Task 12: Log Monitoring & Analysis

1. **Understand log types**
   Logs are records of activities created by systems, applications, and network devices. There are different types of logs such as system logs (OS activities), application logs (software behavior), security logs (login, access, errors), and network logs (traffic and connections). Understanding log types helps us know *where to look* when something goes wrong or when we investigate a security issue.
2. **Analyze authentication logs**
   Authentication logs record login-related activities like successful logins, failed attempts, password changes, and account lockouts. By analyzing these logs, we can check who logged in, from where, at what time, and whether the login was successful. This helps in identifying normal user behavior and spotting suspicious access.
3. **Identify failed logins**
   Failed login attempts happen when someone enters a wrong password or tries to access an account without permission. Multiple failed logins from the same user or IP address may indicate a brute-force attack. Identifying these attempts early helps prevent account compromise.
4. **Detect anomalies**
   An anomaly is any activity that looks unusual compared to normal behavior. Examples include logins at odd hours, access from unknown locations, or sudden spikes in activity. Detecting anomalies helps security teams notice potential attacks or misconfigurations quickly.
5. **Correlate events**
   Event correlation means connecting related log entries from different sources. For example, a failed login followed by a successful login from the same IP could indicate a password guess attack. Correlating events gives a complete picture of what actually happened instead of looking at logs in isolation.
6. **Learn SIEM basics**
   SIEM (Security Information and Event Management) tools collect logs from multiple systems, store them centrally, and analyze them in real time. SIEM helps automate log analysis, detect threats faster, and generate alerts. Learning SIEM basics is important for managing large volumes of logs efficiently.
7. **Write alerts**
   Alerts are rules set to notify administrators when suspicious activity occurs. For example, an alert can be created for more than five failed login attempts within a minute. Writing good alerts ensures that real security issues are noticed quickly without creating too many false alarms.
8. **Document findings**
   Documenting findings means writing down what was observed during log analysis—such as detected threats, anomalies, actions taken, and conclusions. Proper documentation is useful for audits, future reference, and improving security processes. It also helps teams learn from past incidents.