COSMOS
Navigate the Compliance Universe

CEP Magazine - April 2018
The components of strong cybersecurity plans, Part 5: Penetration testing

By Mark Lanterman

Mark Lanterman (mlanterman@compforensics.com) is Chief Technology Officer at Computer Forensic Services Inc. in Minnetonka, MN.

***Part 4 of this article appeared in the March 2018 issue of* Compliance & Ethics Professional.**

In the fifth and final installment of this cybersecurity series, I will discuss the role of penetration testing in developing a strong security program. As described in my previous four articles, a growing awareness of cybersecurity regulations, trends, and threats has led many organizations to request a penetration test of their technical infrastructure—without really knowing what that means, what its purpose is, and what degree of assurance it really offers.

Asking the right questions

When I ask a customer if they have already conducted a security assessment, know their controls, have implemented regular vulnerability scanning, and have security auditing procedures in place, they usually respond with, "That's what we're asking for. We want a penetration test." In this way, penetration testing and all the other components of cybersecurity plans have become synonymous terms. This conflation is especially prevalent in small to medium-sized firms. However, each component is separate and distinct within a mature security program, all components serve different purposes—leveraging different methodologies, providing different levels of assurance and benefits, requiring different skills from the assessor, providing different deliverables—and each component performs at different stages of a security program's development. In order to reap the most benefit from a penetration test, the organization should be able to answer the following five questions based on the previous maturity assessment, security risk assessment, and security audits:

1. Do we know what is connected to our systems and networks at all times?
2. Do we know what software is running, or trying to run, on our systems and networks?
3. Are we continuously managing our systems using "known good" configurations?
4. Are we continuously looking for, and managing, "known bad" software?
5. Do we limit and track the people who have the administrative privileges to change, bypass, or override our security settings?

A penetration test is an attempt to defeat boundary defenses and gain access to an organization's internal network by exploiting vulnerabilities. This test is used to determine whether an unmitigated risk exists. In this sense, it tests whether an outside attacker could bypass perimeter controls, gain access to the internal network, and establish command and control capabilities. Many techniques can be employed during a penetration test, including vulnerability scanning and social engineering attacks.

Social engineering attacks are targeted at exploiting the human vulnerabilities in an organization. Spear phishing emails, unauthorized issuing of credentials, and taking advantage of physical vulnerabilities can all be examples of ways in which an assessor will use social engineering during a penetration test.