Incident response automation using playbooks for ransomware/trojan detection

Aswin Puramadathil Valsalan

Heriot-Watt University

Conclusion

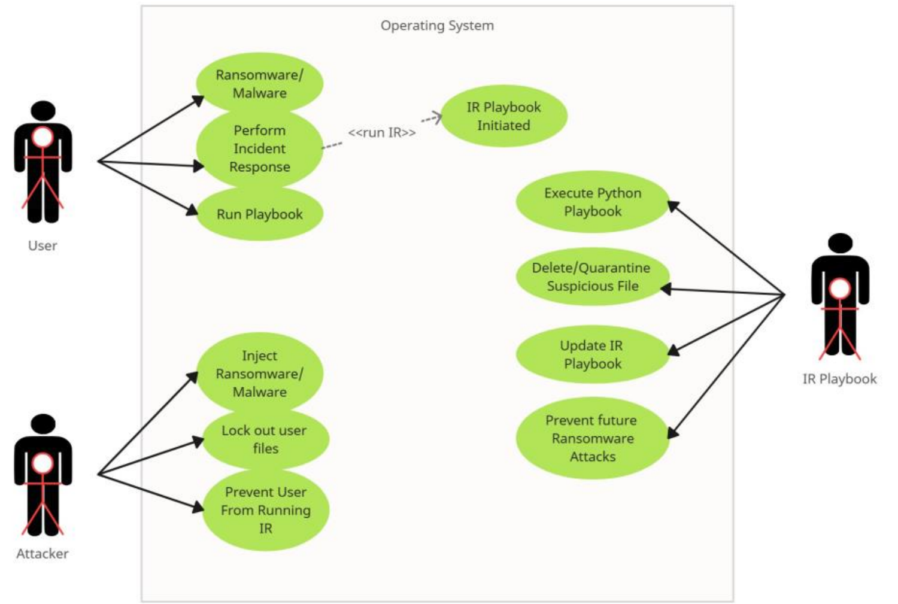
- Incident response automation signifies a critical frontier in cybersecurity.
- It requires interdisciplinary collaboration, ethical adherence, and continuous refinement.
- Overall, it safeguards digital assets and ensures trust in our interconnected world.

Introduction

A brief insight into this project's development of an Incident Response system that will ease of the work for detecting potential malware or cyber threats. Possible automation using playbooks which will speed up the detection process of suspicious files.

Methods

- A technical research based project system that showcases importance of IR.
- Agile Scrum methodology for documentation process.
- Tools like Python, Bash & YAML used for the development of the system.
- Ethical & Legal considerations taken into account.

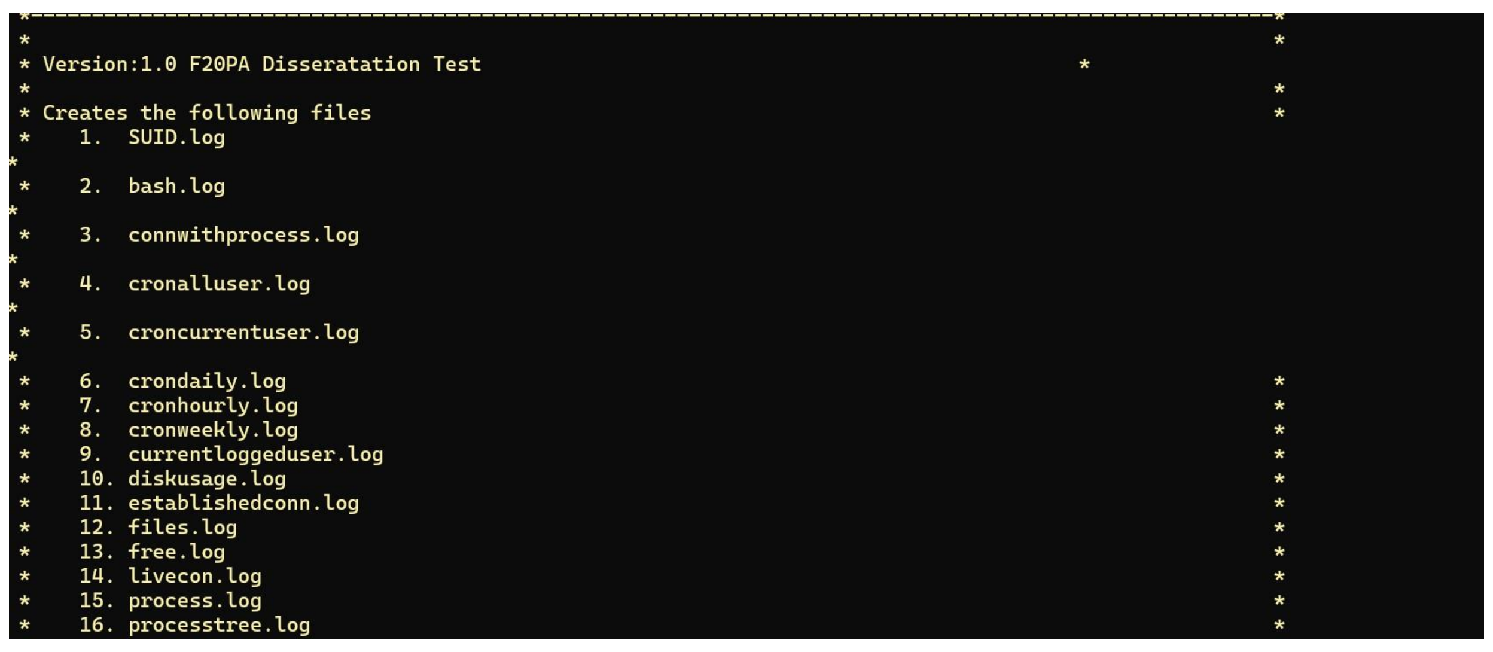


Challenges

- Ensuring system performs IR on the system that it is ran on.
- Ensuring PLES matters are taken into consideration for system architecture.
- Reducing risks of data losses/breach whilst executing the system program.
- Balancing out system performance and ease of system usage.

System Evaluation

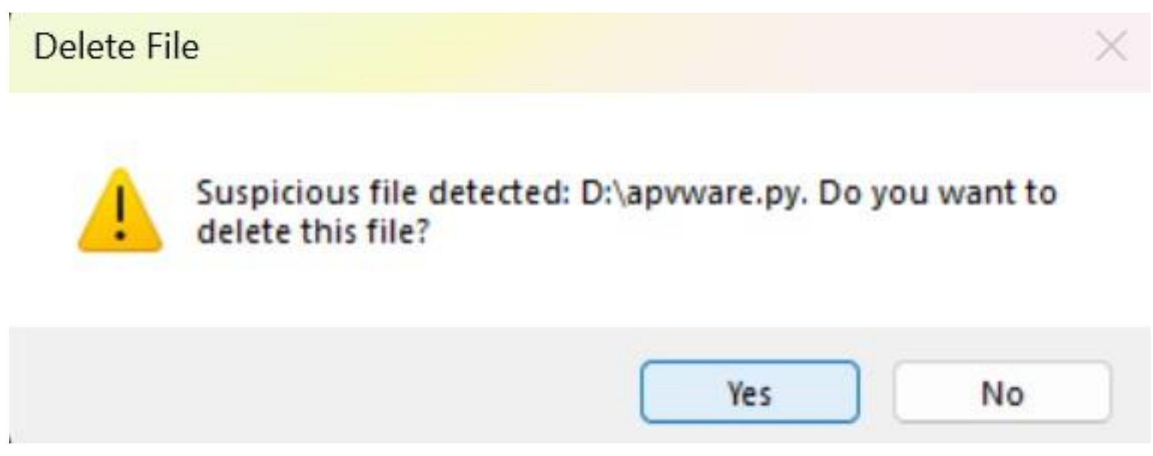
- Execution of bash file which performs a digital forensics based IR system.
- Execution of python file which performs IR on system and creates a playbook which can be used by SIEM.
- Automation of IR using YAML playbooks on Ansible Semaphore



```
*-----------------------------------------------------------------------------------------*
*                                                                                         *
* Version:1.0 F20PA Disseratation Test                                         *
*                                                                                         *
* Creates the following files                                                             *
*    1.  SUID.log
*
*    2.  bash.log
*
*    3.  connwithprocess.log
*
*    4.  cronalluser.log
*
*    5.  croncurrentuser.log
*
*    6.  crondaily.log                                                                    *
*    7.  cronhourly.log                                                                   *
*    8.  cronweekly.log                                                                   *
*    9.  currentloggeduser.log                                                            *
*    10. diskusage.log                                                                    *
*    11. establishedconn.log                                                              *
*    12. files.log                                                                        *
*    13. free.log                                                                         *
*    14. livecon.log                                                                      *
*    15. process.log                                                                      *
*    16. processtree.log                                                                  *
```

Results

- Successful IR on file systems of the user's computer without file loss or risk of potential breaches.
- Any possible errors were recorded and accounted for future works and improvement.
- Generation of a .md IR playbook .
- Potential malware files deleted/quarantined.
- User alerted via e-mail system.



Delete File

Suspicious file detected: D:\apvware.py. Do you want to delete this file?

Future Works

- Anomaly Detection: Use ML for spotting abnormal activities and deviations.
- Predictive Analytics: Prioritize response based on ML-assessed risk.
- User Behaviour Analytics: ML detects insider threats and compromised accounts.
- Adaptive Response: ML-driven responses adjust based on real-time data.

Acknowledgement

This poster was possible because of the assistance and guide from my project supervisor Dr. Fadi Alhaddadin and the university team.

References

- Goundar, Sam. (2021). Introduction to Security Incidents and Response Against Cyber Attacks. 10.1007/978-3-030-69174-5_13.
- Chaudhuri, Ayan. (2023). Network Forensics and Incident Response. International Journal of Scientific and Research Publications (IJSRP). 13. 10.29322/IJSRP.13.05.2023.p13702.

Aswin Valsalan
apv2@hw.ac.uk
H00332881