



What the manager needs to know about planning a penetration test or vulnerability assessment

By Scott Laliberte, Protiviti Director and Jeff Sanchez, Protiviti Director

Like the old joke about the doctor whose operation was a success but the patient was lost, a security test of an organization's IT system might be performed well, but the value could be drained away if the test is not planned and managed effectively.

The system tester – often a consultant performing a penetration test or vulnerability assessment – is roughly analogous to the surgeon leading the operation, but management has an equally decisive role in the process. The responsibility for clearly defining the objective of the test, ensuring quality, and effectively communicating the results largely rests in the business manager's hands.

What is at stake is nothing less than the security of an organization's internal and customer data. Ideally, the tester will bring more than the "techie" perspective to the task; and be capable of understanding how the security of the organization's servers, systems, firewalls and the like relate to specific business risks. Management plays a crucial role in helping testers understand that connection between the IT environment and business objectives. By working in collaboration with the tester, business managers help ensure that the tests are valuable to the organization.

Seeing clearly from the start

As collaborators in penetration tests or vulnerability assessments, managers and testers must communicate clearly with each other, from start to finish. To that end, organizations should exercise care in choosing their tester from a host of companies ranging from small boutique operations to large consulting firms.

Some due diligence is needed to evaluate potential testers. Do companies perform background checks on their employees or hire ex-hackers? Does a company have the financial assets to back up any claims that might be made on insurance? How does the company report its results? Do they employ people who can understand and articulate business risk; or are they the stereotypical techies whose reports will simply catalog technical issues? If the organization has not established clearly defined terms and goals for its test, can the tester help them clarify what they want out of the test?

Achieving that clarity and setting the scope of the test begins with the organization deciding which question it wants to answer:

- *"Is it possible for someone from the outside to break into my systems?"*

In a penetration test, the tester aims to break into a system and access something valuable – a prize, so to speak. To that narrow end, he/she works only with the issues posing the highest risk. Once the tester has found a route to the prize, the test is *usually* over, even though there are a host of smaller vulnerabilities remaining in the environment.

- *"Have we properly designed and implemented effective information security architecture?"*

The answer lies in a vulnerability assessment, a more thorough assessment of weak points across the environment. These points could individually represent small risks, but when combined, they create a greater vulnerability that could be exploited by a hacker. In this test mode, the tester tries to understand why those

weak points appear. Fixing those small points may make the system secure temporarily, but without discovering the root causes, the company may find those same vulnerabilities recreated in the future.

Of course, it is not an either/or choice facing the organization. The tester could recommend a combination of both tests, such as quarterly vulnerability assessments and using the results to identify weaknesses that could be further examined in a penetration test. Again, the value of the chosen test is ensured by clear communication and a full disclosure of information about the network and systems.

Regular status updates during tests keep important lines of communication open. Keeping the organization informed about what has been done and what is still unaddressed can help decide the course of action. A tester could follow one branch of the network and try to compromise one set of systems, or follow another branch and try to penetrate a different set of systems. Receiving input from the sponsoring department helps the organization receive the value they desire from the testing.

Communicating frequently with the IT department helps prevent security breaches that may *result* from the test. A tester could inadvertently create a back door by getting into the company's Web server via the Internet, uploading a "tool kit" onto the system and using it to attack other systems in the network, just as a hacker would do. If this condition is not secured properly, it becomes a point of entry for any hacker who stumbles across it. Likewise, an actual attacker unrelated to the test might find hacking tools left behind on the servers or systems and take advantage of the tester's oversight. It is imperative for testers to keep a careful record of their work so they can assist IT in removing all the hacking tools that were uploaded and closing all the back doors that were created during the test.

Who collaborates with the tester?

Some managers have a romanticized image of what a tester does. They envision consultants huddling in an equipment-filled room, trying to break into a network the way a hacker would. In keeping with this view, these managers tell the tester they will not give him any information about their network so they can approach it "realistically," to find out what a hacker would actually be able to do.

If a tester agreed to this premise, the organization may not obtain a true picture of their environment's security. Hackers have an unlimited amount of time to probe a network for weaknesses, while a consultant is restricted by a budgeted amount of hours. Also, consider how extensive the IT network is in a large organization. In an environment of, say, more than 500 servers, a hacker could randomly stumble onto a point of entry that might never be discovered by a tester with limited time and not know where the most sensitive information is stored. A penetration test or vulnerability assessment performed under these conditions could leave the organization with a false sense of security.

The wise course of action is for an organization to share with the tester the complete picture of how the network is mapped and how the system is secured. Disclosing this information may help prevent accidents during the testing. For example, some organizations may have old network equipment or may be running old operating-system software that cannot handle the traffic created by port scans or vulnerability scans. Obviously, it is hard to predict the likelihood of anything going wrong, but some accidents can be avoided by working from a solid foundation of information.

The probability of accidents occurring is typically higher in penetration tests. Because these test how personnel respond to potential security threats, some organizations, although not all, choose to perform penetration tests without informing IT personnel. (Vulnerability assessments are usually more extensive in scope and IT personnel are typically informed in advance and prepared for action if a system is in danger of failing.) For penetration tests, it is good practice to at least inform employees from departments such as security, internal audit and IT (most likely the chief information officer). By being informed, the organization will better understand how the tester compromised the system. Later, when the tester has issued a report, internal employees can draw on their knowledge to help interpret and communicate the test results to the organization.

The tester also benefits when department representatives observe his/her work and provide crucial information otherwise unknown to the tester. Knowledgeable employees can help manage the risk by identifying older “legacy” equipment that may be too fragile to scan. In addition, selected personnel can inform the tester about the relative business value of the system or servers. A representative from research and development areas could identify the location of intellectual property data whose security carries a high risk to the organization. Using this diverse input, the tester will write a more meaningful, persuasive report on the findings. For example, the company would learn whether a Web server with a particular business function was vulnerable to penetration, posing a specific business risk.

A representative from Human Resources may be included in planning when a penetration test involves “social engineering” (the tester attempts to trick an employee into giving him access or divulging information that will help him gain access). This would include access to an IT system (getting the employee to divulge a user ID and password) or physical access to the building (slipping in an unsecured entrance and pretending to be an employee). Human Resources personnel can play a role in calming emotions in the test’s aftermath, when employees express hurt feelings about being tricked or fear their job is at risk. Testers should not report individuals who divulge information but instead report the statistics. If 20 employees are contacted, and 15 divulge their password, it is clear that the employees’ behavior is a symptom of a more serious root cause, such as an ineffective training program.

The extent of Internal Audit’s involvement likely depends on whether they sponsored the test or not. Ultimately, it is the IT department’s responsibility to ensure the system’s security; they should not rely on Internal Audit to validate their work. While Internal Audit will not be considered the owner of the controls, it is important for auditors to assume some responsibility for making sure IT has fixed everything that it promised. Ideally, the two departments’ responsibilities complement each other. For example, in a high-risk environment, IT might complete vulnerability assessments on a quarterly basis while Internal Audit reviews IT’s methodology and performs penetration tests to validate that problems have been remediated.

There is often a genuine need for Internal Audit to sponsor its own tests. It is not unusual for consultants to find an IT department running vulnerability assessments each quarter – or even every month – while the security problems identified still are not fixed.

Presenting the results

Before the tester writes a report, it is helpful to sit down with management and discuss the findings and their context. Are there factors such as compensating controls that could account for security issues discovered by the tester? Does network architecture created 20 years ago pose problems for long-term fixes? Again, fine-tuning the picture of the network helps to place the test results in context.

Reporting the results does not mean simply listing all the vulnerabilities that were discovered. A catalog of 50 weak points within the system will have little value if the tester has not determined which root causes have created the weak points. Correcting all 50 symptoms without addressing the root cause is only a temporary fix, and the organization can count on the reappearance of more symptoms.

If the tester understands the relationship between the IT environment and business risk, this understanding of that risk needs to be communicated. If managers without a technical background can read the report and understand what the findings mean, the organization receives true value from the process.

The technical wizardry of the tester may be remarkable, but the organization stands to lose much of the value of that wizardry if the tester cannot deliver a well-written report.

Article from Protiviti KnowledgeLeader – www.knowledgleader.com.

KnowledgeLeader is a subscription-based website that provides audit programs, checklists, tools, resources and best practices to help internal auditors and risk management professionals save time, manage risk, and add value. Free 30-day trials available.

Protiviti is a leading provider of truly independent internal audit and business and technology risk consulting services. We help clients identify, measure and manage operational and technology-related risks they face within their industries and throughout their systems and processes. And we offer a full spectrum of audit services, technologies and skills for business risk management and the continual transformation of internal audit functions.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.