IP Table Assignment

Index No: -18001149

A). Explain following `iptables` rules. You have to correct rules if there are any errors and mention that as well.

```
   1) iptables -F
```

Rule flashes all the Chain, which effectively deletes every rule in the chain.

```
   2) iptables -P INPUT ACCEPT
```

This rule specifies Sets the default chain policy, to allow packets to move through a whole chain without a rule to a given objective, such as Accept.

```
   3) iptables -A INPUT -i eth1 -s 10.0.0.0/8 -m limit --limit 5/m --limit-
      burst 7 -j LOG --log-prefix "IP_SPOOF A: "
```

The rule appended to iptables Input chain for incoming packets on "ethernet 1" interface for source address (10.0.0.0/8), should be limited maximumly 5 packets per minute. Should be allowed maximum 7 packets before applying the limit(Set limit bursts to 7). But in the Start of log message of this rule is "IP_SPOOF A "should needed to be printed.

```
   4) iptables -A INPUT -p TCP --syn -m limit --limit \ 5/second -j ACCEPT
```

`There is a significant error in the rule (Highlighted Part)`

Corrected Rule

Iptables -A INPUT -p TCP[I] -syn -m limit --limit 5/second -j ACCEPT

- ➔ **The rule appended to iptables INPUT chain for TCP protocol with Syn Flag, and it will limit the acceptance rate of incoming packets of TCP protocol to 5 per second**

```
   5) iptables -A INPUT -p udp -m time --timestart 02:00 \ --timestop 03:00 -
      j DROP
```

- ➔ **This rule appended to INPUT chain to drop UDP protocol packets coming from 2.00 a.m to 3.00 a.m**

B) Explain following rules collectively

```
i. /sbin/iptables -N port-scanning
```

This rules Create a new user-defined chain by the given name (no name given) to Iptables to port scanning

```
ii. /sbin/iptables -A port-scanning -p tcp \ --tcp-flags SYN,ACK,FIN,RST RST
-m limit \ --limit 1/s --limit-burst 2 -j RETURN
```

➔ **There are errors In this Rule**

Corrected Rule

/sbin/iptables -A port-scanning -p tcp --tcp-flags [I] SYN,ACK,FIN,RST -m limit --limit 1/s --limit-burst 2 -j REJECT

➔ **This rule appends to iptables PORT SCANNING chain for tcp protocol with Flags SYN,ACK,FIN,RST and it allows maximum of 1 packet per second, Should be reject 2 packets before applying the burst limit before applying the limit**

```
iii. /sbin/iptables -A port-scanning -j DROP
```

➔ **This rule appends to iptables Port Scanning chain for drop**

G) Explain following rules collectively

```
i. /sbin/iptables -A INPUT -p tcp --dport ssh \ -m conntrack --ctstate NEW -m
recent --set
```

-> This rule appends to iptables input chain for tcp protocol on destination port of outgoing packets on SSH, in multiple connection tracks with New connection list .The recent packet lists will be added with Source addresses

```
ii. /sbin/iptables -A INPUT -p tcp --dport ssh \ -m conntrack --ctstate NEW -
m recent --update \ --seconds 60 --hitcount 10 -j DROP
```

➔ **This rule appends to iptables input chain for tcp protocol on destination port of outgoing packets on SSH, in multiple connection tracks with New connection list. Sources address will be added in each packet and update in every 60 seconds it will narrow the match to only happen when the address is in the list and packets had been received to 10 the packets will be dropped.**

```
h) iptables -A FORWARD -p tcp -m multiport --dport \ http,https -o eth0 -i
eth1 -m time --timestart 21:30 \ --timestop 22:30 --days Mon,Tue,Wed,Thu,Fri
-j ACCEPT
```

Appended to iptables FORWARD chain for tcp protocol on destination ports of outgoing packets on " ethernet 0" interface and input packets on " ethernet 1" interface to accept on days (Mon, Tue, Wed, Thu, Fri) time between 21:30 and 22:30.

```
i. iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
```

- ➔ **There are errors in the Table**

  Corrected Rule

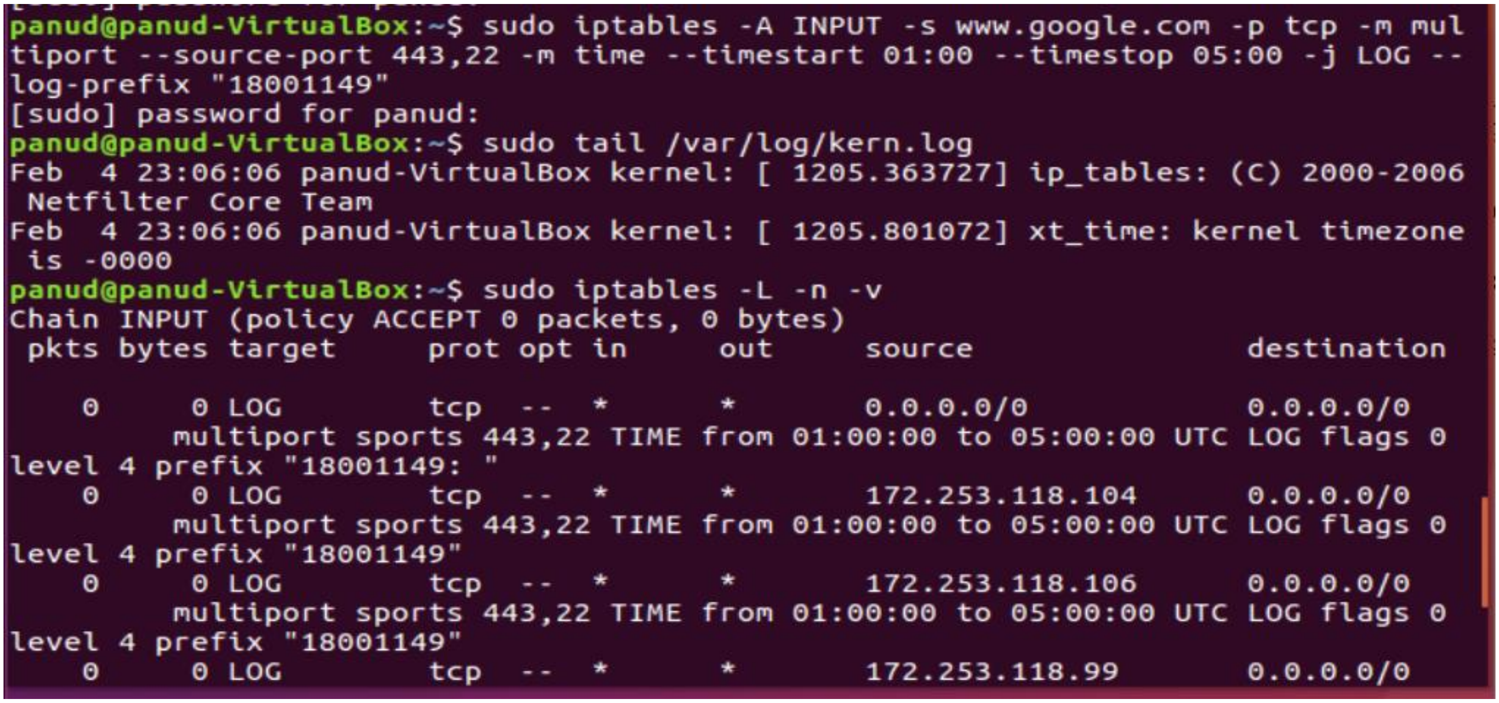
Iptables -A INPUT -p tcp --tcp-flags -j DROP

- ➔ **This rule Appends to INPUT chain to drop all TCP flags for tcp Protocol**

2) Write iptables rules corresponding to following requirements and provide the rule and screen shots of the logs.

a. Write an `iptables` rule to log traffic that are coming from a particular network to the host implementing iptables from 1.00 a.m. to 5.00 a.m. to access https and ssh services. The log entry shall have your index number as a prefix.

- ➔ **Sudo iptables -A INPUT -s www.google.com -p tcp -m multiport --source-port 443,22 -m time --timestart 01:00 --timestop 05:00 -j LOG --log-prefix "18001149 "**



```
panud@panud-VirtualBox:~$ sudo iptables -A INPUT -s www.google.com -p tcp -m mul
tiport --source-port 443,22 -m time --timestart 01:00 --timestop 05:00 -j LOG --
log-prefix "18001149"
[sudo] password for panud:
panud@panud-VirtualBox:~$ sudo tail /var/log/kern.log
Feb  4 23:06:06 panud-VirtualBox kernel: [ 1205.363727] ip_tables: (C) 2000-2006
 Netfilter Core Team
Feb  4 23:06:06 panud-VirtualBox kernel: [ 1205.801072] xt_time: kernel timezone
 is -0000
panud@panud-VirtualBox:~$ sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 LOG        tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
          multiport sports 443,22 TIME from 01:00:00 to 05:00:00 UTC LOG flags 0
level 4 prefix "18001149: "
    0     0 LOG        tcp  --  *      *       172.253.118.104      0.0.0.0/0
          multiport sports 443,22 TIME from 01:00:00 to 05:00:00 UTC LOG flags 0
level 4 prefix "18001149"
    0     0 LOG        tcp  --  *      *       172.253.118.106      0.0.0.0/0
          multiport sports 443,22 TIME from 01:00:00 to 05:00:00 UTC LOG flags 0
level 4 prefix "18001149"
    0     0 LOG        tcp  --  *      *       172.253.118.99       0.0.0.0/0
```