### **Discussion Questions for the SWIFT Banking Hack of 2015**

Answer the following questions based on the information provided about the SWIFT Banking Hack. You are encouraged to use diagrams and charts to illustrate your ideas.

**1. What happened in the SWIFT Banking Hack of 2015?**

* A) Hackers infiltrated customer accounts through online banking portals.
* B) Attackers used stolen credentials and malware to exploit vulnerabilities in SWIFT’s Alliance Access software, allowing fraudulent transfers of millions of dollars.
* C) Hackers exploited vulnerabilities in ATM machines to withdraw cash.
* D) The SWIFT network was directly attacked through a zero-day vulnerability.

**Answer: B) Attackers used stolen credentials and malware to exploit vulnerabilities in SWIFT’s Alliance Access software, allowing fraudulent transfers of millions of dollars.**

**2. What are two effective security mechanisms to guard against vulnerabilities like those exploited in the SWIFT hack?**

* A) Implementing multi-factor authentication (MFA) and network segmentation.
* B) Using only encrypted email services for financial communications.
* C) Disabling SWIFT access for all external banks.
* D) Employing firewalls on all communication channels.

**Answer: A) Implementing multi-factor authentication (MFA) and network segmentation.**

**3. If you were a hacker, how would you launch a similar attack on a financial institution using the SWIFT network?**

* A) Use phishing emails to gain credentials, install malware on critical systems, and escalate privileges to access SWIFT’s systems, then use fraudulent messages to transfer large sums of money.
* B) Hack into the SWIFT mobile app and steal user credentials.
* C) Use brute force to guess SWIFT credentials.
* D) Overload the SWIFT network with spam requests until the system crashes.

**Answer: A) Use phishing emails to gain credentials, install malware on critical systems, and escalate privileges to access SWIFT’s systems, then use fraudulent messages to transfer large sums of money.**

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

* A) Exploiting unpatched vulnerabilities, abusing weak access controls, using malware to steal administrator credentials, or leveraging misconfigured systems.
* B) Guessing passwords and bypassing firewall rules.
* C) Using Wi-Fi networks to bypass security.
* D) Sending large amounts of spam to crash the server.

**Answer: A) Exploiting unpatched vulnerabilities, abusing weak access controls, using malware to steal administrator credentials, or leveraging misconfigured systems.**

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

* A) Using tools like Nessus, Qualys, and OpenVAS to detect unpatched systems, misconfigurations, or open ports that could be exploited.
* B) Sending phishing emails to gather employee credentials.
* C) Manually checking every server for weaknesses.
* D) Using antivirus software to scan for vulnerabilities.

**Answer: A) Using tools like Nessus, Qualys, and OpenVAS to detect unpatched systems, misconfigurations, or open ports that could be exploited.**

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

* A) Use end-to-end encryption for all SWIFT messages and implement regular security audits of transaction systems.
* B) Disable SWIFT services for all foreign transactions.
* C) Only allow transactions during business hours.
* D) Increase the number of daily transaction limits.

**Answer: A) Use end-to-end encryption for all SWIFT messages and implement regular security audits of transaction systems.**

**7. SWIFT introduced new mandatory controls after the hack. How would you ensure compliance while minimizing alert overload?**

* A) Implement a centralized SIEM system to manage alerts, prioritize critical alerts, and fine-tune alert thresholds to reduce false positives.
* B) Disable low-priority alerts to avoid distractions.
* C) Hire more staff to manually review every alert.
* D) Only monitor alerts for fraudulent transactions.

**Answer: A) Implement a centralized SIEM system to manage alerts, prioritize critical alerts, and fine-tune alert thresholds to reduce false positives.**

**8. What solution would you propose to segment and categorize SWIFT’s networks and resources?**

* A) Use network segmentation to separate SWIFT operations from other corporate systems and implement access controls to limit who can access sensitive systems.
* B) Only allow SWIFT services to operate on weekends.
* C) Create a single network for all operations to simplify monitoring.
* D) Disable internet access for employees who handle SWIFT transactions.

**Answer: A) Use network segmentation to separate SWIFT operations from other corporate systems and implement access controls to limit who can access sensitive systems.**

**9. What IT weaknesses were present in SWIFT’s systems that enabled the hack?**

* A) Lack of multi-factor authentication, poor network segmentation, and insufficient monitoring of third-party access to SWIFT.
* B) Weak encryption of all financial transactions.
* C) Inability to detect malware within emails.
* D) Use of outdated SWIFT versions by every bank.

**Answer: A) Lack of multi-factor authentication, poor network segmentation, and insufficient monitoring of third-party access to SWIFT.**

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

* A) Implement a multi-layered security strategy with continuous monitoring, network segmentation, regular security audits, and the use of encryption for all communication.
* B) Disable SWIFT services for small banks.
* C) Prevent employees from accessing the SWIFT system from home.
* D) Hire third-party consultants to handle all security matters.

**Answer: A) Implement a multi-layered security strategy with continuous monitoring, network segmentation, regular security audits, and the use of encryption for all communication.**