### **Discussion Questions for the JPMorgan Chase Data Breach of 2014**

Answer the following questions based on the information provided about the JPMorgan Chase data breach. You are encouraged to use diagrams and charts to illustrate your ideas.

**1. What happened in the JPMorgan Chase data breach of 2014?**

* A) Hackers gained access to JPMorgan's customer accounts through online banking.
* B) Attackers exploited a lack of two-factor authentication on a server, which allowed them to access over 90 servers and steal personal data of 76 million households.
* C) The bank’s mobile app was compromised by malware.
* D) JPMorgan's ATMs were infected with ransomware.

**Answer: B) Attackers exploited a lack of two-factor authentication on a server, which allowed them to access over 90 servers and steal personal data of 76 million households.**

**2. What are two effective security mechanisms that could guard against vulnerabilities like those exploited in the JPMorgan breach?**

* A) Implementing two-factor authentication (2FA) and network segmentation.
* B) Using only encrypted email services.
* C) Employing password managers for all employees.
* D) Disabling user access to all servers.

**Answer: A) Implementing two-factor authentication (2FA) and network segmentation.**

**3. If you were a hacker, how would you launch a similar attack on another financial institution?**

* A) I would use phishing emails to gain initial access, then exploit weak security on internal servers and escalate privileges to access sensitive data.
* B) I would create a fake mobile app to steal user credentials.
* C) I would directly hack into customer accounts through an unprotected Wi-Fi network.
* D) I would disable firewalls using social engineering.

**Answer: A) I would use phishing emails to gain initial access, then exploit weak security on internal servers and escalate privileges to access sensitive data.**

**4. What are some ways to perform privilege escalation in financial networks?**

* A) Exploiting unpatched vulnerabilities, abusing weak password policies, or misconfigured access controls.
* B) Sending spam emails.
* C) Guessing passwords until access is gained.
* D) Using antivirus software to disable security tools.

**Answer: A) Exploiting unpatched vulnerabilities, abusing weak password policies, or misconfigured access controls.**

**5. How can vulnerability scanning be performed in a financial institution's network?**

* A) Using tools like Nessus, OpenVAS, or Qualys to scan for unpatched systems and misconfigurations.
* B) Sending out phishing emails to employees.
* C) Using VPN to bypass security protocols.
* D) Installing malware on servers to track employee activity.

**Answer: A) Using tools like Nessus, OpenVAS, or Qualys to scan for unpatched systems and misconfigurations.**

**6. As the CTO of JPMorgan Chase, what measures would you implement to enhance the security of financial transaction systems?**

* A) Implementing end-to-end encryption for all transactions and real-time fraud detection systems.
* B) Disabling access to external payment systems.
* C) Limiting all transactions to certain hours of the day.
* D) Using email confirmations for all transactions.

**Answer: A) Implementing end-to-end encryption for all transactions and real-time fraud detection systems.**

**7. How should financial institutions balance the need for third-party integrations with maintaining data security standards?**

* A) Conduct regular security audits of third-party vendors and enforce strict data access controls.
* B) Disable third-party integrations altogether.
* C) Allow third parties unlimited access to internal systems for convenience.
* D) Outsource all security to third-party vendors.

**Answer: A) Conduct regular security audits of third-party vendors and enforce strict data access controls.**

**8. If you were responsible for mitigating the misuse of stolen data, what steps would you take?**

* A) Implement encryption for all stored data and monitor for suspicious activity related to stolen information.
* B) Ban all external communications involving sensitive data.
* C) Block access to stolen data after 24 hours.
* D) Encourage users to share personal data openly.

**Answer: A) Implement encryption for all stored data and monitor for suspicious activity related to stolen information.**

**9. What IT weaknesses paved the way for the JPMorgan Chase hackers?**

* A) Lack of two-factor authentication, poor patch management, and insufficient network segmentation.
* B) Use of outdated ATM machines.
* C) Inadequate mobile app security.
* D) Allowing employees to work from home without security measures.

**Answer: A) Lack of two-factor authentication, poor patch management, and insufficient network segmentation.**

**10. As the CIO of JPMorgan Chase, how would you improve IT security?**

* A) Implement a comprehensive security strategy that includes multi-factor authentication, frequent security audits, real-time monitoring, and employee security training.
* B) Ban all employee access to the internet.
* C) Disallow access to the company’s network from mobile devices.
* D) Reduce the number of security tools to minimize complexity.

**Answer: A) Implement a comprehensive security strategy that includes multi-factor authentication, frequent security audits, real-time monitoring, and employee security training.**