# LOGS AND LOG ANALYSIS IN CYBERSECURITY



VAISHALI SHISHODIA

## Introduction to Logs

Logs are detailed records of events that occur within an organization's IT infrastructure. These records contain information about activities performed by users, systems, applications, and networks. They are crucial for monitoring security events, troubleshooting issues, and conducting forensic investigations. Logs serve as digital footprints that help security teams identify suspicious activities, track system performance, and maintain compliance with industry regulations.

## Types of Logs

Logs can be categorized into different types based on their sources and functions:

**a) System Logs**

- Generated by operating systems.
- Include information about system events, errors, security changes, and user activities.
- Useful for diagnosing system failures and security incidents.
- Examples: Windows Event Logs, Linux Syslogs.
- Common events: User logins/logouts, application crashes, system updates, and kernel warnings.

**b) Application Logs**

- Generated by software applications.
- Contain details about application performance, errors, user activities, and security incidents.
- Help in tracking bugs, monitoring user interactions, and identifying malicious activities.
- Examples: Web server logs (Apache, Nginx), database logs (MySQL, PostgreSQL), application error logs.
- Common events: HTTP requests, database queries, authentication attempts, and API calls.

**c) Network Logs**

- Captured by network devices such as firewalls, routers, and intrusion detection/prevention systems (IDS/IPS).
- Contain details about traffic patterns, source/destination IP addresses, ports, and blocked connections.
- Help in identifying anomalies, tracking unauthorized access, and detecting network threats.
- Examples: Firewall logs, IDS/IPS logs, DNS logs, VPN logs.
- Common events: Network traffic flow, bandwidth usage, dropped packets, denied connections, and intrusion alerts.

**d) Security Logs**

- Record security-related activities, such as authentication attempts, malware detections, and access control violations.
- Help in detecting unauthorized access, malware infections, and policy violations.
- Crucial for security monitoring, compliance, and forensic investigations.
- Examples: SIEM logs, antivirus logs, endpoint protection logs.
- Common events: Failed authentication attempts, firewall rule violations, system lockdown events, and encryption key access.

**e) Audit Logs**

- Capture all system and user activity for compliance and governance purposes.
- Provide a historical record of changes made to systems, user permissions, and data access.
- Help in maintaining accountability, tracking insider threats, and fulfilling regulatory requirements.
- Examples: Database audit logs, Active Directory audit logs, compliance audit logs.
- Common events: File modifications, privilege escalations, account creations, and security policy changes.

**f) Cloud Logs**

- Logs generated by cloud services such as AWS, Azure, and Google Cloud.
- Include API activity, access logs, and security event logs.
- Help in monitoring cloud resource usage, detecting unauthorized API calls, and securing cloud workloads.
- Examples: AWS CloudTrail, Azure Security Center logs, Google Cloud Audit logs.
- Common events: Cloud resource provisioning, API key usage, failed login attempts, and serverless function execution.



## Analyze the Logs to Identify Attacks

Security Operations Center (SOC) analysts analyze logs to detect potential cyber threats. The process typically involves:

**a) Log Collection and Normalization**

- Logs from different sources are collected using SIEM (Security Information and Event Management) tools.
- Data is standardized to ensure consistency across logs from various sources.

- Ensures structured and meaningful analysis to correlate events across different platforms.
- Tools: Splunk, ELK Stack, IBM QRadar, ArcSight.

**b) Correlation and Pattern Analysis**

- SOC analysts use correlation rules to detect suspicious patterns across multiple logs.
- Example: Multiple failed login attempts from different IPs could indicate a brute-force attack.
- Uses event correlation techniques to link related security events.
- Helps in reducing false positives and identifying actual threats.

**c) Threat Intelligence Integration**

- SOC teams use threat intelligence feeds to compare logs against known attack patterns and indicators of compromise (IOCs).
- Example: Matching an IP address from logs with a known malicious IP from a threat intelligence database.
- Enhances detection capabilities by leveraging external threat intelligence sources.
- Tools: Threat intelligence platforms, OSINT sources, commercial threat feeds.

**d) Anomaly Detection**

- Machine learning and behavioral analysis techniques help identify deviations from normal user or system behavior.
- Example: A user logging in from an unusual geographic location.
- Uses baselining techniques to define normal behavior and detect anomalies.
- Helps in detecting zero-day attacks and insider threats.

**e) Incident Investigation and Response**

- Analysts investigate flagged security events to determine if they are genuine threats or false positives.
- If a real threat is identified, they initiate an incident response process.
- Includes threat containment, eradication, and recovery.
- Helps in minimizing attack impact and improving security defenses.

## Types of Attacks Identified Through Log Analysis

SOC analysts use log analysis to detect various cyberattacks, including:

**a) Brute-Force Attacks**

- Multiple failed login attempts in authentication logs.

- Can be detected using authentication logs and correlation rules.

**b) Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks**

- Unusual spikes in network traffic logs.
- Identified using network logs and anomaly detection mechanisms.

**c) Malware Infections**

- Antivirus logs showing suspicious file executions.
- Helps in detecting and containing malware threats.

**d) Insider Threats**

- Unusual access patterns in audit logs.
- Detects privileged misuse and unauthorized access.

**e) SQL Injection and Web Attacks**

- Web server logs showing suspicious SQL queries.
- Helps in identifying web-based attacks.



## Importance of Log Analysis in Cybersecurity

**a) Threat Detection and Prevention**

- Helps in identifying potential security breaches before they cause damage.
- Proactive monitoring helps in mitigating risks.

**b) Incident Response**

- Provides forensic evidence to investigate and mitigate security incidents.
- Enables swift action against security threats.

**c) Regulatory Compliance**

- Ensures adherence to security standards such as GDPR, HIPAA, and PCI-DSS.
- Helps organizations meet legal and industry requirements.

**d) Performance Monitoring**

- Helps in identifying system failures and performance bottlenecks.
- Ensures optimal IT infrastructure performance.

**e) Risk Management**

- Enables proactive security measures by identifying vulnerabilities before exploitation.
- Helps in building a resilient cybersecurity framework.

## Scenario-Based Interview Questions & Answers

**1. Log Analysis for Brute Force Attack**

**Q:** You are reviewing authentication logs and notice multiple failed login attempts from the same IP address followed by a successful login. How would you analyze and respond to this?

**A:**

- First, I would examine the source IP, user account, and timestamps to confirm whether it's a brute-force attack.
- Check the log pattern: If there are a high number of failed login attempts followed by a successful one, it may indicate a successful brute-force attempt.
- Cross-check with threat intelligence to see if the IP is associated with known attacks.
- Verify user behavior (e.g., is the login happening from an unusual location or time?).
- If confirmed as an attack, I would block the IP, enforce multi-factor authentication (MFA), reset compromised credentials, and update firewall rules.

**2. Suspicious Network Traffic Detection**

**Q:** A firewall log shows a sudden spike in outbound traffic to an unfamiliar IP address. How would you investigate this?

**A:**

- Review network traffic logs to determine which device or user generated the traffic.
- Check IDS/IPS logs for any intrusion alerts related to this IP.
- Verify DNS logs to see if the domain resolves to a known malicious server.
- Analyze SIEM correlation rules to check if this is part of a larger attack pattern.
- If identified as suspicious, I would isolate the device, analyze for malware, and implement firewall rules to block the malicious IP.

**3. Identifying Insider Threats via Audit Logs**

**Q:** You notice in audit logs that an employee accessed a large volume of sensitive files outside of normal working hours. What steps would you take?

**A:**

- Review the user's access logs to determine the nature of the accessed files.
- Compare the user’s behavior with past activities to see if this is normal or an anomaly.
- Check for failed login attempts or privilege escalations.
- If unauthorized access is confirmed, I would alert the incident response team, revoke excessive privileges, and investigate potential data exfiltration attempts.

**4. Detecting SQL Injection via Web Server Logs**

**Q:** A web server log contains repeated instances of unusual database queries with "OR 1=1" in the request URL. What does this indicate, and how would you respond?

**A:**

- This pattern suggests an SQL injection attack attempt where an attacker tries to manipulate SQL queries.
- I would analyze logs for other similar payloads (e.g., UNION SELECT, DROP TABLE) to confirm the attack.
- Check the affected application for input validation vulnerabilities.
- Implement Web Application Firewall (WAF) rules to block such queries.
- Work with developers to implement secure coding practices like parameterized queries.

**5. DDoS Attack Identification in Network Logs**

**Q:** Your SIEM tool alerts you to a high volume of traffic coming from multiple IP addresses to a single web server. How would you investigate and mitigate this?

**A:**

- Review network logs to analyze the traffic pattern and confirm if it's a volumetric attack.
- Check if the IPs belong to a known botnet by using threat intelligence feeds.
- Monitor firewall and IDS logs to check if requests are overwhelming the server.
- Mitigation steps: Enable rate limiting, block suspicious IPs, use a CDN with DDoS protection, and scale resources to absorb traffic.

**6. Ransomware Detection via Endpoint Logs**

**Q:** You notice unusual file encryption activity in endpoint security logs, followed by a log entry showing files being renamed with a ".locked" extension. How would you respond?

**A:**

- This is a strong indicator of a ransomware attack.
- I would immediately isolate the affected system from the network to prevent further encryption.
- Analyze logs to determine the source of infection (e.g., phishing email, malicious file download).
- Check SIEM for any suspicious processes running on other endpoints.
- Restore affected files from backups and update security policies to block similar attacks in the future.

**7. Privilege Escalation Detection in Windows Event Logs**

**Q:** A Windows security log shows a standard user account executing a process with administrator privileges (Event ID 4673). What steps would you take?

**A:**

- Review the account activity to determine if the user was granted elevated privileges legitimately.
- Check for additional suspicious logs, such as Event ID 4624 (successful logins) and 4688 (new process execution).
- Correlate with endpoint detection logs to see if malware or scripts (e.g., Mimikatz) were executed.
- If it's unauthorized, revoke the elevated privileges, reset credentials, and monitor for further suspicious activity.

**8. Phishing Attack Detection in Email Logs**

**Q:** An employee reports receiving an email with an attachment that, when opened, triggered a suspicious PowerShell script. How do you investigate?

**A:**

- Check email gateway logs for the sender's IP and domain reputation.
- Review logs to see if other employees received the same email.
- Analyze endpoint logs for PowerShell activity and suspicious processes.
- Check network logs to see if the system connected to a known command-and-control (C2) server.
- If confirmed as phishing, I would block the sender, remove similar emails from mailboxes, and educate employees about recognizing phishing attempts.



**9. Data Exfiltration Detection via Proxy Logs**

**Q:** You find logs showing a large volume of outbound data transfers to an external cloud storage provider. What actions do you take?

**A:**

- Verify the source system and user account performing the data transfer.
- Check logs for abnormal file access patterns prior to the upload.
- Cross-reference with DLP (Data Loss Prevention) logs to determine if sensitive data was involved.
- If unauthorized, I would terminate the connection, revoke user access, and notify legal/compliance teams for further action.

**10. Detecting Lateral Movement via Active Directory Logs**

**Q:** You notice multiple failed login attempts from one workstation to different systems, followed by a successful login using a high-privilege account. What does this indicate?

**A:**

- This suggests a potential **pass-the-hash** or **lateral movement** attack.
- I would check for suspicious Event IDs in Windows logs, such as 4625 (failed logins) and 4768 (Kerberos ticket requests).
- Use SIEM to correlate logs and check if an attacker used compromised credentials to move across the network.
- If confirmed, I would isolate affected systems, reset compromised credentials, and implement strict access controls.

**11. Detecting a Rogue Device in Network Logs**

**Q:** You detect an unauthorized device connecting to the corporate Wi-Fi, generating high traffic. How do you handle it?

**A:**

- Check DHCP logs to identify the MAC address and device type.
- Review network logs to determine if it's communicating with suspicious external IPs.
- If unauthorized, I would block the device via NAC (Network Access Control), alert IT security, and investigate if it's an insider threat.

**12. Man-in-the-Middle (MitM) Attack Detection in TLS Logs**

**Q:** You notice SSL/TLS logs showing multiple handshake failures and self-signed certificates being used for connections. What does this indicate?

**A:**

- This may indicate a **Man-in-the-Middle (MitM) attack** where an attacker is intercepting encrypted traffic.
- I would analyze network logs for unusual ARP requests and DNS hijacking attempts.
- If confirmed, I would alert the security team, force TLS encryption, and implement certificate pinning to prevent such attacks.

**13. Unauthorized Cloud Access in IAM Logs**

**Q:** Cloud logs show an IAM user accessing resources from an unusual location. What steps do you take?

**A:**

- Review cloud access logs (e.g., AWS CloudTrail, Azure Monitor) to confirm whether this was an unauthorized login attempt.

- Check if MFA was used; if not, enable it immediately.
- Look for abnormal API calls (e.g., attempts to create new user accounts or modify permissions).
- If unauthorized, revoke access, investigate the credentials used, and rotate compromised keys.

**14. Supply Chain Attack Detection in Software Logs**

**Q:** A third-party software update log shows the installation of an unsigned package on multiple systems. What do you do?

**A:**

- Check software integrity by verifying the hash values of the package.
- Cross-reference logs to see which systems installed the update.
- Check for new network connections from affected devices to unknown servers.
- If identified as a supply chain attack, I would roll back the update, isolate affected systems, and notify vendors for remediation.

**15. Unusual DNS Requests Indicating Command-and-Control (C2) Communication**

**Q:** DNS logs reveal frequent requests to a domain with a randomized name structure. How do you analyze this?

**A:**

- This could indicate **Domain Generation Algorithm (DGA) activity**, commonly used in malware C2 communication.
- I would check threat intelligence sources to see if the domain is linked to known malware.
- Analyze the endpoint that made these requests to check for signs of compromise.
- Block the domain at the firewall level and initiate a malware scan on the infected system.



---