Penetration Testing: What You Need to Know Now

GUIDE TO IMPROVING INFORMATION SECURITY

IDENTIFYING WEAKNESSES & STRENGTHENING SECURITY

DIGITAL DEFENSE® INCORPORATED

EXECUTIVE SUMMARY

Cyber attacks are on the rise, putting businesses at risk and brand loyalty in jeopardy.

Accidental data leaks, corporate espionage and cyber-attacks are serious threats affecting businesses of all sizes and industries. As a result, today's businesses are challenged with implementing and managing effective information security programs while attempting to run their businesses at the same time.

The growing number of data breaches has demonstrated the severity of risk for organizations and the critical need to embrace effective information security practices. No organization is safe. If an attacker can exploit vulnerabilities on large, complex networks like the US Office of Personnel Management, United Airlines, Target, Sony and so many others, it should raise the question, "Is my organization's network security strong enough?"

A key component of any security program is ensuring that the organization has a clear understanding of where risk resides. One of the most effective ways to understand weaknesses within a network is with a penetration test/ethical hacking assessment.

Many organizations understand the need for a penetration test but are challenged with understanding the right level of risk assessment for the organization, the ROI associated, and what to plan for or expect during an engagement.

In this guide, we address these and other commonly asked questions and share insight to help highlight the benefits of penetration testing /ethical hacking as a vehicle to better improve information security.

KEY INCLUSIONS:

- Penetration Test Defined
- The Differences Between a Penetration Test vs. a Vulnerability Scan
- 6 Key Benefits of a Penetration Test
- Common Penetration Testing Myths
- Best Practices for Drafting an Effective Request for Proposal
- Top 5 Questions to Ask a Prospective Penetration Testing Provider
- Testing Rules of Engagement
- Tips & Recommendations

"ALMOST HALF OF ORGANIZATIONS HAVE SUFFERED AT LEAST ONE SECURITY INCIDENT IN THE LAST 12 MONTHS." [i]

WHAT IS A PENETRATION TEST?

It is a security assessment designed to help determine whether a system is vulnerable to attack, if the defenses were sufficient, and which defenses (if any) the test defeated.

A penetration test allows for multiple attack vectors to be explored against the same target. Often it is the combination of information or vulnerabilities across different systems that will lead to a successful compromise.

"A PENETRATION TEST IS AN AUTHORIZED SOFTWARE ATTACK ON A COMPUTER SYSTEM THAT LOOKS FOR SECURITY WEAKNESSES, POTENTIALLY GAINING ACCESS TO THE COMPUTER'S FEATURES AND DATA." [ii]

PENETRATION TESTS VS. VULNERABILITY SCANS

- Vulnerability assessments are often confused with penetration tests. Both are important to a holistic approach to security, but are very different security solutions.
- A vulnerability scan looks for known vulnerabilities in your systems and reports potential exposures. A penetration test is designed to actually exploit weaknesses in the architecture of systems.
- Vulnerability assessments are performed using technology or software that produces a report listing found vulnerabilities. Most penetration tests are conducted by highly trained professionals who take the output of a network scan and probe to find an open port or a service that can be exploited.

EXAMPLE:

A vulnerability assessment will scan your network and notify you that you have a certain vulnerability.

A penetration test will determine whether the vulnerability can be exploited and how much information could be obtained by an attacker.

6 REASONS TO SCHEDULE A PENETRATION TEST

1 Achieve Compliance from Regulators and/or Auditors With Penetration Testing

Businesses today are faced with a daunting number of security standards and regulatory obligations. While the wording in each of them differs, the basic tenet of protecting sensitive and confidential data remains.

Some standards are simply recommended industry best practices and guidance, while others such as GLBA, HIPAA, and PCI-DSS are mandatory, with each carrying large penalties if the company falls out of compliance. To show compliance with these regulations, companies will find that the detailed reports provided by penetration tests assist in helping organizations demonstrate ongoing due diligence to auditors and/or examiners.

2 Test to Determine if Potential Vulnerabilities are Exploitable

Vulnerabilities in modern operating systems such as Microsoft Windows and Linux distributions are often very complex and subtle. Yet, when exploited by very skilled attackers, these vulnerabilities can undermine an organization's defenses and expose it to data loss.[iii] Before a cyber criminal attacks, having a "white hat" hacker test the network will help the organization understand exploitable vulnerabilities and shore up security before a person with malicious intent does.

3 Leverage Penetration Test Reporting as Due-diligence for your Customers

Today's consumers are security savvy and are concerned that businesses they support and partner with may

"TWO-THIRDS OF CONSUMERS SAY THEY'D STOP DOING BUSINESS WITH A COMPANY IF THEIR INFORMATION WAS STOLEN, ESPECIALLY IF THE BUSINESS WAS IN THE BANKING, HEALTHCARE OR LEGAL FIELD."[iv]

be the next cyber criminal's target, allowing their personal information to get into the wrong hands.

Having a security program in place that includes a penetration test can help organizations attract prospects, win business and keep existing customers happy by giving security assurance that the organization is working to harden networks against attack and misuse.

> **"47% OF ALL BREACHES IN THIS YEAR'S STUDY WERE CAUSED BY MALICIOUS OR CRIMINAL ATTACKS. THE AVERAGE COST PER RECORD TO RESOLVE SUCH AN ATTACK IS $170."** [vi]
>
> **-PONEMON INSTITUTE , COST OF DATA BREACH STUDY: GLOBAL ANALYSIS**

4 Test your incident response preparedness

A penetration test simulates a real-world attack and can help an organization measure the success of incident response security controls. An attack that attempts to gain access to sensitive data helps organizations identify strengths as well as opportunities for improving attack detection and response.

5 Communicate Security Posture Easily

When a penetration test is conducted, a detailed report of the assessment findings should be provided. This report should clearly communicate the high level objectives, methods and findings of the exercise. This report can be a communication tool to share insight with technical staff on the organization's security initiatives as well as the security posture of the company. Being able to share the overall effectiveness of the penetration test and the goals for improvement can help the technology leadership of the company to better understand risks and determine what future resources may be needed.

6 Avoid the Cost of a Breach

An information security breach can have devastating financial consequences. Legal fees, remediation, customer protection programs, regulatory fines, loss in sales and reputational damage can negatively hurt an organization's bottom line.

The increased cost required to resolve security incidents and the financial consequences of losing customers when a breach occurs, is sound reason to invest in proactive security such as penetration testing.

PENETRATION TESTING: COMMON MYTHS[vii]

MYTH #1: Penetration tests are not needed. Vulnerability scanning can identify all vulnerabilities in the environment.

While the goal and methodology of both services are similar — to help an organization secure the network — the deliverables can be quite different. Vulnerability assessments are intended to provide a broad high-level view of the security posture of a network by providing a detailed listing of potential vulnerabilities and suggestions on how to mitigate or remediate the weakness or flaw. This is generally across all systems on the network; or should be, as a best practice. Depending on the maturity of your organization's vulnerability management program, the amount of data can be overwhelming.

Penetration tests, on the other hand, are typically driven by a human analyst, and are goal oriented or structured to simulate a real-world attack scenario your network might encounter from an intruder. Penetration testing will often identify blended weaknesses – the combination of two or more vulnerabilities – that can pose a higher composite security risk than individual vulnerabilities themselves and flaws that cannot be discovered in an automated fashion.

MYTH #2: Professional penetration testers use expensive commercial tools

Professional penetration testers use a variety of tools and scripts to achieve their objective. Some of the tools are commercially available, while others are open source or custom, having been developed over the course of the analyst's tenure as a penetration tester. Some will argue that commercial products have all the necessary tools to provide a complete penetration test. The mark of a good penetration tester is their ability to utilize all the tools at their disposal and the experience to know how to use them effectively.

"DEPENDING ON THE MATURITY OF YOUR ORGANIZATION'S VULNERABILITY MANAGEMENT PROGRAM, THE AMOUNT OF DATA CAN BE OVERWHELMING"

-TOM DESOT, DIGITAL DEFENSE EVP, CHIEF INFORMATION OFFICER

THE INTERCONNECTEDNESS OF A NETWORK IS ITS GREATEST BENEFIT AS WELL AS GREATEST WEAKNESS. ONE SYSTEM COMPROMISE CAN GREATLY AFFECT OTHER SYSTEMS ON THE NETWORK AS WELL AS THE NETWORK AS A WHOLE.

MYTH #3: One system compromise has no effect on other systems

The interconnectedness of a network is its greatest benefit as well as greatest weakness. Organizations that test only select segments of their network introduce an incalculable risk to their organization from the untested segments. One system compromise can greatly affect other systems on the network as well as the network as a whole. While a printer may seem somewhat innocuous on the network and no great threat, an intruder can quickly (and often easily) wreak havoc on the network by changing the configuration of the printer and then using it to reroute network traffic. While this issue is distracting IT security teams, the intruder may be elsewhere on the network stealing data and other sensitive information. Alternatively, if the compromised system contains elevated credentials or permissions, then the rest of the network has already been lost.

MYTH #4: Penetration testers use the same approach and are likely to only uncover the same issues seen in the earlier tests.

No two analysts are created equal. The breadth and depth of experience among penetration testing analysts can differ significantly. Their education, training and tools utilized can greatly affect the results and outcome of the penetration testing engagement. The old adage, "You get what you pay for", is true for penetration tests. It's important that the penetration testing entity have the background and experience to competently achieve the goal of the engagement, whether that's a broad external or internal test or a more specialized application focused test.

BEST PRACTICES FOR DRAFTING AN EFFECTIVE REQUEST FOR PROPOSAL (RFP)

- Research and select three to five companies to whom you will be releasing the RFP.
- Identify the point of contact for submission. A single point often gains a better response than a committee.
- Determine who will be the point of contact for the RFP response and during testing. Be sure to include not only the prime contacts but also alternates.
- Communicate what it is you want tested. For example, external/internal systems, key systems only or everything.
- Confirm ownership and/or permission to test all of the IP addresses that you will be including in the RFP.
- List the URLs of the websites you would like tested and details around shared hosting and/or permission to test.
- Determine if you want black box (the attacker has no credentials to the system) or white box (the attacker has credentials to the system) testing.
- Confirm if your organization wants actual exploitation of any vulnerabilities discovered to occur.
- Clearly communicate what should happen if something is exploited and note if the testing should stop or continue.
- Provide a response due date that includes a date and time and details on how late submissions will be treated.
- Communicate the testing time frame such as during normal business hours or after hours.
- List what methodology you prefer the analyst use. Most will request a standard and accepted methodology such as the National Institute of Standards and Technology guidelines.
- Clearly define what types of tools the analyst can use, such as “zero day” exploits, denial-of-service testing, open source or commercial only tools.
- Note how you would like final results or reports delivered and the timing expectation for delivery.

TOP 5 QUESTIONS TO ASK A PROSPECTIVE PENETRATION TESTING PROVIDER

Selecting the appropriate penetration testing vendor involves asking the right questions to properly vet the security testing tools, methods and experts they employ:

1 How does the penetration test differ from other types of security testing—such as a vulnerability assessment?

Beware of any vendor that uses the words "penetration" and "scans" interchangeably, or claims that their penetration testing process is fully automated.

2 What is your process for performing the penetration test?

Even if they do not use a defined methodology, the vendor should be able to provide a straightforward outline of the steps involved and which tools are used at each step in the process.

3 Do your testers hold industry standard certifications?

It's important to know that the individuals conducting your test are knowledgeable and remain up-to-date on security trends.

4 How will you protect my data during and after testing?

Find out how the tester will secure your data during the test and throughout delivery. Confidential data, including test reports, should never be sent via email; secure FTPs or secure file-sharing sites that use SSL should be employed.

5 How will you ensure the availability of my systems and services while the test is taking place?

Because penetration tests are actual attacks against your systems, it is impossible to guarantee uptime or availability of services throughout the test. However, most testers have some idea of whether or not a particular attack will bring down your system or "hang" a service. (You can also assist your tester by alerting them to any legacy or otherwise less-than-robust systems on your network.) The ideal penetration testing vendor will work closely with you to address operational concerns and monitor progress throughout the process.

PENETRATION TESTING RULES OF ENGAGEMENT

The rules of engagement define how the penetration test is to occur, set proper expectations and communicate different aspects which need to be addressed prior to the engagement.

COMMON INCLUSIONS TO THE RULES OF ENGAGEMENT:

Timeline

A clear timeline will define the start and end of the engagement and allow all involved to more clearly identify the work that is to be done and those responsible throughout the process. GANTT Charts are often used to define the work and the amount of time and resources needed for each specific component of the assessment.

Locations

It is not uncommon for an organization to operate in multiple locations and regions. Defining the locations and physically or virtually obtaining access to the information will be necessary.

Evidence Handling

There is a strong possibility that the white hat hackers will gain access to sensitive information. In those situations, the data will needed be treated with extreme care.

Permission to Test

One crucial document you will be asked to review and sign is the Permission to Test document. This contract will state the scope of work and require signatures that acknowledge awareness of the activities. Some activities in common penetration tests could violate local laws. For this reason, it is advisable to check the legality of the penetration tests in the location where the work is to be performed.

RECAP TIPS & RECOMMENDATIONS TO MANAGE A SUCCESSFUL NETWORK PENETRATION TEST

1 Comprehensive network assessment

Be sure that you're assessing your network and systems on an external and internal basis. Some questions to ask: "Can an external phishing attempt on a single user result in a pivot all the way through to administrator privileged access of a high value internal restricted server? Which layers in your security program were successful in blocking the attack?"

2 Plan and structure the tests for effective results

It's important to prepare to have the right resources in place to assess the results of your penetration testing. Treat your penetration test as you would any other technical project rollout.

3 Be prepared for some upfront planning

Real life example: Pay special attention to the penetration testing team's pretest request for information. If incorrect IP addresses are provided, then some of the systems or IP ranges will be missing test coverage.

4 Create a communication and alignment plan

Make sure that the people normally responsible for incident response are not aware of the attack. This is primarily so that management can gauge how well the response team detects and addresses the attack.

5 Come up with a monitoring plan

While the penetration test is being done by an external team to test the layered defenses, it can also be a very good test of your monitoring and incident response program. This means documenting which systems, sensors and teams triggered alerts during the penetration test.[viii]

6 Plan for after the penetration test

Make sure that penetration test results are qualified by the right frame of reference. Example: if the number of vulnerabilities reported has doubled from last year and the number of services and workstations has increased, do you have a large number of vulnerabilities on the same system that were previously tested?

7 Reporting to management

Ensure that reporting to management is part of the penetration test engagement. Furthermore, be sure that the results are comprehensible by executives and board members at the organization.

8 Understand that there is no silver bullet

Understand that there is no simple solution to information security. To stay diligent against cybercrime, an organization needs to be committed to a holistic approach to security and embrace a robust security program.

About Digital Defense, Inc. (DDI)

Founded in 1999, Digital Defense, Inc., (DDI) is a premier provider of managed security risk assessment solutions protecting billions of dollars in assets for clients around the globe. In 2015, the organization has received numerous industry recognitions including a top 50 ranking (#46) in Cybersecurity Ventures' listing of the World's 500 Hottest Cybersecurity Companies, as well as inclusion in CSO Outlook's Top 10 Network Security Companies and CIO Review's 20 Most Promising Cyber Security Solutions. Vulnerability scanning, penetration testing, and security awareness training are DDI's most popular offerings, each of which proactively improves the security of an organization's confidential data. DDI utilizes a unique Vulnerability Management as a Service (VMaaS) delivery model to help organizations establish an effective culture of security and retain information security best practices, bringing lasting value to clients served.

Contact DDI at 888-273-1412 or ddifrontline.com.

References and Resources

[i] http://www.experian.com/data-breach/2014-ponemon-preparedness.html?

[ii] https://en.wikipedia.org/wiki/Penetration_test

[iii] https://www.sans.org/course/advance-exploit-development-pentetration-testers

[iv] http://www.forbes.com/sites/drewhendricks/2014/02/03/is-your-pos-secure-how-to-avoid-a-target-style-disaster/

[v] https://kirkpatrickprice.com/blog/3-reasons-you-should-be-undergoing-regular-penetration-tests/

[vi] http://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

[vii] http://networkingexchangeblog.att.com/enterprise-business/penetration-testing-5-common-myths-explained/#fbid=-dm1Ore_snT

[viii] http://www.csoonline.com/article/2944967/network-security/10-steps-to-managing-a-successful-network-penetration-test.html

Experian® Data Breach Resolution
866-751-1323
www.Experian.com/DataBreach
databreachinfo@experian.com