FORTRA

Pen Testing Use Case – Government

Critical Citizen Services Penetration Test

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.

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, public sector agencies get a comprehensive, multi-vector solution for assessing vulnerabilities within their systems and network. 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 on a weekly basis to ensure there are no unexpected surprises, and no backdoors are left behind.

Core Impact stays current with more than ten new exploits every month, making it the perfect tool to keep any government agency up to date with the latest emerging threats.

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.

