FORTRA


## Offensive Security

# Use Cases

# Table of Context

# Introduction

Cybersecurity today is defined by one constant: determined adversaries who refuse to stand still. As organizations modernize their infrastructure, expand digital access, and depend more heavily on interconnected systems, attackers adapt just as quickly. They relentless probe for weaknesses and exploit the smallest cracks, now with increasingly advanced techniques.

## See Your Defenses Through an Attacker's Eyes

Securing your business-critical assets and operations requires more than traditional protective measures; it requires seeing your organization the way an adversary does. This collection of offensive security use cases illustrates how organizations across critical sectors are doing exactly that.  While the industries differ, the need is shared: to test defenses, understand where real-world attackers could break in, how far they could go, and what safeguards must evolve to stay ahead.

These examples of Red Team engagements and penetration tests reveal how offensive testing uncovers gaps in your detection and response as well as potential attack paths. While Red Team engagements take a broad approach, emulating real adversaries to test an organization's detection, response and resilience, penetration tests focus on identifying and validating specific vulnerabilities in defined systems. Both testing types serve important roles and are often used together as part of an offensive security strategy.

# Red Team
## Use Cases

## USE CASE:
# Government Agency

### Background

A government agency responsible for critical public services commissions a Red Team engagement to assess its cybersecurity resilience. The exercise simulates an advanced persistent threat (APT) attack, testing the agency's ability to detect, respond to, and mitigate cyber threats targeting sensitive government data, public infrastructure, and national security.

Global attacks on critical infrastructure are up by **30%**

www.forescout.com

# Phase 1

### Initial Access Operations

The Red Team begins by gathering intelligence on the government agency's employees, vendors, and internal systems.

- **Reconnaissance:** Open-source intelligence (OSINT) reveals outdated public-facing web servers and a cloud-based document-sharing portal used for inter-agency communication.
- **Spear Phishing Attack:** A well-crafted email impersonating a senior government official is sent to agency employees, containing a malicious attachment disguised as a policy update created using **Outflank Security Tooling's (OST)** Office Intrusion Pack.
- **Web Drive-By Attack:** The Red Team exploits an unpatched content management system (CMS) vulnerability on the agency's public website, embedding a JavaScript-based exploit that executes when employees visit the site.

# Phase 2

### Lateral Movement & Privilege Escalation

Once inside the government agency's network, the Red Team moves laterally to compromise additional systems:

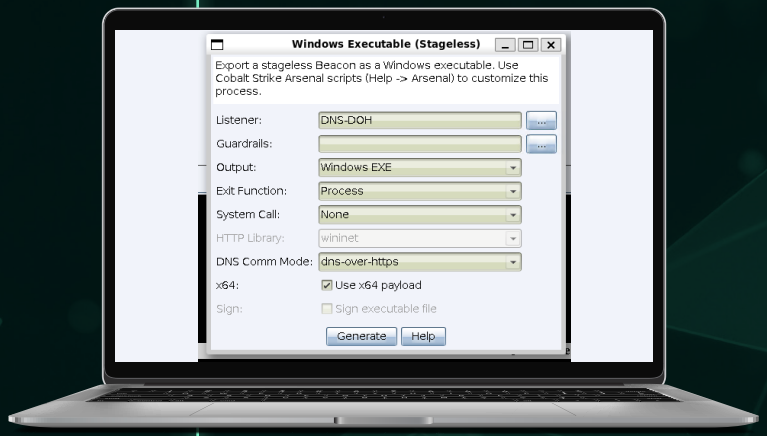
- **Credential Harvesting:** Using tools from OST's Credential Pack, they extract hashed passwords from memory and perform Pass-the-Hash attacks to gain deeper access.
- **Privilege Escalation:** By exploiting an outdated endpoint security solution, they escalate privileges to administrator levels, gaining control over sensitive systems.

# Phase 3

## Maintaining Persistence & Evasion

To maintain access without detection, the Red Team deploys stealth techniques:

- **Quiet Transmission:** They use encrypted HTTPS and DNS tunneling to communicate with their **Cobalt Strike** command-and-control (C2) server.
- **Asynchronous Communication:** Malware beacons at random intervals to avoid detection by security monitoring tools.
- **Remote Access Trojans (RATs):** Custom backdoors are placed in critical systems, ensuring persistent access for future operations.




# Phase 4

## Simulated Attack Scenarios

The Red Team executes targeted attack simulations against government assets:

- **Data Exfiltration:** They extract classified documents, policy drafts, and sensitive citizen data to test the agency's ability to detect data breaches.
- **Critical Infrastructure Disruption:** They simulate an attack on the agency's SCADA (Supervisory Control and Data Acquisition) systems, demonstrating how adversaries could disrupt water supply or traffic control operations.
- **Disinformation & Insider Threat Simulation:** They fabricate fake internal memos and manipulate communication channels to test resilience against misinformation campaigns.

Government agencies were the **Third Largest Target** of ransomware targets in 2023

**homeland.house.gov**

## Phase 5

### Red Team Engagement & Blue Team Training

The engagement involves continuous collaboration between Red and Blue Teams:

- **Shared Sessions:** The Blue Team is allowed to observe and analyze Red Team tactics in real time.
- **Extensive Logging:** Every attack vector is documented for forensic analysis.
- **Purple Team Exercises:** The Blue Team improves its detection capabilities based on Red Team findings.
- **Incident Response Drill:** The agency's security team practices containment, mitigation, and recovery strategies.

In 2024, **70%** of cyberattacks involved critical infrastructure

homeland.house.gov

# Outcome & Lessons Learned

- **Identified Weaknesses:** The exercise exposes vulnerabilities in third-party services, endpoint security, and insider threat detection.
- **Security Improvements:** The agency implements zero-trust architecture, network segmentation, and continuous security monitoring.
- **Enhanced Cyber Resilience:** The agency adopts a proactive security strategy, conducting regular Red Team engagements to safeguard national security assets.

This engagement highlights the importance of cybersecurity in protecting government infrastructure, sensitive data, and public services from advanced cyber threats.

### Advanced Red Team Tools

Cobalt Strike and Outflank Security Tooling (OST) are two red teaming solutions that enable operators to execute the breadth of tasks that advanced red team engagements require. While both platforms operate as sophisticated standalone solutions, OST was developed to work with Cobalt Strike, extending the capabilities of both tools.

## USE CASE:

# Financial Institution

### Background

A large financial institution conducts an assumed breach exercise to test its cybersecurity resilience. The Red Team is tasked with simulating an advanced persistent threat (APT) attack, while the Blue Team monitors, detects, and mitigates threats in real-time.

Financial institutions lose between **$4.64 & $5.11 million** per ransomware attack

www.statista.com

## Phase 1

### Initial Access Operations

The Red Team conducts reconnaissance on the Financial Institution's employees using open-source intelligence (OSINT). They identify a senior financial analyst, "John Doe," who frequently engages in industry webinars.

- **Spear Phishing Attack:** A well-crafted email mimicking an industry event invitation is sent to John. The email contains a malicious Microsoft Compiled HTML Help (CHM) generated with the **Outflank Security Tooling's (OST's)** In Phase Builder.
- **Payload Execution:** Once John clicks the link, a malicious payload executes, establishing an initial foothold through an encrypted reverse shell.

## Phase 2

### Lateral Movement & Credential Harvesting

With initial access to John's workstation, the Red Team moves laterally within the financial institution's network:

- **Credential Harvesting:** They dump credentials from the memory using OST's Credential Pack and extract NTLM hashes from the workstation.
- **Privilege Escalation:** By exploiting a misconfigured service with SYSTEM privileges, they escalate privileges to domain administrator.

## Phase 3

### Maintaining Persistence

To ensure long-term access, the Red Team establishes multiple persistence mechanisms:

- **Quiet Transmission:** They configure C2 communication over HTTPS and DNS tunneling through **Cobalt Strike**, allowing them to bypass traditional network monitoring tools.
- **Asynchronous Communication:** A Beaconing mechanism is used to send periodic encrypted packets to evade detection.

## Phase 4

### Actions on Targets

With initial access to John's workstation, the Red Team performs previously agreed actions within the financial institution's network:

- **Money Transfer:** Using **Hidden Desktop**, the Red team is able to launch the internal banking application from a compromised asset and proves that it is possible transfer money to an external account.

The number of cybersecurity attacks on financial institutions in the US has been rising, **experiencing a 430% increase between 2020 and 2023 alone**

**www.statista.com**

## Phase 5

### Red Team Engagement & Purple Teaming

The exercise involves real-time collaboration with the Financial Institution's security teams:

- **Shared Sessions:** The Red Team allows the Blue Team to observe certain attack techniques in real-time.
- **Extensive Logging:** All Red Team activities are logged for forensic analysis.
- **Purple Team Exercises:** The Red and Blue Teams analyze detections, fine-tune security tools, and improve response procedures.
- **Blue Team Training:** Defensive teams are trained to detect and mitigate similar real-world threats.

# Outcome & Lessons Learned

- **Identified Gaps:** The exercise reveals weaknesses in the Financial Institution's email filtering, endpoint detection, and privilege management.
- **Security Enhancements:** Multi-factor authentication (MFA), stricter browser security policies, and improved lateral movement detection are implemented.
- **Continuous Improvement:** The organization adopts a proactive security strategy, conducting regular assumed breach exercises to stay ahead of emerging threats.

## USE CASE:
# Hospital Network

### Background

A regional hospital network conducts a Red Team engagement to evaluate its cybersecurity defenses. The exercise aims to simulate a sophisticated cyberattack targeting patient data, medical devices, and critical infrastructure, testing the hospital's ability to detect, respond to, and recover from an intrusion.

The average cost of US Healthcare data breach is a record setting **$10.22 million,** up 9.2% in 2025 from 2024 reports.

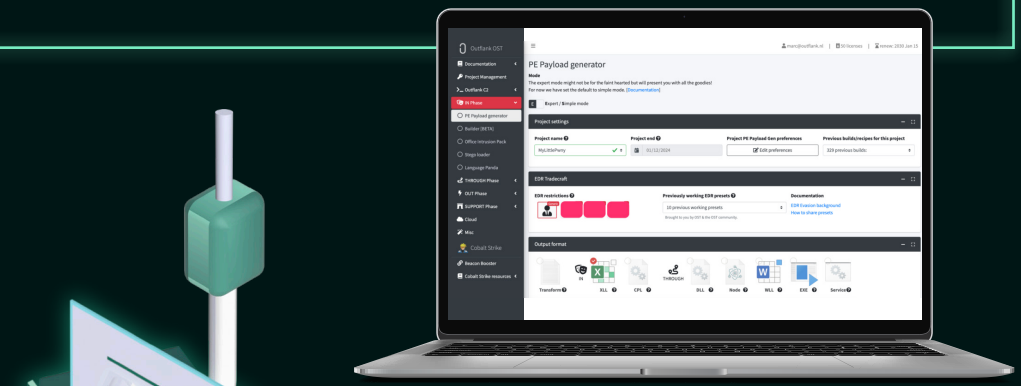
www.hipaajournal.com

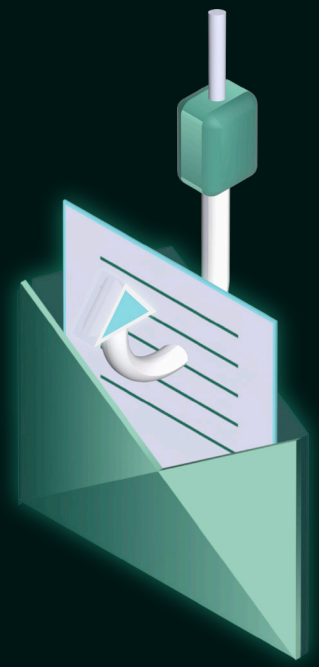
## Phase 1

### Initial Access Operations

The Red Team begins by gathering intelligence on the hospital network's employees, vendors, and third-party service providers.

- **Reconnaissance:** They identify a vulnerable third-party billing vendor with weak cybersecurity controls.
- **Spear Phishing Attack:** Using social engineering, the Red Team sends a phishing email to a vendor employee, impersonating the hospital network's IT department. The email contains a malicious link that deploys a payload generated using the OST's Payload Generator when clicked.
- **Web Drive-By Attack:** The Red Team also compromises a medical industry website frequently visited by hospital staff, injecting a browser exploit to gain initial access.



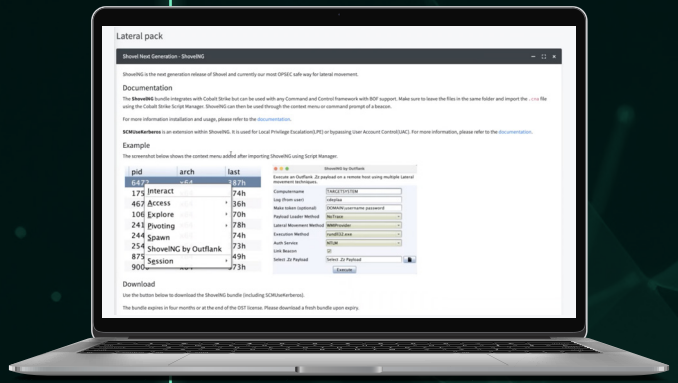



# Phase 2

## Lateral Movement & Privilege Escalation

Once inside the hospital network network, the Red Team moves laterally and escalates privileges:

- **Credential Harvesting:** Using Credential Pack, they extract cached credentials from compromised workstations.
- **Lateral Movement:** They pivot across the network, accessing electronic health record (EHR) systems and connected medical devices using Lateral Pack.
- **Privilege Escalation:** Exploiting a misconfigured domain controller, they elevate privileges to a domain admin level using Impacket, allowing unrestricted access.




# Phase 3

## Maintaining Persistence & Evasion

To remain undetected, the Red Team establishes multiple persistence mechanisms:

- **Quiet Transmission:** They use DNS over https tunneling and encrypted HTTPS communication through **Cobalt Strike** to exfiltrate data without triggering alerts.
- **Asynchronous Communication:** A covert Beaconing technique allows them to maintain control over compromised systems while avoiding detection.

**The ongoing shift of clinical systems to cloud environments continues to entice hackers resulting in compromised patient care.**

**61%** of cloud compromise incidents resulted in disrupted patient care

**52%** led to longer hospital stays

**36%** were linked to increased mortality

**www.proofpoint.com**

## Phase 4

### Targeted Attack Scenarios

The Red Team simulates real-world cyber threats targeting healthcare infrastructure:

- **Medical Device Exploitation:** They compromise an IoT-connected MRI scanner, demonstrating how attackers could manipulate scan results or disrupt patient care.
- **Ransomware Deployment:** Using Ransomware Simulator, they encrypt non-essential patient records to test the hospital's incident response plan.
- **Data Exfiltration:** They exfiltrate sensitive patient data, including medical histories and insurance records, highlighting potential HIPAA violations.

## Phase 5

### Red Team Engagement & Blue Team Training

This exercise involves collaboration between offensive and defensive teams:

- **Shared Sessions:** The Red Team provides real-time insights into attack methodologies.
- **Extensive Logging:** Every action is documented for forensic analysis and post-engagement review.
- **Purple Team Exercises:** The Blue Team improves detection capabilities based on Red Team findings.
- **Incident Response Drill:** The hospital's cybersecurity team practices containment, eradication, and recovery strategies.

# Outcome & Lessons Learned

- **Identified Weaknesses:** Gaps in third-party security, endpoint detection, and network segmentation were exposed.
- **Security Improvements:** The hospital network implements multi-factor authentication (MFA), network segmentation, and enhanced monitoring for medical devices.
- **Enhanced Preparedness:** The hospital now conducts regular Red Team engagements to maintain a proactive security strategy.

This Red Team exercise demonstrates how healthcare organizations can identify and mitigate cyber risks before real attackers exploit them, ensuring patient safety and data security.


Pen Testing
Use Cases

## USE CASE:
# Government Agency

### Background

A national government agency operates a secure web platform for delivering citizen services such as benefits applications, licensing, and tax filings. The agency wants to proactively identify weaknesses in its public-facing and internal systems before they can be exploited by hostile actors.

## Phase 1

### Planning and Reconnaissance

The pen testers gather critical information about the target organization, its employees, its network, and systems.

- **Passive Reconnaissance:** They leverage Open Source Intelligence (OSINT), or publicly available data like public records, social media posts, the public-facing website, and online databases, to glean intelligence on the government agency's key stakeholders and material assets.
- **Active Reconnaissance:** Pen testers perform a perimeter assessment. This tests the agency's public-facing web apps, customer/citizen portals, and exposed services for vulnerabilities in line with OWASP Top 10 and CWE/SANS Top 25.

## Phase 2

### Scanning

The public sector agency is probed with automated tools to identify vulnerabilities, open ports, and exploitable services.

- **Validate 20+ Scanners:** Using **Core Impact**, pen testers can validate the results of more than 20 third-party scanners. These include **Fortra VM**, Nessus, and BurpSuite.
- **Prioritize Results:** Following the scan, Core Impact prioritizes the results to give the government agency's security team a severity-based list of where to begin remediations.

## Phase 3

### Gaining Access

The penetration testers use the information gained in reconnaissance and scanning to gain unauthorized access to the agency's network and systems. The goal is to gain control over the target and demonstrate potential damage by an outside attacker.

- **Access Control Testing:** They validate that only authorized roles can access sensitive citizen records (benefits forms, tax documents, business licenses), even under complex multi-role workflows. In this case, they discover a vulnerability in a public-facing website that can be exploited to allow unauthorized access to a database containing business license numbers and contact information.
- **Password Cracking:** Pen testers leverage Core Impact to communicate securely with password-cracking service CloudCypher. The communication is encrypted with mutual authentication. Any Windows NTLM hashes discovered are passed back to Core Impact for further use in the agency's penetration test.
- **Social Engineering:** Using Core Impact, pen testers launch an automated phishing campaign impersonating a CISA threat sharing advisory, warning the agency to be wary of tax season scams. The campaign is sent to the head of the agency, key stakeholders, and the CISO.
- **Infrastructure Security Review:** The pen testing team includes firewall, VPN, and email gateway testing (for additional resilience against phishing-based initial access) when attempting to gain entry to the target.

## Phase 4

### Maintaining Access

At this stage, the pen testers try to establish persistence into the agency's systems to increase their chances of exfiltrating sensitive citizen data over time.

- **Privilege Escalation & Lateral Movement:** They attempt to escalate privileges within the agency's internal network and pivot into systems holding sensitive PII (tax filing databases, SSNs associated with Social Security benefits, etc.).
- **Data Exfiltration Simulation:** Pen testers assess how easily sensitive datasets could be extracted from public-facing systems (SQL attacks), and whether data loss prevention (DLP) tools trigger alerts.
- **Establish Backdoors:** The pen testing team has the option of partnering with Cobalt Strike Beacon to create backdoors to establish persistence and maintain access to the target.

## Phase 5

### Reporting

A report is delivered to the agency providing a detailed account of the vulnerabilities discovered during the penetration test. The agency receives a summary of key findings and actions taken at each phase, along with prioritized recommendations for remediation.

The pen testers recommend regular vulnerability scans and patch management across internal systems and the agency's public-facing website, increased password security standards, and multi-factor authentication (MFA) as a second line of defense against credential abuse.

Number of records compromised in federal breaches annually - **2.3M**

www.comparitech.com

# Outcome & Lessons Learned

This government agency had several objectives in mind when deciding to perform a penetration test. They included:

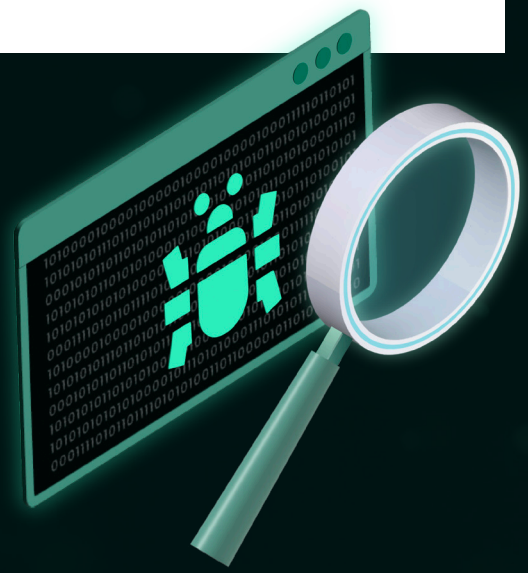
- **Demonstrating Regulatory Compliance:** Standards like NIST 800-53 and FISMA both require pen testing as a mandatory security control for federal agencies.
- **Improve Citizen Trust:** Publicizing the fact that they perform regular, third-party penetration tests earns them the trust of the public and increases the number of citizens likely to interact with that agency's services.
- **Harden Defenses Against Both Nation-State and Cybercriminal Threats:** Unpatched vulnerabilities are an open invitation to sophisticated nation-state actors who can do a lot with these easy entry points.

## Advanced Penetration Testing Tools

With Fortra's Core Impact, penetration testers get a comprehensive, multi-vector solution for assessing vulnerabilities within systems and networks. Get commercial-grade exploits in this automated pen testing software with a solution that tests all its exploits in-house, supports third-party exploits, and subjects its exploit library to rigorous testing.

## USE CASE:
# Financial Institution

### 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.

**Proportion of financial institutions that experience a cyber attack annually - 66%**

www.securitymagazine.com

## 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.

Average number of days it takes companies to discover a cyber attack - **207**

sqmagazine.co.uk/

Average global cost of breach in financial industry - **$6.08M**

www.ibm.com

## 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.

Remediation cost per stolen healthcare record vs non-healthcare record **$408** vs **$108**

www.aha.org

# 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 enables penetration testers, 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.

**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.



(fta-g-0126-r1-am)