2023

Report on Honeypot 2

HONEYPOT EXPLANATION

PRASHANJIT BASU

INDIAN INSTITUTE OF ENGINEERING SCIENCE AND TECHNOLOGY | Shibpur

About Honeypot 2.01

With the help of watchdog library and its sub-components observer and filesystemeventhandler I have created a class which includes member functions as modified, created and deleted provided by filesystemeventhandler, if any of the event occurs it is captured and the path of the target file is printed in the terminal (can be also made to print in a log file). Alone the file system handler can't work so we use the observer library functions for e.g., Schedule a directory to assist it. We schedule the target directory (can also be schedules to the whole system but would just flood the terminal). Here a manual check is required to recognise a suspicious activity or a machine learning model can be used for such a purpose of monitoring the incoming data from the code output. Such a honeypot based on the monitoring of system files, resembles a file auditing system.

Mechanism of the Honeypot:

1. Functions for different events like modified, created and deleted.
2. Observer scheduled on an important file/directory.
3. Observer runs in a loop until user terminates the code.
4. Provides details of the changes in the file.
5. Provides path of the updated file.

Use-case and speciality:

- Such type of honeypots is actively good against dealings things inside the system for example malwares, basic ransomwares and unauthorised/suspicious manual activities.
- This honeypot mainly focuses on monitoring and detection but can also be programmed to counterattack with some touch of machine learning.
- This is one of the best ways to secure personal files even if someone tries to interfere manually with the system.
- The implementation and deployment of such honeypots is quite simple.

Disadvantages:

- The main down point to such honeypots is, detection is acquired when the attack is already initiated.
- Since the honeypot lies within the system, it can be sabotaged by a professional hacker if not implemented properly.
- Sometimes, if there is a lack of implementation of data in the honeypot software, it may consider unknown actions as malicious.