Tests: Associate Application Support Engineer

TEST-1

Please download the file and save it as ‘ip.csv’. Now please write a python script to read the dataset from that CSV file, gather geo-information of each IP calling https://ipinfo.io/ as API and follow the following instructions given below:

1. Generate a CSV file with the postal code of IPs’ by descending order. For example, the CSV file may look like:

IP	postal code
192.168.2.1	1206
192.168.2.2	8008

2. Generate a CSV file enlisting all IPs where the region of the IP starts and ends with a consonant and contains more than one vowel.

3. Generate a CSV file enlisting all IPs where the city of the IP contains two vowels side by side index.

4. Generate a CSV file showing the count of IPs grouping by country. For example:

Country	IPs
CN	5
BN	2

5. It would be good if you can convert all of these CSVs into one Excel file with separate sheets.

TEST-2

Here is a sample database table named **marks**:

id	name	mark
1	Habib	41
2	Fuad	7
3	Imran	99
4	Nancy	43
5	Kona	35
6	Pritom	18
7	Anila	93
8	Sumon	84
9	Tahsan	39
10	Shuvo	75

Please write an SQL query to find the name who has got the 3rd highest mark and another query to find the name who has got the 2nd lowest mark.

TEST-3

You are required to write a program in Python to parse the below SSH Logs and produce a CSV file (Example: SSH_Log.csv) according to the below table.

Datetime	Server	Process Name	Process ID	Message
Oct 18 11:07:27	dummy_server	systemd-logind	4405	Removed session 109336.
Oct 18 11:10:26	dummy_server	sudo	NULL	pam_unix(sudo:session): session opened for user root by maateen(uid=0)

SSH Logs:

```
Oct 18 11:07:27 dummy_server systemd-logind[4405]: Removed session 109336.
Oct 18 11:07:27 dummy_server systemd-logind[4405]: New session 109337 of user ubuntu.
Oct 18 11:07:31 dummy_server sshd[25163]: Received disconnect from 192.168.12.45: 11: disconnected by user
Oct 18 11:07:31 dummy_server sshd[25041]: pam_unix(sshd:session): session closed for user ubuntu
Oct 18 11:09:01 dummy_server CRON[26000]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 18 11:09:01 dummy_server CRON[26000]: pam_unix(cron:session): session closed for user root
Oct 18 11:10:01 dummy_server CRON[26561]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 18 11:10:05 dummy_server sshd[26500]: Accepted publickey for maateen from 192.168.12.45 port 36970 ssh2: RSA 1b:c6:57:28:06:fd:4e:45:6a:a9:27:03:98:77:8c:42
Oct 18 11:10:05 dummy_server sshd[26500]: pam_unix(sshd:session): session opened for user maateen by (uid=0)
Oct 18 11:10:05 dummy_server systemd-logind[4405]: Removed session 109337.
Oct 18 11:10:05 dummy_server systemd-logind[4405]: New session 109338 of user maateen.
Oct 18 11:10:08 dummy_server sshd[26721]: Authentication refused: bad ownership or modes for file /home/ubuntu/.ssh/authorized_keys
Oct 18 11:10:08 dummy_server sshd[26721]: Accepted password for ubuntu from 192.168.12.45 port 36998 ssh2
Oct 18 11:10:08 dummy_server sshd[26721]: pam_unix(sshd:session): session opened for user ubuntu by (uid=0)
Oct 18 11:10:08 dummy_server systemd-logind[4405]: New session 109339 of user ubuntu.
Oct 18 11:10:09 dummy_server CRON[26561]: pam_unix(cron:session): session closed for user root
Oct 18 11:10:09 dummy_server sshd[26851]: Received disconnect from 192.168.12.45: 11: disconnected by user
Oct 18 11:10:09 dummy_server sshd[26721]: pam_unix(sshd:session): session closed for user ubuntu
Oct 18 11:10:11 dummy_server sshd[27136]: Authentication refused: bad ownership or modes for file /home/ubuntu/.ssh/authorized_keys
Oct 18 11:10:11 dummy_server sshd[27136]: Accepted password for ubuntu from 192.168.12.45 port 37008 ssh2
Oct 18 11:10:11 dummy_server sshd[27136]: pam_unix(sshd:session): session opened for user ubuntu by (uid=0)
Oct 18 11:10:11 dummy_server systemd-logind[4405]: Removed session 109339.
Oct 18 11:10:11 dummy_server systemd-logind[4405]: New session 109340 of user ubuntu.
Oct 18 11:10:14 dummy_server sshd[27220]: Received disconnect from 192.168.12.45: 11: disconnected by user
Oct 18 11:10:14 dummy_server sshd[27136]: pam_unix(sshd:session): session closed for user ubuntu
Oct 18 11:10:26 dummy_server sudo:  maateen : TTY=pts/5 ; PWD=/home/maateen ; USER=root ; COMMAND=/bin/bash
Oct 18 11:10:26 dummy_server sudo: pam_unix(sudo:session): session opened for user root by maateen(uid=0)
```

TEST-4

You are required to produce an ideal postmortem/root cause analysis report for an incident reported below. Create a PDF document (example: postmortem.pdf) with the relevant structure and content.

Problem Statement:

A Jira issue (TH-64669) was logged that the customer data got changed into the database without any proper change request. 486,000 records were affected. The investigation showed that the change was made by a database user (aes_admin) which is used only in a particular microservice called AES, but AES isn’t supposed to do this type of bulk operation. A deep investigation showed that an endpoint (/api/username/update) of that microservice was vulnerable to SQL injection and the database was affected due to an external attack. Later, the development team fixed the bug with a quick patch, affected records were restored to the previous state from the daily backup and the issue got resolved. The affected records were discovered at 10:30 AM, restored at 3:45 PM.

TEST-5

Here is a sample database table named **customers**:

id	customer
1	Habib
2	Fuad
3	Imran
4	Nancy
5	Kona

Another database table named **products**:

id	products
1	{‘name’: ‘shirt’, ‘amount’: 500}
2	{‘name’: ‘pant, ‘amount’: 400}
3	{‘name’: ‘t-shirt’, ‘amount’: 200}
4	{‘name’: ‘pollo-shirt’, ‘amount’: 300}
5	{‘name’: ‘shoe’, ‘amount’: 900}

Another database table named orders:

id	customer_id	product_id
1	2	2
2	5	4
3	4	3

4	1	1
5	5	5
6	3	2
7	5	5

Please write an SQL query to find the customer who has spent the most amount of money as per order.