ASSESS IDENTIFIED SECURITY BREACHES AND DEVELOP RECOMMENDATIONS FOR THEIR PREVENTION

Narzikulova Sevinch Aktamovna
Faculty of Computer Engineering
Student of Information Systems and Technologies

Annotation: *This thesis project is devoted to the study of methods for detecting security breaches through the analysis of log files in information systems. The research examines the role of log files in identifying unauthorized access, brute-force attacks, repeated authentication failures, suspicious IP addresses, and attempts to access privileged accounts. Particular attention is paid to the analysis of SSH authentication logs in Ubuntu Server, including “Failed password” and “Accepted password” events recorded in the /var/log/auth.log file.*

Keywords*: log files, log analysis, information security, cybersecurity, security breach, SSH, authentication, brute-force attack, unauthorized access, failed password, accepted password, root account, Fail2ban, firewall, SSH keys, IP address, SIEM, security monitoring, Linux, Ubuntu Server.*

In the process of detecting security breaches by analyzing log files, simply finding suspicious events is not enough. It is important to assess the identified events for the level of risk, determine their impact on the system, and develop specific recommendations for the prevention of such cases in the future. Therefore, this paragraph summarizes the results of the practical analysis conducted in paragraph 2.2, assesses the identified security breaches and focuses on protective measures to mitigate them.

During the practical experiment, SSH service was run on Ubuntu Server system, and attempts were made to connect to the server from another Linux device. Entering the wrong passwords resulted in "Failed password" entries in the /var/log/auth.log file. Later the correct password was entered and the entry "Accepted password" was noted. These records served as the basis for assessing the security incidents that occurred during the authentication process.

Assess identified security incidents. As a result of the log analysis, several important security incidents were identified. Their main ones are failed authentication attempts, multiple login attempts from a single IP address, possible unauthorized connection via SSH, and time-based brute-force attack symptoms. These events have varying degrees of impact on system security.

Table 1.1

Identified security breaches and their assessment

No	Detected Event	Log character	Level of risk	Possible outcome
1	Failed authentication attempts	Failed password	Medium	Password guessing attempts, possibility of unauthorized access to account
2	Multiple login attempts from the same IP address	Duplicate Failed password entries	High	Could a brute-force attack be carried out and credential retrieval

3	Successful login after unsuccessful attempts	Failed password → Accepted password	High	Account compromise and possible unauthorized access
4	Administrator (root) log in	Failed password for root	High	Getting a graced account and taking full control over the system
5	Repeated retries at a certain time interval	Logged login attempts every 5–10 minutes	Medium	Time-based brute-force or automated attack activity
6	Connections from unknown IP address	Unknown IP address or geographic source	Medium	Suspicious External Connections and Potential Unauthorized Access

From the table, you can see that the most dangerous cases are instances of multiple authentication attempts from the same IP address, an attack on the root account, and a successful login logged-in after an unsuccessful attempt. Such cases indicate that there is a risk of unauthorized entry into the system.

Brute-force attack assessment. Brute-force attacks are one of the most common types of attacks based on password guessing. In log analysis, such attacks are usually detected by the appearance of "Failed password" entries, often many times in a short period of time. If these recordings were made from the same IP address, it becomes possible to identify the source of the attack.

Multiple failed authentication attempts from a single IP address were observed in the log records analyzed in this paper. This case indicates the possibility of a brute-force attack. Such an attack can be successful if the system has a weak password policy, an absent account-blocking mechanism, or the SSH service is left open. The effect of a brute-force attack on a system is manifested in the following:

1. breach of the user's account;
2. unauthorized access to confidential information;
3. possession of administrative rights;
4. change system configuration;
5. to carry out further attacks on other internal systems.

That is why such events are considered to have a high level of risk.

Assessment of the likelihood of unauthorized access. If the log file has more than one "Accepted password" entries followed by "Accepted password", it requires special attention from a security point of view. Because this case means that the attacker may have found the password or the user's credentials have been compromised. For example, a timeline might look like this:

Table 1.2

Assessment of Accepted Password status after Failed Password events

Time	**Event**	**Assessment**
09:12:01	Failed Password	Incorrect password entered by the user. In the individual case, this may be a simple mistake.
09:12:05	Failed Password	Logging of a short period of repeated authentication attempts indicates the presence of suspicious activity.
09:12:09	Failed Password	A serial failed login attempt could mean a brute-force attack or using an automated password picker.
09:12:15	Accepted Password	Successful authentication was attempted after several unsuccessful attempts. This status indicates the possibility of unauthorized access or account compromise.

In this case, a successful login event should definitely be investigated. The administrator should check if the user is really logged in, check the IP address and, if necessary, change the user's password.

Evaluating attempts to root account. On Linux systems, root is considered to have the highest permissions. If the attacker successfully logs into the root account, he can take full control of the system. Therefore, the appearance of "Failed password for root" entries in the logs is rated as a high-risk event. Attacks targeting the root account may present the following risks:

1. modify system files;
2. create new admin accounts;
3. install malware;
4. disabling safety equipment;
5. delete or hide log entries.

Therefore, blocking root account access via SSH is one of the most important protective measures.

Evaluate a time-based brute-force attack. In time-based brute-force attacks, the attacker makes authentication attempts over a period of time rather than a short period of time. This approach is used to circumvent common protective mechanisms. For example, if an attempt is made once every 5–10 minutes, the system may treat this as a simple error. Log analysis plots a timeline to detect such attacks. Using journalctl or AWK, events are sorted by time and their recurrence periodicity is analyzed. If an attempt is repeated with continuous intervals from the same IP address, it is considered a time-based brute-force attack token. This type of attack is rated as moderate risk because it may not cause significant damage in the short term, but the longer it lasts, the more likely it is that the password will be found.

Criteria for assessing security breaches. It is desirable to use the following criteria in the assessment of identified security events:

1. number of recurrences of the incident;
2. the time interval in which the incident occurred;
3. manba IP manzil;
4. type of user account;
5. whether it was completed with a successful entry;
6. the level of damage that can be inflicted on the system.

Table 1.3

Criteria for assessing security incidents

Criterion	**Past xavf**	**Medium risk**	**High risk**
Number of chunks downloaded	1–2 authentication attempts	3–5 consecutive attempts	Repeated attempts more than 5 times
IP manzil	Trusted address in internal network	Unknown location not previously tracked	Suspected or blacklisted external address
User account	Normal user account	Service account	Root or admin account
Conclusion	Failed authentication	Successive failed attempts	Accepted Password after

			Failed Password events
Vaqt oralig'i	No unusual status is observed	It repeats at certain intervals	A lot of attempts are made in a short time

With these criteria, an administrator can determine the extent to which each incident is impacting system security, not limited to just monitoring log records. For example, one-time failed authentication attempts might be a typical user error, but logging multiple attempts from the same IP address over a short period of time increases the likelihood of an attack. It should also be noted whether successful authentication is recorded after an attempt or failed logins to the root account requires separate verification. A systematic evaluation of log records thus enables an administrator to sort security incidents by priority, properly allocate resources, and take swift action.

In addition, the results of the security incident assessment are also important in improving an organization's overall information security policy. Log analysis identifies the most common threats, weak points, and tactics of attackers. Based on this information, it will be possible to implement new security mechanisms, configure existing security features and develop additional security requirements for users.

Recommendations for preventing security breaches. Several safeguards have been developed to minimize the identified security breaches and prevent such incidents in the future. These recommendations are aimed at fixing the problems identified during log analysis, which serve to improve the security of the SSH service, prevent unauthorized access, and make the authentication process more reliable. The recommended measures, when applied together, significantly increase the system's attack resilience and allow for the early detection of security incidents.

Disable root access via SSH. Preventing root user login via SSH is an important safeguard measure. To do this, set the following option in the /etc/ssh/sshd_config file:

PermitRootLogin no

Then the SSH service will be restarted:

sudo systemctl restart ssh

This measure helps prevent attacks targeting roots.

Use SSH keys instead of password. Password-based authentication is considered vulnerable to brute-force attacks. It is therefore recommended to implement SSH key authentication. In this case, the user connects to the system not with a password, but with a special cryptographic key. This approach has the following advantages:

1. reduces the risk of password guessing;
2. makes the authentication process more secure;
3. renders automated brute-force attacks ineffective.

Implement the fail2ban tool. Fail2ban is a tool that monitors log files and automatically blocks an attacker's IP address when it detects repeated failed authentication attempts. The following protection is implemented using fail2ban:

1. "Failed password" records are monitored;
2. IP address is blocked if more than the set number is detected;
3. the blocking period is set by the administrator;

4. Brute-force attacks are automatically limited.

Fail2ban is one of the most effective tools for SSH protection.

Implement a strong password policy. Weak passwords cause brute-force attacks to succeed. Therefore, it is imperative to implement a strong password policy for users. A strong password should meet the following requirements:

1. at least 12 characters;
2. contain both uppercase and lowercase letters;
3. the use of numbers and special symbols;
4. must not contain a username or simple words;
5. Regular updates.

Change the SSH port. The default SSH port is 22. It is precisely this port that attackers often scan. Changing the SSH port to another port can reduce brute-force attempts. For example, in the file /etc/ssh/sshd_config: Install port 2222 and start the SSH service again. This measure does not provide complete protection, but it does reduce the number of automated simple attacks.

Restrict access through the firewall. We are recommended to allow SSH service access only from trusted IP addresses. To do this, firewall rules are configured. For example:

sudo ufw allow from 192.168.0.0/24 to any port 22

sudo ufw deny 22

Only internal network connections are allowed to SSH service through this service.

Automate log monitoring. Even if manual log analysis is effective in small test environments, in real corporate networks, the number of logs is still high. That's why it's recommended to automate log monitoring. To do this, you can use the following tools:

1. Fail2ban;
2. Wazuh;
3. ELK Stack;
4. Graylog;
5. Splunk;
6. Integration with Zabbix or Prometheus.

These tools allow for real-time monitoring of logs, generating alerts, and analyzing security events in a centralized way.

Table 1.4

Identified problems and recommendations for eliminating them

Problem	**Level of risk**	**Recommended protective measure**
An abundance of failed password records	Medium	Implement a strong password policy, limit login attempts and use the Fail2Ban tool
Brute-force hujumi	High	Automatic blocking of attacker's IP address, implementing authentication based on SSH keys, and configuring the Fail2Ban service
Attempts to log in to root account	High	Prevent root user direct access via SSH (PermitRootLogin no) and shield admin accounts
Accepted Password after	High	Account temporarily blocking, password change, audit of user

Failed Password events		activity, and additional checks
Time-based brute-force hujumi	Medium	Create correlation rules in the SIEM system, strengthen periodic monitoring and control the number of login attempts
Connections from unknown IP address	Medium	Enforcing firewall rules, filtering IP addresses based on whitelist and using geolocation control
Illegal Abuse of Admin Rights	High	Implementation of the Least Privilege principle, monitoring of sudo logs and the application of multi-factor authentication
Constant attacks on SSH service	High	Change SSH port, implement MFA, and control traffic using IDS/IPS tools

Summarize recommendations. These recommendations serve to improve the security of SSH authentication on Linux servers and to mitigate log-based security breaches. The recommended measures are inextricably linked, and their comprehensive application gives the highest effect. For example, the implementation of a strong password policy alone cannot eliminate all threats, however, when applied in combination with SSH keys, Fail2ban, firewall rules, and regular log monitoring, the level of system protection increases significantly. Also, constant log analysis enables admins to detect security incidents at an early stage and provide rapid response to them.

The results of case study have shown that failed login attempts, repeated authentication failures as well as connections made from suspicious IP addresses recorded in authentication logs are an important source of information for the system security assessment. For this reason, log monitoring should be regarded not only as an event recording tool but also as an essential element of security management. Especially in server infrastructures where SSH service is widely used, such monitoring tools are of great value in the timely detection and prevention of unauthorized access attempts.

The proposed protection model. The following protection model is proposed to prevent detected security breaches. This model consists of several layers of defense, with each layer aimed at mitigating certain types of threats. The main goal of the model is to detect attacks on the SSH service as early as possible, prevent unauthorized accesses, and provide the system administrator with prompt information about security incidents. Because of the multi-layered protection approach, even if one protection mechanism is bypassed, other mechanisms will continue to ensure system security.

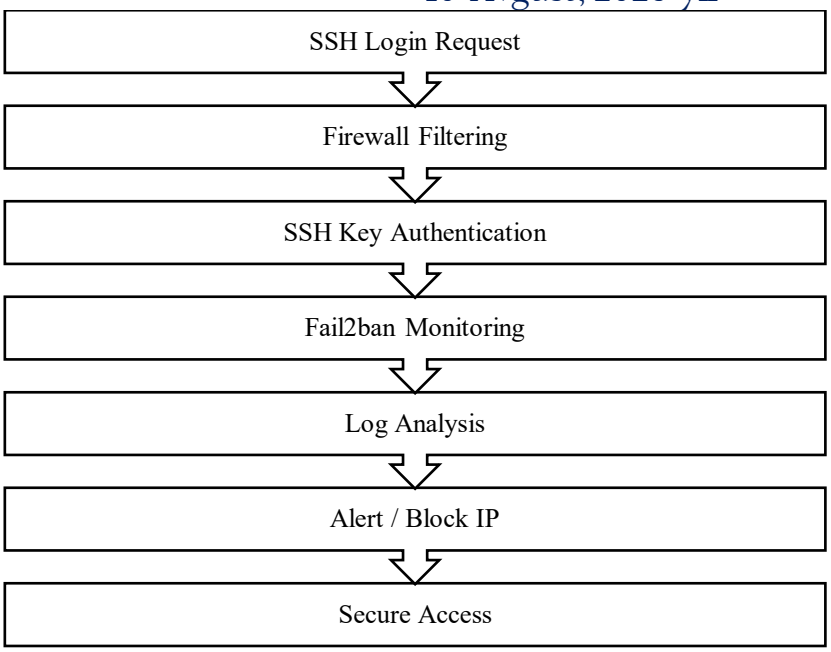

Figure 1.1. SSH Authentication Security Model

In this model, SSH requests are first controlled through a firewall. The user then authenticates using SSH keys. Fail2ban and log monitoring tools monitor for failed attempts. If suspicious activity is detected, the IP address is blocked or an alert is sent to the administrator.

This paragraph evaluated the security breaches identified based on Linux authentication logs and developed recommendations to prevent them. The analysis found that brute-force attacks, root account attempts, post-failed and time-based attacks can pose a serious threat to system security. To mitigate these threats, it was recommended to disable root access via SSH, implement authentication based on SSH keys, use the Fail2ban tool, enforce a strong password policy, limit access through the firewall, and automate log monitoring. These measures reduce the risk of unauthorized access to Linux servers and improve the overall security of information systems.

Conclusion

In this thesis project, the topic "Detection of security breaches by analyzing log files" was studied. In the course of the work, the concept of log files, their types, the main sources of logs in Windows and Linux operating systems, and the importance of logs in information security were analyzed. Logs are an important source of information that records events that occur in the system, and it was substantiated to substantiate user actions, authentication processes, system failures, and security breaches.

In the theoretical part, methods to detect cyberattacks based on security incidents and logs are examined. In particular, the log records of attacks such as brute-force, unauthorized access, privilege escalation, and time-based brute-force were highlighted in the logs. Also, the functions of log monitoring and analysis tools such as auth.log, syslog, journalctl, Event Viewer, SIEM systems, grep, awk, tail are studied. Possibility to identify security insiders via log collection, filtering, timesheet generation, and event correlation has been demonstrated.

The results of the diploma project showed that the systematic collection, storage and analysis of log files is one of the effective ways to detect security breaches in information systems. Brute-force and unauthorized login attempts can be detected at an early stage, especially by analyzing SSH authentication events based on auth.log and journalctl records on Linux systems. The proposed approach can be used as a practical solution for organizing security monitoring, checking for insiders, and strengthening system protection in small and medium-sized information systems.

REFERENCES:

1. Theis, M. C., Trzeciak, R. F., Costa, D., Moore, A. P., Miller, S., Cassidy, T., Claycomb, W. R. *Common Sense Guide to Mitigating Insider Threats, Sixth Edition*. Carnegie Mellon University, Software Engineering Institute, 2019.
2. IBM Security, Ponemon Institute. *Cost of a Data Breach Report 2025*. IBM, 2025.
3. Ponemon Institute / DTEX Systems. *2025 Cost of Insider Risks Report* bo‘yicha tahliliy ma’lumotlar.
4. Kent, K., Souppaya, M. NIST SP 800-92: Guide to Computer Security Log Management. National Institute of Standards and Technology, 2006.
5. NIST CSRC. Security Information and Event Management - Glossary. National Institute of Standards and Technology.
6. IETF. RFC 5424: The Syslog Protocol. Internet Engineering Task Force.
7. Microsoft Learn. Sysmon - Sysinternals. Microsoft documentation
8. NIST. Cybersecurity Framework 2.0, 2024.
9. NIST. SP 800-207: Zero Trust Architecture, 2020.
10. CISA. Zero Trust Maturity Model Version 2.0, 2023.
11. CISA. More than a Password: Multifactor Authentication.
12. MITRE. MITRE ATT&CK: Lateral Movement, TA0008.
13. Labor Code of the Republic of Uzbekistan. RU-798, 28.10.2022.
14. Law of the Republic of Uzbekistan "On Labor Protection". RU-410, September 22, 2016.
15. Law of the Republic of Uzbekistan "On Fire Safety". RU-226 No. 30.09.2009.
16. ISO 45001:2018. Occupational health and safety management systems — Requirements with guidance for use. International Organization for Standardization, 2018.
17. National Institute for Occupational Safety and Health (NIOSH). Hierarchy of Controls. Centers for Disease Control and Prevention.
18. Occupational Safety and Health Administration (OSHA). Computer Workstations eTool. United States Department of Labor.