Name: Niloofar Thaha
Student ID:THA21540701
Course: Bsc.Cyber Security

Reflection on the Security Monitoring with Graylog SIEM Project

Completing the Security Monitoring with Graylog SIEM project for Catnip Games International incredibly improved me as it pushed my technical, as well as problem-solving, skills to unprecedented new heights. As a beginner in cybersecurity and log management, I gained hands-on exposure to SIEM tools, Elasticsearch, MongoDB, and also automation workflows throughout this project. The adventure included many challenges and each singular obstacle became a valuable learning opportunity.

1. Deployment Hurdles

Issues, for example, version mismatches, configuration errors, and system instability, made the initial deployment phase especially daunting. An exacting attention to each detail was required when ensuring that Graylog, Elasticsearch, and MongoDB were completely compatible. For example, I, in effect, resolved the Elasticsearch authentication issue by duly updating Graylog's configuration file with the correct credentials, and this, effectively, taught me that dependency management and security configurations are of importance.

2. Alerting Mechanism Failures

Establishing alerts proved to be quite a particular challenge. Graylog did not, in fact, initially trigger any notifications, despite the rules being set up as they were. Troubleshooting revealed an array of misconfigured streams and a number of indentation errors within the Filebeat YAML file. The criticality of precision in configuration files was highlighted when fixing these issues, as was the value of detailed log analysis for debugging.

3. Email Notification Issues

One unresolved challenge was the inconsistency with email notifications. The SMTP settings had been configured and also tested over and over again. However, the alerts did not always manage to reach the inbox. It did highlight certain gaps with regard to my own comprehension of email server configurations, so additional further learning is indeed needed specifically in this particular area.

1. Performance Optimization

Ensuring the system could handle 10,000 events per second (EPS) required fine-tuning memory allocation and query execution. Load testing revealed bottlenecks, which we addressed by optimizing Elasticsearch indexing and adjusting Graylog's journal size. This experience emphasized the importance of scalability planning in real-world deployments.

Successes and Achievements

- Centralized Log Management: Successfully set up log collection from diverse sources, including game servers, network devices, and authentication systems.
- Real-Time Monitoring: Developed dashboards for authentication monitoring, DDoS detection, and network security, providing actionable insights for the SOC team.
- Automation: Implemented scripts for automated incident response, such as blocking malicious IPs and generating weekly security reports.
- Collaboration: Worked effectively as a team, with each member contributing specialized skills to overcome challenges and achieve project goals.

Lessons Learned

1. Debugging is Critical: System logs (e.g., /var/log/graylog-server/server.log) were invaluable for diagnosing issues. Learning to parse and interpret these logs was a game-changer.
2. Attention to Detail: A single misconfiguration or typo could break the entire system. This project reinforced the need for meticulousness in IT deployments.
3. Persistence Pays Off: Despite setbacks, perseverance and collaborative problem-solving led to successful outcomes.
4. Documentation Matters: Maintaining detailed records of configurations, errors, and resolutions streamlined troubleshooting and knowledge sharing.

Areas for Improvement

- Email Notifications: I aim to deepen my understanding of SMTP configurations to resolve the inconsistency in alert deliveries.
- Advanced Correlation Rules: Exploring more sophisticated rule designs to reduce false positives and enhance threat detection.
- Scalability: Further optimizing the system to handle even higher EPS loads for enterprise-grade environments.

Final Thoughts

This project was a cornerstone in my cybersecurity journey. It transformed theoretical knowledge into practical expertise and demonstrated the complexities of real-world SIEM implementations. While not everything went perfectly, the struggles and triumphs have left me more confident and motivated to tackle future challenges in security operations.

Note to Evaluator:

"I acknowledge that some components, like email notifications, were not fully perfected. However, the process of troubleshooting and documenting these challenges has been invaluable. As a beginner, I am proud of what I accomplished and excited to continue refining my skills in SIEM technologies and cybersecurity."

This experience has proved that how my passion for cybersecurity, and I look forward to applying these lessons in future projects to build even more robust and efficient systems.