FORTRA™

Penetration Testing: What You Need To Know

Proactive Testing for Security Weaknesses

Executive Summary

Increased cyber attacks and a growing number of data breaches has demonstrated the severity of risk for organizations and the critical need to embrace proactive information security practices. If an attacker or nationstate actor can exploit vulnerabilities on large, complex networks like financial institutions, government organizations, companies working in the political stratosphere, as well as SMBs, it should raise the question, "Is my organization's network security powerful 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 and 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

The number of data breaches continues to increase each year, rising 20% from 2022 to 2023.[i]

i *Harvard Business Review 2024

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 Scan

- 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.

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

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 examiner.

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 breaches defenses.

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 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.

66% of consumers will not buy a product from a company if they don't trust the company to protect their data.[iv]

iii - IBM Cost of Data Breach Report 2023
iv - Verizon DBIR Report 2023

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 impact 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.

Global average cost of a data breach - $4.45 million [v]

US average cost of a data breach - $9.5 million [vi]

Penetration Testing: Common Myths

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: Pen Testing Will Significantly Disrupt Network Operations

Only if it's done carelessly. Typically, if there are any disruptions at all, they are pretty minor and very temporary. It's true; you need to take a step back to go forward. Driving requires pulling over for gas and walking requires you to bend down and tie your shoes. But overall, the minor inconvenience is worth it when you consider the massive benefits.

To offset any minor adjustment in flow, plan appropriately and choose a reputable vendor. Smaller providers may be limited in their resources, forcing you to work on their timelines. Larger, more established pen testing vendors schedule on your time – even on nights and weekends. Email your employees about blackout windows and develop the mindset that a small disruption is well worth it to avoid a long-term outage that a real breach may cause.

Use this to your benefit. Set expectations at the outset and be open with employees that can be informed when a pen test is being run. If they understand the importance of pen testing as much as you do, they'll be much more likely to endure any slight inconveniences that might occur (like a temporary spike in bandwidth) if they know what's at stake if they don't. This transparency also translates into a more security-aware company culture.

Vulnerability management and penetration testing are intended to work together. One identifies vulnerabilities, the other verifies if they are exploitable.

MYTH #3: Pen Testers Use Illegal or Unapproved Methods to Gain Access

Quite to the contrary. Not only is it best practice, it is often a regulatory requirement that testers stay within the bounds of what's lawful. Only industry standard methods and tooling are used, which are provided to customers as part of the rules of engagement. Proper authorization is what draws the line between ethical and unethical hacking, between professional penetration testers and digital vigilantes, and between right and wrong.

In addition, the right pen testing vendor will put analysts in communication before and during the test to address any concerns that may arise. But the short answer is, no. When an organization grants explicit permission and a pen testing provider is completely transparent about their techniques, tools, and methodology, everything is perfectly above board. This also implies absolute confidentiality on the part of the vendor.

However, because this myth proliferates, many are concerned that penetration puts their network at risk.

MYTH #4: Pen Testing Vendors Need to be Rotated

While there is no regulatory statute stating that organizations need to rotate their pen testing contractors, it often feels like an unwritten rule. The logic behind this is that one team will catch what the other leaves behind. And this logic holds up. Each pen tester has a "very particular set of skills" and can bring something different to the table. But today you can find pen testing service vendors with multiple unique pen testers on call. They can easily swap out skillsets, give you a different perspective, and change things up all while maintaining continuity.

When you start in with a pen testing service, a lot goes into getting to know your company, its architecture, your goals and security objectives – even an organization's personal style. When you've found a vendor that you trust, switching out pen testers or even pen testing teams from their internal pool is a way to get the best of both worlds.

The right pen testing service vendors have multiple unique pen testers on call and can easily swap out skillsets, giving you a different perspective with different approaches.

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 & Recommenations 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 work-stations 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.

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-dd-gd-0424-r2-vm