FORTRA

Pen Testing Use Case – Finance

Core Banking & Customer Portal Penetration Test

Background

A major retail bank relies on a cloud-hosted customer banking portal and an internally developed mobile app for millions of customers worldwide. The bank wants to ensure these systems are resistant to real-world cyberattacks that could compromise customer data, disrupt transactions, or damage trust.

Phase 1: Planning and Reconnaissance

To begin, Pen Testers gather as much information as possible about the bank's systems, employees, network, website, application, and architecture.

- **Passive Reconnaissance:** They use Open Source Intelligence (OSINT) techniques to gather information for social engineering attacks (via social media, the bank's website, public records, and online databases), as well as for technical inroads (IP addresses, domain names, and technologies used).
- **Active Reconnaissance:** They perform a perimeter test, probing the public-facing mobile app, the customer banking portal, and any other exposed services for vulnerabilities in line with OWASP Top 10 and CWE/SANS Top 25.

Phase 2: Scanning

Next, Pen Testers subject the bank's mobile app, customer portal, and other public-facing services to further investigation using automated tools that scan for exploitable weaknesses.

- **Validate Scans:** Core Impact can validate vulnerabilities from over 20 scanners, integrating with Fortra VM, Burpsuite, Nessus, Qualys, Tenable, and more.
- **Prioritize Findings:** After completing a scan of the environment, Pen Testers use Core Impact to provide a prioritized validation of the bank's internal weaknesses.

Phase 3: Gaining Access

Pen Testers attempt to gain control over the bank's services using the information gained in the Reconnaissance and Scanning stages.

- **External Application Testing:** They simulate attacker attempts to exploit customer-facing banking portals and APIs (e.g., injection, broken authentication, improper access controls).
- **API Security Review:** Testers focus their efforts on FinTech integrations and open banking APIs (in line with PSD2 compliance).
- **Payment Workflow Tampering:** Pen Testers try to manipulate transaction parameters or bypass transaction confirmation steps.
- **Mobile App Reverse Engineering:** Testers assess whether the mobile app's code, APIs, and local storage leak sensitive data or expose keys.
- **Social Engineering:** They leverage Core Impact to conduct an automated phishing campaign. Posing as the FDIC, Pen Testers create a simulated malicious phishing email that notifies banking executives about the soon-to-be-retired FFIEC Cybersecurity Assessment Tool (CAT). The link provided in the email contains malware that will download upon clicking.

Phase 4: Maintaining Access

Pen Testers now look to leverage initial access, maintain persistence, and demonstrate avenues for additional damage within the bank's digital infrastructure.

- **Privilege Escalation Attempts:** They test for ways to move from a standard customer account to administrative or back-end access. With Core Impact, this step is automated.
- **Lateral Movement:** Using elevated access, Pen Testers attempt to pivot into systems holding sensitive PII, such as databases containing account numbers, addresses, and login credentials.
- **Data Exfiltration Simulation:** Using Core Impact, testers assess how easily sensitive datasets could be extracted and whether the data loss prevention (DLP) tools in place effectively trigger alerts.
- **Establish Persistence:** Core Impact's patented Core Agents help Pen Testers establish persistence within the bank's internal systems. OS agents operate like malware, and persistent agents can be planted in the bank's file system to provide a longer-lasting foothold.

Phase 5: Reporting

The bank receives a detailed report of the results of the penetration test, outlining the scope, methods used, vulnerabilities discovered, and prioritized security remediation recommendations.

Core Impact's automated reporting feature supports a number of reporting formats, based on the type of pen test used, and helps prove compliance with standards such as HIPAA, GDPR, and PCI DSS.

Outcome & Lessons Learned

At the outset, the retail bank commissioned the penetration testing report with several objectives in mind.

- **Identify exploitable vulnerabilities before threat actors do:** By the time financially motivated attackers probe the bank's website, app, or customer portal, it is already too late. Pen testing lets the financial institution experience this same level of awareness within a safe setting and with time to spare.
- **Ensure compliance with PCI DSS, FFIEC guidance, and internal risk controls:** Increasingly, compliance mandates require penetration testing as a necessary security measure to test defenses and reduce risk within the financial sector.

After receiving the pen testing report, the bank understands key areas of concern within the network, its end-users, and its mobile application that could jeopardize these objectives.

Advanced Penetration Testing Tools

Fortra's Core Impact provides multi-vector, comprehensive penetration tests for major retail banks looking to reduce risk and meet compliance standards. Supported by a dedicated team of exploit writers, threat researchers, and data scientists, this automated pen testing solution provides financial firms with a stable, up-to-date library of commercial-grade exploits.

Don't let your bank be beaten by intrepid attackers. Get automated, centralized, consistently current penetration tests from Fortra's Core Impact.

FORTRA

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.

