Group 8

Group Project Final Report

**Introduction**

The purpose of this project was for us to experience creating a mock cybersecurity system for a hypothetical organization. It gave us a chance to see what kind of issues might arise in a real world scenario that we will likely experience at some time in our careers, as well as giving us some experience with creating a lot of diagrams, code, and documentation we may be expected to create later in our careers as well. The organizational problem that we addressed was mostly creating scripts to monitor fake logs and resource utilization of our machines. There were significant administrative security issues in the organization that we were given as well, however all we were able to do for that was creating a document with all of our security recommendations, such as applying the principle of least privilege to their organization among other suggestions.

**Methodology**

The tools we used for this project include Python, Github, UML for multiple diagrams, and various cybersecurity best practices found in slides or lectures either from this class or relevant classes. Most of these techniques were new to us so it was a good chance to try them out in a group setting with practical applications. We approached these tasks from the perspective of cybersecurity consultants being brought in to assist our given company with hardening their organizational security. Log analysis and automation was accomplished with a mixture of using the code provided to us, past assignments, and a healthy bit of research for the things that we had never seen or written before.

**Results**

Our scripts were able to find hundreds of suspicious logs using mock system logs we found online and filters that we deemed reasonable such as anything containing the words “Failed” or “Warning”. Our diagrams also helped us to get a realistic view of how we wanted the system’s architecture to work, allowing us to effectively make the decisions we needed and have an easy view of how we wanted our final product to look. Analyzing the organization we were given was fairly straightforward, as they unfortunately had very poor security to start, so we were able to quickly recommend several immediate changes to improve their security.

Some of the detected vulnerabilities that we found included no intrusion detection systems or activity logging of any sort, free access to the entire company for any employee regardless of their role, no indication of any sort of security audit scheduling, and no company policies encouraging employees to report suspicious activity. In our scenario, all of these vulnerabilities helped contribute to months of packet leaks with no knowledge from the company itself. We felt that our automation was decently efficient, opting to scan about once every hour for suspicious logs to help lower resource demands for the system and reduce overhead.

**Challenges and Solutions**

We faced several challenges throughout this project, although most were able to be easily resolved within a matter of hours or days. Our first major obstacle was trying to get our script to properly analyze the logs that we provided. We were running into issues with the logs even being readable until we manually downloaded them on our machine, and then we struggled to filter them for suspicious activity until we realized we could use variable[‘header’].str.contains(‘filter’) to accurately locate any logs with “failed” or “warning” filters. Our second real obstacle was setting up the automated emails for suspicious resource utilization of our machines. We really struggled with being able to actually send the email as gmail accounts have security policies restricting automated emailing. We found our solution to this problem by talking to our classmates and learning that we could register an email for free using a third party service known as sendgrid. Once we set up a new gmail account and linked it with sendgrid using an app key we were able to easily send the emails whenever computer resource usage was suspiciously high.

**Recommendations**

Our recommendations for improvements or additional features include many organizational or physical changes, such as multifactor authentication for all users, increasing what would be considered suspicious logs, and possibly decreasing the time between scans if resources allow.

**Conclusion**

Overall, this project was a great way for us to experience what might be awaiting us in our future careers when working as part of a team, as well as what some of the work could look like. We learned a lot about collaboration and documentation we were not expecting when beginning the project, as well as the obvious lessons we learned about python scripts, log analysis, and automating different services and actions that would be tedious to perform manually. This project also required some of us to create their first github accounts, and made all of us comfortable with git commands and repositories.

**Appendices**

Github Link: <https://github.com/Dfurey/130-Group-Project>

UML Activity Diagram:

**A diagram of a process

Description automatically generated**

Use Case Diagram:

A diagram of a person's account

Description automatically generated

Sample Script:

A screen shot of a computer program

Description automatically generated

Sample email alert:

A screenshot of a computer error message

Description automatically generated