Security Log Analyzer - Incident Response Plan & Security Policy

Project Overview

Project Name: Security Log Analyzer - Incident Response Tool
Purpose: Automated detection and analysis of security incidents through authentication log monitoring
Version: 1.0
Date: November 18, 2024

---

1. Incident Response Plan

1.1 Detection Method

Automated Log Analysis System

Our Security Log Analyzer implements real-time detection of security incidents through:

- **Continuous Monitoring:** Parses authentication logs in real-time to identify suspicious patterns
- **Threshold-Based Detection:** Flags IP addresses with 3+ failed login attempts within a session
- **Pattern Recognition:** Identifies brute-force attacks by analyzing failed authentication sequences
- **Automated Alerts:** Generates visual alerts with severity ratings (HIGH/MEDIUM) based on threat level

Detection Mechanism:

```
IF failed_login_attempts >= 3 from same IP THEN
   Flag as MEDIUM THREAT
IF failed_login_attempts >= 5 from same IP THEN
   Flag as HIGH THREAT
```

1.2 Containment Strategy

Immediate Response Protocol

When a threat is detected, the following containment steps are executed:

1. **Automatic Identification:** System flags suspicious IP addresses in real-time
2. **Alert Generation:** Security team receives immediate notification via GUI alert panel
3. **Recommended Actions:**
    - Block identified malicious IPs at firewall level
    - Suspend affected user accounts temporarily
    - Enable enhanced monitoring for flagged IP ranges
    - Isolate compromised systems from network if breach is confirmed
4. **Documentation:** All incidents are logged with:
    - Timestamp of detection
    - Source IP address
    - Number of failed attempts
    - Affected user accounts
    - Actions taken

1.3 Eradication and Recovery Steps

Phase 1: Eradication

1. Remove threat source by permanently blocking malicious IPs
2. Patch vulnerabilities exploited during the attack
3. Reset credentials for all affected user accounts
4. Scan systems for malware or unauthorized access
5. Remove any backdoors or persistent threats

Phase 2: Recovery

1. Restore systems to normal operation after verification
2. Monitor restored systems for 72 hours for anomalies
3. Gradually restore user access with enhanced authentication
4. Update security configurations based on lessons learned
5. Conduct post-incident review meeting with security team

Phase 3: Post-Incident Activities

1. Document full incident timeline and response actions
2. Update threat intelligence database
3. Refine detection thresholds based on incident data
4. Conduct team debriefing and training updates
5. Report to management and relevant stakeholders

---

2. Cyber Attack Type: Brute-Force Attack (Credential Stuffing)

2.1 Attack Description

What is a Brute-Force Attack?

A brute-force attack is a trial-and-error method where attackers systematically attempt multiple username/password combinations to gain unauthorized access to systems. In our project context, this manifests as repeated failed login attempts from external IP addresses.

2.2 How the Attack Works

1. **Reconnaissance:** Attacker identifies target system (authentication portal)
2. **Tool Selection:** Uses automated tools (e.g., Hydra, Medusa) to generate login attempts
3. **Execution:** Sends hundreds or thousands of authentication requests
4. **Success:** Gains access if correct credentials are found

Example from our logs:

IP: 203.0.113.45 attempted logins:
- 08:18:12 | LOGIN_FAILED | user: admin
- 08:21:07 | LOGIN_FAILED | user: root
- 08:24:18 | LOGIN_FAILED | user: admin
- 08:27:02 | LOGIN_FAILED | user: administrator
- 08:46:51 | LOGIN_FAILED | user: admin
- 08:56:03 | LOGIN_FAILED | user: admin

2.3 Detection in Our System

Our analyzer detects brute-force attacks by:

- Tracking failed authentication attempts per IP address
- Flagging IPs exceeding failure threshold
- Identifying common target usernames (admin, root, administrator)
- Analyzing time patterns between attempts

2.4 Impact and Risks

- **Unauthorized Access:** Successful attacks grant attackers system access
- **Data Breach:** Compromised accounts can lead to data exfiltration
- **System Disruption:** Can overload authentication services (DoS effect)
- **Reputation Damage:** Security breaches harm organizational credibility

- **Compliance Violations:** May breach regulations like GDPR, HIPAA

2.5 Prevention Measures

1. **Account Lockout Policies:** Lock accounts after 3-5 failed attempts
2. **Multi-Factor Authentication (MFA):** Require additional verification beyond passwords
3. **Strong Password Policies:** Enforce complex passwords (12+ characters, mixed case, symbols)
4. **IP Blacklisting:** Block known malicious IP addresses
5. **CAPTCHA Implementation:** Require human verification after failed attempts
6. **Rate Limiting:** Restrict number of login attempts per time period

---

3. Comprehensive Security Policy

3.1 Key Security Rules and Guidelines

Rule 1: Access Control and Authentication

- **Mandatory MFA:** All users must enable multi-factor authentication
- **Password Requirements:**
  - Minimum 12 characters
  - Mix of uppercase, lowercase, numbers, symbols
  - No dictionary words or personal information
  - Changed every 90 days
- **Account Review:** Quarterly review of user access rights
- **Least Privilege:** Users granted minimum necessary permissions

Rule 2: Monitoring and Detection

- **Continuous Monitoring:** 24/7 log analysis using automated tools
- **Alert Thresholds:**
  - 3 failed logins = Medium alert
  - 5 failed logins = High alert + automatic block
- **Log Retention:** Security logs retained for minimum 1 year
- **Regular Audits:** Monthly security audit reports

Rule 3: Incident Response Protocol

- **Immediate Reporting:** All security incidents reported within 1 hour
- **Response Team:** Designated IR team available 24/7
- **Communication Plan:** Stakeholder notification within 24 hours
- **Documentation:** All incidents logged in incident management system

3.2 Incident Response Plan (Detailed Steps)

Step 1: Preparation

- Maintain updated contact lists for IR team
- Ensure all security tools are operational
- Conduct quarterly IR drills and training

Step 2: Detection and Analysis

- Security Log Analyzer runs continuously
- Analyst reviews alerts within 15 minutes
- Classify incident severity (Low/Medium/High/Critical)

Step 3: Containment

- **Short-term:** Block malicious IPs immediately via firewall
- **Long-term:** Implement permanent security controls
- Isolate affected systems if compromise suspected

Step 4: Eradication

- Remove malicious code or unauthorized access
- Patch vulnerabilities that were exploited
- Reset compromised credentials

Step 5: Recovery

- Restore systems to normal operation
- Verify system integrity before full restoration
- Monitor for 72 hours post-recovery

Step 6: Post-Incident Review

- Document lessons learned
- Update security policies and procedures
- Provide training to prevent recurrence

3.3 CIA Triad Compliance

Our security policy maintains the CIA Triad principles:

Confidentiality

- **Implementation:** User authentication, encryption, access controls
- **In Our Tool:** Only authorized security personnel can view logs

- **Policy:** Data classification and handling procedures

Integrity

- **Implementation:** Log file integrity checks, digital signatures
- **In Our Tool:** Tamper-evident logging ensures data hasn't been modified
- **Policy:** Change management procedures, version control

Availability

- **Implementation:** Redundant systems, backup procedures, DDoS protection
- **In Our Tool:** Continuous monitoring ensures system availability
- **Policy:** Business continuity plan, disaster recovery procedures

How Our Project Upholds CIA:

1. **Confidentiality:** Access to security logs restricted to IR team only
2. **Integrity:** Logs stored in append-only format, preventing tampering
3. **Availability:** System designed for 24/7 operation with minimal downtime

---

4. Encryption Techniques Demonstration

4.1 AES Encryption Example

Plain Text: `SecurePassword123!`

AES-256 Encrypted (Base64 encoded):

U2FsdGVkX1+8vKjKL5J9mNxZ3qK8pVnYtL9kF3zH2Ao=

Encryption Process:

1. Generate random 256-bit encryption key
2. Apply AES cipher in CBC mode
3. Use PKCS7 padding for block alignment
4. Encode result in Base64 for transmission

Decryption Process:

1. Decode Base64 string to binary
2. Apply same 256-bit key with AES decryption
3. Remove PKCS7 padding

4. Retrieve original plaintext: `SecurePassword123!`

Python Implementation Concept:

```
# Encryption Method
def encrypt_data(plaintext, key):
    cipher = AES.new(key, AES.MODE_CBC)
    ciphertext = cipher.encrypt(pad_data(plaintext))
    return base64_encode(ciphertext)

# Decryption Method
def decrypt_data(ciphertext, key):
    cipher = AES.new(key, AES.MODE_CBC)
    plaintext = unpad_data(cipher.decrypt(base64_decode(ciphertext)))
    return plaintext
```

4.2 Hash Function Example (SHA-256)

Plain Text: `AdminPassword2024`

SHA-256 Hash:

a3c6f891e2ab5f2c3d8e9b1f4c7a5d9e8b3f6c2a1d4e7b9c8f5a2d3e6b1c4a7d

MD5 Hash (for comparison):

5f4dcc3b5aa765d61d8327deb882cf99

Key Properties:

- **Deterministic:** Same input always produces same hash
- **One-way:** Cannot reverse hash to get original password
- **Collision-resistant:** Different inputs produce different hashes
- **Fixed length:** Always 256 bits regardless of input size

Use Case in Security:

- Passwords stored as hashes in database
- Login verification compares hash values, not actual passwords
- Even if database compromised, passwords remain protected

---

5. Legal and Ethical Compliance

5.1 Relevant Laws and Regulations

Law 1: General Data Protection Regulation (GDPR)

Applicability: Protects EU citizens' personal data

Compliance Requirements:

- Log data containing user information must be encrypted
- Users have right to access their authentication logs
- Data retention limited to legitimate business purposes
- Breach notification within 72 hours

Our Plan's Compliance:

- Logs encrypted at rest and in transit
- Access controls limit log viewing to authorized personnel only
- Retention policy: 1 year for security logs, then secure deletion
- Incident response plan includes breach notification procedures

Law 2: Computer Fraud and Abuse Act (CFAA) - United States

Applicability: Prohibits unauthorized access to computer systems

Compliance Requirements:

- Only authorized monitoring of systems we own/operate
- Clear policies defining authorized vs unauthorized access
- No excessive or retaliatory actions against suspected attackers

Our Plan's Compliance:

- Monitoring limited to organization's own systems
- Clear definition of authorized users in security policy
- Response actions proportional and legally defensible
- All blocking actions documented with justification

5.2 Ethical Considerations

Ethical Principle: Privacy and Proportionality

Consideration: While monitoring is necessary for security, it must respect user privacy and avoid excessive surveillance.

Ethical Guidelines:

1. **Transparency:** Users informed that authentication logs are monitored
2. **Proportionality:** Only collect data necessary for security purposes
3. **Anonymization:** Personal identifiers removed where possible
4. **Limited Retention:** Logs deleted after legitimate retention period
5. **Accountability:** Regular audits ensure monitoring isn't misused

Implementation in Our Plan:

- Clear privacy policy explains what data is collected and why
- Logs contain only authentication events, not content of user activities
- Access to logs restricted by role-based access control
- Annual privacy impact assessments conducted
- Users can request their log data under data subject rights

Ethical Principle: Fairness and Non-Discrimination

Consideration: Security measures must be applied equally without bias or discrimination.

Implementation:

- Alert thresholds same for all users regardless of role or identity
- No profiling based on protected characteristics
- False positives reviewed promptly to avoid unfair account lockouts
- Appeals process for users who believe they were wrongly flagged

5.3 Legal and Ethical Compliance Summary

Our Incident Response Plan upholds legal requirements and ethical principles through:

1. **Data Protection:** Encryption, access controls, limited retention
2. **Lawful Monitoring:** Only authorized systems, proportional responses
3. **Transparency:** Clear policies communicated to users
4. **Privacy Respect:** Minimal data collection, user rights honored
5. **Accountability:** Regular audits, documented decisions
6. **Fairness:** Equal application of security measures

Compliance Review Schedule:

- Quarterly: Internal compliance audit
- Annually: External legal and ethical review
- Ongoing: Staff training on legal and ethical obligations

---

6. Conclusion

This Security Log Analyzer project demonstrates comprehensive understanding of:

- **Incident Detection:** Automated threat identification through log analysis
- **Response Procedures:** Structured containment, eradication, and recovery
- **Cyber Threats:** Real-world brute-force attack recognition and mitigation
- **Security Policy:** Practical implementation of security best practices
- **CIA Triad:** Maintaining confidentiality, integrity, and availability
- **Encryption:** Application of AES and hashing for data protection
- **Compliance:** Adherence to legal requirements and ethical principles

This tool provides a foundation for real-world incident response capabilities and demonstrates the practical application of cybersecurity concepts in Python.