GWDG
AG Computing
Trevor Khwam Tabougua

Exercise 1 / October 18, 2023
HPC System Administration / WiSe 2022/23
0 Minutes Total

Exercise Introduction

Contents

Task 1: Security concerns of an FTP server (0 min)

In the original FTP model, security measures were not included. As a result, there are many significant security problems. Here are two websites you will some vulnerabilities and solutions.

- FTP Security Best Practices – FTP Vulnerabilities and Mitigation
- Three significant risks of FTP use and how to overcome them

Task 2: Service catalog for Performance Data Dashboards and Security (0 min)

- **InfluxDB Token for Grafana Integration:**
  - **Risk:** Using an InfluxDB user token for writing data from Grafana can pose a security risk. If this token is compromised, an attacker may gain unauthorized write access to the InfluxDB database.
  - **Solution:** Implement secure management of tokens. Create a dedicated token with the least necessary privileges for Grafana to write data. Rotate tokens periodically and follow best practices for token security such as implementating token revocation, using short-lived tokens, securing token transmission, token encryption, etc.
- **Single User in InfluxDB:**
  - **Risk:** Having only one user in InfluxDB, especially with administrator rights, presents significant security risks. If the user's credentials are stolen or misused, it could lead to a severe system compromise. Lack of role-based access control limits security.
  - **Solution:** Create multiple user accounts with the principle of least privilege. Implement role-based access control, restricting access to specific users based on roles and permissions. Avoid using administrator-level accounts for routine tasks.
- **Granular Data Source Permissions in Grafana:**
  - **Risk:** The open-source version of Grafana lacks granular data source permission settings, meaning all users with access to a data source can view all the data within it. This can expose sensitive information to unauthorized users.
  - **Solution:** If possible, consider upgrading to the enterprise version of Grafana to access advanced permission settings. In the absence of enterprise Grafana, implement measures to secure data at the

data source level. This might involve isolating sensitive data sources or creating separate instances for critical data.

- **Securing Grafana:**
  - **Risk:** Grafana may not be adequately secured, potentially exposing dashboards and data. This could lead to unauthorized access or data leaks.
  - **Solution:** Secure Grafana by implementing measures such as an SSH tunnel, a reverse proxy, or using HTTPS to encrypt traffic. Implement authentication and access controls within Grafana to ensure only authorized users can access the dashboards.