ENABLING YOU TO DO MORE

Service Handbook

Penetration Testing

Document Owner

All enquiries regarding the content of this document should in the first instance be directed to:

Product Team	Phone:	0330 332 7933
Intercity Technology Limited	Email:	product@intercity.technology
101-114 Holloway Head		
Birmingham		
B1 1QP		

Document Control

The creation, review and issue of this document follow:

Issue	Author	Date	Classification	Amendments
1.0	NW	01/04/2022	Controlled	

Contents

Glossary

APT	Advanced Persistent Threat
DNS	Domain Name System
IPv6	Internet Protocol version 6
OS	Operating System
OSINT	Open Source Intelligence
SQL	Structured Query Language
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
VPN	Virtual Private Network

1. Introduction

1.1 Penetration Testing

A Pen Test comprises a consultant looking to exploit security weaknesses with the infrastructure and application layers. They then report back on those weaknesses so that the client can act. Infrastructure tests can be conducted remotely (external assessment) or on-site (internal assessment). The scope of testing includes, for example, servers, Wi-Fi access points, computers and firewalls. A typical test would be to determine whether credit card data is secure. Application tests are conducted remotely. The scope of testing includes, for example, websites, mobile apps and customer applications. It also looks at public endpoints and API connections. A typical test would be to examine how a secondary app would interface with a social media site.

In both cases – infrastructure and application pen testing – the scope of the testing is captured in a scoping form. We can do this together with you on a call or send it to you to complete yourself and return to us. On completion of the testing and analysis by a security consultant, the findings are published on a secure portal for you to review and determine what action to take.

1.2 Red Team Assessment

This is a way to simulate an Advanced Persistent Threat (APT) against your organisation. APTs are attacks typically conducted by organised groups. They comprise organised, stealthy activities, intended to steal assets which are of financial, security and strategic economic importance. APTs use tactics such as misinformation, social engineering and sophisticated hacking techniques over a sustained period, sometimes culminating in attacks on assets such as offices and IT environments.

Red Team Assessments span multiple attack vectors, aiming to simulate a realistic attack by an APT group. This includes covertly attacking an organisation's external and internal networks, applications, people and physical security controls. Assessments are carried out with the agreement of only the essential stakeholders, providing a true test of an organisation's security posture, exposing vulnerabilities and enabling remediation.

1.3 Dark Web Monitoring

The dark web comprises World Wide Web content which exists on darknets - covert networks on the internet, accessible using specific software, configurations or authorisation. It enables computers to communicate and conduct business anonymously, without divulging identifying information, such as a user's location. Whilst the dark web has many legitimate uses, it has also become a place where cybercriminals trade stolen data records such as user credentials, personal information and payment card details.

Dark Web Monitoring is an always-on service which scans the dark web (as well as the regular web) on your behalf. It searches for any mention of your organisation's brand, domain name or specific data assets. This offers you peace of mind that your assets are safe and not being traded. However, if any issues arise, the service generates alerts, enabling you to take remedial action against any compromised assets.

1.4 An Introduction to our Technology Partner – Pentest People

Pentest People is a specialist Penetration Testing as a Service (PTaaS) supplier. Founded in 2017 and based in Leeds, the company has *c.*60 employees, including 50 testers. It sells PTaaS only, so provides an agnostic approach to security. Pentest People is CHECK registered and CREST approved. Its key staff and testers have worked together for over 10 years, developing innovative

technology and techniques. The key deliverables from Pentest People are the assessment reports, which are provided via its SecurePortal. The portal also provides a secure location for dialogue with clients about their assessments, remediation and retests. Case studies of the company's work are available on request.

2. Scope

2.1 External Infrastructure Assessment

2.1.1 Overview

A business' external infrastructure is typically a first port of call for attackers, potentially presenting a significant attack surface which can be examined and exploited with little risk of identification. The compromise of services providing remote access to corporate resources (such as VPNs and email portals) could result in the disclosure of highly-sensitive information or even provide a foothold from which to attack other internal resources.

Pentest People's External Infrastructure Assessment service aims to identify software and configuration vulnerabilities which exist on your public-facing infrastructure. The testing is performed typically from Pentest People's office and data centre locations.

2.1.2 Methodology

External infrastructures vary in size, complexity, technologies and in approaches to configuration, so Pentest People's exact technical approach to each infrastructure may be very different. However, there are certain fundamental areas which are examined, as set out in Table 2-1 below.

Category	Description
Open-source intelligence (OSINT)	The External Infrastructure Assessment has a strong focus on publicly-available information which could be leveraged in targeted attacks. Information such as DNS records, document metadata, email addresses and social media posts is gathered and used to identify and attack vulnerable external-facing services.
Service discovery and fuzzing	The live public-facing services are systematically probed and closely examined until their purpose is confirmed and any associated vulnerabilities identified. The consultant works with your nominated subject matter expert(s) until the full attack surface is confirmed.
Automated vulnerability scanning	This is performed using one or more scanning engines to identify 'low-hanging fruit' issues and providing the foundational security information on which a full manual penetration test is performed.
Web server configuration	As the most common services are public facing, the assessment focuses on the configuration of the web servers. Any configuration issues with SSL and TLS are highlighted, along with common version information disclosures, encryption levels and token-based access.
Password attacks	Targeted word-list attacks are performed against all public-facing services with authentication controls (infrastructure and web-based) where safe to do so. The attacks use default and common credentials, as well as any usernames or custom password lists created during the OSINT gathering stage.

Table 2-1 – External Infrastructure Assessment Methodology

2.2 Internal Infrastructure Assessment

2.2.1 Overview

Establishing a security baseline by assessing the internal infrastructure is commonplace in many organisations. Whether the drivers are from industry compliance or from security-focused company leaders, the benefits of risk mitigation are widely understood and accepted. Pentest People's Infrastructure Assessment service aims to identify software and configuration vulnerabilities which exist on the internal network and systems. The assessment also simulates what is achievable should an endpoint be compromised, for example by a phishing attack or malware infection. The testing is performed typically at your office or data centre, with the consultant patched directly into the infrastructure.

2.2.2 Methodology

Internal infrastructures vary in size, complexity, technologies and in approaches to configuration, so Pentest People's exact technical approach to each infrastructure may be very different. However, there are certain fundamental areas which are examined, as set out in below.

Category	Description
Service discovery and traffic analysis	One of the initial stages of any internal assessment is to identify live services on the target hosts through automated port scanning. The remote operating system is fingerprinted and service versions identified. This stage typically identifies high-value services likely to provide access to sensitive information. The visible network traffic is collected and analysed using packet capture tools. The aim of this test is to identify issues such as clear-text credentials, unauthenticated routing information and default IPv6 configurations. Traffic analysis can also be used to partially map out network resources and identify security issues with traffic flow.
Automated vulnerability scanning	This is performed using one or more scanning engines to identify 'low-hanging fruit' issues and provide the foundational security information on which a full manual penetration test is performed.
Network infrastructure configuration	The network infrastructure is examined using topology diagrams, the results of port and vulnerability scans and through discussions with your nominated subject matter expert(s). Issues such as insecure network management protocols, overly permissive firewall rules and lack of segmentation are highlighted at this stage.
Windows domain security configuration	The configuration of the Microsoft Windows domain (if applicable) is assessed, identifying issues such as (but not limited to): insecure trust relationships; exploitable vulnerabilities in the assigned user privileges; outdated password hashing algorithms; insecure use of Group Policy Preferences; susceptibility to token impersonation; patch management status and known vulnerabilities for older OS versions.
Password management	Where possible, a full password audit of all Windows domain users is performed, providing a statistical breakdown of configured passwords. This information provides a valuable insight into the effectiveness of user awareness training and the current password-related technical controls.
Database security configuration	The security controls surrounding your most sensitive and business-critical data are subjected to thorough testing. This typically involves an

Category	Description
	assessment of database security configuration and current access rights to sensitive data.

Table 2-2 – Internal Infrastructure Assessment Methodology

2.3 Web Application Assessment

2.3.1 Overview

The web technologies and applications we use daily have advanced in recent years. This advancement and our reliance upon such services has exposed users to a variety of new security risks. Their complexity and availability have made them an ideal target for attackers, evidenced by the many publicised major data breaches. Protecting web applications from new threats is a constant challenge, especially for developers who may not be security aware and who are working typically toward a performance deadline. Pentest People has a professional Web Application Assessment service which can be used to identify vulnerabilities which exist on your web applications and has a wealth of knowledge in the area of application security testing. Its testers have created and contributed to many open source web application security projects.

2.3.2 Methodology

Web applications can use a variety of techniques and development frameworks, so Pentest People's exact technical approach to each application may be very different. Pentest People consultants follow the Open Web Application Security Project web application testing methodology as closely as possible. At a minimum they examine the fundamental areas as set out in Table 2-3 below.

Category	Description
Public information	Publicly available information on the target company and application(s) is gathered and inspected. This information may include DNS records, email addresses, document metadata, website content and social media posts.
Authentication	Any authentication controls such as login portals are tested in detail, identifying any vulnerabilities that could be exploited to bypass the control, enumerate information such as valid users or exploit weaknesses such as lack of anti-automation.
Authorisation	The application's pages and functionality are mapped from the perspective of the core user profiles (with varying privileges) identifying any discrepancies with access and highlighting potential horizontal and vertical privilege escalation issues.
Session management	The session management solution is examined in detail to identify vulnerabilities such as session fixation and hijacking, excessive timeouts, concealed sequences and flaws in the randomness of the token.
Input validation / sanitisation	All user-controllable input is tested closely to identify any instances of malicious code injection weaknesses. Common vulnerabilities such as Cross-Site Scripting and SQL Injection fall within this category.
Business logic	The functionality of the application is examined from a business logic perspective, identifying edge cases, where users perform an action or sequence not foreseen by the developers.

Category	Description
Web server configuration	The configuration of the web server is included in testing to identify any instances of version disclosure, outdated software packages, SSL configuration weaknesses and unnecessary public-facing ports.

Table 2-3 – Web Application Categories & Descriptions

2.4 Red Team Assessment

2.4.1 Overview

Red Team engagements simulate APTs to fully test the ability of your organisation's staff, technology and policies to identify and mitigate such threats. Pentest People's Red Team consultants will assess the whole attack surface of your organisation and identify areas where sensitive information and critical assets are at risk of compromise. Owing to the comprehensive methods the consultants use, Red Team engagements can detect many of the vulnerabilities that are often overlooked and inherently restricted by scopes in traditional security testing methods.

Cyber criminals and state-sponsored actors will use any method to exploit any and all vulnerabilities they can to compromise your organisation's security and achieve their end goal. The Red Team consultants will apply the same tools, procedures and tactics to ensure that the APT simulation is as realistic as possible. The Red Team engagement will use a blend of attack tactics to challenge the virtual and physical defences of your organisation, including social engineering campaigns, simulated malware, ransomware attacks and physical intrusions on company sites.

2.4.2 Methodology

The consultants use the Red Team Assessment framework as set out in **Error! Reference source not found.** below.

Category	Description
Engagement	This first stage is an opportunity for you and the consultants to establish boundaries and rules of engagement for the assessment, ensuring minimal risk to the day-to-day running of your organisation. The consultants will identify current risks associated with your organisation and build goals to simulate them.
Reconnaissance	The consultants will use a number of covert tactics to gain information on your organisation that is available within the public domain. Information gathered at this stage will be used in phishing-style attacks and for obtaining access to the physical target, such as your organisation's headquarters.
Delivery	The consultants will use the information from the reconnaissance phase to gain a foothold into your networks or breach your buildings. Stand-off electronic attacks against wireless networks, electronic bypass methods and spear phishing can be used by our consultants to breach your locations.
Command & Control	Once a foothold has been established, the consultants will test the resilience of your organisation to establish its response to an APT and its capability to identify any ingress and egress of sensitive or malicious data.
Lateral Movement	Simulating the movements of a real world hacker, the consultants will use techniques often found during a penetration test to move laterally

Category	Description
	through the organisation to gain access to critical or company-sensitive data.
Post Engagement	This is an opportunity for the consultants to debrief you prior to report submission. They will offer expert tactical and strategic recommendations to help develop further your security strategy and enhance your future response to potential cyber-attacks.

Table 2-4 – Red Team Assessment Framework

2.5 Dark Web Monitoring

2.5.1 Overview

This service is designed to identify when customer data acquired through a breach is posted to locations on the regular and dark web. Unless you are performing this level of proactive monitoring, it is unlikely that you will be aware of any compromised data assets which are publicly available on various dark web data sources.

Using this service enables you to identify via the Pentest People SecurePortal any issues which arise and take action to remediate against them.

2.5.2 Methodology

Most data breaches are performed for financial gain. Cybercriminals exploit a vulnerability that results in a data breach and then extract the data. They then sell the data on the dark web, on various underground forums and to user groups where the majority of such data is advertised.

Identifying its data for sale via the regular or dark web is often the way by which an organisation finds out that a data breach has occurred. It is therefore imperative that organisations proactively scan the regular and dark webs as part of their defence-in-depth strategy for risk management.

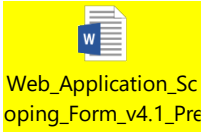
The Dark Web Monitoring service comprises multiple tools which search the regular and dark webs for data assets which belong to your organisation and are being traded between cybercriminals. Any relevant findings are highlighted on the Live Vulnerability Dashboard on your SecurePortal instance. This enables you to quickly identify any compromised data assets and take remediate actions.

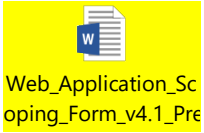
3. Presales

3.1 Pen Testing

Following agreement that you require pen testing, we complete a scoping form with you, which enables us to determine the quantity of days' worth of work required.

The templates for each type of assessment are as follows:





3.2 Red Team Assessment

Following agreement that you require a Red Team Assessment, we agree with you on the number of days required to conduct it, which is one of the following:

Size of Organisation	Planning Days	Contingency Days	Total Days
Small	5	5	10
Medium	20	5	25
Large	30	5	30
Enterprise	40	5	40

Table 3-1 – Red Team Assessment Day Requirement

3.3 Dark Web Monitoring

Following agreement that you require Dark Web Monitoring, we confirm the company name and URL which you require us to monitor.

4. Delivery

4.1 Assessments

Your assessments are carried out by Pentest People, scheduled to start and end as agreed with you. The findings are then made available for you to view on the Pentest People SecurePortal on the agreed availability date. Your ITL account manager then arranges a follow-up call with you and Pentest People to discuss the findings.

4.2 Cyber Essentials Phase One

A Cyber Essentials Phase One assessment is included with every pen test.

4.3 Free Retest

Pen test assessments typically reveal multiple vulnerabilities requiring corrective action. Our pen testing includes a free retest of the top five vulnerabilities identified.

4.4 Dark Web Monitoring

Dark Web Monitoring commences on an agreed start data and continues for an initial term of 12 months.