WHITE PAPER

CAPITAL CYBER

SECURITY FIRST: AN ESSENTIAL GUIDE TO PENETRATION TESTING

INTRODUCTION

Penetration testing, also known as pen testing, can pose a challenge for numerous businesses. A lack of familiarity with its intricacies may serve as a significant hurdle in selecting the appropriate test, potentially jeopardizing your business's security.

This white paper is designed to assist businesses in comprehending every facet of penetration testing services, covering aspects such as planning, management, and deriving genuine value and benefits from the outcomes. Unlike a guide for practitioners, this white paper is specifically tailored for individuals involved in procuring, planning, and overseeing the lifecycle of a penetration testing project.

So what is it?

Penetration testing is akin to ethical hacking, often referred to as white-hat hacking. This structured technical procedure systematically evaluates the security of your IT systems and the behavior of your staff, leveraging strategies and techniques that real-world hackers might employ. Unlike malicious hacking, experts conduct penetration testing within specified parameters and at scheduled times.

This technical evaluation encompasses both active and passive assessments of IT systems and applications, along with probing human vulnerabilities through techniques like social engineering. Integrating penetration tests into your risk management strategy is essential. The primary objectives are twofold: first, to pinpoint and exploit vulnerabilities affecting information confidentiality, integrity, and availability; second, to provide actionable solutions and recommendations to mitigate the impact of these vulnerabilities.

"Penetration tests should be viewed as a cornerstone of your risk management strategy."

Why do it?

Stay ahead of cyber threats by assessing your security posture regularly. Evaluating your defenses gives you a clear picture of how you measure up against the dynamic landscape of threats. This proactive approach helps you pinpoint and rectify vulnerabilities before malicious actors exploit them.

Manage your technological foundation effectively. As your business expands and technology advances, the intricacy of your technical infrastructure grows. It's easy for elements to become overlooked or for gaps to emerge due to a lack of specialized knowledge. Each assessment illuminates the nuances of your setup, highlighting any interconnected elements that might compromise security. Remember, your security is only as strong as its weakest component.

Validate your security measures. While you may believe that your infrastructure is robust, backed by established procedures, processes, and staff training, how can you be certain? Conducting a penetration test offers tangible evidence of your security measures' effectiveness. This real-world evaluation confirms that your defenses meet industry standards and function as intended, providing assurance not only to you but also to your customers and partners.

Effective Risk Management
Every penetration test evaluates the potential risks to your business, emphasizing the potential effects on the confidentiality, integrity, and availability of your data. This assessment equips both management and technical teams with insights to prioritize, strategize, allocate resources, and address risks systematically.

Necessity of Compliance
The landscape is increasingly governed by legal mandates, regulatory guidelines, industry benchmarks, and best practices that emphasize the importance of regular penetration tests. Notable frameworks such as PCI DSS, ISO 27001, CMMC, FCA, HMG, and CoCo, among others, underscore this need. While compliance doesn't equate to absolute security, adhering to these standards offers a roadmap to fortify your infrastructure's security posture.

Safeguard Your Enterprise
Undoubtedly, security breaches pose significant threats, jeopardizing your brand's image and leading to substantial financial losses. By conducting penetration tests, you significantly diminish the likelihood of such breaches, safeguarding your organization's investments, credibility with both existing and potential clients.

GETTING IT RIGHT

You've now understood the significance of penetration tests for all businesses. However, before delving deeper into the intricacies of penetration testing, it's essential to recognize certain considerations and constraints.

Considerations

1. **Understanding the Scope**: Accurately defining the scope is crucial. A poorly defined test scope might render the results ineffective, wasting both time and effort.

2. **Focus on Your Goals**: Failing to grasp your objectives can result in setting impractical test conditions.

3. **Allocate Adequate Funds**: Your budget will influence the size and intricacy of the systems and applications under scrutiny. Ensure your budget accommodates all necessary testing requirements.

4. **Choose the Right Test Method**: Various penetration tests exist, and selecting the appropriate one is essential. Further details on specific test types will be discussed later in this document.

5. **Rely on Competent Professionals**: Engaging the wrong professionals can jeopardize the test outcomes or even damage systems. Prioritize researching the company to ensure they possess the requisite expertise.

6. **Stay Prepared**: Certain tests might demand significant resources, extended response times, or numerous alerts. Ensure readiness by selecting the right targets, duration, and test methodologies.

7. **Really be prepared**: The tests may have an impact on your running services, so it's best practice to perform a full backup before the testing begins.

Limitations

Penetration testing is not a magical solution.
No penetration test can offer a guarantee of 100% security because new vulnerabilities, techniques, and technologies emerge daily. However, what a penetration test does provide is evidence that you have maximized the security of your systems. This significantly diminishes the likelihood of a successful attack.

Penetration tests are time-limited.
They offer a snapshot of your environment's security posture at a specific moment. Consequently, many security standards require regular repetition of tests, usually every 6 months or annually, to ensure ongoing security effectiveness.

What's the Limitation?
Always bear in mind the boundaries of your testing scope. Penetration tests are inherently confined to predefined parameters. While you could task a penetration testing firm with a broad directive like "access everything," doing so might result in significant time and financial expenditures. It's more prudent to focus on a well-defined and comprehensive scope.

Human Factors
Don't solely prioritize technical tests; recognize the critical role of people. With escalating sophistication, attacks exploiting human vulnerabilities are becoming more prevalent and effective. Incorporating elements of social engineering in evaluations helps gauge the effectiveness of your staff in safeguarding your organization.

"Be cautious of assessments that solely concentrate on technical infrastructure, as the human factor can be equally crucial."

BOX CLEVER

Penetration testing can be categorized into three primary methods: black box, white box, and grey box. It's essential to grasp the distinctions between these terms when discussing them.

Black box
This is what you think of as a typical controlled hack. It's a realistic scenario, so very little information is provided upfront to the penetration testing company. It's useful as the penetration tester is placed in the same situation as a real-world hacker, with little or no prior knowledge of the environment in question. The drawbacks with black box testing is that the agreed time frame may not be sufficient to test everything, and some parts of the target infrastructure may be left untested, as they may not have been discovered.

Grey box
As you might have guessed from the name, a grey box test discloses partial information about the target systems to the penetration testers. This hybrid approach is the most common form of penetration test, as the tester can simulate a methodical attack without needing to know every detail of the target systems.

White box
If a black box test says nothing up front, then a white box test tells you everything. Full disclosure is given to the testers, including a breakdown of target systems, network diagrams and firewall rules. Whist not as 'real-world' as a black box exercise, it allows for a much more thorough test. By testing all aspects of the environment, security issues can be uncovered faster and in greater numbers. The obvious drawback of this test is that it's not a realistic scenario, as a real-world hacker attacker would not have a complete picture of the nitty-gritty bits of the architecture and would not be as biased as the tester. But when it comes to security, is there ever really such a thing as 'too much'?

"Is there such a thing as having 'too much' security?"

HOW TO POSITION THE PENETRATION TESTS

Penetration tests can be conducted externally, internally, or from both perspectives. While the objective remains consistent, the distinction lies in the source location of the attack.

External
External penetration testing mimics an attacker's attempt to access the internal network from outside sources or extract sensitive information from public-facing assets like web applications and email servers.

Internal
Internal-based penetration testing replicates an intrusion that has already breached the security boundaries. It examines the capabilities of an attacker or an insider once inside the network, including activities like transitioning between networks and intercepting internal communications.

TEST TYPES

Various types of penetration tests exist, each tailored to assess distinct facets of your security measures. The subsequent categories are widely recognized and typically applicable to all organizations. However, it's essential to recognize that terminology may differ among companies. To prevent misunderstandings, it's advisable to obtain a comprehensive service description rather than solely relying on the test names.

1. Network and Infrastructure Penetration Testing

This form of testing evaluates the security posture of an infrastructure or network, considering factors like active services, patch levels, configuration errors, design flaws, and the efficacy of security measures. The objective is to pinpoint and exploit any vulnerabilities present.

2. Application Penetration Testing

In this evaluation, applications undergo scrutiny from both authenticated and unauthenticated viewpoints. The assessment delves into aspects like access management, session and configuration handling, error management, data safeguarding, and input validation. Engaging in application testing offers insights into potential security risks arising from interactions between different components.

3. Configuration/Build Review Testing

This testing methodology scrutinizes the existing configuration of various system elements. Employing a non-intrusive approach, it assesses configurations against hardening practices and industry standards. By ensuring adherence to best practices, this review minimizes risks associated with unauthorized modifications and potential exploits.

4. Social Engineering Assessments

Addressing the human dimension of security, social engineering tests involve attempts to extract confidential data by exploiting human vulnerabilities. This encompasses tactics like phishing emails, deceptive phone calls, and capitalizing on procedural gaps to breach physical security.

5. Wireless Penetration Testing

This assessment zeroes in on vulnerabilities within wireless setups. Through meticulous examination of packets, access points, unauthorized devices, encryption mechanisms, and patching statuses, potential weak spots in wireless architectures are identified and addressed.

ANATOMY OF A PENETRATION TEST

Penetration testing firms generally adhere to a comparable methodology when conducting penetration tests. This commonly encompasses a 7-step lifecycle, as delineated below.

1. Scope definition & pre-engagement interactions

This is where all requirements are gathered and goals are set. It's where types of tests, forms, timelines and limitations are codified and agreed. This is essential for smooth and well-controlled exercise.

2. Intelligence gathering & threat modelling

Intelligence gathering is an information reconnaissance approach that aims to gather as much information as possible. This information is used as attack vectors when trying to penetrate the targets during the vulnerability assessment and exploitation phases.

3. Vulnerability analysis

This phase aims to discover flaws in networks, systems and/or applications, using active and passive mechanisms, which can include host and service misconfiguration, current patching levels, or insecure application design.

4. Exploitation

With the help of the vulnerability analysis from the previous step, all external and internal-facing systems that are in scope are attacked. This involves a combination of available and custom-made exploits and techniques in order to tamper with improper configurations, bypass security controls, access sensitive information and in general to establish access to the targets in question.

> "An effective penetration testing firm should furnish you with a comprehensive report that is both thorough and easily understandable."

5. Post-exploitation

The purpose of this phase is to determine the value of the compromised targets by trying to elevate privileges and pivot to other systems and networks that are defined within the scope. Importantly, the compromised systems will be cleaned of any scripts and further attacks that have been launched to make sure the systems are not subjected to unnecessary risks as a consequence of the tester's actions.

6. Reporting

Documentation of all information gathered in the preceding steps is imperative. An effective penetration testing firm should furnish you with a comprehensive report that is both thorough and easily understandable, covering:

- Risks associated with the current server/application setup/configuration.
- Vulnerabilities and running services on servers and applications.
- Detailed actions taken to exploit each security issue.
- Recommendations for remediation.
- Short-term and long-term action plans.

It is noteworthy that even vulnerabilities that cannot be exploited should be included in the final report. We strongly advise requesting a sample report in advance to ensure clarity and understanding. If a report is laden with jargon and difficult to decipher, its utility is limited.

7. De-briefing Session

While not mandatory, conducting a de-briefing session after concluding a penetration test is recommended. This session clarifies the findings and risks outlined in the report, providing you with a chance to address any queries you may have.

HOW TO PLAN AND MANAGE A PENETRATION TEST

"If you're uncertain about what should be encompassed within the scope, the penetration testing company can offer support throughout the entire scoping process."

1. Define your business needs and establish the goals you aim to achieve.

2. Decide on the specific penetration testing methodologies and requirements, taking into account any constraints or particular scenarios you wish to explore.

3. Pinpoint essential elements that will define the project scope. If uncertain about scope details, seek guidance from the penetration testing firm.

4. Evaluate the potential risks associated with testing these systems. If you cannot afford disruptions to vital operational systems, consider replicating the target environment.

5. Set a schedule for conducting the tests, specifying whether you prefer them during regular working hours or outside of them.

6. Establish a budget for these tests. With regular testing throughout the year and during significant infrastructure modifications, costs can be managed effectively.

7. Coordinate daily with your designated company representative to monitor test progress.

8. Obtain a comprehensive report that is both user-friendly and highlights all identified risks, organized by severity.

9. Collaborate with relevant teams to formulate a mitigation strategy. After discussing findings with your testers, determine the subsequent steps.

10. Conduct re-tests as needed to confirm that all identified issues have been adequately addressed..

"If you cannot risk any disruptions to a vital live system, alternative approaches like replicating the target environment in a separate system are available."

WHAT DO I NEED TO DO?

To ensure a smooth and effective test, consider the following steps:

Obtain a signed Non-Disclosure Agreement (NDA) to maintain confidentiality.

Inform all relevant personnel within your organization about the upcoming penetration tests.

Backup essential data from systems involved in the tests to prevent potential disruptions.

Prior to the initiation of penetration tests, provide necessary resources such as VPN access and IP white-listing to prevent any delays in test provision.

Promptly notify your penetration testing firm of any interruptions, faults, or concerns encountered during the testing process.

PENETRATION TESTING MYTHS

There are numerous misconceptions and incomplete truths surrounding penetration tests, even from what may appear to be trustworthy sources. Let's clarify some of these misunderstandings.

Penetration tests are just for large corporations.

Penetration testing is not exclusively relevant to large enterprises. Regardless of your company's size, these tests are crucial to ensure comprehensive cybersecurity measures, as cybercriminals target vulnerabilities irrespective of organizational scale.

It's exclusive to governmental or financial sectors

Contrary to common belief, penetration testing is not reserved solely for government or financial institutions. Security plays a pivotal role in every industry, safeguarding business continuity and mitigating the substantial reputational and financial repercussions associated with a security breach.

Penetration tests are the same as vulnerability assessments.

It's essential to distinguish penetration testing from vulnerability assessments, a common source of confusion. Vulnerability assessments employ automated tools with predetermined signatures to check for known security issues and patching levels. However, they fall short in validating exploitability and may overlook vulnerabilities not in their database. In contrast, penetration testing combines manual and automated techniques to validate each weakness by attempting to exploit them. These tests rely on the tester's creativity, ingenuity, and knowledge, transcending automated tools to achieve predefined objectives.

"A cybercriminal isn't concerned about the size of your organization; if it's an easy target, they'll exploit it."

SUMMARY

Penetration testing allows you to assess and fortify your existing security measures, safeguarding your business. By carefully defining the scope and choosing the appropriate test type, you can pinpoint and address potential security weaknesses effectively. It's crucial to partner with a trusted penetration testing firm equipped with skilled professionals.

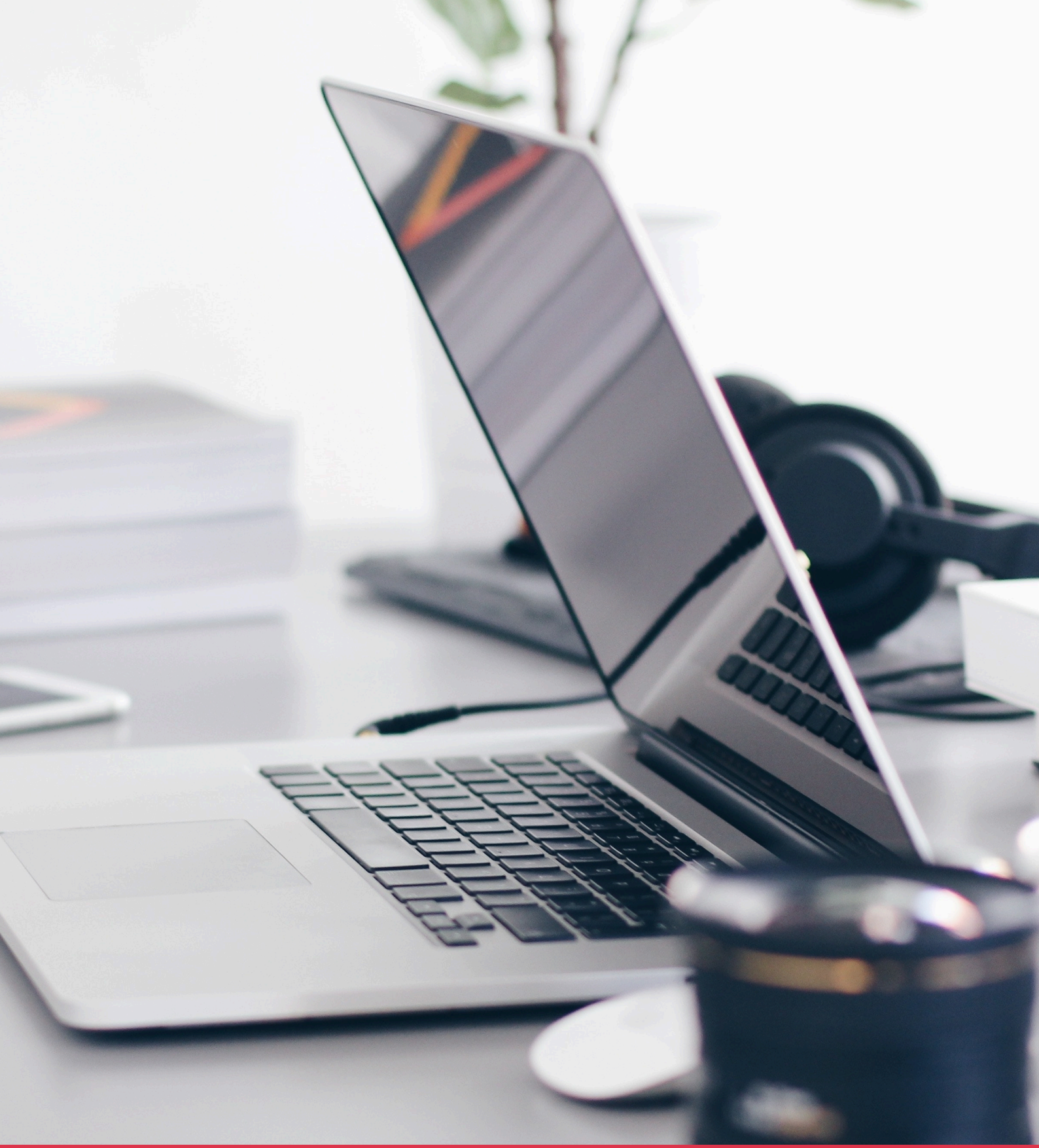
This partnership ensures thorough guidance throughout the entire process until vulnerabilities are addressed and risks are reduced.

Rather than an isolated activity, penetration tests should seamlessly integrate into your broader risk management strategy. It's essential to recognize that genuine security transcends mere technical solutions. Instead, fostering a culture of robust security within your organization, emphasizing continuous enhancement, is paramount.

Reach out today to identity security risks and remediating.

+1 (307) 227 6889

info@capital-cyber.com



CAPITAL CYBER

+1 (307) 227 6889

www.capital-cyber.com