WHITEPAPER

Penetration Testing

Why Having the Right Penetration Testing Strategy Matters More Than Ever

DIFENDA

Why You Need to Take a Strategic Approach to Penetration Testing

Choosing the right penetration testing strategy can be complex. This whitepaper will explore the many factors involving the right strategy for your company. Penetration testing is vitally important, and cybersecurity consultants need to perform tests correctly, especially online.

A **2019 SANS INSTITUTE WHITEPAPER** found that, when testing three application security scanners on Web 2.0 web applications, "almost three-quarters of vulnerabilities went undetected. Similar to SANS's recommendation of a multi-faceted approach to improve web security, this whitepaper will provide a multi-faceted approach to understanding penetration testing so that your company's digital assets can remain safe from prying eyes.

The following topics will be covered in this whitepaper:

- Why regular testing is important
- FAQs you need to know when hiring cybersecurity penetration testing consultants
- The scope of a penetration test
- Why it is necessary to hire the right consultants and the right company
- Difenda's strategy when approaching penetration testing and how it can help you

Table of Contents

Today's Business Climate Demands Strong Cyber Security Measures

Protecting critical data is of vital importance to any company. Leaked data can negatively affect revenue streams and clients' willingness to continue working with your business. Clients expect that you will protect and safeguard their data, especially their financial information, from bad actors like black-hat hackers.

However, even with adequate preparation, your company may still be the target, and victim, of hacking. To maintain trust in your organization, you need to plan for this contingency. Suppose your clients know that you understand the threat of hacking and that your company is taking safeguards to prevent this eventuality. In that case, your clients will be happy to continue doing business with you, as you are making as much effort to help protect their data as possible.

Target, for example, is now known within cybersecurity circles for being the victim of a **2014 HACK** that targeted their HVAC systems. Hackers used those systems to gain entry to Target's central systems and steal non-financial and financial customer data.

While Target is still known for this hack, fewer people know that the United States Secret Service **CONDUCTED AN INVESTIGATION** with Target's cooperation. Additionally, in 2014, Target had "at least $100 million of cyber insurance, including self-insured retentions, and $65 million of directors and officers liability coverage, according to **INSURANCE INDUSTRY SOURCES**" Finally, Target now has a **SECURITY VULNERABILITY REPORTING POLICY** for security researchers to report potential security vulnerabilities with their public-facing systems.

Target was, and still is, taking measures to meet the demand for cybersecurity professionalism in the workplace, the hack notwithstanding. Even though Target was hacked, it has shown itself to be a good business partner because they take the cyber threat landscape seriously, whereas a competitor may not. Like Target, your company should prioritize cybersecurity and penetration testing, as it is a unique tool in your cybersecurity toolbox.

Identify Your Vulnerabilities Before Hackers Do

Boxers train to fight and fight to train. The same mentality is involved with penetration testing. In short, you will be providing cybersecurity consultants with access to your systems, as well as potential goals they need to accomplish.

The consultants you choose will "hack" your systems using specific techniques like social engineering without doing any long-term damage and write reports that provide insights into how you can strengthen your cybersecurity. By simulating a hack, you can better defend against real hackers in the future.

Hackers look for weaknesses inherent in systems to exploit for gain. If your company's defenses are too strong, hackers will look elsewhere for data, unless they specifically target you. Then, it's a matter of motivation, which makes your cybersecurity defenses even more critical to implement and maintain correctly.

The idea behind increasing your cybersecurity defenses is to make the ordeal of hacking your company too expensive or bothersome for the hackers. Strong passwords, limited access to resources like security cameras, and patching network vulnerabilities are some recommendations consultants will provide you with, and for good reason.

Beyond common recommendations like these, regularly visiting the OWASP (Open Web Application Security Project) Foundation's website is a vital resource to being aware of recent attacks hackers are using, especially the **OWASP TOP 10**.

Awareness plays a big role in your cybersecurity program's effectiveness, which is exactly what penetration testing aims to provide.

An Effective Cybersecurity Program Needs Regular Penetration Testing

The only way to effectively leverage penetration testing is to perform it frequently. Testing **MUST BE DONE AT REGULAR INTERVALS**, either time- or event-based, depending on your company's needs and goals. Some popular times when companies perform penetration testing include:

- During the installation of new systems, especially client-facing systems
- To ensure companies are following industry standards like PCI DSS
- When companies are implementing major infrastructure and application changes
- When systems are updated
- At regular intervals: monthly, quarterly, or yearly

Your cybersecurity consultant will work with you to identify when you need to perform penetration testing and how you can secure your systems better after the testing is complete.

Penetration Testing Helps You Stay Compliant With Security Regulations

Compliance is a significant motivator for most companies when it comes to expanding their cybersecurity programs.

Depending on your industry, your company may need to stay in compliance with regulations like PCI DSS, HIPAA, or ISO 27001. The standards you need to follow will require your company to meet specific objectives if you want to comply with them, like regularly scheduled penetration testing and security audits. Reference the appropriate regulations to determine what your company's responsibilities are.

The benefits of following these regulations are twofold. First, doing so will attract clients that also wish to remain in compliance. Second, you may require consultants with specialized skills and knowledge in these regulations. For example, you may be a healthcare-adjacent company that requires strict adherence to HIPAA because you are collecting private medical information from customers.

In the following section, we will cover common questions you should ask cybersecurity consultants during your initial meetings.

Questions to Ask Your Next Penetration Testing Team

No two penetration tests are the same. The results—and the outcomes that you achieve—will depend on the capabilities of the service provider you choose to work with.

Here are a few questions you should ask your next penetration provider:

How long does your team take to deploy a penetration test?

The length of time to deploy a penetration test will depend primarily on the scope of the test. Testing one system will take less time than testing every system. That stated, conducting penetration tests regularly, and with the same cybersecurity consultants, may improve time efficiency as these consultants will become more efficient in their work and more familiar with your systems over time.

How many cybersecurity professionals will be working on the penetration test?

The number of professionals and their skills working on your penetration test will significantly influence the testing speed. The more consultants you hire, the higher the labor costs will be.

Does your cybersecurity team have industry-standard certifications?

While by no means a panacea, industry-standard certifications are a quick way to verify your consultants are as skilled and knowledgeable as they claim to be. Relevant certifications include:

- CompTIA PenTest+
- EC-Council CEH
- OSCP
- OSWE
- GIAC GPEN
- GIAC GWAPT

What is your data protection procedure during and after running the penetration test?

You will be allowing consultants to access your data, as they will have permission to hack into your systems. Ensure that you have a procedure in place to ensure your data can be backed up and saved so that you do not lose any information resulting from the penetration test.

Is a penetration test the same as a vulnerability assessment?

A penetration test is more invasive and active, while a vulnerability assessment is less invasive and reactive. Be sure to consult with relevant C-level executive/IT/legal staff and departments and implement strict rules regarding access to your systems and sensitive data before you provide anything to your consultants. Consultants perform vulnerability assessments as one of the stages of penetration testing.

What is your process for conducting penetration testing?

Consultants will have a defined process for conducting penetration testing, and they will share it with you. You need to know what they are doing to your systems and what data they are accessing. You should receive a summary report after the consultants complete testing.

Can you make sure my systems continue to run while you are penetration testing?

We can, but we do not recommend this. Consultants will need access to your systems and may temporarily disrupt operations while they conduct their testing. Consider having penetration testing conducted during off-hours when fewer clients, customers, and staff will access your systems and be negatively affected by the testing.

The Right and Wrong Way to Scope a Penetration Test

The larger the scope, the better. There is no telling how a hacker will approach your organization, or what previous knowledge the hacker possesses. After all, a system that can be accessed by anyone, can be accessed by anyone. It is just a matter of time, budget, and motivation. Likewise, you need to conduct penetration testing on aspects of your systems beyond the typical database servers holding private or financial data.

Many aspects to conducting a penetration test exist like:

- Are your servers locked away?
- Are your technical security measures, like cameras, working?
- What are the patrol routes of your security details?
- How much access does any one employee have?
- Do some employees have more access to systems than others? Why?
- How strong are your password requirements at your company?
- Do your client-facing staff know what social engineering is and how to prevent it?

Hackers will take advantage of all this information, as well as information that you may initially consider. Remember that hackers attacked Target via its HVAC system, not its main systems. Hackers instead used the HVAC system to gain access to other systems.

Hackers can do the same to you, which is why the scope of your penetration testing needs to be as large and deep as possible, including peripheral systems you may not immediately think of as important to hackers.

Social Engineering: The Weakest Link Is Human Error

Employees typically do not want to harm their workplace. However, if not trained well, they make mistakes. They provide classified information over the phone or forward suspicious spam emails to others in the workplace. These are two common forms of social engineering hackers use to gain access to digital systems or sensitive information.

You can prevent this with internal controls and employee training. Ensure that employee passwords are sufficiently complex and lengthy and that employees understand communication protocols within the company. Teach them how to spot suspicious emails and other documents and never provide information without checking with their immediate boss and following work protocols.

Every employee needs defensive cyber training to store data and information from hackers securely. Everyone from the CEO to the interns should be aware of the need to protect data and information.

When your entire organization understands how to detect malicious emails, files, and hacking attempts—they'll know what steps to take to keep the company protected.

WiFi Security: Testing Wireless Components

Configuring your WiFi network is essential to maintaining good security. Often, especially with smaller or newer businesses, the guest wifi login portal is not well-guarded. Companies may either provide free WiFi or allow people to connect with minimal effort.

However, once a hacker is in your system, they are in your system — even if they are just in your WiFi network. Ensure you only allow specific guests to log in, if at all, and require strong passwords. In addition, choose enterprise-level security for your WiFi connections rather than the default consumer-brand configuration.

Web Application Testing

Websites and web applications can be targeted as well. You should secure your web presence just as much as you secure your data servers.

After all, anyone can access your data servers via your website, especially if you don't protect yourself from SQL injections, for example. Good penetration testing consultants will test these and other potential issues your website may face from hackers.

External Versus Internal Penetration Tests

Whether you have an external versus internal penetration test performed will depend on the scope of the test itself.

If a consultant has to perform penetration testing as if they are outside your company, they are performing an external test.

If a consultant performs a test as if they are inside your organization and may even have privileged information regarding your company, they perform an internal test. You should ideally have both types of tests performed for maximal testing coverage.

The Cost of Hiring the Wrong Cybersecurity Company to Conduct a Penetration Test

You get what you pay for. This same phrase is relevant in the world of cybersecurity.

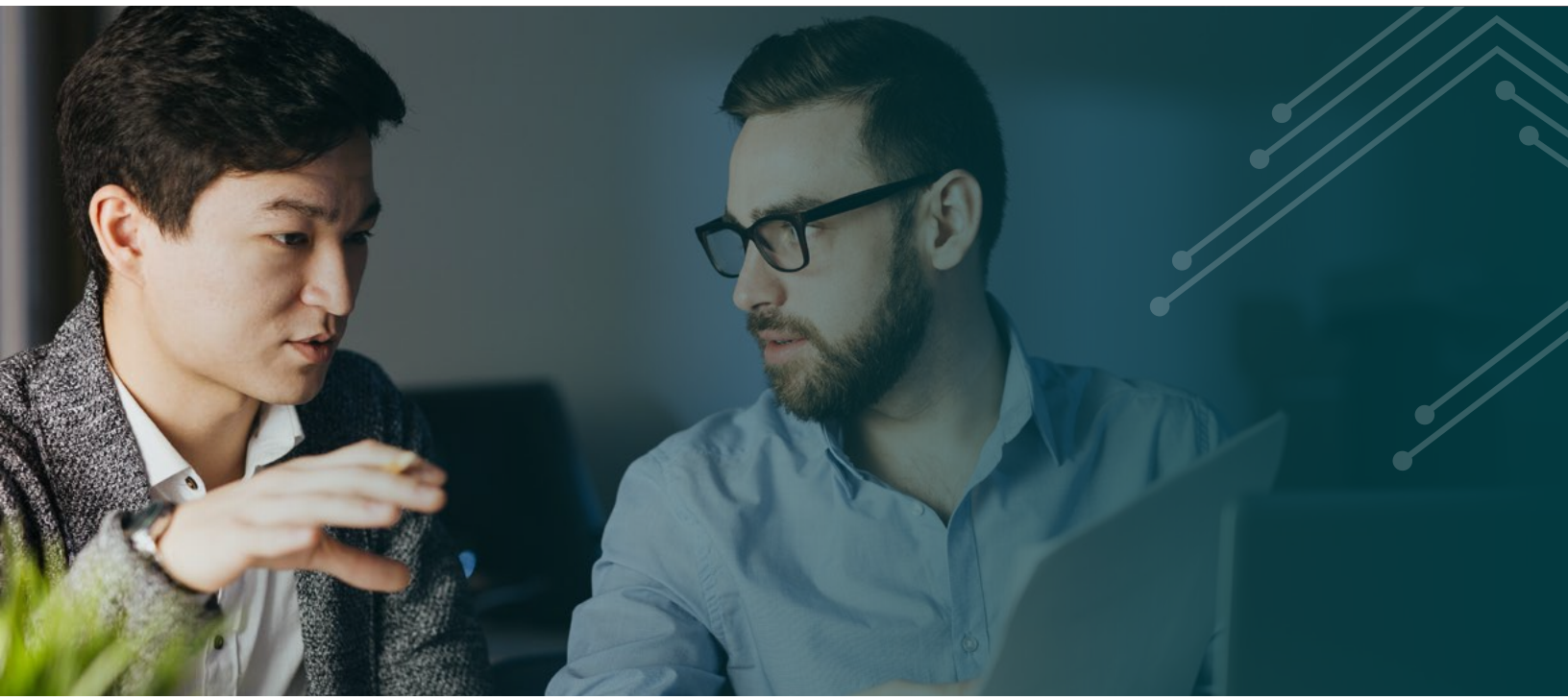
Consider the costs of an inexperienced consultant performing a penetration test. Cybersecurity requires both skills and knowledge, spanning the theoretical and practical realms of the subject.

Hiring a good firm with industry recommendations and contacts is necessary to ensure your tests are solid and invasive, and that known security issues and vulnerabilities are uncovered and patched.

Your budget and timing may be limited. The consulting firm's staffing and scope may be limited. You need to determine the best consulting firm based on your needs and budget.

It's better to spend more on preventive measures performing testing rather than lose untold revenues by leaving your systems defenseless against hackers.

Before hiring consultants to perform your penetration tests, reach out to other clients they mention and obtain a reference. Choosing the right firm for you is vital for success in cybersecurity.



Difenda's Strategic Approach to Penetration Tests

Difenda's approach is simple, yet effective. We provide a leading cybersecurity team with advanced cyber knowledge, experience, and skill to test your company's cyber defenses.

Our customers receive constant feedback throughout testing, including an executive summary and technical report.

We also leverage various testing types and methodologies to provide you with the information you need regarding your organization's defenses and the possible solutions you can implement to secure your data.

We have a proven track record and can provide insights that competitive companies cannot.

Difenda's Penetration Testing Methodology

Each company determines its methodologies. At Difenda, our methodology relies on detecting threats quickly for maximal preventive cybersecurity. We value quick execution and turnaround time, allowing us to be more efficient than other companies in the field.

How We Conduct Penetration Testing at Difenda

Our penetration tests typically involve six stages, each of which contributes to understanding your company's current protections and areas of improvement. Specific testing formats and scope depend on our clients' needs.

1. RECONNAISSANCE/INTELLIGENCE GATHERING

In this stage, consultants collect information from various sources — formal, informal, public, private, and more. While hackers will also resort to illegally acquiring information, consultants will not because laws and regulations still bind them.

Hackers use the following resources, among other avenues, to glean information:

- Websites
- Social media
- Company memos
- Phone conversations with employees
- Coworker conversations

2. THREAT MODELLING

Threat modeling provides clients with a likely scenario of how a threat can look. These models are then used during testing overall to determine how a company's website, for example, will act and react to potential threats.

Consultants can map out application content and discover weak points via which to attack. By mapping out and deconstructing an application, consultants can determine how likely it is that a hacker will target specific company assets.

3. VULNERABILITY ASSESSMENT

Consultants also analyze applications for various known vulnerabilities. During this analysis, unknown vulnerabilities are discoverable as well. Focus on evident weaknesses, as increasing their security, if not entirely nullifying hacking threats, is vital to ensuring that your applications are secure from the harm hackers pose.

Depending on your company's resources, both server-side and client-side assets will be analyzed, based on the requested scope of the penetration testing, as well as your consultants' areas of expertise.

4. EXPLOITATION/POST EXPLOITATION

This stage is the main testing phase. Based on the issues and vulnerabilities uncovered in the previous stages, consulting cybersecurity professionals will test your applications to determine their strengths.

Consultants will deploy various attack scenarios and compile impact analysis statistics. When unskilled people think of hacking, they think of this stage.

5. REPORTING

This stage provides a detailed and comprehensive report on the overall scope of the penetration testing process. Consultants will prioritize various measures and issues, and your company will be assigned a risk profile as well. Furthermore, consultants will provide you with a technical report, which consists of:

- An executive summary
- Overall posture
- Risk ranking/profile
- General findings
- Technical details
- Identified vulnerabilities, successful exploitations, and prioritized remediation strategies

6. REMEDIATION AND RETESTING

Typically, this stage involves closing now-known vulnerabilities and revisiting previous stages in the testing process. Revisiting stages, similar to a spiral methodology in software engineering, is essential to ensure that the security of your systems increases incrementally and phases in the process repeat over time.

At Difenda, we go a step further with our testing, offering white-box, grey-box, and black-box approaches to penetration testing, combining the results of our testing with vulnerability assessments to provide a complete view of your organization's cybersecurity needs.9

DIFENDA

The Difenda Advantage

Every company needs cyber defences today. Working with external consultants to implement a penetration testing strategy is a great way to give your company an unbiased outside perspective. By regularly testing your systems, you will have a better understanding of current threats, vulnerabilities, and implement a cybersecurity program that's better able to deter hackers.

We believe human efficiency is more important than having the latest piece of trending cybersecurity software.

Difenda provides several key advantages that our competition typically does not. First, we provide a security operations center, operating 24/7 to monitor and respond to threats when they emerge. Second, we can update our clients with the latest in threat intelligence and modeling as a result of our center operations.

Are you interested in seeing how our penetration testing and offensive security services can enhance your cybersecurity program? Get in touch with our team today to get started.

Email: sales@difenda.com

Phone: 1.866.252.2103

LEARN MORE