## **Project: Investigation of a Data Breach**

### **Objective:**

Investigation of a data breach on a renowned website to test investigative and forensic skills.

### **Scenario:**

#### **Company Name: ABC SecureBank (a highly reputable financial institution).**

#### **Breach Discovery:**

* The breach was identified during a routine security audit.
* Sensitive customer data, including names, account numbers, and transaction history, may have been exposed.

#### **Scope of Breach:**

* Potential exposure of critical customer information.

### **Real-Life Example Scenario:**

#### **Example Company: Equifax (based on the 2017 data breach incident).**

#### **Incident Summary:**

* Equifax, a consumer credit reporting agency, suffered a major data breach in 2017.
* Sensitive data, including Social Security numbers, credit card numbers, and driver’s license information, was exposed.
* The breach was attributed to unpatched software vulnerabilities in their web application framework (Apache Struts).

### **Tasks and Execution:**

#### **1. Incident Analysis:**

##### **Objective:**

* Investigate how the breach occurred.

##### **Findings:**

* **Point of Entry:** A vulnerability in an unpatched Apache Struts framework allowed unauthorized access.
* **Extent of Breach:** Data of over 147 million individuals was exposed.
* **Timeframe:** Unauthorized access began in mid-May 2017 and was discovered in late July 2017.

##### **Tools Used:**

* Wireshark for analyzing network traffic.
* ELK Stack (Elasticsearch, Logstash, Kibana) for log analysis.

#### **2. Forensic Analysis:**

##### **Objective:**

* Conduct digital forensics on affected systems to identify malware or suspicious activities.

##### **Findings:**

* **Evidence:** Logs indicated repeated exploit attempts targeting the Apache Struts vulnerability.
* **Malware:** No persistent malware was found, but the attackers deployed scripts to exfiltrate data.

##### **Steps Taken:**

1. Collected system logs and reviewed server configurations.
2. Performed memory dumps for analysis.
3. Captured file integrity changes using tools like Tripwire.

#### **3. Data Recovery:**

##### **Objective:**

* Determine the type and quantity of exposed data and develop a recovery strategy.

##### **Findings:**

* **Exposed Data:** Names, Social Security numbers, birth dates, addresses, and driver’s license details.
* **Recovery Strategy:**
  1. Isolated the affected servers.
  2. Restored systems from secure backups.
  3. Implemented stricter access controls and encryption protocols.

#### **4. Regulatory Compliance:**

##### **Objective:**

* Ensure compliance with legal and regulatory reporting requirements.

##### **Actions:**

1. Filed breach notifications with relevant regulatory bodies within the stipulated timeline.
2. Ensured compliance with GDPR (General Data Protection Regulation) and state-specific laws like CCPA (California Consumer Privacy Act).
3. Consulted legal advisors to mitigate potential lawsuits.

#### **5. Communication and Notification:**

##### **Objective:**

* Notify affected stakeholders clearly and transparently.

##### **Communication Plan:**

1. **Customers:** Sent personalized emails detailing the breach, steps to protect themselves, and free credit monitoring services.
2. **Media:** Issued a public statement to address concerns and provide updates.
3. **Regulators:** Submitted detailed reports with timelines and mitigation actions.

#### **6. Post-Incident Review:**

##### **Objective:**

* Conduct a thorough review to identify security weaknesses.

##### **Recommendations:**

1. **Patch Management:** Ensure timely updates of all software and frameworks.
2. **Network Segmentation:** Limit access to sensitive data.
3. **Monitoring:** Deploy advanced intrusion detection systems (IDS) and threat intelligence platforms.
4. **Training:** Conduct regular security awareness training for employees.
5. **Audits:** Perform regular penetration testing and vulnerability assessments.

### **Deliverables:**

1. **Incident Report:**
   * Detailed timeline of the breach.
   * Analysis of vulnerabilities and attacker behavior.
2. **Forensic Report:**
   * Evidence collected and tools used.
   * Detailed findings from system and memory analysis.
3. **Recovery Plan:**
   * Actionable steps to contain and recover from the breach.
4. **Compliance Report:**
   * Documentation of compliance with regulatory requirements.
5. **Post-Incident Report:**
   * Recommendations for improving overall security posture.

### **Assessment Criteria:**

1. **Investigative Skills:** Ability to identify the breach's root cause.
2. **Forensic Proficiency:** Skillful use of forensic tools and evidence collection.
3. **Recovery Strategy:** Effectiveness of data recovery and containment plan.
4. **Compliance Knowledge:** Adherence to legal requirements.
5. **Presentation:** Clarity and thoroughness in documentation and communication.

### **Sample Timeline:**

1. **Week 1:** Incident analysis and breach containment.
2. **Week 2:** Forensic analysis and evidence collection.
3. **Week 3:** Data recovery and regulatory compliance actions.
4. **Week 4:** Communication and notification.
5. **Week 5:** Post-incident review and reporting.

This project outlines a structured approach to investigating a data breach, focusing on real-world scenarios and challenges faced by cybersecurity professionals.