**Assignment 4**

1. **Research a high-profile security incident related to a CVE (e.g., Log4Shell - CVE-2021-44228). Answer:**

* **What was the root cause of the vulnerability?**

Ans:The vulnerability stemmed from improper handling of user input in the Apache Log4j library's logging functionality. Specifically, Log4j allowed JNDI (Java Naming and Directory Interface) lookups via user-supplied data. Attackers could exploit this by sending crafted log messages containing malicious JNDI lookups, leading to remote code execution (RCE).

* **What impact did it have on organizations and users?**

Ans: **Organizations**: Affected virtually any Java application using Log4j, impacting major companies like Amazon, Apple, Microsoft, and Cloudflare.

**Users**: Sensitive data breaches, system hijacks, and service outages due to widespread exploitation.

* **How was the vulnerability mitigated?**

Ans: **Patching**: Immediate updates to Log4j 2.15.0 and later to 2.16.0 when additional issues were discovered.

**Disabling JNDI Lookups**: For systems unable to patch, disabling JNDI lookups or setting system properties to prevent exploit paths.

**WAF Rules and Network Monitoring**: Deployment of Web Application Firewall rules to block exploit attempts and monitor unusual traffic patterns.

1. **EternalBlue (CVE-2017-0144) - The Exploit Behind WannaCry**

* **What is EternalBlue, and how does it exploit the SMB protocol?**

Ans: EternalBlue is an exploit developed by the NSA and later leaked by the hacking group Shadow Brokers. It targeted a vulnerability in Microsoft’s Server Message Block (SMB) protocol v1, enabling unauthenticated remote code execution on unpatched systems by sending specially crafted packets.

* **How was EternalBlue used in the WannaCry ransomware attack?**

Ans:WannaCry used EternalBlue to propagate itself across networks rapidly. Once a system was infected, it encrypted files and demanded ransom in Bitcoin, causing widespread disruption globally.

* **Why did EternalBlue remain a significant risk even after Microsoft released a patch?**

Ans: Many systems in critical infrastructure (e.g., hospitals, manufacturing), were slow to apply patches. Older versions of Windows (like Windows XP) no longer received regular updates but were still widely used. Large organizations with complex IT environments struggled to identify all vulnerable systems.

* **Suppose you are a security engineer in 2017—what immediate actions would you take after learning about this CVE?**

Ans: Taking the system offline. Contaminating it from the network. Updating patches and limiting movement of the data across the network. Ensure reliable offline backups and update incident response plans.

* **How did the cybersecurity community respond to the widespread impact of WannaCry?**

Ans: Governments and security firms issued urgent patching advisories. Researcher Marcus Hutchins accidentally discovered a domain killswitch that slowed the attack. Raised global awareness of ransomware risks and the importance of proactive patch management.

**3. Apache Struts Vulnerability (CVE-2017-5638) - The Equifax Breach**

* **How did this Apache Struts vulnerability contribute to the Equifax data breach?**

Ans: The Apache Struts vulnerability allowed attackers to perform remote code execution via maliciously crafted Content-Type HTTP headers. Equifax failed to patch this vulnerability, enabling attackers to access sensitive data, including Social Security numbers, birth dates, and addresses of 147 million people.

* **Why is input validation important in preventing such attacks?**

Ans: Proper input validation prevents untrusted data from being processed in ways that could compromise system integrity. In this case, inadequate validation of HTTP headers led to arbitrary code execution.

* **What was the main reason Equifax failed to patch the vulnerability in time?**

Ans: Internal miscommunication meant security teams were unaware of the patch requirement. Lack of a robust patch management process to track vulnerabilities and ensure timely updates.

* **Discuss the legal and reputational consequences Equifax faced due to this breach**

Ans: Equifax faced numerous lawsuits, culminating in a $700 million settlement. Massive loss of public trust and resignation of key executives, including the CEO.

* **What lessons can organizations learn from this incident regarding patch management and vulnerability disclosure?**

Ans: Establish clear processes to track and apply security patches promptly. Transparent communication about vulnerabilities helps maintain trust. Frequent internal audits to detect unpatched systems.

**4. Sony PlayStation Network (PSN) Breach (2011) - CVE-2011-1290**

* **What vulnerability (CVE-2011-1290) was exploited in the Sony PSN breach?**

Ans: The attackers exploited a vulnerability in Sony’s Web Application Server involving improper SSL certificate handling and poor network segmentation, allowing unauthorized access to Sony’s systems.

* **How did the attackers gain access to the PlayStation Network’s database?**

Ans: They used a combination of SQL Injection and exploitation of weak SSL implementations (CVE-2011-1290) to infiltrate Sony’s database, exposing personal information of 77 million users, including credit card data.

* **What were the major consequences of this breach for Sony and its users?**

Ans: Estimated financial losses of over $170 million, legal actions, and damage to its reputation. Risk of identity theft and fraudulent credit card transactions. PSN was shut down for 23 days, disrupting services for millions.

* **Sony shut down PSN for 23 days after the attack. What security measures should have been in place to prevent such an extended outage?**

Ans: Identify vulnerabilities before attackers can exploit them. Limit the damage by isolating critical systems. Robust Incident Response Plan: Faster recovery processes to minimize downtime.

* **How did Sony respond legally and technically after the breach?**

Ans: Faced numerous lawsuits and had to testify before the U.S. Congress. Overhauled its security infrastructure, hired new security experts, and provided one year of free identity theft protection to affected users.