET.........")
ip = IP(src="1.2.3.4", dst="4.3.2.1")
http = HTTP()
pkt = ip/http
pkt.ttl = 20
```

Modified HTTP spoof script

```
[04/27/20]seed@VM:~/sniffspoof$ sudo python httpspoof.py
SENDING SPOOFED http PACKET.........
Traceback (most recent call last):
  File "httpspoof.py", line 6, in <module>
    http = HTTP()
NameError: name 'HTTP' is not defined
```

Same error

----------Example Questions----------

17.10) ufw is ubuntu's firewall configuration tool, so its not a firewall it is a tool to make them

17.11) rule for iptables:

Iptables -P INPUT -s 192.168.10.0/24 ACCEPT