Logs to Look at for Suspicious Activity Detection

When investigating potential security incidents, **analyzing specific types of logs is crucial for identifying malicious activities**. Logs can provide valuable insights into an attacker's behavior, help detect anomalies, and reveal the full scope of a breach. Below are important logs to monitor and analyze:

1. DNS Queries to Suspicious Domains:

- DNS query logs track requests made by devices on the network to resolve domain names into IP addresses. Monitoring these logs **can help identify when devices attempt to connect to suspicious or malicious domains**, which is often an indicator of command and control (C2) communication or malware trying to exfiltrate data.
- What to look for:
  - Domains associated with known threats: Malware often communicates with hard-coded or dynamically generated domain names. Queries to known malicious domains should trigger alerts.
  - Unusual domain patterns: Look for strange, randomized domain names (e.g., hsadf12sd.com), which may indicate DGA (Domain Generation Algorithm) usage by malware.
- Example: DNS requests for newly registered domains or domains associated with phishing campaigns could indicate an ongoing attack.

2. HTTP Headers Containing Suspicious Information:

- HTTP headers provide metadata about web requests and responses. Attackers may inject malicious or malformed data into HTTP headers to exploit vulnerabilities or carry out attacks.
- What to look for:
  - **Unusual user-agent strings**: Attackers might spoof user-agent strings or use abnormal ones to disguise malware or bots.
  - **Referrer headers**: Unexpected or suspicious referrers could indicate phishing or redirection to malicious sites.
  - **Custom or missing headers**: Some malware may use non-standard headers or omit headers that are expected in normal traffic.
- Example: HTTP requests with overly long or malformed headers (buffer overflow attempts) or requests missing common headers like User-Agent can signal malicious activity.

3. Metadata of Files (Forensic Focus):

- File metadata logs store information such as the file's author, creation time, and modification details. **In a forensic investigation, this data can help track how files were created, modified, or distributed**.
- What to look for:
  - **Unusual file author**: Metadata showing an unexpected or suspicious file author might indicate tampered or malicious files.
  - **Creation and modification times**: Inconsistent timestamps or creation times that don't align with normal user activity may suggest unauthorized changes or malicious files.
  - **File origin details**: Metadata showing where a file originated (e.g., downloads from suspicious URLs) can provide critical clues.

- Example: A malicious Word document with metadata showing it was created by an attacker's tool can provide important forensic evidence.

4. Traffic Volume Logs:

- Traffic volume logs track the amount of data being sent and received by a network device. **Monitoring for spikes or drops in traffic volume can help detect data exfiltration or DDoS attacks**.
- What to look for:
  - Sudden spikes in outbound traffic: Unusual amounts of data being uploaded could indicate an ongoing data exfiltration attempt.
  - Increased inbound traffic: This could be a sign of a DDoS attack or scanning activity from an attacker probing the network.
- Example: A significant increase in traffic volume from a workstation at an unusual time could suggest an insider threat or compromised machine exfiltrating sensitive data.

5. Traffic Patterns Logs:

- Traffic pattern logs provide insights into the behavior of network traffic over time. **Analyzing these patterns can help identify suspicious activity such as scanning, lateral movement, or connections to unexpected services**.
- What to look for:
  - **Unusual connection destinations**: Devices communicating with unknown or foreign IP addresses.
  - **Odd timing patterns**: Traffic occurring during off-hours, weekends, or holidays, when legitimate activity is low.
  - **Scanning patterns**: Repeated attempts to connect to multiple ports across many IPs could indicate a port scan or lateral movement attempt.
- Example: Multiple failed connections to internal IP addresses in quick succession may be an indicator of an internal reconnaissance or lateral movement attack.

6. Execution Logs:

- Execution logs capture details about the processes and commands being executed on a system. Monitoring these logs **can help detect unauthorized or malicious activity such as malware execution or privilege escalation attempts**.
- What to look for:
  - **Suspicious or unauthorized command execution**: Unusual commands being executed (e.g., privilege escalation attempts with sudo, or running scripts from unexpected locations).
  - **Execution of known malicious files**: Log entries showing that malware binaries (e.g., ransomware.exe) have been run on the system.
  - **Abnormal process activity**: Processes that are typically not run by normal users, or processes starting at odd times, might indicate malicious activity.
- Example: Detecting the execution of PowerShell scripts or binaries downloaded from the internet outside of normal administrative tasks can be a strong indicator of compromise.

Summary:

- DNS Queries to Suspicious Domains: Look for queries to known malicious domains or **randomized domain names (DGA)**.
- HTTP Headers: Monitor for unusual or malformed HTTP headers (e.g., odd User-Agent strings or missing headers).
- Metadata of Files: Use file metadata to track suspicious file creation, modification, or distribution.
- Traffic Volume: Unusual spikes or drops in data volume could signal exfiltration or DDoS attacks.
- Traffic Patterns: Look for abnormal traffic behaviors such as off-hour connections or scanning attempts.
- Execution Logs: Analyze process execution logs for unauthorized commands, malware execution, or suspicious process behavior.

> By carefully monitoring these logs, organizations can detect potential threats early, investigate suspicious behavior, and respond to security incidents more effectively.