Experiment No. 10

Aim: Case Study: Analyze a real-world security breach (e.g. Facebook, Equifax) and prepare a report with mitigations.

Learning Objective: The objective of this case study is to deconstruct the 2017 Equifax data breach to understand the sequence of events, identify the multiple cascading failures in security processes, and formulate a comprehensive mitigation strategy to prevent similar incidents.

Case Study: Equifax Data Breach (2017):

Background

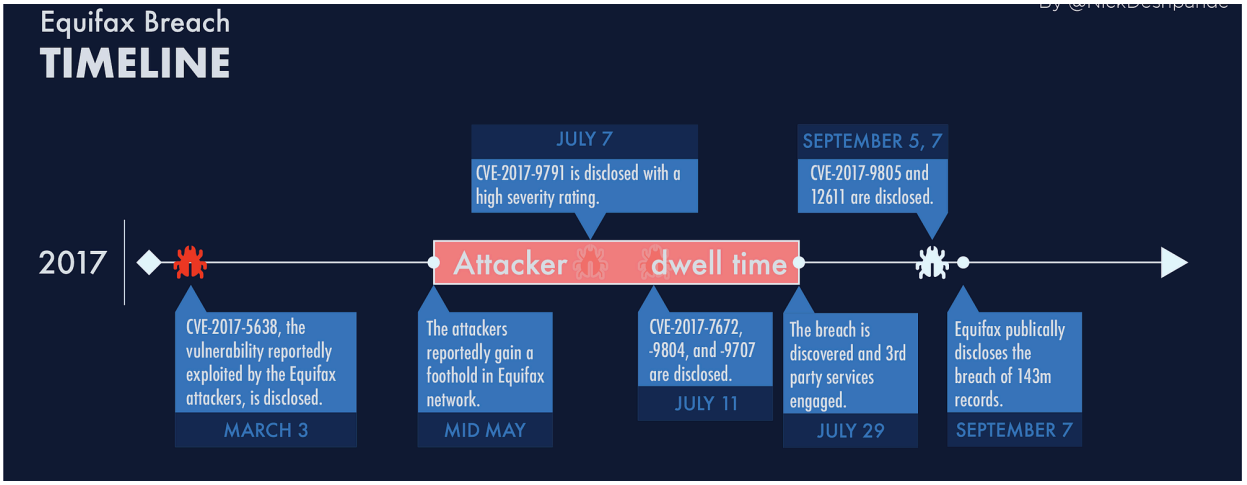
Equifax is one of the three largest consumer credit reporting agencies in the United States, responsible for managing the highly sensitive financial and personally identifiable information (PII) of hundreds of millions of people. In September 2017, the company announced it had suffered a massive data breach that exposed the names, Social Security numbers, birth dates, addresses, and driver's license numbers of an estimated 147 million individuals. The breach was one of the most severe in history due to the high sensitivity of the compromised data.

Attack Timeline and Analysis

The breach was not the result of a sophisticated, zero-day exploit but rather a chain of basic security failures.

1. **March 7, 2017 - The Vulnerability:** A critical vulnerability is discovered in **Apache Struts** (CVE-2017-5638), a popular open-source framework used for building web applications. A patch is released the same day.
2. **March 9, 2017 - The Notification:** The US Department of Homeland Security's Computer Emergency Readiness Team (US-CERT) issues an alert about the vulnerability. Equifax's internal security team receives this alert and circulates it internally, requesting that all relevant systems be patched within 48 hours.
3. **March 15, 2017 - The Failure to Scan:** Equifax runs scans to find vulnerable versions of Apache Struts on its network. However, the scans **fail to identify** the vulnerable system that was later exploited. This points to an incomplete or faulty asset inventory.

4. **May 13, 2017 - The Initial Breach:** Attackers, having discovered the unpatched, internet-facing Equifax server, exploit the Apache Struts vulnerability to gain their initial foothold in the network.
5. **May 2017 to July 2017 - The Dwelling and Exfiltration:** For **76 days**, the attackers move laterally through Equifax's network, undetected. They locate databases containing PII, run dozens of queries to find sensitive data, and then compress and exfiltrate it in small chunks to avoid detection.
6. **July 29, 2017 - The Discovery:** Equifax's security team finally notices suspicious traffic when they renew an expired SSL certificate on an internal security monitoring device. With the certificate updated, the tool was able to decrypt and inspect traffic, immediately spotting the data exfiltration.



Key Failures and Mitigation Strategies

The breach was caused by a series of preventable failures. Below is an analysis of each failure and the corresponding mitigation strategy.

Failure 1: Ineffective Vulnerability Management

The root cause of the breach was the failure to patch a known critical vulnerability. The internal scans failed to even identify the vulnerable asset.

- **Mitigation Strategy: Robust Patch and Asset Management**
  - **Comprehensive Asset Inventory:** Implement an automated system to maintain a complete, real-time inventory of all hardware and software assets. You cannot protect what you do not know you have.

- **Automated Scanning and Patching:** Deploy automated vulnerability scanners that run continuously. Integrate them with a patch management system that can automatically deploy critical security patches within a strict, policy-defined timeframe (e.g., 24-48 hours for critical vulnerabilities).

Failure 2: Lack of Network Segmentation

Attackers were able to move from a public-facing web server to internal databases containing the company's "crown jewels." This indicates a flat, poorly segmented network.

- **Mitigation Strategy: Zero Trust and Micro-segmentation**
  - **Isolate Critical Systems:** Segment the network into smaller, isolated zones. A web server should never be in the same network segment as a critical database. Access between segments must be strictly controlled by firewalls.
  - **Implement Least Privilege:** Ensure that systems can only communicate with other systems that are absolutely necessary for their function. A breach of one system should not provide a gateway to the entire network.

Failure 3: Failure of Security Tools

The Intrusion Detection System (IDS) that should have spotted the data exfiltration was rendered useless for months because an internal SSL certificate had expired.

- **Mitigation Strategy: Proactive Security Tool Health Monitoring**
  - **Automated Certificate Management:** Use a Certificate Lifecycle Management (CLM) tool to automatically track, renew, and deploy all SSL/TLS certificates well before they expire.
  - **Continuous Monitoring of Security Tools:** The security tools themselves must be monitored. An alert should be generated if a critical security device (like an IDS) is not functioning correctly.

Learning Outcome: After analyzing this case, you will understand the critical importance of timely vulnerability management and proactive security monitoring within a large enterprise. You will also be able to identify systemic failures in security posture and recommend specific technical and procedural controls to protect sensitive data effectively.

Conclusion: The 2017 Equifax data breach stands as a stark reminder that the most damaging cyberattacks often exploit basic, well-known security weaknesses rather than complex, novel techniques. It was a catastrophic failure of foundational security processes, including asset management, patching, network segmentation, and operational oversight. The key takeaway for any organization is that cybersecurity is not just about buying advanced tools; it's about the disciplined and consistent execution of fundamental security hygiene. This case proves that neglecting the basics can, and will, lead to devastating consequences.

Name:

Class: BE-CSE

Roll No.:

For Faculty Use

Correction Parameters	**Formative Assessment [40%]**	**Timely completion of Practical [40%]**	**Attendance / Learning Attitude [20%]**	
Marks Obtained				