WHITE PAPER

Security and Risk Consulting
The Value of Penetration Testing

Executive Summary

The threat posed by hackers is persistent, and it is important to maintain a strong defense to protect your organization. Using real-world testing on your network determines areas where you may be vulnerable.

Learn the difference between vulnerability assessments and penetration tests to ensure you are properly testing your environment and getting the right solution to meet your needs.

This paper provides practical information to consider as you determine the proper testing needed to strengthen and improve your security posture.

Process

People

Intelligence

Technology

Recent security breaches create a new imperative for the optimal blend of people, process and technology fueled by intelligence for security to be effective.

Getting value from a penetration test involves a lot more than simply pointing a tool at a system and clicking a button. Companies must articulate both their own needs and what they expect from the people they are hiring to poke holes in their environment.

Who Should Read This White Paper

- CISO/CSOs
- CIOs
- IT/IT Security Directors
- IT/IT Security Managers
- Security Architects

Value of Testing

It seems counterintuitive for a company to hire someone to break into its network, but that is exactly what firms do in the name of improving security.

Penetration testing is a vital part of assessing security — particularly at a time when data breaches continue to make the headlines and escape detection for long periods. A study from the Ponemon Institute[1] released earlier this year, for example, noted that the financial services firms they surveyed took an average of 98 days to detect a breach.

Such breaches can be costly in terms of both money and reputation. For that reason, it is critical for organizations to understand how hackers may compromise their environment, eliminate easily exploitable vulnerabilities and prioritize security gaps according to the risk they pose to business operations so the most serious issues can be dealt with. But getting value from a penetration test involves a lot more than simply pointing a tool at a system and clicking a button. Companies must articulate both their own needs and what they expect from the people they are hiring to poke holes in their environment.

What's in a Name?

A rose may always be a rose by any other name, but in the world of security and marketing, things are not that simple. Many times, what has been called a penetration test by some vendors is actually a vulnerability assessment. These are very different offerings that need to be distinguished.

Vulnerability assessments and scans, while critical for organizations, should be used to establish a baseline. Rather than focus on the hacker's endgame of accessing sensitive data or compromising critical systems, vulnerability scans look for known issues that can be prioritized and patched. This is a good way for organizations to take care of low-hanging fruit — the easily exploitable, publicly known bugs that can be the gateway for hackers to enter a business.

These scans tend to be highly automated and concentrate on whatever system or application the client wants tested. For example, vulnerability scans aimed at testing compliance with regulations such as the Payment Card Industry Data Security Standard (PCI DSS) key in on systems storing credit card data for any violations.

> "The main thing that separates a penetration tester from an attacker is permission."
>
> —SANS Institute "Penetration Testing: Assessing Your Overall Security Before Attackers Do," page 3

Penetration tests may use tools, but are much more manual. The goal of a penetration test is not simply to find a vulnerability — it is to exploit it and either steal data or move laterally throughout the environment. Testers are not simply compiling a list of issues based on how a network stands up to an attack. Rather, they are poking holes in security that has undergone vulnerability assessments and is assumed to be strong.

Getting Started

Those organizations who require penetration testing for compliance mandates or are mature enough to undergo a penetration test need to be clear on a number of topics in order to get the most out of their test. First on that list is an understanding of what their most business critical assets, applications and pieces of data are. Since these are what hackers will be after, it makes most sense for the penetration test to be focused on those — in fact, all penetration tests should be focused on either accessing sensitive data or showing some sort of business risk, such as compromising a key server that hosts a critical application.

After gaining an understanding of the most critical data and systems in their environment, organizations can then determine the scope of the test. The more specific the parameters of the test, the more businesses can get out of it. For example, if a company knows it wants systems on a certain IP range to be the focus of the test, then the testers know what to target and can spend their time on the assets that matter most. If organizations do not properly define the scope of the test, critical systems may get missed.

Penetration Testing in the Cloud

This is particularly important as more and more companies use cloud services to store business data. For businesses that want to include cloud applications in the scope of the test, there are a few considerations to take into account. If their cloud providers conduct their own penetration tests, they may be willing to make the results available

[1]Ponemon Institute, "Advanced Threats in Financial Services: A Study of North America & EMEA," May 2015, survey of 844 IT and IT security professionals .

to customers. In that case, organizations should closely examine the scope of the test, how it was conducted and its findings.

If organizations want to hire another party to do a penetration test or conduct testing on their own, the providers may need to be contacted to ensure third-party testing is approved. Many times the hosting companies have already established policies and provisions regarding penetration testing. Either way, companies should review their agreements with their cloud providers and check with them if there are any questions.

Deciding on an Approach

Traditionally, there have been three forms of penetration testing: black-box, white-box and gray-box. In black-box testing, the testers are not starting off with any knowledge of the system being attacked. Conversely, in white-box testing, the testers have full knowledge of the systems being targeted. Gray-box testing occupies the middle ground between these two approaches.

All three of the strategies have their benefits. White-box testing allows organizations to simulate what an attack would be like if it is launched by a malicious insider, while black-box testing more closely resembles an act of cyberwar or an external attacker. In some situations where penetration testing also involves assessing whether organizations are adhering to compliance regulations, a mix of both approaches may be necessary, as compliance testing may require previous tests be examined.

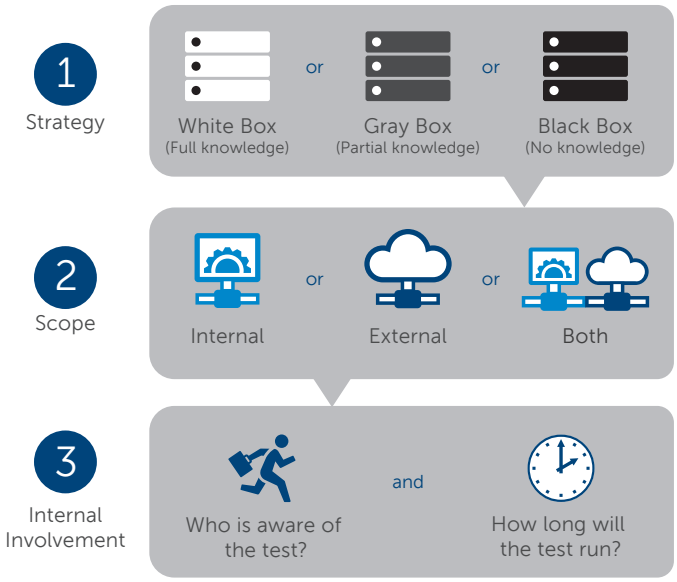
Once a company's leadership has decided on an approach, they will need to determine whether to launch an internal or an external penetration test, or both. Internal penetration tests are designed to find and exploit vulnerabilities that could be used to compromise resources accessible via authorized network connection inside the network of the organization. Like white-box testing, this is aimed at emulating actions by a malicious insider. External penetration tests on the other hand identify issues that could be exploited by an external attacker. Choosing the type of test to conduct requires that businesses have a clear understanding of what they want tested – a choice that should be made based on what they feel are the most likely scenarios they will face and the amount of risk those scenarios pose.

A final element that needs to be decided is who should know about the penetration test ahead of time. Some knowledge by the organization is of course required. Testers should inform organizations of what IP addresses their attack traffic will be coming from so that it can be distinguished from illegitimate activity. For similar reasons, there should also be a set time frame for the test.

Penetration Testing Approach

Generally, if a decision is made to focus on employees — such as how they respond to attacks and their response time — it may make sense for only a small portion of the IT department to know about the penetration test. If the focus, however, is on testing the tools used to detect and respond to adversaries, it may be best for the entire department to be in the loop.

Penetration Testing Approach



Drawing Value from the Test

A large portion of how much value an organization gets from a penetration test is a function of how carefully they have chosen the approach and how well they understand what is most critical to their business. However, the skill of the penetration testers and their ability to translate their findings into business terms is critical as well.

For those companies that do not have their own internal penetration testing team, deciding between service providers involves a few important considerations. The first is the background of the service provider. What is their reputation? Some Internet research as well as recommendations from partners, colleagues and others should go a long way toward culling the herd.

From there, organizations should question testers about their methodology. Service providers should be able to provide basic answers regarding how they go about attacking customer environments. Their answer should make clear that they have a plan of attack that does not simple rely on automated vulnerability scanning. This is important because hackers do not simply use such tools. They think outside-the-box; they chain together vulnerabilities; they exploit trust between applications and devices and leverage a mix of systems administrator, software developer, network engineer, and hacker. In short, hackers are not bound by the constraints of a vulnerability scanner.

Some of the better known testing methodologies include the Penetration Testing Execution Standard (PTES) and the Open Source Security Testing Methodology Manual (OSSTMM). What is important is that the tester can answer questions about how they will conduct their test, and that their answers indicate their approach will mix both automated tools and manual processes. Additionally, listen for their focus on the compromise of critical systems and data, not just the identification of low-hanging fruit.

After the test has been conducted, it is up to the organization how to proceed with fixing any of the issues that have been uncovered. Figuring out how to prioritize and remediate security gaps is an area where service providers should be able to help organizations by ensuring their test reports are written for both a technical and business audience. Few things will infuriate a board of executives more than being asked to spend $1 million to fix an issue that is of minimal consequence if exploited.

Organizations should ask testers to provide sample reports to make sure they also appeal to management needs. In addition to technical information, the reports should also have an executive summary that explains the issues and offers advice on general areas where improvement is needed, written at an executive management level. For example, instead of stating that SQL injection vulnerabilities were found in certain applications, this section would advise management about the importance of training application developers to improve security during the development process. The more technical portion on the other hand should dive down into more specific issues, such as what patches were missing on what systems.

This underscores a very important issue — communication. There needs to be regular communication between the business and the testers throughout the process. Penetration testers are trying to break into networks, after all, and their success could create pains for the organization. When the test is over, the tester must know how to communicate not only the nature of the vulnerabilities, but also their true risk to the company in terms of cost and potential disruption to business operation if successfully exploited.

Conclusion

Organizations with unknown security holes are like leaving a window unlocked in your home. It may keep the rain out and look fine from the outside, but a determined burglar can use it to loot your valuables. Penetration tests are a critical part in identifying vulnerabilities in an IT environment that a scanner will not pick up. To ensure they are done properly, companies must clearly define their scope and have an understanding of what assets and data in their environment are most critical and attractive to hackers.

Attackers do not operate like tools; they think and adapt. By undergoing a properly administered penetration test, companies can test their defenses against real-world conditions before an actual threat appears at the door.

より詳細な内容に関しては下記のメールアドレスにご連絡ください
SWRX_PreSales@Dell.com
代表03-6893-2317
www.secureworks.jp/
SecureWorks Japan株式会社