

Zeenos Demo Assignment

This is simple application tool for checking the activate process that is actually running on the system.

This tool program to determine changes between period of time with user input decisions.

The tool support Windows and Linux – Ubuntu and does not support any other operating system.

Due to the differences between Linux and Ubuntu this program running 2 different versions.

In this particular tool we have 2 major modes such as: Monitor and Manual.

Monitor – play the part of the ongoing activities, he simply write to two different text log and gives us the data we need.

serviceList.txt – logs by dates that determine the running services on the system.

Status_Log.txt – the changes in the services between the last 2 logs.

Manual – examine two logs with different dates and output the changes that occurred.

Some protections:

- Root authentication for Linux version
- Authentication for admin for Windows users as follow:
UserName: MyklePerry
Password: 1@3\$5^7*9)
- Waiting random period time after giving authentication in Windows to prevent crypto-analyze attack.
- Create hidden .txt files for backups
- Wrong username or password 3 times will drop you from the system.
- Checking and validation of each input user for Buffer Over Flow attack.
- More comfort user input in Linux.
- In a case of any hack printing to console and sending to email
- In a case of changed data hack the tool will print the changed line.
- Shutting down with sys.exit() where someone hacked the logs, alert the user and write it to the Status_Log.txt for investigation.
If there is other super users that using simultaneously the tool and doing manual mode where someone inject or change some information I prefer to stop and not allowing something worst to happened.

Libraries Information:

- Time – for scheduling the algorithm and security reasons.
- Datetime – for input user and record the date and time of each log.
- Ast – for string manipulation.
- Inquirer – comfort user input in Linux version and more secure input user.
- Os – for operating system check if file exist.
- Sys – execute fatal errors such as: unexpected changes\deletion files.

- Platform – python designed to work well with Linux so platform give me the chance to determine which version I am running and due to this I design the functions.
- Stat – inside OS library, and helped me to save the date time of user changes.
- Random – preventing crypto analysis attack when entering password and username.
- Subprocess.call – helped me to execute cmd calls in windows to make the backups an hidden files.
- DiffliB – helped me to print the changes when change files hacked occurred.
- Requests – make connection with gps locator to truck the hucker.
- Smtplib – connection with gmail.com to execute email hacker track information.
- Win32Sevices – to construct the list of windows running services.

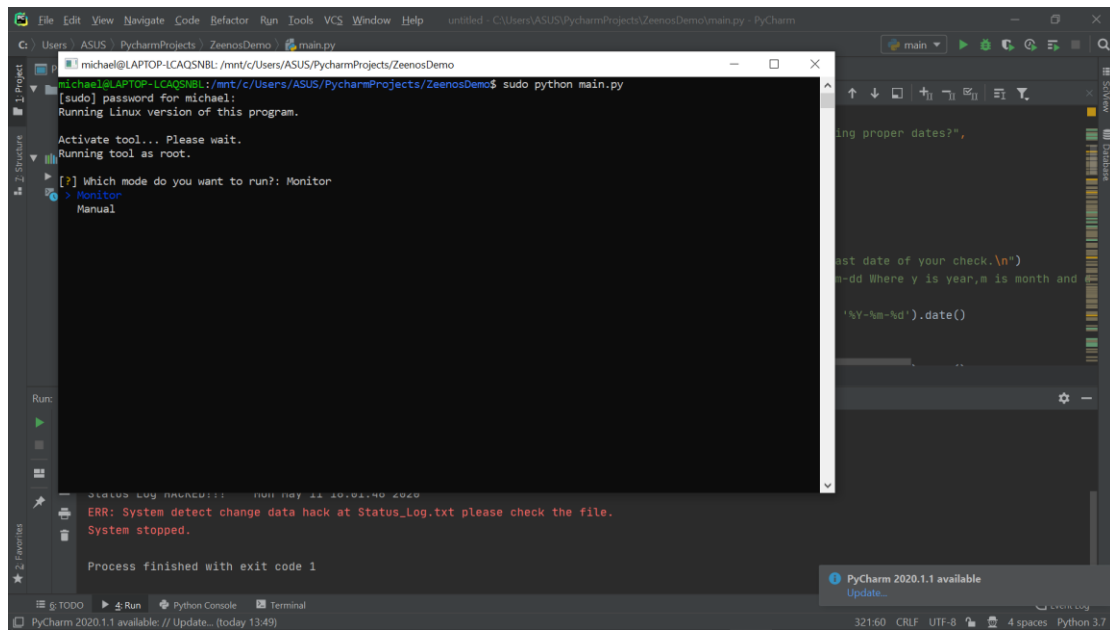
More information:

- In Linux version of this tool you have filter function that allowing you to filter which dated do you want to examine.
- In Windows it is simply print all the dates and time and you need to pick the dates from there.
- User inputs are case sensitive for avoiding silly mistakes from user.

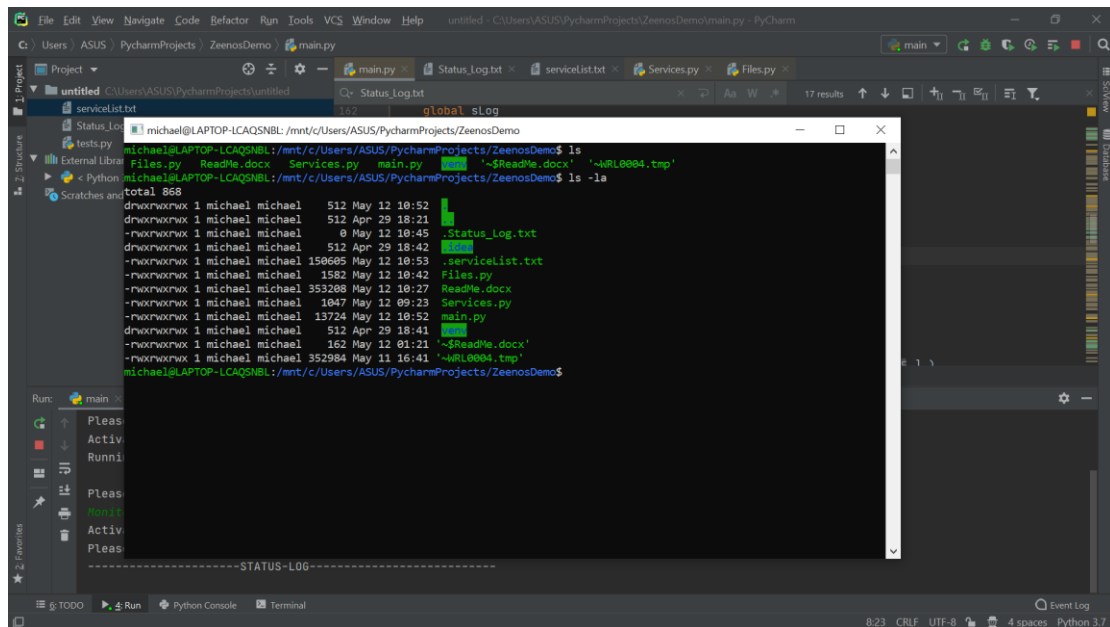
Things for improvement:

- The hacker tracker work well if the attacker run the code from his computer, The problem occurred where the attacker have ssh connection to the running computer.
- Because of lack of knowledge in python in this short time I used function and not classes, so that the code that is actually manage the whole program is bellow – this is not the prettiest program design but I prefer functionality over well designed in the case of my knowledge.
- There is some differences between Linux and Windows version because the options that python and libs give you for linux.
- The backup files is inside the running directory, it is not the optimal way to prevent attacks or restoration, it should be inside some log directory of the system.
- Authentication of Windows version can be hacked with reading the file, so I should store the authentication inside encrypted file.
- In Linux I succeed to produce root permission for preventing execute this sensitive python script.

Linux Version:



```
File Edit View Navigate Code Refactor Run Tools VCS Window Help untitled - C:\Users\ASUS\PycharmProjects\ZeenosDemo\main.py - PyCharm
C:\Users\ASUS\PycharmProjects\ZeenosDemo
main.py
[?] Which mode do you want to run?: Monitor
> Monitor
Manual
Status_Log hacked!!! run may 11 10:01:40 2020
ERR: System detect change data hack at Status_Log.txt please check the file.
System stopped.
Process finished with exit code 1
PyCharm 2020.1.1 available
Update...
```



```
File Edit View Navigate Code Refactor Run Tools VCS Window Help untitled - C:\Users\ASUS\PycharmProjects\ZeenosDemo\main.py - PyCharm
C:\Users\ASUS\PycharmProjects\ZeenosDemo
main.py
[?] Which mode do you want to run?: Monitor
> Monitor
Manual
Status_Log hacked!!! run may 11 10:01:40 2020
ERR: System detect change data hack at Status_Log.txt please check the file.
System stopped.
Process finished with exit code 1
PyCharm 2020.1.1 available
Update...
```

Windows Version:

