WHITE PAPER

BULLET PROOF

# SECURITY FIRST:

# AN ESSENTIAL GUIDE TO PENETRATION TESTING

# INTRODUCTION

**Penetration testing, or pen tests, can be a confusing subject for many businesses. Not knowing the ins and outs can be a major stumbling block to getting the right test and, crucially, could have a big impact on your business security.**

**This Security First white paper will help businesses understand all aspects of penetration testing services, from planning and managing through to getting real value and benefit from the results. This whitepaper is not a guide for practitioners, but instead is aimed at people who need to procure, plan, and manage the lifecycle of a penetration testing project.**

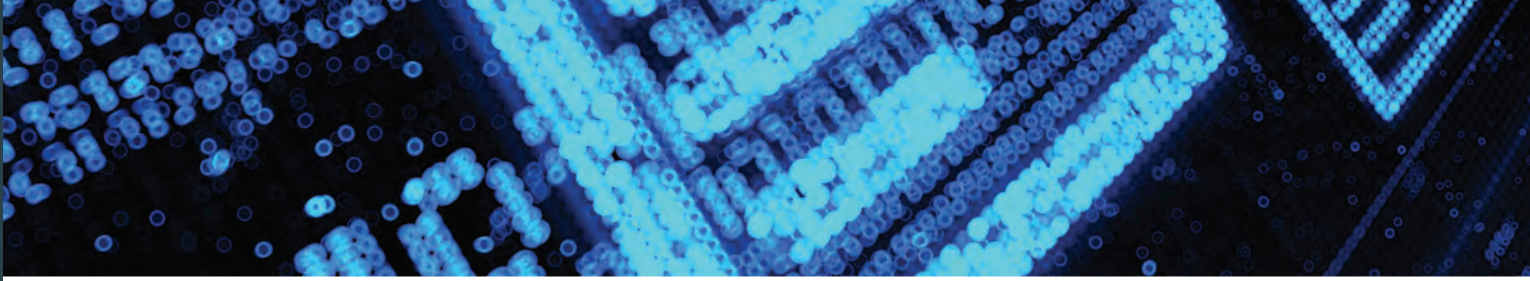
## SO WHAT IS IT?

Penetration testing can be thought of as ethical hacking, sometimes termed white-hat hacking. It's a controlled technical exercise that aims to methodically test the security of your IT infrastructure and your employees, using all the tips and tricks available to real-world hackers. Unlike a malicious hack, penetration testing is performed by an expert company against a pre-defined scope at an arranged time.

As a technical exercise, it involves an active and passive analysis of IT infrastructures and applications as well as testing human elements (social engineering). Penetration tests should be considered a fundamental component of your risk management programme.

The aim of penetration testing is twofold: firstly, to identify and exploit shortcomings in the confidentiality, integrity and availability of information. Secondly, it should provide remediation advice and offer guidance on how to reduce the impact of the identified shortcomings being exploited.

> *"Penetration tests should be considered a fundamental component of your risk management programme."*



# WHY DO IT?

### Stay a step ahead of the hackers

Testing your current security posture provides a clear indication on where you stand against an ever-changing threat landscape. It's how you can efficiently identify and address vulnerabilities before an attacker does.

### Take control of your infrastructure

As technology evolves and your business grows, technical infrastructures become increasingly complex. It's not uncommon for things to slip out of your control, or you might not have the relevant expertise to ensure that your controls are implemented the right way. Each test reveals the flow of your environment and any interdependencies that have a direct or indirect impact to security. Don't forget that you're only as secure as your weakest link.

### Prove your security

You might think you have a very secure infrastructure in place, with all the processes, procedures and staff training to back it up. But how do you know? A penetration test is an ideal way to test your security implementations, giving you real-world proof that your security controls are up to standard and working as expected. This can be as much for the benefit of your customers' and suppliers' peace of mind as your own.

### Solid risk management

Each penetration test addresses your business risks and the impact to confidentiality, integrity and availability of your data. This provides a good indication to management and the technical teams on how to best prioritise, plan, budget and remediate the risks in a structured manner.

### Because you have to

There are increasing numbers of legal and regulatory requirements, industry standards, and best practices that all say you should or must have regular penetration tests. These include PCI DSS, ISO 27001, FCA, HMG and CoCo among numerous others. Though compliance does not guarantee security, these standards provide good directions on what is needed to ensure your infrastructure is in a good overall state of security.

### Protect your business

It goes without saying that security breaches are bad news, with potentially enormous impacts on your brand's reputation and the financial repercussions. Penetration tests drastically reduce the risk of a breach, protecting the time and money invested in your organisation as well as the confidence of existing and potential customers.

# GETTING IT RIGHT

By now you've learnt what penetration tests are and why they're so vital to every type of business. Before we get into the more detailed analysis of the anatomy of penetration testing, there are considerations and limitations to bear in mind.

## CONSIDERATIONS

1. **Think about the scope**
   Getting the scope right is paramount. A test that's mis-scoped will be of limited use, or even no use at all, and all the time and effort will have been wasted.

2. **Keep your objectives in mind**
   Not understanding your requirements can often lead to unrealistic test conditions.

3. **Set appropriate budgets**
   The scale and complexity of the systems and applications in scope will be impacted by your budgetary constraints. Make sure you've set a budget that enables you to test all that you need to.

4. **Get the right type of test**
   There are lots of different types of penetration tests, and getting the right one is vital. We'll go into the detail of different test varieties later in this white paper.

5. **Trust your testers**
   Not getting the right people to do the job could lead to a ruined test, or worse, ruined systems. Check out the company beforehand so you're happy they have the right knowledge and skill sets.

6. **Be prepared**
   Depending on the type of tests, there might be high resource consumption, longer latency and a lot of alerts triggered. You need to be ready for all of these, so make sure you've chosen appropriate targets, time and types of tests.

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.

> *“Be wary of tests that focus only on the technical infrastructure, as the human element can be just as important.”*

## LIMITATIONS

### Penetration testing is not a magic solution

No penetration test could ever provide a guarantee that you’re 100% secure, as new vulnerabilities, techniques and technologies are disclosed or discovered every single day. What a penetration test does provide, however, is proof that you’ve made your systems as secure as you can. By doing so, the chances of an attack being successful are drastically reduced.

### Tests are time-limited

A penetration test addresses the security posture of your environment as only a snapshot in time. That’s why most security standards mandate that tests must be repeated regularly, typically every 6 months or a year.

### What’s the scope?

Always remember that you’re only testing items that are in your scope. Penetration tests by their nature are limited to pre-agreed limitations. Of course, you could engage a penetration testing company and say “hack everything”, but it’s likely to waste a great deal of time and money. Correctly concentrating on a scope that’s wide and deep enough is a much better option.

### Human components

Be wary of tests that focus only on the technical infrastructure, as the human element can be just as important. Attacks that target the soft, fleshy part of your security system are increasing in complexity, maturity and success. An element of social engineering should ideally always be included, so you know how well your people protect your business.

# BOX CLEVER

Penetration testing comes in three main approaches: black box, white box, and grey box. You'll often hear them described in such ways, so it's important to understand the difference.

**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'?

> *"When it comes to security, is there ever really such a thing as 'too much'?"*

# HOW TO POSITION THE PENETRATION TESTS

Penetration tests need to be positioned and executed externally, internally or from both angles. The target is the same: the difference is from where the attack will originate.

**External**
External-based penetration testing simulates the ability of an attacker to gain access from external resources to the internal network or to retrieve sensitive data from public-facing resources, such as web applications or email servers.

**Internal**
Internal-based penetration testing simulates an attack that has already bypassed the security perimeter. This addresses what an attacker (or an insider) can see and what they can do internally, such as moving from one network to another, intercepting internal communications, and so on.

# TEST TYPES

There are different types of penetration tests, each designed to target and test different aspects of your security process. The following types of tests are the most common, and will generally suit all organisations.

It should be noted that the description of tests vary, with each company using different terminology. We recommend you get a full service description to avoid getting misled, and not to focus entirely on the name given to each test.

1. **"Infrastructure" or "Network" penetration testing**
   This type of test is assessing an infrastructure or a network for its current operational security levels, such as running services, current patch levels, improper configurations, flaws in design and effectiveness of security controls. The goal is to identify and exploit any associated vulnerabilities.

2. **Application penetration testing**
   Here the functionality, process flow and security controls of applications are tested from an unauthenticated and/or authenticated perspective. These tests specifically address access control, session/configuration management, error handling, data protection and input. Application testing is for when you would like a second pair of eyes on your application to review how different parts interact – interactions that could create direct or indirect security issues.

3. **Configuration/build review testing**
   This type of test aims to review the current setup of different system components. It's a non-invasive testing approach, designed to audit the configuration from a hardening and best-practice standpoint. It helps ensure current and future infrastructure is deployed in-line with industry best practices, thus reducing the probability of tampering and exploitation.

4. **Social engineering**
   Social engineering covers the human element of security, where testers will try to access sensitive information by manipulating human psychology. This usually involves a lot of techniques, such as targeting employees over the internet with phishing emails, phone calls, as well as exploiting pitfalls in operational procedures and trying to compromise physical security.

5. **Wireless penetration testing**
   This type of testing involves identification of weaknesses in wireless architectures by analysing and inspecting packets, access points, rogue devices, encryption features and patching levels.

# ANATOMY OF A PENETRATION TEST

Most penetration testing companies should follow a similar methodology when executing penetration tests. This typically involves a 7-step lifecycle, outlined 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.

> *"A good penetration testing company should provide you with a thorough yet easy-to-read report."*

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**
   All information mentioned in the above steps must be documented. A good penetration testing company should provide you with a thorough yet easy-to-read report, including:

   - All risks based on the current server/application setup/configuration
   - Vulnerabilities and running services for the servers and applications
   - What has been done to exploit each security issue
   - Remediation steps
   - Near-term and long-term actions

   It should be noted that vulnerabilities that cannot be exploited must also be included in the final report. We strongly recommend you ask the penetration test company for a sample report in advance – this way you'll know what you can expect to receive. If a report is full of jargon and difficult to decipher, its use to you is limited.

7. **De-brief session**
   This step isn't a strict requirement but is good practice. Upon the completion and delivery of a penetration test, a de-brief session can explain the findings and risks listed in the report, as well as giving you the opportunity to ask any questions.

# HOW TO PLAN AND MANAGE A PENETRATION TEST

If you're unsure of what needs to be included in the scope, ask your penetration testing company. They should be able to provide advice and guidance throughout the whole scoping process.

1. Determine your business requirements and set objectives that need to be met.
2. Determine the approach and types of penetration tests you require. This will include any limitations/restrictions, as well as any specific test scenarios you might need.
3. Identify the critical components that will eventually form the scope. If you are unsure on what needs to be included in scope, the penetration testing company can provide assistance in the whole scoping process.
4. Assess the risks of testing these systems. If you can't afford any impact to a mission-critical live system, there are other ways, such as mirroring the target scope in a replica system.
5. Determine a timeframe for the tests to be executed, including your preference on time – do you want it to be in office hours or out of office hours?
6. Allocate a budget for such tests. Penetration tests do not have to be expensive if they are exercised throughout the year and on occasions of major infrastructure changes.
7. Liaise with your company contact at the end of each day to get progress of the tests.
8. Ensure you get a report that's easy to read and which also outlines all the risks, ranked and prioritised.
9. Set a mitigation plan with the relevant teams and decide your next course of action after a de-briefing with your testers.
10. Re-test if necessary to ensure that all shortcomings have been remediated.

> *"If you can't afford any impact to a mission-critical live system, there are other ways, such as mirroring the target scope in a replica system."*

# WHAT DO I NEED TO DO?

For a test to be conducted smoothly and properly, there are few things that you must do.

Get a signed NDA to ensure confidentiality.

Ensure all relevant people within your organisation are aware of the penetration tests.

Proactively back up all critical data from systems that will form part of the penetration tests, as they may be affected during the testing.

Provide any resources needed – such as VPN access, IP white-listing etc., prior to the commencement of any penetration tests to ensure no delays during the provision of the tests.

Immediately let your penetration testing company know if you experience a fault, some interference, or any other issues during the test.

# PENETRATION TESTING MYTHS

There are a lot of myths and half-truths when it comes to penetration tests, some of which are repeated by seemingly reputable sources. So here's our attempt to end the confusion once and for all.

## Penetration testing isn't appealing to small businesses

No matter what the size of your company, penetration tests are there to make sure you've done all you can to not go out of business. A cybercriminal doesn't care how big or small your organisation is: an easy target is an easy target.

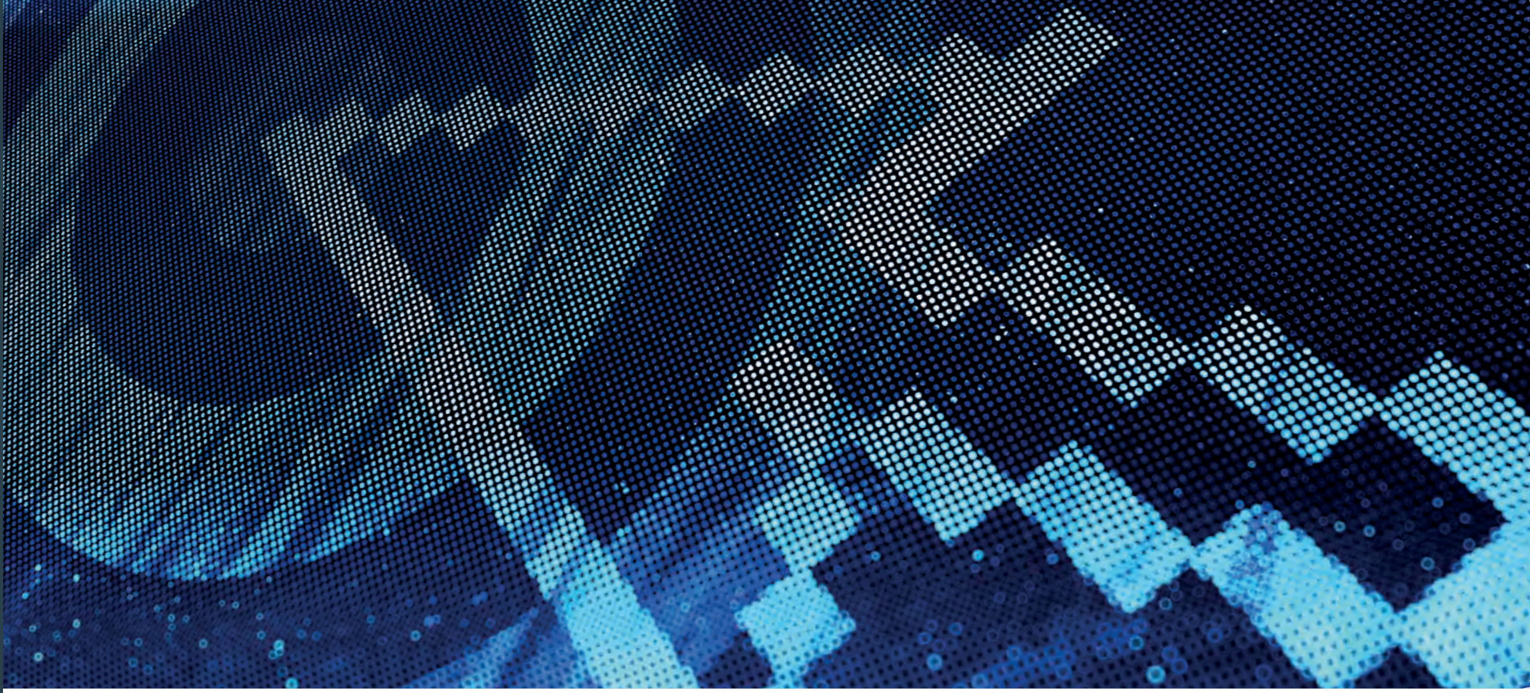
## It's only for Government or financial institutions

Security is an integral component of your business no matter what industry you operate in. It's vital to ensure the continuity of your business operations and, crucially, to avoid the immense reputational and financial losses that come with a breach.

## They're the same as vulnerability assessments

Organisations often confuse penetration testing with vulnerability assessments. Vulnerability assessments rely on automated tools with pre-defined signatures that check for known security issues and patching levels, without validating if the vulnerability is exploitable. It's also important to bear in mind that these automated scanning tools do not pick up vulnerabilities that aren't in their database.

Penetration testing on the other hand uses both manual and automatic techniques to validate each weakness by trying to exploit it and prove what the impact will be. These tests do not rely on the tools but on the creativity, ingenuity and knowledge of the tester to put together all the puzzle pieces to achieve your pre-defined objectives.



# SUMMARY

Penetration testing offers the opportunity to validate your current security posture and to protect your business. By selecting the right scope and the right type of test, you can easily identify and remediate your security vulnerabilities. Finding a penetration testing company you trust, with the right people to do the job well, is a fundamental aspect of the whole process.

The company should help you through each and every stage of the process, until the flaws are remediated and your risk is minimised.

Far from being a standalone procedure, penetration tests need to be an integral part of your overall risk management program. And always remember that true security is a holistic, overall approach that goes far beyond technical measures. Good security should be a culture within your company, based on a cycle of continuous improvement.

> *"A cybercriminal doesn't care how big or small your organisation is: an easy target is an easy target."*

**Get in touch today to ensure that your business and your customers are protected:**

**+44 (0)1438 532 900** **www.bulletproof.co.uk** **contact@bulletproof.co.uk**

BULLET PROOF

✉ contact@bulletproof.co.uk ☎ +44 (0)1438 532 900 🌐 www.bulletproof.co.uk

BULLET PROOF is the dedicated cyber security arm of SERVERCHOICE