# Customer Type: U.S. Government National Security Laboratory

## Challenge

Validating vulnerability scanner results and preparing for mandated compliance audits, in addition to testing the efficacy of defensive mechanisms and gauging the security awareness of end users.

## Solution

CORE IMPACT Pro, the first comprehensive penetration testing software solution for assessing organizations' most significant IT vulnerabilities and information security threats.

## The Company

**Based in the Western U.S., this government national security laboratory is tasked with reducing the risk of cyber-attacks carried out against the nation, including protection of critical infrastructure assets ranging from the power grid to financial trading markets, as well as the environment itself.**

**Founded in the 1950s, the lab employs hundreds of physicists, chemists, biologists, engineers and other researchers who work on technical and scientific projects aimed at aiding the cause of protecting the U.S. from potential threats. The lab itself is made up of over a dozen individual facilities with hundreds of networks and thousands of endpoints, many of which handle information and/or materials that would be considered among the most sensitive in the world – and thus must be tested for security risks on a regular basis.**

**As a senior security engineer part of the Incident Management Team, the customer leads the group responsible for overseeing management of all the organizations' defensive mechanisms as well as ensuring that users are complying with established policies and preparing for mandated external compliance audits. In addition to meeting the explicit guidelines set forth in existing regulations such as the Federal Information Security Act (FISMA) and by the National Institute of Standards and Technology (NIST), the security team is also tasked with keeping an eye toward emerging policy-making efforts such as the next-generation Consensus Audit Guidelines (CAG).**

## The Challenge

With a massive database of sensitive information related to some of the most critical aspects of national cyber-security, the lab has an extremely demanding mandate to protect its IT assets from being infiltrated by external attackers or improperly accessed or manipulated via internal activities. It also sought to address CAG Requirement 17 which calls for all government agencies to complete penetration tests on a regular basis.

On a practical level, the lab was also looking for a new method of interpreting its volumes of vulnerability scanner results to eliminate false positives and prioritize existing points of risk, as well as a process for addressing low-hanging issues ahead of compliance audits to prove due diligence to third party examiners. In this sense the lab also needed a testing product to help it meet the terms of CAG Requirement 10 around "continuous vulnerability assessment."

In addition, the lab sought a solution that it could use to test the security practices of end users both to refine its security training efforts and illustrate ongoing assessment of user awareness to auditors, in part to meet CAG Requirement 20 which addresses "security skills assessment and training." The lab is also looking to add penetration testing to its web applications development and certification process to complement its existing scanning and source code analysis practices.

## The Solution

To meet its multi-tiered security and compliance requirements and reduce its exposure to potential cyber-attacks, the security lab opted to license CORE IMPACT Pro to perform regular penetration tests across much of its IT systems and applications, and to assess policy adherence among its end users.

IMPACT Pro was first licensed by the lab in 2006, and the organization currently maintains two implementations of the solution, which is marketed via an annual subscription model. IMPACT Pro is specifically installed on a pair of laptops that are moved around the lab's environment to carry out testing on select groups of IT assets including many networks, applications, web applications and sets of end users.

By performing more frequent penetration testing the organization is hoping not only to reduce the resources it must commit to time-consuming security tasks such as interpreting vulnerability scanner results and tuning defensive mechanisms, but also to facilitate greater trust with its external auditors that it is constantly measuring its exposure to potential threats to address its most highly available and critical points of risk.

"The truth of the matter is that testing more frequently is simply a very powerful method for aggregating the types of information we need to make more informed decisions about where to focus our future investments and initiatives," said the senior security engineer. "Before we had IMPACT we might have carried out tests on a scheduled basis, but now we have the ability to do so whenever we need to based on emerging demands."

CONTINUED ON NEXT PAGE

## The Result

### Complementing Vulnerability Scanning

While the lab has long employed network vulnerability scanning tools to find all of its potential points of risk, using IMPACT Pro to exploit the flaws discovered by those products has allowed it to greatly reduce the amount of time and manual work necessary to eliminate false positives and prioritize its most critical IT security exposures, as well as meet the terms of CAG Requirement 10. The lab specifically uses the Tenable Nessus scanner, with which IMPACT Pro has a fully supported integration that allows organizations to feed their vulnerability scan results directly into the penetration testing solution to speed and lend consistency to the overall vulnerability management process.

### Preparing for Security Audits

The lab must undergo annual third party security audits under FISMA, and using IMPACT Pro to prepare for those assessments has not only helped the organization understand where it needs to address potential problems before its engagements, but also allowed it to prove due diligence to auditors by sharing the results of its internal pen tests. By illustrating its ongoing efforts to auditors, the lab feels it has established a level of trust with the assessors such that the experts already understand that it is making a good faith effort to build and maintain its mandated security controls. In meeting specific terms of CAG Requirements 17, the lab has been able to automate many penetration testing and vulnerability assessment tasks that otherwise would require manual intervention, from information gathering to reporting results.

### Testing End User Security Awareness

Understanding that end users stand as the most vulnerable line of any organizations' defenses in the face of complex social engineering attacks, the lab is using IMPACT Pro to conduct regular assessments of user awareness, such as through the dissemination of mock phishing and spear phishing campaigns aimed at determining which individuals or groups of people need to be diverted into additional training. The lab has also been able to automate a number of related processes spelled out in CAG Requirement 20.

*"I see IMPACT Pro as a well seasoned product that allows us to meet many of our security testing and compliance goals faster. Being resource constrained it's key that a single product allows us to carry out internal testing, verify vulnerabilities and eliminate false positives faster, which has made it much easier to enhance our overall security posture."*

CORE SECURITY TECHNOLOGIES

SANS