Investigating an Incident

Objective 4.9: Given a scenario, you must be able to use data sources to support an investigation

- **Investigating an Incident**
    - Data Sources for Incident Investigation
        - Dashboards and Automated Reports
            - Purpose
                - Provide high-level insights
            - Role
                - Initial overview of the security landscape
        - Vulnerability Scans
            - Purpose
                - Identify system vulnerabilities
            - Role
                - Foundation for understanding potential entry points
        - Packet Captures
            - Purpose
                - Capture and analyze network traffic
            - Role
                - Reveal communication patterns and potential threats
        - Logs (Various Types)
            - *Firewall Logs*
                - Monitor network traffic, detect unauthorized access

- *Application Logs*
  - Record application-specific events, identify abnormal behavior
- *Endpoint Logs*
  - Capture activities on individual devices
- *OS-Specific Security Logs*
  - Monitor operating system security events
- *IPS and IDS Logs and Alerts*
  - Track intrusion attempts and system compromises
- *Network Logs*
  - Record network activities and connections
- *Metadata*
  - Provide contextual information about other data sources

- **Investigative Data**
  - *SIEM (Security Information and Event Monitoring System)*
    - Real-time analysis of security alerts from applications and network hardware
    - Combination of different data sources into one tool
    - Provides a consolidated view of network activity
    - Allows for trend analysis, alert creation, and correlation of data
    - Considerations
      - Sensors
      - Sensitivity
      - Trends
      - Alerts
      - Correlation

- *Log Files*
  - Records events and messages in operating systems, software, and network devices
  - Includes network, system, application, security, web, DNS, authentication, dump files, VoIP, and call managers
- *Syslog, Rsyslog, Syslog-ng*
  - Tools for centralizing log data from different systems into a repository
  - Commonly used to feed data into SIEM
- *JournalCTL*
  - Linux command-line utility for querying and displaying logs from the Journal Daemon (SystemD's logging service)
- *NXLog*
  - Multi-platform, open-source log management tool
  - Identifies security risks and analyzes logs from server, OS, and applications
- *NetFlow*
  - Network protocol for collecting active IP network traffic data
  - Provides information on source, destination, volume, and paths
- *SFlow (Sampled Flow)*
  - Open-source alternative to NetFlow
  - Exports truncated packets and interface counter for network monitoring
- *IPFIX (Internet Protocol Flow Information Export)*
  - Universal standard for exporting IP flow information
  - Used for mediation, accounting, and billing by defining data format for exporters and collectors
- *Metadata*
  - Data that describes other data

- Useful for understanding details about events, calls, emails, web visits, and files during investigations
- Use Cases for Metadata
  - Email
    - Analyze metadata for phishing campaigns
  - Mobile
    - Review data transfer, call duration, and contacts
  - Web
    - Determine website visits and user behavior
  - File
    - Examine file details, such as creation time and viewer statistics

- **Dashboards**
  - *Dashboards*
    - Graphical displays of information across multiple systems
  - *Single Pane of Glass*
    - A single screen for analysts to access everything across the organization
  - *Splunk*
    - A big data platform for ingesting various types of data, including security and incident response data
    - Collects data from firewalls, applications, endpoints, operating systems, intrusion detection systems, intrusion prevention systems, antivirus software, and networks
  - Dashboards help analyze trends over time and inform actions
  - Use the dashboard as a central starting point for investigations and incident response

- **Automated Reports**
    - *Automated Reports*
        - Generated by computer systems to provide information about various aspects of a network's security
        - Common sources are antivirus software, endpoint detection response capabilities, and other security tools
    - Automated Security Incident Report Key Elements
        - *Report ID*
            - A unique identifier for the report
        - *Generation date*
            - The date the report was generated
        - *Report period*
            - The time frame covered by the report
        - *"Prepared by"*
            - The entity responsible for creating the report
        - *Executive Summary*
            - Provides a brief overview of the report's content, helping readers determine its relevance
        - *Incident Alerts*
            - Can be categorized into different levels
                - Critical
                - High
                - Moderate
                - Informational

- Incident Details
  - Timestamps
  - User accounts
  - Affected systems
  - Incident descriptions
  - Actions taken
    - Automated responses can include suspending user accounts, blocking IP addresses, and resetting passwords
    - Outbound traffic and software installations may trigger alerts, which require investigation to determine their nature and potential security implications
- *Incident Analysis*
  - May include threat trends, user behavior, and data flow anomalies
- *Security Recommendations*
  - Suggest actions to address identified security issues
- *Conclusion*
  - Summary of the report's findings and contains outlines of any further actions to be taken
- *Appendices*
  - May include log snippets, IP addresses, domains, or other relevant data

- Automation and orchestration enable real-time responses to security incidents, helping to prevent major security breaches and network outages

- **Vulnerability Scans**
  - *Vulnerability Scan Report*
    - Generated automatically after completing a vulnerability scan

- Analysis of the report is essential to confirm the validity of identified vulnerabilities

- False Positives
  - Vulnerability scanners may produce false positives, meaning they report vulnerabilities that don't actually exist on your system
  - It is crucial to differentiate real vulnerabilities from false positives
- Analysis of Vulnerabilities
  - For each identified vulnerability, assess whether it was detected by the scanner and if it exists on your system
  - Determine the severity and criticality of each vulnerability
  - Create a plan of action and milestones for remediation
- Components of a Vulnerability Scan Report
  - Report ID
  - Scan Date and Time
  - System or Software Version
  - *Scan Initiator*
    - The person who ran the scan
  - *Executive Summary*
    - Highlights themes and trends for large networks
  - Vulnerabilities – listed by severity (critical, high, medium, low, informational) or by hosts
    - CVE (Common Vulnerability and Exposure) ID – Vulnerability ID
      - CVE website (cve.org) contains detailed information about vulnerabilities
    - Description
    - Affected system

        - Impact
        - *Common Vulnerability Scoring System (CVSS) Score*
            - Measures severity
        - Remediation Recommendations
    - Additional Findings
    - Recommendations
    - Conclusion

- **Packet Captures**
    - *Packet Capture*
        - Captures data going to or from a network device
        - Can be set up on a span port to capture all data going to and from devices on the network
        - Packet captures in exam are typically short snippets, not massive data dumps
    - Packet Capture Columns
        - *Number*
            - Packet sequence number in the capture
        - *Time*
            - Elapsed time since the capture started
        - *Source/Destination IP Addresses*
            - Show where the data is coming from and going to
        - *Protocol*
            - Typically TCP or UDP
        - *Length*
            - The size of the packet

        - *Info*
            - Provides information from the packet header, including flags, sequence, window, length, MSS, source port, and destination port
    - Look for patterns that indicate attack types, such as SYN floods or DDoS attacks
    - Consider the relationship between source and destination IP addresses to identify the type of attack

- **Metadata**
    - *Metadata*
        - Information about a file, application, or other data
    - *MD5/SHA256 Checksum*
        - Serves as unique digital fingerprint for file identification, including potential malware