Document regarding Automated Script for Security Monitoring

Introduction -

The Automated Script for Security Monitoring is a Python Script for monitoring malicious logins based on the location they login.

- An alert is raised when 2 logins are recorded for the same user from 2 locations and 2 timestamps and it is physically impossible to be at the 2 locations at those times.
- Airplanes are the fastest mode of transport available and hence the maximum velocity that a person can travel is taken as that of an airplane. This threshold is by default defined as 500 mph. This value can however be changed in the config file.
- The Velocity that a person has travelled is taken by dividing the difference in the 2 distances and timestamps recorded from the 2 logins.
- If the velocity is greater than the threshold velocity, an alert is sent including the details of the user to the email mentioned in the config file.

Running the Python Script -

The Python Script is kept in /home/gautamot/prgs under the name qelk.py in the ses-arc-data server.

Note: The version of Python in the server when the code was developed was Python 2.6. In case the python version is upgraded it is advisable to run the program with Python 2.6.

Eg : python2.6 qelk.py -c config.yaml -D -H 1

The various options that are available to run the script via command line are -

-h : for calling Help
-D : For each malicious user output, the raw IP records get dumped to a file called iprec.txt
-c : Lets the user define the config file for search in ldap system
-H : Lets the user define the last number of hours from which the records are to be retrieved
-u : Lets the user define the user UBIT from which the records are to be retrieved

Note that -c (config filename) and -H (number of hours) are required parameters while running the program and -D(output file for storing the malicious records), -h(Help) and -u (Specific username to be search) are optional parameters.

Config File -

The config file contains the details regarding the following four areas -

1. Email address to which the malicious details are to be sent.
2. Email to which errors in the program are to be sent.
3. Ldap configuration details of University at Buffalo ldap.
4. Threshold velocity beyond which alerts are sent.

Cron Job -

This script is running via a Cron Job which runs hourly. The Cron Job is present in

/etc/cron.hourly

Use crontab -e to view/edit the list of cronjobs running.

0 * * * * python2.6 /home/gautamot/prgs/qelk.py -c /home/gautamot/prgs/config.yaml -H 1

This is the record pertaining to the security monitoring script. The script runs at the start of every hour.

Script and Config File -

The Script and Config file is stored in Github in the repository named Automated Script for Security Monitoring.

Link : https://github.com/UBISO/Automated-Script-for-Security-Monitoring