Case Study

CORE SECURITY
A HelpSystems Company

U.S. GOVERNMENT LABORATORY

Background

This U.S. government laboratory is tasked with monitoring cyber-attacks and other matters of national security, encompassing a wide range of intellectual property, critical infrastructure, and electronic assets.

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 United States 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 sensitive information and/or materials.

As senior security engineer and part of the lab's Incident Management Team, the customer helps lead the group responsible for overseeing management of all the organizations' defensive mechanisms and ensuring that users are complying with established policies, as well as preparation 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 tasked with keeping an eye toward emerging policy-making efforts such as the next-generation Consensus Audit Guidelines (CAG).

In performing these duties, the security engineer is also responsible for recommending and deploying the many IT security solutions and services employed by the lab to help defend its critical data and operations from potential cyber-threats and prepare for compliance audits.

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.

Overview

Core Impact helped this U.S. Government Lab:

+ Compliment vulnerability scanning
+ Prepare for security audits
+ Test end-user security awareness

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 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. 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.

"Organizations need to concede that their defenses cannot stop every attack and instead take the approach of assuming that networks, endpoints, and applications have been compromised and will likely be again," said the senior security engineer. "Penetration testing is highly complementary to scanning and other vulnerability management practices as it allows you to gain insight into which issues truly represent your most important points of exposure in direct relation to real-world attacks."

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 to perform regular penetration tests across much of its IT systems and applications, and to assess policy adherence among its end users.

Impact 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. Core Impact is 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 vulnerabilities and threats, and ongoing changes to our IT environment."

The Result

Complimenting Vulnerability Scanning

While the lab has long employed network vulnerability scanning tools to find all of its potential points of risk, using Core Impact 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. The lab specifically uses the Tenable Nessus scanner, with which Core Impact 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.

"It's very hard to verify scanner results, and as the number of vulnerabilities has increased, so has the volume of false positives," said the senior security engineer. "Using Impact to filter and prioritize those results truly helps us grasp where we need to focus our resources and delegate remediation efforts."

> "The beauty of Core Impact is how dynamic it is; it has so many canned modules, but if I want to modify or create my own modules and take the test a step further I can. There's also the issue of testing safely. With some testing products you can't predict what might happen after you run a particular exploit, but with Core Impact you can, and you know that when you're done testing everything will be removed."

Preparing for Security Audits

The lab must undergo annual third party security audits under FISMA, and using Impact 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.

"We wanted to get to the point where we could give the auditors our results and pinpoint those issues that they truly need to examine," said the senior security engineer. "By showing them that we're always looking to address the low-hanging fruit it has changed the entire interaction into more of a collaborative effort because they know they can trust us on a lot of matters."

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 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.

"Organizations tend to spend a lot of time looking at vulnerabilities on their assets but they fail to consider the all-important human factor," the senior security engineer said. "We're running quarterly phishing exercises to educate our employees and enhance their overall awareness to threats, and we've been able to measure significant improvements over time based on these programs."