International Journal of Science, Strategic Management and Technology
Volume **02** Issue **03** March-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Data Leakage Detection and Prevention System

HARI HARAN S, Student, 231ct110@drngpasc.ac.in

Dr. B. Leelavathi, MCA., M.Phil., Ph.D. Professor, leelavathi@drngpasc.ac.in Department of Computer Technology, Dr. N. G. P. Arts and Science College, Coimbatore, Tamil Nadu, India.

https://doi.org/10.55041/ijsmt.v2i3.311

Cite this Article: S, H. H. (2026). Data Leakage Detection and Prevention System. International Journal of Science, Strategic Management and Technology, *02*(03). https://doi.org/10.55041/ijsmt.v2i3.311

ABSTRACT:

HONEYPOT BASED Security Operations Center (SOC) is developed to address the rising security threats faced by modern web applications, particularly brute force attacks that attempt to gain unauthorized access through repeated login attempts. Detecting such attacks at an early stage is essential to prevent data breaches, service disruption, and unauthorized system access.

The system deploys a honeypot website using Apache2 on Ubuntu Linux to simulate a realistic web environment that attracts malicious login activity. Multiple login attempts are generated through the Ubuntu Terminal to produce detailed log data capturing attacker behavior. These logs are forwarded to Splunk, which functions as the Security Operations Center (SOC) platform for collecting, indexing, and analyzing security events. Splunk enables the identification of attack patterns, tracking of source IP addresses, and generation of alerts when suspicious behavior exceeds predefined thresholds.

The implementation environment includes Windows 11 as the host system, Oracle VirtualBox for virtualization, Ubuntu Linux as the guest operating system, Apache2 as the web server, and Splunk as the SOC analysis tool. Integration of Apache log files with Splunk supports automated detection and response, including real-time blocking of attacker IP addresses and associated services to reduce further malicious activity.

The system also supports operational analytics by examining normal website traffic patterns such as peak login times, assisting in better traffic management and security planning. By combining honeypot technology with SOC monitoring, the system strengthens threat visibility, improves incident response, and enhances overall web security. This approach provides practical insight into log analysis, alert configuration, and proactive cybersecurity monitoring within a controlled environment.

INTRODUCTION:

A Security Operations Center (SOC) plays an important role in protecting systems and networks from cyber threats by continuously monitoring and analyzing security-related data. One of the most common attacks faced by web applications is the brute force attack, where attackers repeatedly attempt to log in using different credentials. If such attacks are not detected in time, they can lead to unauthorized access, data loss, or service disruption. This project focuses on understanding these attacks and demonstrating how SOC tools can be used to detect and respond to them effectively.

In this project, a honeypot-based approach is used to simulate a real-world attack scenario. A honeypot website is created

using Apache on Ubuntu Linux to attract repeated login attempts. The attacks are generated locally using the Ubuntu terminal, ensuring that the system remains secure and under control. All access attempts are logged automatically by the web server. These logs are then analyzed using Splunk, which helps in identifying attack patterns, generating alerts, and monitoring website traffic behavior. The project provides hands-on experience with SOC concepts such as log monitoring, alerting, and incident response.

EXISTING SYSTEM:

In many traditional web systems, security monitoring is limited to basic logging without advanced analysis. Although web servers generate access logs, these logs are often not actively monitored or analyzed in real time. As a result, brute force attacks may continue for a long period without being detected. Administrators usually have to manually inspect log files, which is time- consuming and inefficient. This approach does not provide timely alerts or immediate response mechanisms

Additionally, existing systems lack the ability to analyze traffic patterns such as peak login times or abnormal access behavior. Without proper SOC tools, it becomes difficult to distinguish between legitimate users and malicious attackers. This limitation increases security risks and reduces the overall effectiveness of system protection.

1. PROPOSED SYSTEM

The proposed system introduces a honeypot-based SOC model to overcome the limitations of the existing system. A honeypot website is deployed using an Apache web server on Ubuntu Linux to capture brute force login attempts. The attacks are simulated using repeated login attempts from the Ubuntu terminal itself, ensuring a safe and controlled environment.

All generated logs are forwarded to Splunk, which acts as the SOC analysis tool. Splunk is used to detect brute force patterns, generate security alerts, and analyze high peak login times. Based on the analysis, the attacker IP address and related services are blocked using firewall rules. This proposed system provides real-time monitoring, improved visibility, and effective incident response, closely simulating real-world SOC operations

Advantages of Proposed System

1. **Real-Time Threat Detection**

By integrating Splunk with Apache HTTP Server logs, the system detects brute force login attempts immediately instead of relying on manual log checking.

2. Centralized Log Monitoring

All web server logs are collected and analyzed in a single SOC platform, improving visibility and making security monitoring more efficient.

Automated Alert Generation

The system generates alerts when login attempts exceed predefined thresholds, reducing the need for continuous manual supervision.

3. Effective Attack Mitigation

Suspicious IP addresses can be blocked using firewall or Apache configuration rules, preventing further unauthorized access attempts.

4. Practical SOC Simulation in a Safe Environment

The honeypot deployed on Ubuntu using Oracle VM VirtualBox provides hands-on experience with real-world SOC

operations without risking a live production system.

PROPOSED MODEL:

Algorithms for Methodology:

1. Data Collection Algorithm

The system collects web server access logs generated by the honeypot website. Each login attempt is automatically recorded with details such as IP address time stamp request method and response status. These logs act as the primary input data for further security analysis.

2. Log Processing Algorithm

The collected log files are parsed and structured inside the SOC platform. Important fields such as client IP request count and time intervals are extracted. The data is organized in a searchable format to support efficient monitoring and detection.

3. Brute Force Detection Algorithm

The system checks the number of login attempts made by a single IP address within a specific time window. If the request count exceeds a predefined threshold the activity is marked as suspicious. This logic
helps in identifying brute force attack patterns.

4. Alert Generation Algorithm

When suspicious behavior is detected the system automatically triggers an alert. The alert contains details such as attacker IP address number of attempts and time of occurrence. This ensures timely notification for security monitoring and response.

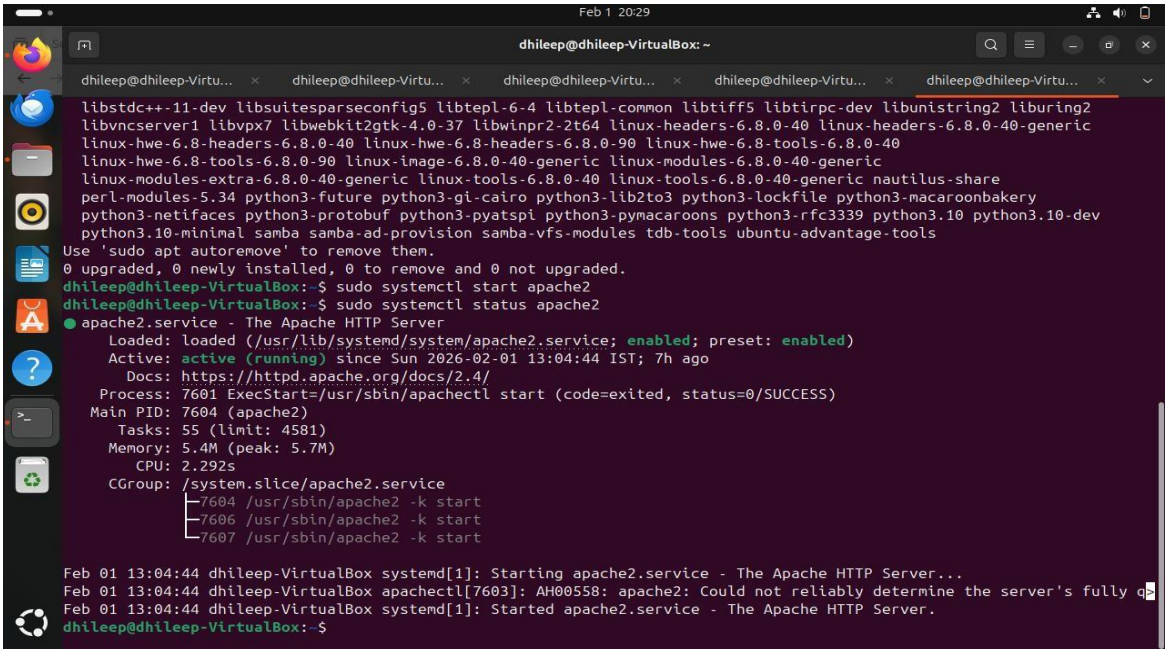
5. Mitigation and Response Algorithm

After confirmation of malicious activity the identified IP address is blocked using firewall rules. The system verifies that access from the blocked IP is denied successfully. This completes the cycle of detection analysis alerting and response in the SOC environment.

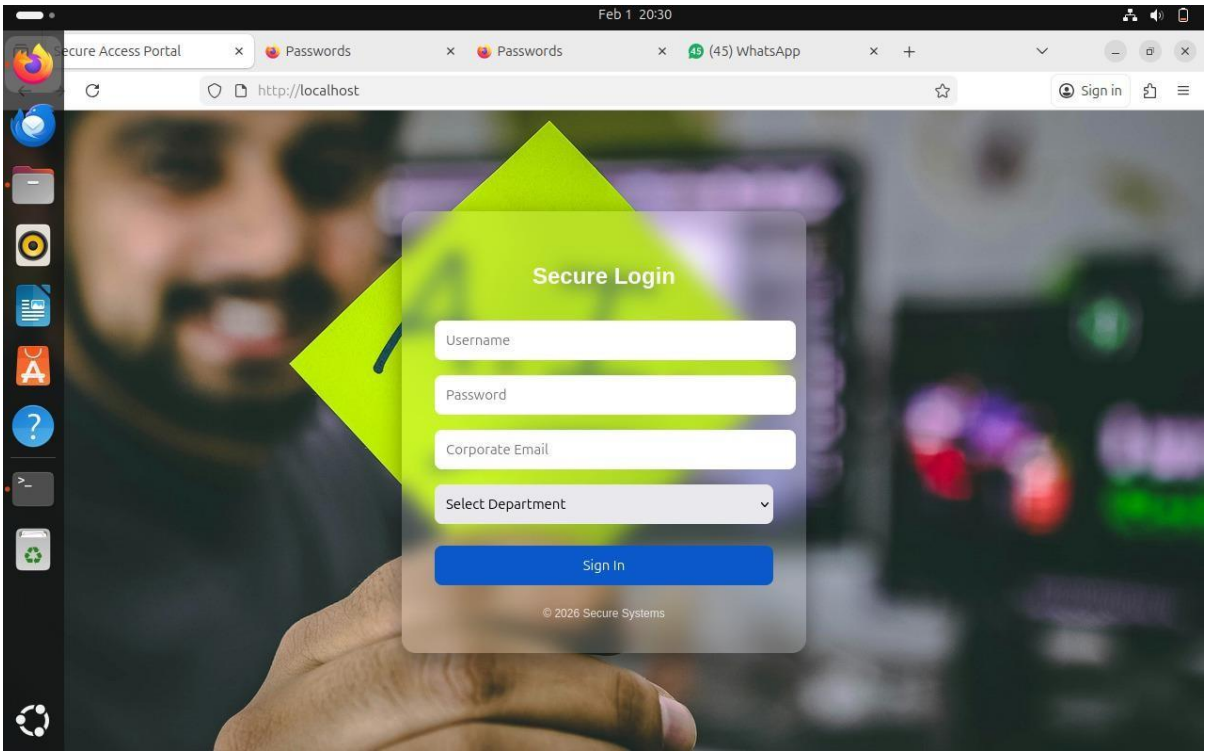
International Journal of Science, Strategic Management and Technology
Volume **02** Issue **03** March-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

EXPERIMENTAL RESULTS:

APACHE ACTIVATED ON LIVE

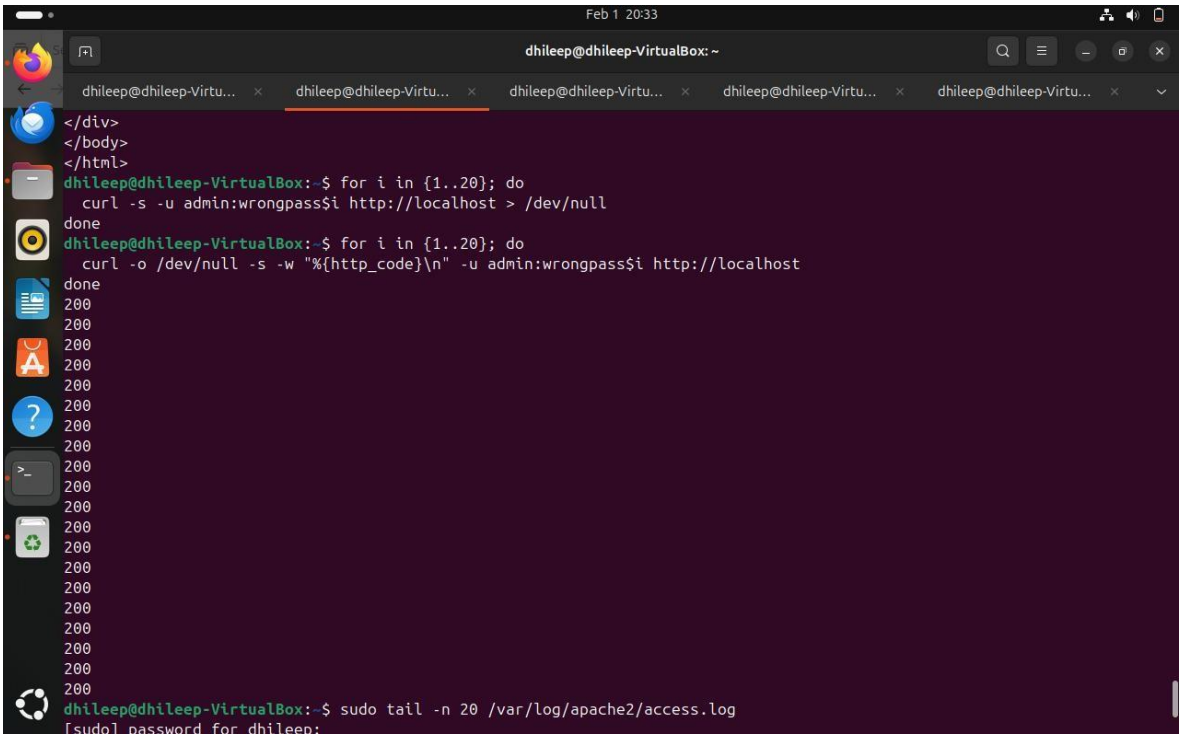


HONEYPOT WEBSITE FOR TRAP ATTACKS

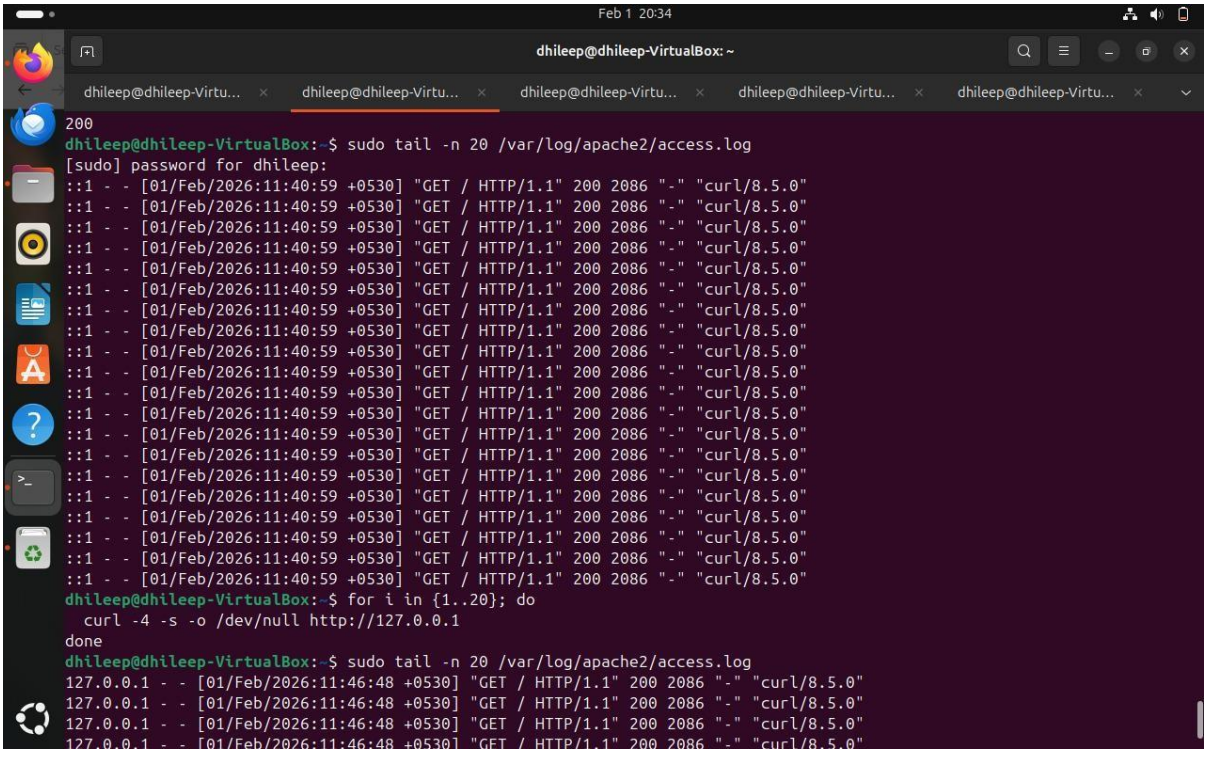


International Journal of Science, Strategic Management and Technology
Volume **02** Issue **03** March-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

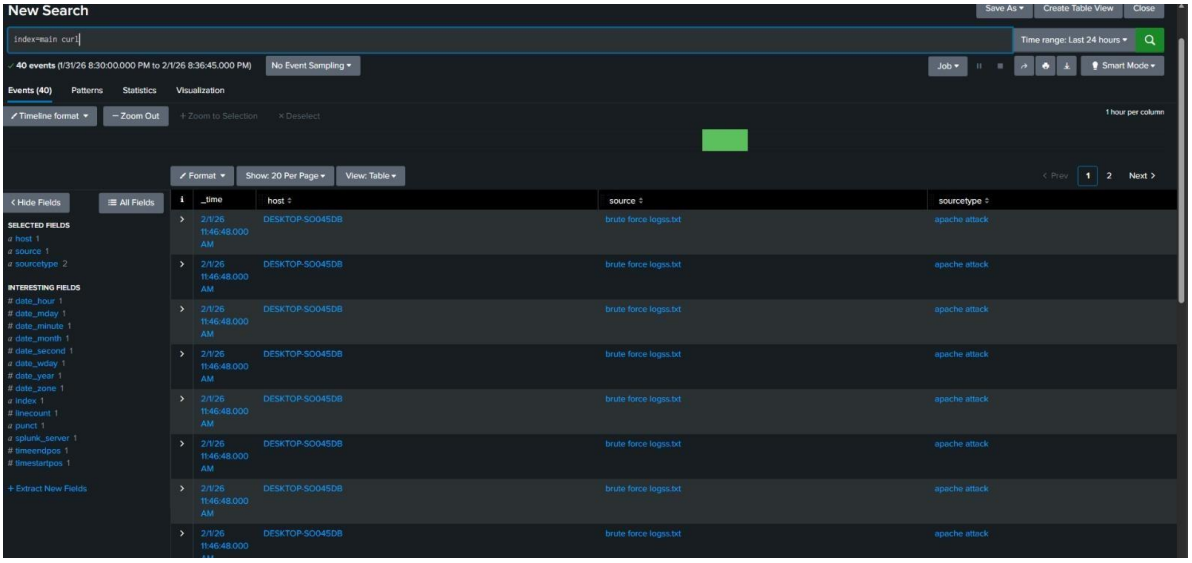
ATTACKS



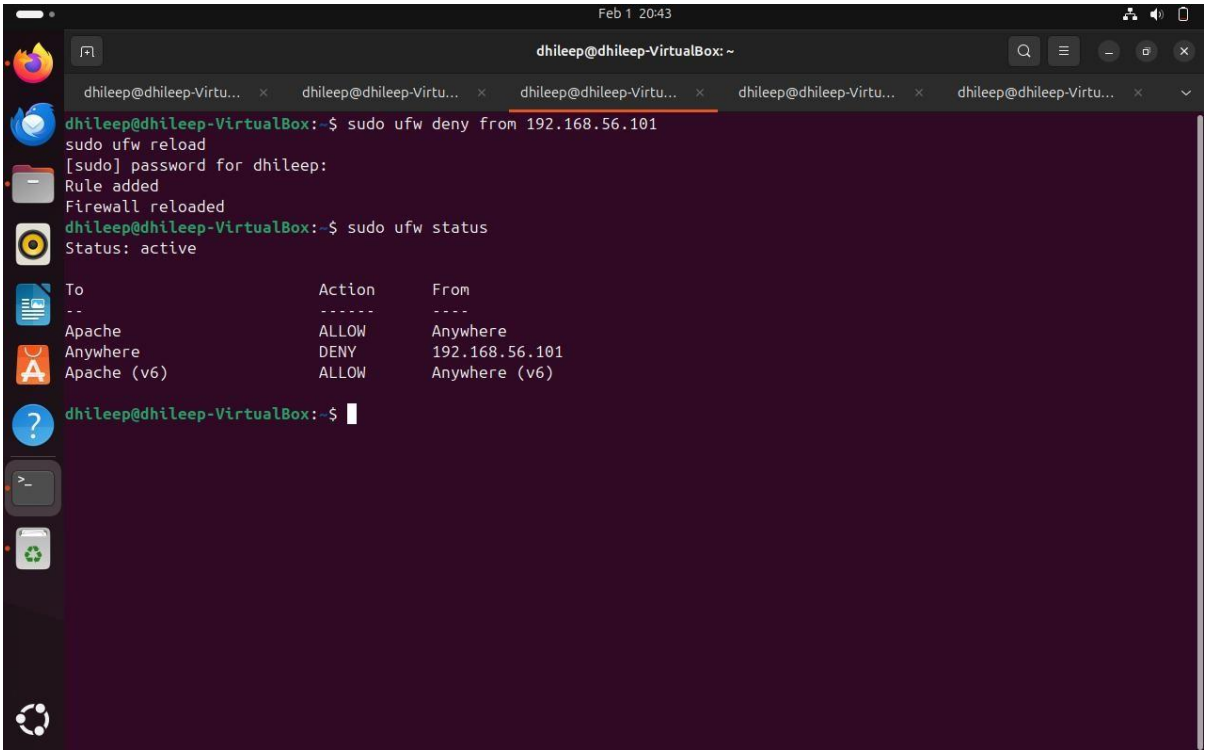
LOG FILES



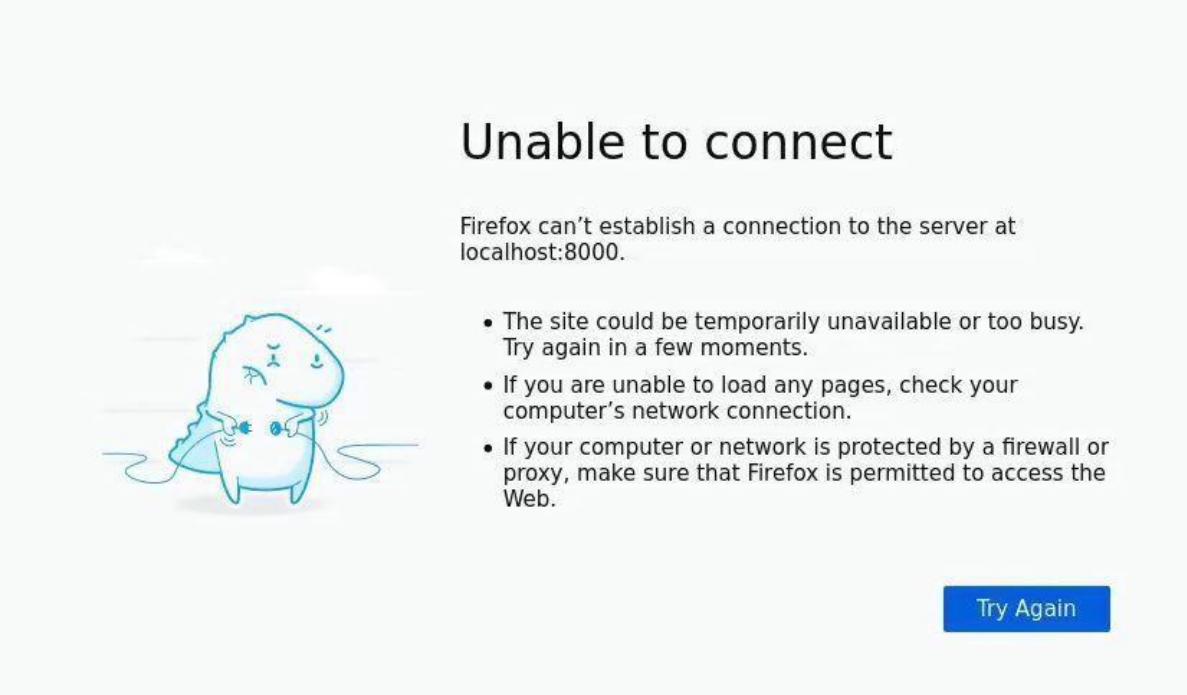
SPLUNK ANALYSIS



BLOCKING IP



SERVICE BLOCKED



CONCLUSION

The honeypot-based SOC project successfully demonstrates how brute force login attempts can be monitored and analyzed using a combination of web server logging and SOC tools. By deploying a honeypot website and integrating it with Splunk, the system provides real-time visibility into attack behavior and normal traffic patterns such as high peak login times. The project highlights the importance of centralized log analysis, alerting, and timely response in cybersecurity. The implementation offers practical exposure to SOC operations and reinforces the effectiveness of honeypots as a valuable security monitoring tool.

FUTURE WORK

Future enhancements to this project may include deploying the honeypot in a live network environment to capture real-world attack data, integrating automated alert notifications through email or messaging services, and implementing automated response mechanisms to block attackers dynamically. Additional analysis features such as long-term trend analysis, user behavior analytics, and integration with other security tools can further improve the system. These enhancements would make the project more scalable and closer to a real-world enterprise SOC implementation.

REFERENCE

1. Lance Spitzner, Honeypots: Tracking Hackers, Addison-Wesley Professional — Classic book explaining honeypots, including web-based honeypots and attacker analysis.

2. Chris Sanders, Practical Web Penetration Testing, Wiley — Covers web application attacks, logging, and monitoring techniques useful for web honeypots.

3. Mukesh Choudhary, Mastering Honeypots: Art of Deception for Cybersecurity Defense, BPB Publications — Practical guide on deploying and managing web-based honeypots integrated with SOCs.

4. Chee Keong Ng, Lei Pan & Yang Xiang, Honeypot Frameworks and Their Applications: A New Framework, Springer — Includes framework design for web honeypots and analysis workflows.

5. Alfred Basta & Nadine Basta, Open Source Security Operations Center (SOC): A Complete Guide — Explains SOC monitoring, log analysis, and response mechanisms relevant for web-based honeypots.

REFERENCE WEBSITES

1. OWASP Web Application Security Testing Guide — Guidelines for testing web apps, attacks, and monitoring which is useful for web honeypots.
https://owasp.org/www-project-web-security-testing-guide/

2. The Honeynet Project – Web Honeypot Resources — Tools, research, and case studies specifically for web-based honeypots.
https://www.honeynet.org/projects/

3. Splunk – Monitoring Web-based Honeypots — Blog explaining how to log, analyze, and visualize web attack data in SOC dashboards. https://www.splunk.com/en_us/blog/learn/cybersecurity-honeypots.html

4. GitHub – HoneyWeb Project — Open-source web honeypot examples and scripts for research and SOC integration. https://github.com/search?q=web+honeypot