Assignment Day 18 | 12th November 2020 By Sameer Kulkarni

Question 01. Instructions:-
1. Grab IP address of all ssh attackers in a file.
2. Use this file to append entries to /etc/hosts.deny.
3. Expose the content of hosts.deny in a web page.
4. If there is a change in hosts.deny file with the number of IP address, you should get a notification on your mobile.
5. The script should run every 5 minutes automatically and notification should trigger every 10 minutes.

Answer 01.

In CentOS, the failed SSH sessions are recorded in /var/log/secure file. The script to find failed SSH login attempts on a CentOS system and generating report in /reports directory is as follows:-

```
#!/bin/bash
cat /etc/hosts.deny.bak > /etc/hosts.deny
for z in $(find /var/log -name "secure*" -exec cat {} \; | grep ssh| grep -i Failed |   grep -E -o "([0-9]{1,3}[\.]){3}[0-9]{1,3}" | sort -u)
do
        echo "sshd : $z" >> /etc/hosts.deny
done
dt=$(date)
        totalfailure=$(grep sshd /etc/hosts.deny |wc -l)
        echo "#Total attack is $totalfailure. Last updated on $dt" >> /etc/hosts.deny
```

For exposing the content of hosts.deny file to webpage, add following line in the above script

```
cat /etc/hosts.deny >> /var/www/html/reports/sshdenial.txt
```

And the reports can be accessed at http://localhost/reports/sshdenial.txt. If there is a change in this file, to get notification every 10 min, same URL is configured in Mobile App Web Alert. The configuration for every 10 min check is done in the app itself.

For running a script in every 5 min, add following in crontab:-

```
sudo crontab -e
5,10,15,20,25,30,35,40,45,50,55 * * * * /root/protectssh
```