Task 2

Security Alert Monitoring & Incident Response Simulation

Table of Contents

1. Introduction

In this activity, we focused on monitoring and analyzing security logs using **Splunk**, a widely adopted SIEM (Security Information and Event Management) solution. The primary objective was to generate, collect, and analyze system and authentication logs in order to detect security incidents such as failed logins, brute-force attempts, unauthorized access, and application errors.

Splunk enables security professionals to handle massive volumes of raw log data and transform them into meaningful insights using queries, dashboards, and visualizations. By indexing and correlating log data from different sources, Splunk helps identify abnormal activities that would otherwise go unnoticed.

In enterprise environments, SIEM platforms like Splunk play a critical role in:

- **Threat Detection:** Identifying suspicious activities such as brute-force attempts, privilege misuse, or unusual login behavior.
- **Incident Response:** Assisting analysts with actionable intelligence to trace attacks and mitigate them effectively.
- **Compliance Monitoring:** Maintaining logs to demonstrate adherence to security standards, regulations, and policies.
- **Operational Visibility:** Offering administrators centralized visibility into system health and overall security posture.
- **Proactive Defense:** Automating alerts and predefined responses to stop threats before they escalate.

This hands-on exercise provided practical exposure to how SIEM solutions are deployed, how log data is ingested and analyzed, and how security incidents can be simulated and investigated. By performing each step in Splunk, we not only gained experience in log analysis but also strengthened our understanding of how attackers leave traces and how defenders can use these traces for early detection and incident response.

2. Generating Logs

Authentication Logs (SSH)

1. **Installed SSH server:**

- sudo apt install -y openssh-server
- sudo systemctl enable --now ssh

2. **Created failed login attempts (simulating brute force):**

- for i in {1..5}; do ssh wronguser@127.0.0.1 -o ConnectTimeout=2 || true; done

3. **Created a successful login:**

- ssh kali@127.0.0.1
- exit

4. **Exported SSH-related logs:**

- sudo journalctl -u ssh --no-pager > ~/future_interns/logs/auth.log
- sudo journalctl -b --no-pager > ~/future_interns/logs/syslog.log

3. Uploading Logs to Splunk

1. Opened Splunk Web → Settings → Add Data → Upload.
2. Uploaded auth.log, syslog.log.

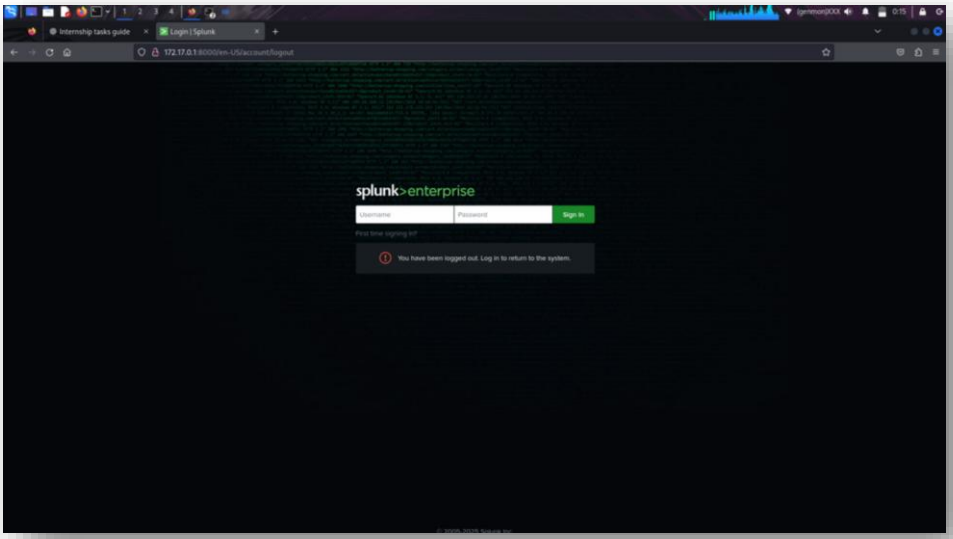

Figure 1: Splunk Login Page

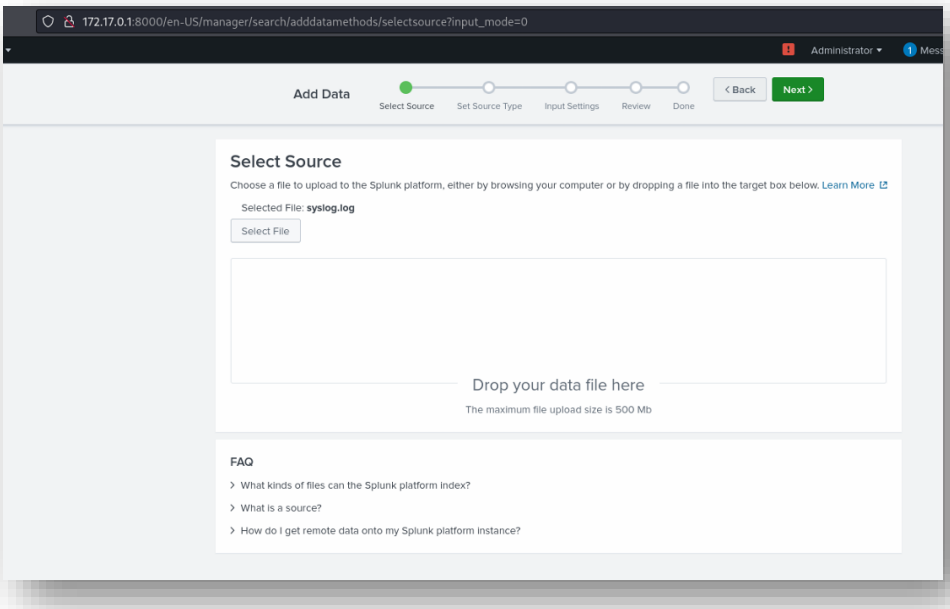

Figure 2: Uploading Logs

3. Assigned Source Types: a. syslog → auth.log and syslog.log

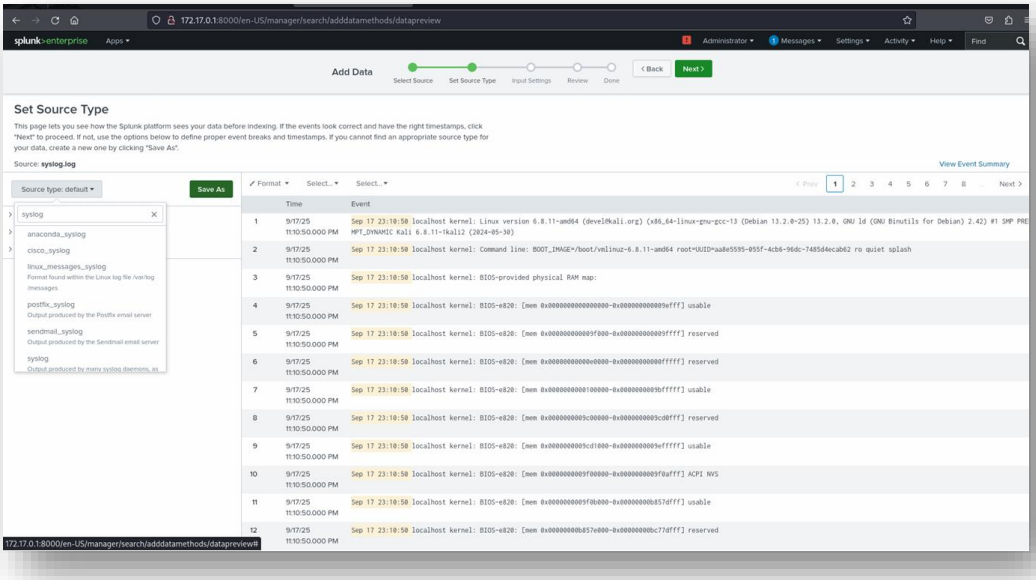

Figure 3: Setting Source Type

4. Indexed all logs under main.

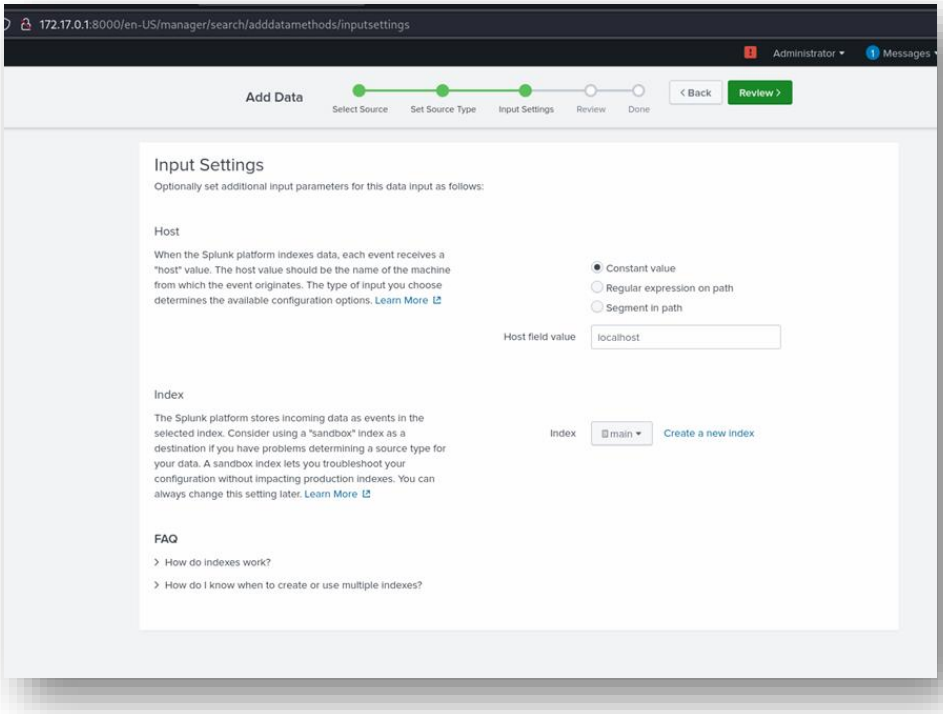

Figure 4: Indexing Logs

4. Analysis Logs in Splunk

1. **Show all events**
   index=main | head 20

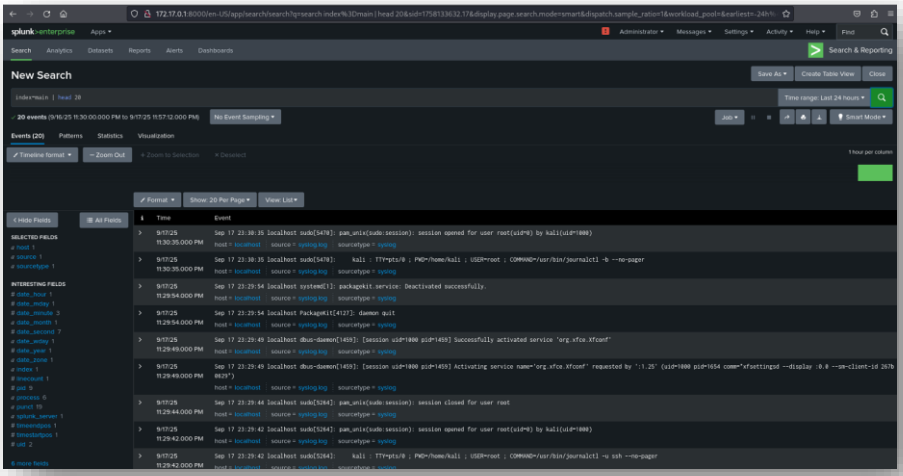

Figure 5: Top 20 Logs

2. **Detect Failed SSH Logins**
   index=main "Failed password" OR "authentication failure"

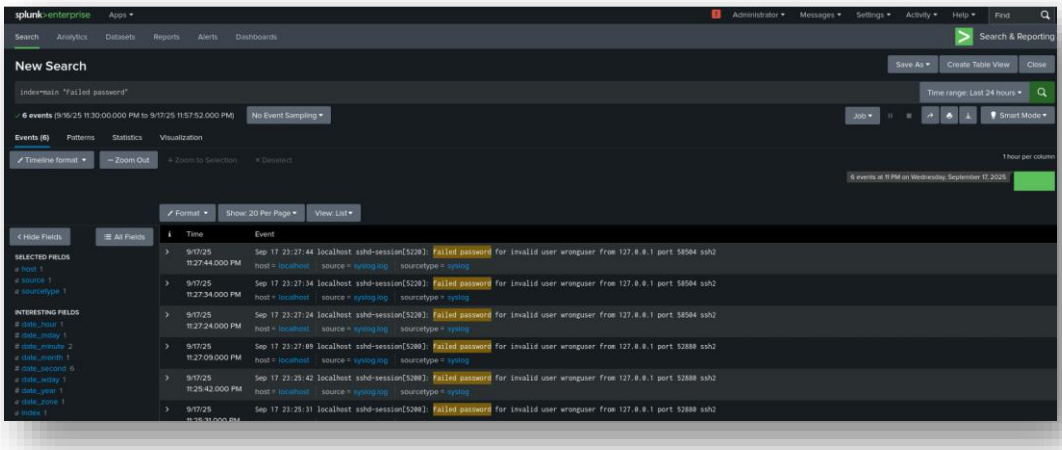

Figure 6: Logs with Failed Passwords

5. Findings

Event	Splunk Query	Impact	Mitigation
Failed SSH logins (Brute Force)	index=main "Failed password"	Attackers attempting to brute force passwords	Enable account lockouts, use SSH key authentication, rate limiting
Successful SSH login	index=main "Accepted password"	Valid login (verify if authorized)	Monitor authorized logins, use MFA
Unauthorized Web Access	index=main	Attempted access to restricted resources	Proper access control, WAF, strict role-based permissions

6. Remediation

1. Enforce robust passwords & account lockout policies.
2. Implement Multi-Factor Authentication (MFA).
3. Limit SSH to allowed IP ranges. Monitor authorized logins, use MFA Proper access control, WAF, strict role-based permissions
4. Deploy a Web Application Firewall (WAF) for unauthorized request filtering.
5. Centralize log monitoring & enable automated alerts for repeated failures.

7. Conclusion

We learned how to do the following through this exercise:

- Install and set up Splunk as a SIEM solution.
- Create and gather authentication, system, and web server logs.
- Employ Splunk SPL queries to identify failed logins, brute force attempts, and unauthorized access.
- Develop alerts and reports to continuously monitor suspicious activity.
- Learn the significance of log analysis for incident detection and response.

This hands-on exercise reinforced how SIEM offerings like Splunk turn raw log data into actionable security intelligence, which is essential for real-world threat prevention and monitoring. Through the simulation of brute force attempts, invalid requests, and legitimate logins, we saw how logs expose patterns that point to threats, and how Splunk facilitates automation.

In an enterprise context, having the capability to centralize and analyze logs enables security teams to:

- identify and categorize incidents rapidly.
- Promptly take remediation measures prior to damage.
- Enhance compliance posture by maintaining extensive audit trails.
- Enhance the overall security maturity of the organization through incident-based learning.

Overall, this exercise not only showcased Splunk's technical capabilities but reinforced the general significance of log analysis within an effective overall cybersecurity approach. It underscored how visibility, detection, and response are interdependent pillars of a strong defense system.

8. References

1) https://docs.splunk.com/
2) https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html
3) https://access.redhat.com/solutions/2112