Anomaly or Behavior-based Detection

Anomaly or behavior-based detection **focuses on identifying abnormal activities by comparing current actions against an established model of "normal" behavior**. This method allows security systems to detect suspicious activity, even if it doesn't match known attack signatures. By understanding the typical behavior of users, devices, or networks, **anomaly-based detection can spot potential threats based on deviations from expected patterns**.

Key Concepts:

1. **Learning Normal Behavior**:

- In anomaly-based intrusion detection systems (IDS), the system **first learns a baseline of normal behavior by monitoring patterns such as typical network traffic, login times, accessed files, URLs, and user activity**.
- Once the model of normal behavior is established, the system **can flag activities that deviate too far from this baseline**.
- Examples:
    - Unusual URLs: If a user or system starts accessing URLs that are highly unusual compared to their normal browsing behavior, this could indicate malicious intent (e.g., contacting command-and-control servers or downloading malware).
    - User-Specific Activity: If a user typically logs in during regular work hours and suddenly logs in during odd hours or accesses files they don't usually handle, these deviations can trigger alerts. This could be a sign of a compromised account or insider threat.

2. **Detecting Actions Associated with Hackers**:

- Anomaly-based systems also look for specific actions that are often linked to malicious behavior or hacker activity. **Even if these actions don't directly match known signatures, their unusual nature can still be detected**.
- Examples:
    - HISTFILE Commands: If a user executes commands that interact with HISTFILE, it could indicate an attempt to erase command history, a tactic often used by attackers to hide their tracks.
    - Accessing /proc Files: /proc is a special directory in Unix/Linux that contains information about system processes. Unusual access to /proc files by non-administrative users could indicate an attempt to gather sensitive information or exploit system vulnerabilities.

3. **Detecting Insider Threats**:

- If an attacker has gained access to the network (whether as an outsider or as an insider threat), anomaly-based systems are well-suited to detect abnormal behavior that could indicate malicious intent.
- For example, if a user begins to access files, systems, or applications outside of their normal scope, or behaves inconsistently with their usual patterns, the system will flag these as suspicious actions.

Response:

- **When a suspicious activity is detected, the system may increase log verbosity for that user or system to gather more detailed information about their actions**. This allows security analysts to conduct a more thorough investigation into whether the behavior indicates a breach.

- Example Scenarios:

    - Unusual Login Times: If an employee usually logs in between 9 AM and 5 PM but suddenly logs in at 3 AM, this deviation from normal behavior would trigger an alert.
    - Accessing Sensitive Files: A user who typically works in marketing suddenly starts accessing finance-related documents, which is out of the ordinary for their role. This behavior could indicate a compromised account or an insider threat.
    - Increased Log Verbosity: If a user starts accessing sensitive directories or executing commands linked to privilege escalation, the system might increase the log verbosity for that user, capturing more detailed logs for closer analysis.

Benefits of Anomaly / Behavior-Based Detection:

- **Detecting Unknown Threats**: Unlike signature-based detection, which relies on known patterns of malicious activity, anomaly-based detection **can detect new or previously unseen threats by identifying deviations from normal behavior**.

- **Insider Threat Detection**: This method is particularly effective in identifying insider threats or attackers who have gained access to the network, as their actions may stand out from regular users' activity.

- **Adaptive Security**: As systems and users evolve, the model of "normal" behavior can be continuously updated, allowing the IDS to adapt to changes over time.

- Challenges:

    - **False Positives**: If the definition of "normal" is too strict, anomaly detection systems can generate a lot of false positives, flagging benign activities as suspicious. This can lead to alert fatigue for security teams.
    - **Learning Period**: These systems require a period of time to learn normal behavior before they can effectively detect anomalies. During this learning phase, they may not detect all threats.
    - **Context Required**: Anomaly-based systems might detect suspicious activity, but human analysts often need to investigate further to determine whether the activity is genuinely malicious or just unusual but harmless.

Summary:

- Anomaly/Behavior-Based Detection relies on learning what "normal" behavior looks like in a system or network and detecting activities that deviate from that baseline.
- It can detect things like unusual URLs being accessed, strange login times, or file access patterns that don't match a user's usual behavior.
- It can also spot specific hacker tactics, such as commands to manipulate HISTFILE or accessing sensitive directories like /proc.

- When suspicious activity is detected, the system can increase logging for the user or process in question, providing more data for further analysis. This approach is especially useful for detecting insider threats or unknown attacks.