Using an Ubuntu Linux machine in the Linux lab, create a bash shell script to block IP addresses of ssh attackers. Your script should analyze the sample authentication log file and create a syslog entry for each IP address with more than 10 invalid login attempts. Your script should also create an IP tables firewall rule to block each IP address with more than 10 invalid login attempts.

★ The sample authentication log may be downloaded from the "Final project" assignment on Canvas.

After testing your "block" script, create a cron job to run your "block" script every 15 minutes of every day.

Next, create a second bash shell script to reset the IP tables firewall. The purpose of the second script is to remove all the blocked IP addresses by restoring the basic IP tables firewall.

Finally, create a cron job to run your "reset" script at 11:59 p.m. every Sunday.

Copy and paste the following items into a document and upload the file to the "Final project" assignment on Canvas.

1. Your "block" bash shell script
2. A long directory listing showing your "block" script filename and permissions
3. The line added to the cron job configuration file to run your "block" script
4. An IP tables verbose listing showing at least one block rule added by your "block" script
5. A tail of syslog showing at least one log entry added by your "block" script
6. Your "reset" bash shell script
7. A long directory listing showing your "reset" script filename and permissions
8. The line added to the cron job configuration file to run your "reset" script

Use the following rules for your "basic" IP tables firewall.

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp --dport ssh -j ACCEPT
iptables -A OUTPUT -j LOG
iptables -A INPUT -j DROP

iptables -A OUTPUT -o lo -j ACCEPT
iptables -A OUTPUT -p udp --dport domain -j ACCEPT
```

```
iptables -A OUTPUT -p udp --dport ntp -j ACCEPT
iptables -A OUTPUT -p tcp --dport www -j ACCEPT
iptables -A OUTPUT -p tcp --dport https -j ACCEPT
iptables -A OUTPUT -p tcp --dport ssh -j ACCEPT
iptables -A OUTPUT -p icmp -j ACCEPT
iptables -A OUTPUT -j DROP
```

**Due date**:

Tuesday May 7 before 11:59 p.m.

**How to submit**:

Upload your document to Canvas in the "Final Project" assignment.