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.


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:

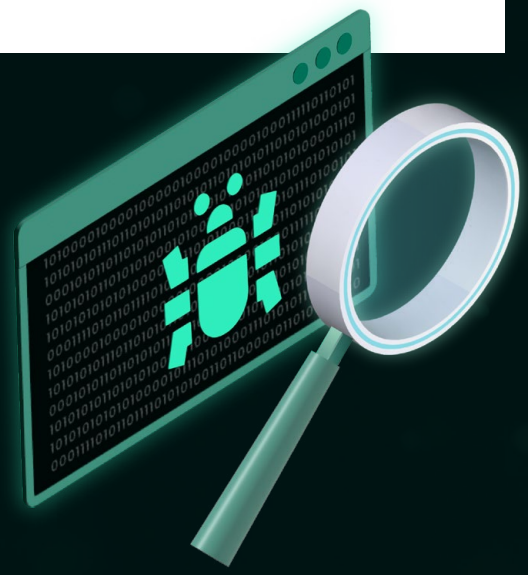
- **Demonstrating Regulatory Compliance:** Standards like NIST 800-53 and FISMA both require pen testing as a mandatory security control for federal agencies.
- **Improve Citizen Trust:** Publicizing the fact that they perform regular, third-party penetration tests earns them the trust of the public 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.

USE CASE:
Hospital Network

Background

A major hospital system relies on a complex digital ecosystem—including a patient portal, Electronic Health Records (EHR), IoTconnected medical devices, and an internal clinical network—to support daily operations and patient care. With rising cyber threats targeting healthcare environments, the hospital needed a way to continuously assess weaknesses without disrupting clinical workflows. To achieve this, the security testing team used penetration testing software, such as Core Impact, to simulate real-world attack scenarios safely and efficiently.

Phase 1

Planning & Reconnaissance

Before executing any tests, the team defined a clear scope to avoid operational disruptions, particularly important in environments that support patient care. Key reconnaissance tasks included:

- Mapping the hospital network and identifying interconnected systems such as EHR servers, medical imaging devices, IoT endpoints, and Wi-Fi access points.
- Identifying open ports, active services, and operating systems used across clinical and administrative devices.

By leveraging Core Impact, the team was able to automate early reconnaissance steps and streamline their testing workflow.

Phase 2

Scanning

With the scope established, automated scanning began across multiple systems:

- Network scanning to reveal outdated firmware, misconfigurations, and exposed services. \
- Web application scanning to identify injection vulnerabilities associated with patient portals or internal web-based tools.
- IoT/medical device scanning to detect hardcoded credentials or unrestricted permissions.

Core Impact's ability to integrate scanning results from top vulnerability management solutions provided the team with a consolidated view of vulnerabilities, helping them prioritize by risk and clinical impact.

Phase 3

Gaining Access (Exploitation)

Once vulnerabilities were identified, exploitation testing was performed to validate risk levels:

- Running CVE-based exploits against outdated firmware on Wi-Fi access points, confirming the potential for remote code execution.
- Testing for hardcoded credentials on medical imaging systems.
- Attempting privilege escalation on compromised systems.
- Simulating ransomware propagation, helping the hospital visualize how fast an attack could spread.

Core Impact's certified exploitation capabilities proved critical for safely demonstrating real-world attack paths while maintaining hospital uptime.

Phase 4

Lateral Movement & Post-Exploitation

After initial access was achieved, the security team simulated internal attacker behavior:

- Mapping reachable clinical systems from compromised devices.
- Assessing whether PHI (Protected Health Information) was accessible due to misconfigured file permissions.
- Evaluating segmentation controls between administrative and clinical networks.

Core Impact's structured workflow enabled repeatable and safe post-exploitation testing across sensitive healthcare systems.

Average cost of a healthcare data breach **$10.9M**

www.ibm.com

Average time between breach and discovery in the healthcare sector **213 days**

www.ibm.com

Phase 5

Reporting & Remediation

The automated penetration testing platform generated two levels of reports:

- Technical reports for IT teams, containing details on exploited vulnerabilities and recommended fixes.
- Executive summaries highlighting business impact, regulatory implications (HIPAA, NIST, ISO 27001), and prioritized action items.

Once remediation steps were completed, the team retest vulnerabilities and verify closure.

Outcome & Lessons Learned

At the outset, the hospital launched automated penetration testing to strengthen security and reduce risk across patientcare systems.

Identify Critical Vulnerabilities Before Attackers Could

Testing uncovered several high impact weaknesses— including outdated WiFi firmware vulnerable to remote code execution, hardcoded credentials on medical imaging systems, and misconfigured file permissions exposing PHI— giving the hospital early visibility into threats that could jeopardize operations and data privacy.

Support Compliance With HIPAA, NIST, and Internal Controls

Automated testing, enhanced through Core Impact, enabled continuous, scalable assessments, early detection of vulnerabilities across EHR, IoT, and network assets, and streamlined verification of remediation efforts to meet healthcare security standards.

Clarify Key Areas of Concern Across Clinical and Network Systems

With clear findings and compliance ready reports, the hospital improved its cybersecurity posture and established a recurring testing schedule to ensure ongoing risk reduction and operational resilience.

Advanced Penetration Testing Tools

With Fortra's Core Impact, healthcare organizations gain a powerful, multivector penetration testing platform designed to evaluate vulnerabilities across critical clinical systems, connected medical devices, and hospital networks. The solution delivers commercial grade, certified exploits within an automated framework—each exploit vetted internally, compatible with thirdparty modules, and subjected to routine testing to ensure reliability, stability, and the absence of hidden backdoors.

Core Impact's continually updated exploit library—expanded regularly—helps hospitals stay ahead of fast-evolving cyber threats. For environments where patient safety, PHI protection, and uninterrupted clinical operations are paramount, this makes Core Impact an ideal tool for maintaining strong, proactive cybersecurity defenses.

(fta-gd-0626-r1-as)