Report on Penetration Testing
Conducted on the Physical and Information Security Systems of Qi Bank.

By
Timi Ogunjobi
Information Security Analyst & Project Manager
timiasservice@gmail.com
470-727-0678

Executive Summary

This report presents a comprehensive overview of the penetration testing conducted on the physical and information security systems of Qi Bank. The purpose of this assessment was to identify potential vulnerabilities within the bank's security posture and to provide actionable recommendations to mitigate these risks. The testing covered various aspects, including physical security controls, network security, application security, and employee security awareness.

Scope of the Penetration Test

1. Physical Security Controls

- Access Controls: The evaluation of mechanical and electronic systems designed to limit access to the bank's facilities. This included key card systems, biometric scanners (such as fingerprint and retinal scanners), and physical keys. Special attention was given to the integration and redundancy of these systems to prevent unauthorized entry through tailgating or bypass mechanisms.

- Surveillance Systems: Analysis of the deployment and effectiveness of CCTV cameras, motion detectors, and alarm systems. This also encompassed the review of the surveillance monitoring protocols, data storage policies, and the ability of security personnel to respond to incidents identified by these systems.

- **Intrusion Detection Mechanisms**: Assessment of both physical intrusion detection systems (such as glass break sensors and door sensors) and cyber intrusion detection systems. The focus was on the integration of these systems into the overall security posture of the bank, ensuring that any unauthorized access or attempts would trigger immediate and appropriate response actions.

2. Network Security

- Firewalls: Examination of the configuration and effectiveness of firewall systems in place to protect the internal network from unauthorized external access. This included the review of rules, NAT policies, and the ability of the firewalls to defend against sophisticated cyber attacks.

- Intrusion Detection Systems: Assessment of the deployment and tuning of intrusion detection systems (IDS) and intrusion prevention systems (IPS) to detect and respond to malicious network traffic and cyber threats.

- Network Segmentation: Evaluation of the network architecture with a focus on segmentation practices. This involved ensuring that sensitive information and critical systems (such as transaction processing systems and customer databases) were isolated from less secure networks, thereby limiting the potential impact of a network breach.

3. Application Security

- Web Applications: Testing of public-facing web applications for common vulnerabilities such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). The security of online banking portals was a priority, with an emphasis on authentication, data encryption, and secure session management.

- Mobile Banking Apps: Examination of mobile banking applications for security weaknesses, including insecure data storage, improper use of cryptographic functions, and vulnerabilities to man-in-the-middle (MITM) attacks.

- Internal Software: Analysis of internal software applications used by bank employees for potential vulnerabilities. This included applications for customer relationship management (CRM), financial transactions, and internal communications.

4. Employee Security Awareness

- Phishing Attempts: Conducting simulated phishing campaigns to evaluate the awareness and response of bank employees to malicious emails. This tested the ability of employees to identify and report potential phishing attempts.

- **Social Engineering Tactics**: Execution of social engineering exercises aimed at assessing the susceptibility of employees to techniques such as pretexting, baiting, and tailgating. This involved attempts to gain physical access to restricted areas or to obtain sensitive information through deceit.

Methodology

1. Planning and Reconnaissance

- Objective Setting: Defining clear objectives and expected outcomes for the penetration test, including specific systems and assets to be tested, while ensuring compliance with legal and ethical standards.
- Information Gathering: Collecting information about the bank's physical infrastructure and digital assets. This included public domain information, network architecture, application details, and physical security measures.

2. Threat Modeling

- Identify Threat Actors: Determining potential threat actors, including internal threats, external cyber criminals, and state-sponsored hackers, and their possible motives.
- **Identify Attack Vectors:** Outlining possible attack vectors for both physical and cyber threats, taking into consideration the information gathered during the reconnaissance phase.

3. Vulnerability Analysis

- **Automated Scanning**: Utilizing automated tools to scan for vulnerabilities in the bank's network, applications, and systems. This included vulnerability scanners, web application scanners, and network mappers.
- **Manual Testing and Verification**: Conducting manual testing to verify automated scan results, identify false positives, and uncover issues that automated scans may miss, particularly in the context of complex application logic or sophisticated physical security systems.

4. Exploitation

- **Simulated Attacks**: Executing controlled attacks to exploit identified vulnerabilities without causing harm or disruption. This included both cyber attacks on networks and applications and physical intrusion attempts on the bank’s facilities.
- **Breach Simulation**: Simulating breaches to test the efficacy of incident response protocols and the ability of security systems to detect and mitigate unauthorized access.

5. Post-Exploitation and Analysis

- **Data Access and Exfiltration:** Assessing the impact of successful exploitations, including the types of data accessible and the potential for data exfiltration, while always adhering to ethical guidelines.
- **Persistence:** Evaluating the potential for attackers to maintain access within the system, simulating advanced persistent threats (APTs).

6. Reporting and Recommendations

- Comprehensive Reporting: Documenting all findings, including successful exploitations, vulnerabilities, and security gaps identified during the test. The report prioritizes issues based on their severity and potential impact.
- Actionable Recommendations: Providing detailed, actionable recommendations for remediating identified vulnerabilities, enhancing security postures, and improving incident response capabilities.

Alignment with Industry Best Practices

- OWASP Guidelines: Adhering to the OWASP Top 10 for application security testing ensured a focus on the most critical web application security risks.
- PSP Guidelines: Following the Physical Security Professional (PSP) guidelines ensured that the assessment of physical security controls was comprehensive, covering aspects such as risk analysis, security design, and integration of physical security systems.
- **Manual Techniques and Ethical Hacking Expertise**: Leveraging manual testing techniques and the expertise of certified ethical hackers to complement automated tools and provide insights into complex security vulnerabilities.

This methodology not only facilitated a thorough examination of the bank's security measures but also ensured that the testing was conducted in a controlled, ethical manner, minimizing any risk to the bank's operations while identifying critical vulnerabilities and security improvements.

Key Findings

Physical Security

- Access Control Vulnerabilities: The assessment identified that several critical access points within the bank’s infrastructure rely solely on key card systems without the added layer of biometric authentication. This reliance on a single authentication factor makes the system vulnerable to key card cloning and social engineering tactics, allowing unauthorized individuals to gain access.

- **Surveillance Gaps**: The testing uncovered significant surveillance coverage gaps in several high-risk areas, including server rooms and sensitive document storage rooms. These gaps in surveillance coverage provide opportunities for unauthorized individuals to access and potentially exploit sensitive areas without being detected.

Network Security

- **Firewall Misconfigurations:** The analysis of the bank's firewall configurations revealed improperly configured rules that permit unnecessary traffic from both the internet and between internal networks. This misconfiguration creates potential entry points for attackers to exploit and gain access to sensitive areas of the network.

- Insecure Protocols: Several internal applications were found to be using outdated and insecure communication protocols, such as FTP and Telnet, for data transmission. These protocols lack encryption, making data susceptible to interception, modification, and eavesdropping during transmission.

Application Security

- **Injection Vulnerabilities:** Our testing identified critical SQL injection vulnerabilities within the online banking web application. Attackers could exploit these vulnerabilities to execute arbitrary SQL commands, potentially accessing, modifying, or deleting sensitive customer data without authorization.

- Inadequate Session Management: The mobile banking applications exhibited weaknesses in session management, specifically around session expiration and secure cookie handling. This inadequacy could allow attackers to hijack active sessions, gaining unauthorized access to user accounts and sensitive financial information.

Employee Security Awareness

- **Phishing Susceptibility:** Simulated phishing exercises demonstrated that a significant number of employees are unable to recognize or properly respond to phishing attempts. Employees frequently interacted with malicious links and attachments, indicating a critical need for ongoing security awareness training to enhance the bank's defense against social engineering attacks.

Recommendations

Physical Security

1. Implement Multi-factor Authentication at All Access Points: Introduce a multi-layered authentication mechanism combining key cards with biometric verification (such as fingerprint, facial recognition, or retinal scans) at all critical access points. This approach significantly reduces the risk of unauthorized access due to lost, stolen, or cloned key cards.

2. **Enhance Surveillance Coverage:** Perform a comprehensive review of the current surveillance system to identify and address coverage gaps. Install additional cameras in identified blind spots, particularly in sensitive areas such as server rooms, cash handling areas, and entry/exit points. Ensure that surveillance systems are equipped with motion detection capabilities and are monitored in real-time by security personnel to facilitate immediate response to unauthorized activities.

Network Security

1. **Review and Update Firewall Configurations:** Conduct a thorough audit of existing firewall rules and configurations to ensure that only necessary traffic is allowed, based on the principle of least privilege. Eliminate redundant, obsolete, or overly permissive rules. Regularly review and update these configurations to adapt to changing security needs and to protect against emerging threats.

2. **Phase Out the Use of Insecure Protocols:** Identify and discontinue the use of outdated and insecure communication protocols (e.g., FTP, Telnet, HTTP) within the bank's network. Transition to secure alternatives such as SFTP, SSH, and HTTPS to ensure the confidentiality and integrity of data during transmission. Implementing encrypted protocols will protect against eavesdropping and

data interception attacks.

Application Security

1**. Remediate Injection Vulnerabilities:** Address SQL injection and other injection-related vulnerabilities by implementing rigorous input validation, sanitation procedures, and parameterized queries. Adopt secure coding practices and utilize prepared statements to prevent attackers from injecting malicious code into the bank's applications. Regular code reviews and application security testing should be institutionalized to detect and remediate such vulnerabilities proactively.

2. **Strengthen Session Management:** Enhance the security of mobile banking applications by implementing robust session management policies. This includes enforcing secure cookie attributes (such as HttpOnly and Secure flags) and strict session expiration mechanisms. Develop and implement a comprehensive session handling strategy that includes secure generation, storage, and expiration of session tokens to mitigate the risk of session hijacking.

Employee Security Awareness

1. **Conduct Regular Security Awareness Training Sessions:** Develop an ongoing security awareness program that includes regular training sessions for all employees. These sessions should cover the recognition and response to phishing attempts, the dangers of social engineering tactics, secure handling of sensitive information, and adherence to security policies and procedures. Incorporate interactive elements such as simulated phishing exercises and gamified learning to enhance engagement and retention of security best practices.

Conclusion

The penetration test revealed several critical vulnerabilities within both the physical and information security systems of the bank. Addressing these vulnerabilities is imperative to safeguarding the institution's assets, customer data, and reputation. The recommendations provided herein should be prioritized and implemented in a timely manner to enhance the bank's overall security posture.