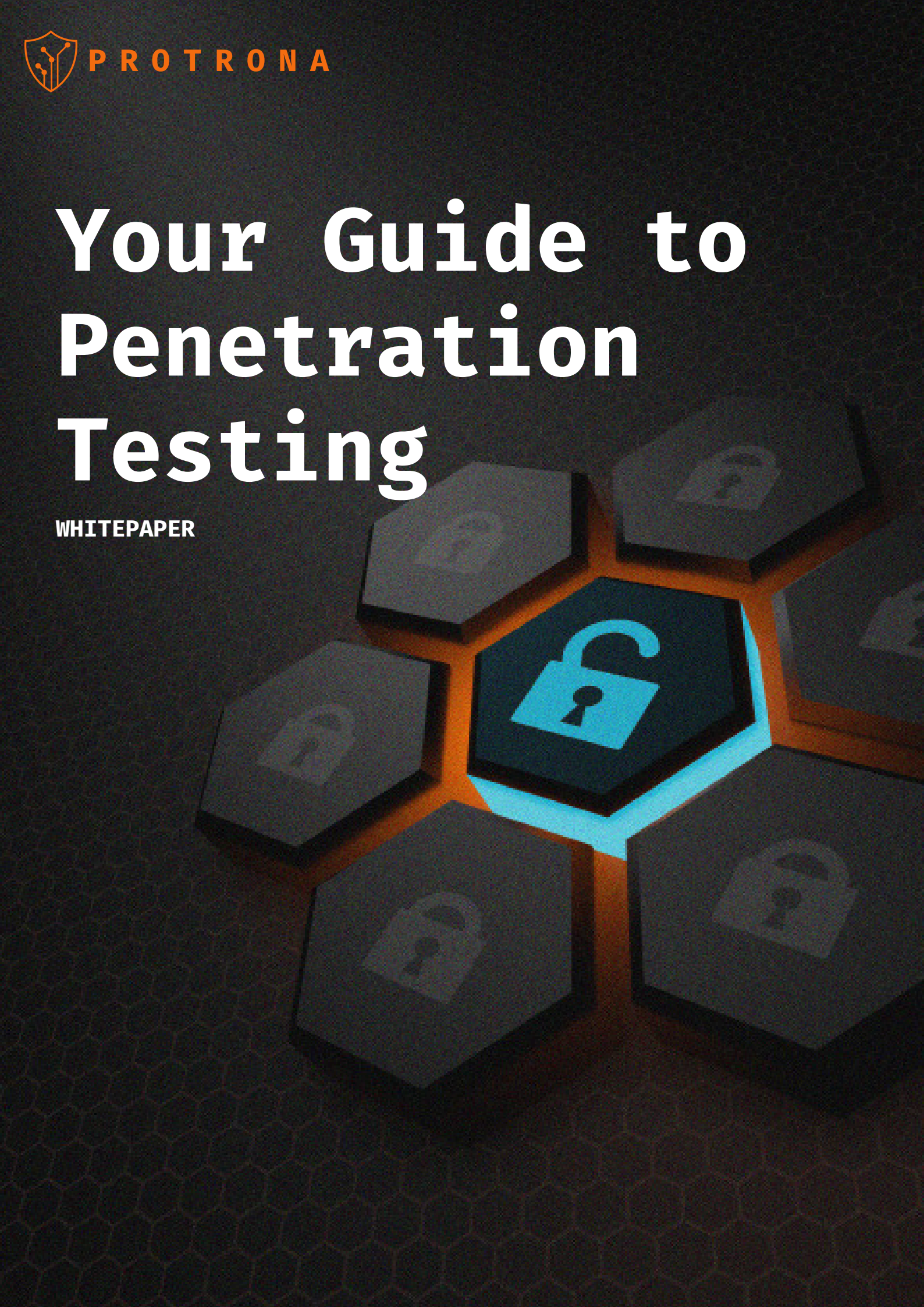
PROTRONA

Your Guide to Penetration Testing

WHITEPAPER



INTRODUCTION

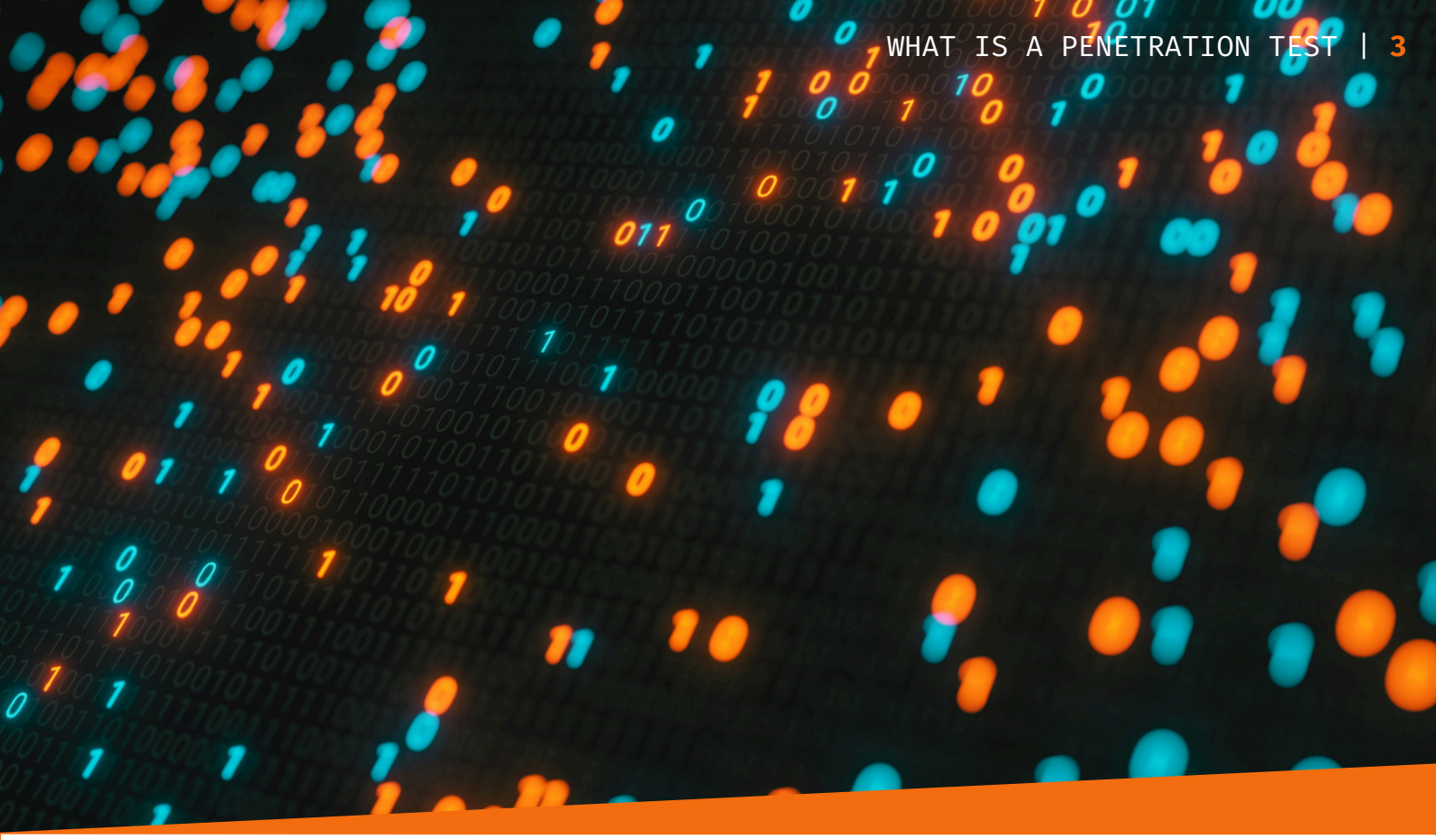
Penetration Testing, or Pen Tests, is a key part of a business's Cybersecurity. As most of us are aware, cybersecurity encompasses multiple processes to ensure that your business and clients are safe. Penetration Testing can be a confusing subject for any business. Knowing the ins and outs of the types of Pen Tests can be a major stumbling block to getting the right type of test and could have a costly impact to your business security.

This Protrona whitepaper will help you understand all aspects of a Penetration Testing service, from industry compliance and steps that can be taken before a Pen Test to the types and stages of the process. Each section will educate the reader on the benefits of the service, not just for the business but also for the end-users and clients.

This whitepaper is for those who know that Penetration Tests are a key component of Cybersecurity but want further information on where to start and what is expected.

If you would rather talk to an expert about any questions you may have after reading this, please get in touch.

Table of Contents



WHAT IS A PENETRATION TEST?

A Penetration Test is an authorised attempt to gain unauthorised access to a computer system, application or data. It is often referred to as a 'Pen Test' or 'ethical hacking'. This involves imitating strategies that hackers often use in order to identify where a system may be vulnerable. This will give organisations an opportunity to address these vulnerabilities before a malicious hacker.

CYBER SECURITY TODAY

Cyber-crime is impacting businesses and users across the globe. In 93% of cases, an external attacker can breach an organisation's network perimeter and gain access to local network resources1. In 2022 39% of businesses identified a cyber-attack, yet only 19% of businesses have a formal incident response plan2.

In a 2022 report, it was found that cyber-attacks on companies often resulted in disruption of core business and leakage of confidential information. As a result of this, 69% of individuals were victims of confidential information leakage and therefore resulted in suffering

Data breaches have increasingly become a huge concern, leading the General Data Protection Regulation (GDPR) to issue a number of fines since the regulation was first introduced in 20184.

Cybersecurity is vital for businesses' survival. When an organisation doesn't have a cyber security strategy, it fails to defend itself from cyber threats, therefore leaving itself and its users vulnerable to malicious attackers. Pen Testing is a strategy that assesses and reduces your corporate cyber security risk, whilst also ensuring compliance.

INDUSTRY COMPLIANCE

GDPR (General Data Protection Regulation)

GDPR is a regulation that will impact almost every organisation that operates both in the UK and globally. GDPR covers all aspects of data protection, if you as a business handle a user's personal data than you are responsible to keep that data safe and secure.

Within the regulations, Article 32 requires UK businesses to implement 'A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data processing'.

The Information Commissioner's Office (ICO) recommends that you conduct GDPR Penetration Testing and Vulnerability scanning on a regular basis, and crucially, ensure they address any risks identified.

At Protrona we recommend a Web Application Penetration Test to be done annually to ensure there are no gaps for cyber criminals to breach.

ISO 27001 (International Organisation for Standardisation)

ISO 27001 is an international information security standard that outlines a framework of controls for Information Security Management Systems (ISMS). To become certified, a business must build a personalised suite of security controls to identify and address security risks across their networks and ensure they meet changing security needs over time.

Here at Protrona we are ISO 27001, 45001, 9001 and 14001 certified and experts in ensuring your systems are safe.

PCI DSS

If you are an organisation that accepts or processes online card payments than you are required to undertake annual PCI security audits to ensure security compliance.

PCI DSS 3.2, Requirement 11 specifically mandates the performance of regular Penetration Testing. Organisations that fall within the scope of PCI DSS must perform internal and external Penetration Testing at least annually, or after any significant changes to infrastructure.

If you are unsure if the e-commerce platform you use is already compliant (Shopify is PCI DSS Level 1) contact us and we can investigate if your business needs to take action to comply.

STEPS TO TAKE BEFORE A PENETRATION TEST

Before committing to a full Penetration Test with your security partner, there are several steps and tests you can take to scope out potential vulnerabilities in your corporate systems.

Firstly, address any issues that could allow for individual attacks on users and internal weaknesses. It's important to focus on corporate log ins and credentials - verify that usernames and passwords are encrypted and transferred via secure connections (such as https).

Further verify that no usernames or passwords are hardcoded in the system, also checking that sensitive credentials are not stored within your documents or systems.

To prevent individual email attacks, ensure email best practice is being followed. It's essential to verify that incoming and outgoing email traffic is filtered, and inbuilt spam filters are configured, blocking any unsolicited emails.

Additionally, run checks on admin and authorisation security. Critical resources within your corporate environment should only be available to authorised persons and services; all access logs should be maintained with proper access permissions.

STEPS TO TAKE BEFORE A PENETRATION TEST CONT.

To prevent more generalised threats, run a full check of your web applications and servers; ensure your web application can identify spam attacks on contact forms used on your website.

Also check if network traffic is monitored by proxy appliances, as proxy servers make it difficult for hackers to gain internal details of the network, protecting from external attacks. Establish whether your network is protected by firewalls - which can be software or hardware that blocks unauthorised access to your systems.

You should also run checks to ensure specific attack types are prevented; spoofing, cross-site scripting, brute force attacks and denial-of-service (DOS) are common attack types to monitor.

Whilst these actions can help secure your business' data, thorough and complete assessment by a cybersecurity professional is always advisable. Your security partner can run a myriad of tests to gain complete insight into your system weaknesses, providing industry standard reports and action plans.

Penetration Tests are essential for businesses of all sizes; no business is too small to be attacked by cyber-criminals. In order to protect yourself from a data breach, regularly testing your systems and network will enable you to identify potential weaknesses and rectify them immediately. For this reason, there are now regulatory requirements for businesses of all statures to undergo Penetration Testing.

WHAT SIZE OF BUSINESS NEEDS A PEN TEST?

IN 2022 MEDIUM SIZED ENTERPRISES ON AVERAGE LOST **£19,400** PER CYBER-ATTACK WHILE SMALL ENTERPRISES LOST AN AVERAGE OF **£4,200.**

Pen Tests aren't only a preventative measure, they also protect your business from the costs associated with security incidents, therefore making them an integral safeguarding measure for businesses of all sizes.

BENEFITS OF A PENETRATION TEST

There are a number of tangible benefits for your business when conducting Penetration Tests. First and foremost, regular Penetration Testing is essential in the maintenance of secure IT infrastructure as regular assessment enables your cybersecurity consultant to highlight and remediate any exploitable weaknesses. However, there are several more top benefits to testing.

1 Identify, Prioritise and Remedy Vulnerablilties

The primary concern of a Penetration Test is to expose external and internal vulnerabilities that would have gone otherwise unnoticed. In identifying risks, your business is then able to prioritise, rectify, and remediate such weaknesses to keep out hackers and threat actors.

2 Attain Regulatory Compliance

Penetration Testing can help your business gain compliance and certification with certain industry regulators - such as the PCI and ISO 27001 certifications. Regular Penetration Testing displays due diligence and adequate security policy, necessary to several certifiers. Complete Pen Test records also protect businesses from non-compliance issues.

3 Protect Clients, Partners and Business Reputation

Any flaws in your cyber infrastructure can put clients, partners, and business data at risk. In rooting out potential vulnerabilities, business trust is protected and your enterprise is safe from the ramifications of a data breach.

4 Cut Security Costs

Hacks and data breaches can have costly ramifications for businesses; data loss, legal fees, loss of clients and resulting damage in trust can add up. On average, medium sized enterprises in the UK lose £19,4005 per cyber-attack, a significant cost that can be avoided with regular Penetration Testing, and strict implementation and adherence to resulting cybersecurity policy.

TYPES OF PENETRATION TESTS

Before conducting a Penetration Test within your organisation, it's essential to understand the different types of test available.

Your MSP or MSSP partner will be able to offer you three types of test; White Box Penetration Testing; Black Box Penetration Testing; and Grey Box Penetration Testing. These tests are defined by the level of information provided to the assessor before and during the test. To accurately gauge the exploitable vulnerabilities present within your IT infrastructure, it's important to select the most suitable type.

Black Box

The tester is provided with the bare minimum information on the company they will be attempting to exploit. Aside from the name of the enterprise, the tester will have no prior knowledge and zero access to the target. The assessor carries out significant reconnaissance to discover internal network information and prepare an attack strategy based on the identified assets' properties.

This test type is best suited to a mature environment in which there are already strong identification and recovery processes in place. Whilst this is the least detailed and thorough of the test types, it most closely simulates the perspective of an unauthorised outside attacker.

Grey Box

A grey box Penetration Test represents the intermediate level of information provision; the assessor is provided with some information and access to the targeted organisation. For example, the tester may be given access to information such as specific hosts or networks to target.

Grey box testing reduces the reconnaissance phase, allowing the tester to exploit the target's vulnerabilities more rapidly. This form of Pen Test is particularly useful for uncovering issues such as cross-site scripting, SQL Injection, and broken authentication.

White Box

Here the assessor is provided with the highest level of information and access to the target. They will be given access to internal documentation, configuration plans, and user access - acting much in the way of an internal security team.

This form of test offers the most detailed and insightful exploration of the target's systems; internal and external vulnerabilities are comprehensively exploited, providing a detailed response plan. This is the fastest of the Pen Tests, with the reconnaissance phase being significantly reduced.

STAGES OF A PENETRATION TEST

There are five stages that are involved in a Pen Test. It includes Planning and Reconnaissance, Scanning, Gaining Access and/or Exploitation, Maintaining Access and lastly, Analysis and Reporting.

1 **Planning and Reconnaissance**
During this stage the team will define the scope of the task and decide what to prioritise. They'll also examine potential network entry points.

2 **Scanning**
Once planning and reconnaissance is complete, the ethical hackers will gain an understanding of how the system responds to various automated intrusion attempts and attacks. Here the ethical hackers will be able to identify its vulnerabilities.

3 **Gaining Access and/or Exploitation**
In this phase of the Pen Test, the ethical hackers will use the information they've learnt during the previous stage to gain access to the system and its sensitive data.

4 **Maintaining Access**
After gaining access, this stage seeks to confirm whether persistent access to the system can be maintained. The aim is to establish whether advanced threats can remain in a system undetected.

5 **Analysis and Reporting**
Provides a report with an analysis on the systems vulnerabilities and how to immediately combat them to improve the security posture.

WHAT OUR CLIENTS RECEIVE

At Protrona, we offer our clients a comprehensive Penetration Testing service, designed to identify and eradicate all potential weaknesses in their corporate systems. Our expert Cybersecurity Team provide an all-encompassing service to clients, utilising their extensive security experience to deliver outstanding results.

The Types of Penetration Test Provided by Protrona

Infrastructure Testing

This involves testing of core server operating systems in order to understand which systems can be exploited.

Application Testing

This is a test of web applications against the OWASP framework to ensure web applications are secured against critical vulnerabilities.

Database Testing
This is a test of database platforms to ensure that business critical databases that store privileged and sensitive data are secured correctly

System Builds/Review
This is a review of desktop/server operating system against a well known base standard such as CIS to ensure there is no configuration drift.

Cloud Platform Testing
This is a test of cloud security controls to ensure that cloud platforms are securely built and controls are operating correctly.

Wireless Testing
This is a test of wireless networks to ensure they are securely built and segmented.

Network Testing
This involves testing of network controls and network segregation across the entire system.

Adaptable to your business needs.

WHAT OUR CLIENTS RECEIVE CONT.

Included in this service is a full penetration test report outlining critical vulnerabilities, exploitable and non-exploitable weaknesses, risks mapped to each finding, a technical explanation of each finding and its impact, as well as a remediation summary.

This report is delivered in a digestible PDF format, which can be retained for future reference and auditing.

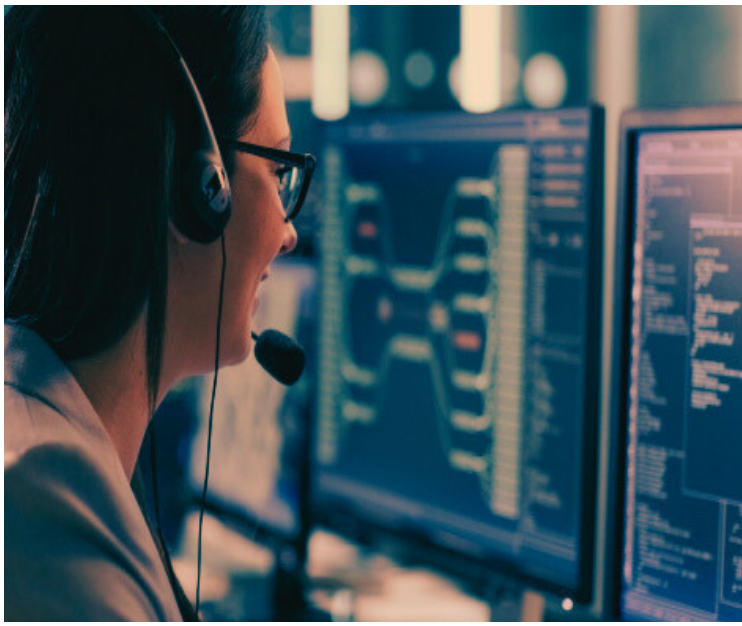
Our cybersecurity partnership doesn't end with the Penetration Test findings, as we continue to provide our clients with the support and services needed to move forward with impenetrable cybersecurity.

SUMMARY

Penetration Testing is an excellent opportunity to certify your current cybersecurity defences and protect your business and its users. By selecting the right type of test, you can easily identify and remediate your cyber weakness, lower the chance of threats from malicious attackers.

Protrona's Security Team is a team you can trust, partnering you with the right people to do the job well, which is a fundamental aspect of the whole process.

As an award-winning MSP, The Protrona Team guides you through each and every stage of the process, until the flaws are remediated and your risk from cyber threat is minimised.



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

www.protrona.com

P R O T R O N A

www.protrona.com
020 3727 6020

REFERENCES
[1] Business in the crosshairs: analyzing attack scenarios (ptsecurity.com)
[2] Comprehensive Penetration Testing | https://Protronaroviait.com/services/penetration-testing
[3] Cybersecurity threatscape: Q2 2022 (ptsecurity.com)
[4] DLA Piper GDPR fines and data breach survey: January 2022 | Novedades | DLA Piper Global Law Firm
[5] Cybersecurity Breaches Survey 2022, UK Government, 2022. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022