Assignment Day 21 | 19th November 2020
By Sameer Kulkarni

Question 01. Instructions:-

1. Spin up a CentOS VM in alibaba cloud.
2. Create a web server with some content in the default page.
3. Watch out for the communication logs and create a file with information containing the IP address who visited the website.
4. Watch for any suspicious activity.
5. Monitor the website from two different monitors, if the website is down you should get an alert.
    1. Monitor 1 should give a notification on mobile
    2. Monitor 2 should send you an email.

Answer 01.

The CentOS VM was spun up in GCP. A web server was created with some content with following commands:

```
sudo yum update                 # For updating the software version
sudo yum install httpd          # Install Apache
sudo systemctl start httpd      # Activate Apache
sudo systemctl enable httpd
```

Created index.html and placed it in /var/www/html folder.

To check about the suspicious activity on the website, following commands are used:

```
egrep -e fail /var/log/messages     # indicate a failed login or a failed attempt to connect on a given port.
egrep -n UDP /var/log/messages      # list all of the attempted connections with UDP instead of TCP.
egrep -e root /var/log/messages     # look for any messages that refer to the root user
```

To create a file with information containing the IP addresses who visited the website, following shell script is used.

```
awk '{ print $1}' /var/log/httpd/access_log | sort | uniq -c | sort -nr | head > >> /var/www/html/reports/ipvisitingwebsite.txt
```

And the reports can be accessed at http://localhost/reports/ipvisitingwebsite.txt. To monitor, same URL is configured in Mobile App Web Alert.

The script to send email about all the suspicious activity is as follows:-

```
#!/bin/bash
prev_count=0      #Set the variable which equal to zero
count=$(grep -i "`date --date='yesterday' '+%b %e'`" /var/log/messages |
egrep -wi 'warning|error|critical' | wc -l)
if [ "$prev_count" -lt "$count" ] ; then
# Send a mail to given email id when errors found in log
        SUBJECT="WARNING: Errors found in log on "`date --
        date='yesterday' '+%b %e'`""
# This is a temp file, which is created to store the email message.
        MESSAGE="/tmp/logs.txt"
        TO="daygeek@gmail.com"
        echo "ATTENTION: Errors are found in /var/log/messages. Please
        Check with Linux admin." >> $MESSAGE
        echo  "Hostname: `hostname`" >> $MESSAGE
        echo -e "\n" >> $MESSAGE
        echo "+---------------------------------------------------+" >> $MESSAGE
        echo "Error messages in the log file as below" >> $MESSAGE
        echo "+---------------------------------------------------+" >> $MESSAGE
        grep -i "`date --date='yesterday' '+%b %e'`" /var/log/messages | awk
        '{ $3=""; print}' | egrep -wi 'warning|error|critical' >>  $MESSAGE
        mail -s "$SUBJECT" "$TO" < $MESSAGE
        #rm $MESSAGE
fi
```