PentestPeople®

PSN IT Health Check (ITHC)

Client Guide

Version: 1.2

Author: Gavin Watson

Email: gavin.watson@pentestpeople.com

Tel: +44 (0) 780 540 125

Document Details

Any queries relating to this document should be addressed to the document author directly.

Basic Information

Title	PSN IT Health Check (ITHC)
Original Release	February 6th, 2019
Page Count	19
Author	Gavin Watson gavin.watson@pentestpeople.com 07804 540125

Change History

The following table lists details of document version revisions.

Version	Date	Author	Description
1.0	06/02/2019	Gavin Watson	First Release
1.1	11/02/2019	Gavin Watson	Expanded Methodology Section
1.2	16/02/2019	Gavin Watson	Minor formatting changes

1. Table of Contents

2. Introduction

2.1 Document Purpose

Pentest People offer a wide range of security assessment services, and each have unique aims and objectives, prerequisites, deliverables, and certain expectations from the perspective of both the consultant and the client themselves. To ensure that each assessment is performed as efficiently and thoroughly as possible, and to ensure that all parties understand what is required and what the final outcome should be, Pentest People have created a set of detailed guides.

These guides aim to answer the most important questions about an assessment, such as what a client should prepare before the assessment dates, and what tools the consultants are likely to be using. Whilst the content is not exhaustive, it should provide valuable information to ensure all parties understand the fundamental elements of the assessment.

2.2 Document Structure

This document contains the following nine sections:

1. **Overview**
   A high-level description of the PSN IT Health Check assessment.
2. **Prerequisites - What do I need to prepare?**
   This section covers the tasks (if any) that Pentest People recommend the client complete prior to the agreed testing days, ensuring that the testing can be performed without unnecessary delays.
3. **Methodology - What tests will the consultant(s) be performing?**
   This section covers the tools and techniques used by Pentest People's consultants during the assessment. Each step is explained in detail, including the commercial, open source and proprietary tools associated with each stage.
4. **Risks - What are the risks when performing these tests?**
   This section covers the methods used by Pentest People's consultants to mitigate the risk of network disruption and loss of business data.
5. **Presentation - Will the results of the assessment be discussed?**
   This section covers the standard policy followed by all consultants, including onsite assessment shadowing, end of test debrief sessions, and post-test presentations.
6. **Reporting - What can I expect from the assessment report?**
   This section covers the structure of the assessment report(s) delivered by SecurePortal and for bespoke reports delivered as a PDF document.
7. **Remediation - What remediation support will I receive?**
   This section covers the options available for assessment retests and onsite remediation services.
8. **Further Testing - What other services would Pentest People recommend?**
   This section covers the assessments that compliment a PSN IT Health Check, focusing on other important areas of security that are not included in the PSN requirements.
9. **Appendices**
   This section includes additional information that readers may find useful.

3. Overview

3.1 The PSN IT Health Check Assessment

The Public Services Network (PSN) is a high-performance network managed by the government, allowing public sector organisations such as councils to share resources and avoid duplication of work. The PSN uses a 'walled-garden' approach, allowing internet facing content to be shared and controlled. Users must therefore hold a valid PSN compliance certificate, proving that their organisation's security arrangements, policies, and controls are sufficiently rigorous. Therefore, the purpose of the PSN IT Health Check assessment is to identify any software or configuration vulnerabilities in the systems controlled and managed by the client, and to determine whether any such vulnerabilities could pose a threat to the Public Sector Network (PSN).

The overall assessment is a collection of individual security tests focusing on myriad systems including, servers, workstations, switches and routers, mobile device management solutions, mobile handsets, wireless infrastructure, remote access solutions, network management solutions, network based firewalls, PSN gateway authentication controls, and external public facing services.

3.2 The Requirements

The PSN IT Health Check 'requirements' included in the official documentation are not detailed. This may be by design, leaving the interpretation open to security professionals and allowing for its application to a variety of very different client solutions. Therefore, although some of the core ITHC tests are consistently performed by most security consultancies, there are likely to be differences. Additionally, the interpretation of exactly what is required can also differ significantly between PSN assessors, so an ITHC report may be accepted by one assessor, but rejected by another, and both assessors could arguably be correct.

Pentest People perform a variety of tests following an interpretation of the guidance that aims to be as thorough as possible, each test addressing a very specific requirement stated in the PSN ITHC Guidance document. The following table provides a reference for how each test addresses each PSN ITHC requirement. The Pentest People ITHC Report also contains the specific report sections that provide evidence, allowing the client's assessor to better understand Pentest People's approach and process the results.

3.3 The Individual Assessments

3.3.1 Onsite Assessments

Internal Infrastructure Assessment	10% Authenticated Vulnerability Scan	Wireless Infrastructure Assessment
PSN Gateway Authentication Controls Review	Server and Workstation Standard Build Review	Mobile Device Management Configuration Review

3.3.2 Offsite Assessments

External Infrastructure Assessment	Remote Access Solution Review	Firewall Configuration and Ruleset Review

3.2.1 Onsite Tests

The following tables list the individual assessments and the specific PSN requirement that they aim to meet.

These tests are performed onsite at the client's office location(s).

Test Type	PSN Requirement Statement
Internal Infrastructure Assessment	Internal testing should include vulnerability scanning and manual analysis of your internal network
	…network management security
10% Authenticated Vulnerability Scan	Patching at operating system, application and firmware level
	The testing should include representative vulnerability scanning across the entire estate covering end-points (including thick and thin clients), servers, network devices and appliances.
PSN Gateway Authentication Controls Review	Internal security gateway configuration (including PSN gateway)
Wireless Infrastructure Assessment	Wireless network configuration
Server and Workstation Standard Build Review	Desktop and server build and configuration
	Build and Configuration of laptops
Mobile Device Management Review	…solutions for managed devices and BYOD
	…other mobile devices such as phones and tablets used for remote access

3.2.2 Remote Tests

These tests are performed remotely from the Pentest People Leeds based office and data centre locations.

Test Type	PSN Requirement Statement
External Infrastructure Assessment	External testing should also include any systems you have in place to allow staff to connect into your organisation remotely. These remote access solutions normally involve VPN that should be tested as part of your external assurance.
Remote Access Solution Review	Configuration of remote access solutions
PSN Firewall Ruleset Review	…systems that provide services on the internet such as email servers, web servers and other systems such as the firewalls that are in place to prevent unauthorised access from the internet into your organisation.

The PSN IT Health Check guidance document can be downloaded from: https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance

4. Prerequisites

What do I need to prepare?

The PSN IT Health Check includes myriad individual tests, and each have specific prerequisites. It is important that these are arranged by the client prior to the assessment to avoid unnecessary delays. Typically, the scope and all prerequisites are confirmed by the consultant during the initial briefing session on the first day of the assessment.

4.1 Inform Any Support Teams

☐ The testing can often involve a large quantity of requests made over a relatively short time, potentially resulting in a sudden increase in log files and alerts. For this reason, it is recommended that any support teams monitoring network activity are made aware of the testing.

4.2 Assign a Technical Contact

☐ Should any critical vulnerability be identified or any network disruption occur, then an onsite contact should be available to acknowledge the incident. It is therefore recommended that a technical contact associated with the target infrastructure be made available during the testing window.

4.3 Backup Critical Business Data

☐ Pentest People take every precaution to ensure that the risk of network disruption or data loss during an assessment is very low. However, to mitigate the risk further still, it is recommended that the client backup any critical business data, and ensure that any data recovery solutions are working correctly.

4.4 Prepare List of Internal Target IP Addresses

☐ Unless already provided, the consultant will require a list of all target IP addresses for the servers, workstations and infrastructure devices within scope. This should include target IP addresses for the hosts within scope of the Server and Workstation Build Review part of the assessment. It is strongly recommended that individual IP addresses and/or hostnames are provided, rather than CIDR ranges. Whilst scanning of large ranges may be required in some instances, the consultants time is better spent identifying vulnerabilities, and not port scanning large ranges to identify live hosts. This information is typically collected in the IT Health Check Post-Sales Scoping form or via a SecurePortal online scope questionnaire.

4.5 Prepare List of External Target IP Addresses and URLs

☐ Similarly to 4.4, the Pentest People consultant will require a list of all public facing IP addresses and Web application URLs hosted and managed by the client. This information is also typically collected in the IT Health Check Post-Sales Scoping form.

4.6 Prepare List of Business Associated Wireless SSIDs

☐ The individual SSIDs within the scope of the assessment should be provided to the consultant if not already done so. This ensures that the assessment does not include wireless networks that are not managed by the client.

4.7 Prepare Required Authentication Credentials

☐ A temporary account with ‘Domain Admin’ privileges will be required to perform the 10% Authenticated Vulnerability Scan part of the internal security assessment. Additionally, either SNMP community READ strings or SSH credentials will be required to perform an authenticated scan of infrastructure devices such as switches and routers.

☐ The credentials to access each wireless network should also be provided to the consultant to be used as required during the assessment. This will allow the consultant to identify issues such as lack of wireless isolation, dual-homed hosts and lack of network segmentation.

4.8 Arrange Access to MDM Solution Configuration

☐ The Pentest People consultant(s) will require either access to the MDM solution management console or be provided with a human-readable export of the solution's configuration. This is necessary to identify common configuration vulnerabilities and to compare the solution's policy with what is actually enforced on an employee's handset.

4.9 Arrange Access to Business Handsets and Tablets

☐ The Pentest People consultant(s) will require access to each make and model of device associated with the MDM solution, including passcodes to access the device and any credentials necessary to access business mobile applications.

4.10 Export PSN Firewall Configuration

☐ In order to perform the required firewall configuration review, the Pentest People consultant(s) will require either an export of the firewall configuration, or a human-readable export of the rules. The former is preferred, and will allow a more thorough inspection to be conducted.

5. Methodology

What tests will the consultants be performing?

5.1 Internal Infrastructure Assessment

This test can be divided info the following high-level sections:

Test Type	Description	Tools	NIST Ref.
Network traffic Analysis	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 and unauthenticated routing information. Traffic analysis can also be used to partially map out network resources and identify security issues with traffic flow. The reconnaissance stage also focuses on active target identification which involves identifying live services, their version and information about the hosting device. This information lays the foundation for the vulnerability assessment, and the majority of this information is used to identify software associated vulnerabilities.	Wireshark, Yersinia, TCPdump	800-115 - 4.1 800-115 - 4.3 800-115 - 4.6
Port/Service Discovery	One of the initial stages of any internal assessment is to identify live ports / services on the target hosts through automated port scanning. The remote operating system is fingerprinted and the service versions are identified.	Nmap, Scanline, NetCat, ARPScan	800-115 - 4.1 800-115 - 4.3 800-115 - 4.6
Unauthenticated Vulnerability Assessment	The results of the initial vulnerability scans provide the foundations for the entire assessment. The automated tools will probe each live service and identify known vulnerabilities based on the results of version banner checks and vulnerability specific plugins. This is the most network intensive part of the assessment as multiple checks will be conducted simultaneously on multiple hosts.	Nessus, Saint, Nexpose	800-115 - 4.4 800-115 - 7.1 800-115 - 7.2 800-115 - 7.3 800-115 - 7.4
Manual Confirmation / Exploitation of Infrastructure Vulnerabilities	The consultant will manually confirm the identified medium to critical level (CVSS Score 4-10) vulnerabilities. This may involve using techniques such as (but not limited to) exploitation code, malformed queries and password attacks, depending on the vulnerability identified. The manual confirmation of vulnerabilities mitigates the risk of reporting false positives. In addition, the compromise of target hosts provides a platform on which to identify additional issues (post-exploitation).	Metasploit Framework	800-115 - 5.2
Brute-force / Wordlist Attacks	Any service that supports authentication will be assessed with either brute-force or wordlist attacks to identify weak passwords and other security issues. The most common services assessed are Telnet, SSH, FTP, SMB, LDAP, MSSQL and RDP.	Hydra, Medusa, Burp Suite (Intruder) and Metasploit Modules	800-115 - 5.1

Test Type	Description	Tools	NIST Ref.
Internal Web Application Checks	The automated scanning results will return low level Web application issues, considered the 'lowest hanging fruit'. Therefore, a Web application specific assessment is performed to identify more complex vulnerabilities.	Burp Suite Professional, SQLMap, Nikto, WPScan, DNSRecon, DirBuster, theHarvester, SSLScan and Nmap	800-115 - 5.2
Post Exploitation Techniques	As the consultant elevates their privileges and compromises additional services they will attempt to access more areas of the scope to achieve their main objective. Therefore, this stage of the assessment will also examine vulnerabilities associated with areas such as network segmentation and firewall restrictions. The consultant will attempt to identify security weaknesses in the infrastructure that may allow them to access restricted areas such as a cardholder data environment (CDE) in assessments driven by PCI DSS compliance. Once targets have been compromised it is then possible to identify additional vulnerabilities. These will often include local administrator password reuse, the use of weak hashing methods such as LM, cached credentials and weak domain admin passwords.	Tools used: Metasploit, PowerShell Empire	800-115 - 5.2

5.2 10% Authenticated Vulnerability Scan

Test Type	Description	Tools	NIST Ref.
Authenticated Vulnerability Assessment	Pentest People will perform an automated and authenticated vulnerability scan using administrative credentials against the provided scope. This will cover at least 10% of all servers and workstations, but also infrastructure devices such as switches, routers and firewalls. This scan will identify vulnerabilities such as missing patches, outdated third-party software, deprecated firmware versions, and common local security configuration vulnerabilities.	Nessus, Saint, Nexpose	800-115 - 4.4 800-115 - 7.1 800-115 - 7.2 800-115 - 7.3 800-115 - 7.4

5.3 PSN Gateway Authentication Controls Review

Test Type	Description	Tools	NIST Ref.
PSN Gateway Review	Pentest People will perform an assessment of the specific authentication controls (implemented by the client) associated with the PSN gateway services. This aims to identify any vulnerabilities with the authentication and authorisation controls that could be leveraged to access services that should otherwise be restricted.	Nessus, Saint, Nexpose	800-115 - 4.4 800-115 - 7.1 800-115 - 7.2 800-115 - 7.3 800-115 - 7.4

5.4 Wireless Infrastructure Assessment

Test Type	Description	Tools	NIST Ref.
Passive Scanning	Pentest People will perform a passive scan of the wireless networks broadcasting in the immediate vicinity.	Aircrack Suite, Wifite	800-115 - 4.6
Wireless Authentication Review	The authentication controls such as WPA pre-shared key, 802.11x, and any captive portals will be assessed, identifying any vulnerabilities that could be leveraged by an attacker within range of the wireless signal.	Aircrack Suite, Wifite	800-115 - 4.6
Wireless Isolation and Segmentation Review	When connected to guest wireless networks, the segmentation from critical business resources will be reviewed. Additionally, the effectiveness of wireless isolation will be confirmed.	Aircrack Suite, Wifite	800-115 - 4.6

5.5 Server & Workstation Build Review Assessment

Test Type	Description	Tools	NIST Ref.
Server / Worksation / Laptop Authenticated Scan	Pentest People will perform an authenticated vulnerability scan against the host, identifying issues such as missing Microsoft patches, outdated third-party software and common local security policy configuration issues.	Nessus, Saint, Nexpose, Paws,, PowerShell scripts, Empire	-
Server / Worksation / Laptop Local CIS Security Configuration Review	A manual inspection of the hosts' security configuration will be cross-referenced with the CIS Benchmarks for the associated operating system	Nessus, Saint, Nexpose, Paws, CIS-CAT, PowerShell scripts, Empire	-
Workstation / Laptop Physical Security Review	Controls around BIOS/BOOT, Antivirus and Full Disk Encryption will also be reviewed.	Manual	-

5.6 Mobile Device Management Review

Test Type	Description	Tools	NIST Ref.
Mobile Device Management Configuration Review	Pentest People will review the Mobile Device Management solution and cross-reference the current configuration settings against NIST recommendations, ensuring that mobile devices are sufficiently secured to mitigate the risk of business data loss or compromise.	Manual	-
Mobile Handset Review	The individual handsets (and tablets where applicable) will be inspected to confirm the correct application of the MDM configuration profiles.	Manual	-

5.7 External Infrastructure Assessment

Test Type	Description	Tools	NIST Ref.
Business OSINT Review	The consultants will gather information on the target business from freely available online resources. This will include (but is not limited to) employee email addresses, DNS records, document meta-data, public facing portals, and social media information.	Maltego, Sublis3r, theharvester, fierce, recon-ng, dnsenum, bluto…	-
Port/Service Discovery	One of the initial stages of any external assessment is to identify live ports / services on the target hosts through automated port scanning. The remote operating system is fingerprinted and the service versions are identified.	Nmap, Scanline, NetCat, ARPScan	800-115 - 4.1 800-115 - 4.3 800-115 - 4.6
Unauthenticated Vulnerability Assessment	Pentest People will perform an unauthenticated vulnerability scan against all external hosts, and manually verify all results. This test typically identifies vulnerabilities such as SSL misconfigurations, support for vulnerable protocols, dangerous public facing services, and weak Web portal authentication controls.	Nessus, Saint, Nexpose, SSLscan, TestSSL	800-115 - 4.4 800-115 - 7.1 800-115 - 7.2 800-115 - 7.3 800-115 - 7.4
Brute-force / Wordlist Attacks	Any service that supports authentication will be assessed with either brute-force or wordlist attacks to identify weak passwords and other security issues. The most common services assessed are SSH and Web application portals.	Hydra, Medusa, Burp Suite (Intruder) and Metasploit Modules	800-115 - 5.1

5.8 Remote Access Solution Review

Test Type	Description	Tools	NIST Ref.
Configuration Review	Pentest People will examine the configuration of the remote access solution used by remote workers to access corporate resources. This will include identifying support for weak encryption or hashing algorithms, lack of two-factor authentication, lack of brute-force protections, weak password policies, and overly permissive rules where applicable.	Titania Nipper, Propriety configuration parsing scripts	-

5.9 PSN Firewall Ruleset Review

Test Type	Description	Tools	NIST Ref.
Firewall Ruleset Review	The firewall rules with be manually assessed for common issues, such as being overly permissive, allowing access to vulnerable cleartext protocols, duplication, and lack of logging.	Titania Nipper, Propriety configuration parsing scripts	800-115 - 3.3
Firewall Configuration Review	Pentest People will use internal parsing tools and line-by-line manual inspection to identify configuration specific vulnerabilities. The severity of the issues will be amended as each is considered in business context.	Titania Nipper, Propriety configuration parsing scripts	800-115 - 3.3

6. Risks

What are the risks when performing these tests?

All tests performed by a security consultant come with an element of risk. The relatively large quantity of requests can cause issues if bandwidth is limited, and malformed requests can potentially cause unexpected behaviour in systems that could lead to Denial-of-Service. However, Pentest People's consultants take every possible step to mitigate the risk of disruption.

6.1 Denial-of-Service Specific Checks

Pentest People's consultants will not perform any attacks that aim to cause a Denial-of-Service situation on the network infrastructure, hosts, or services. This is standard policy, and is strictly adhered to unless the client specifically requests that such a test should be performed. In the instances where DoS attacks are requested, Pentest People will discuss a suitable time and scope to perform the tests.

6.2 Domain Account Lock-Out

Automated password attacks are only attempted when the associated password policy is understood and confirmed by the client, ensuring that lockout thresholds are not exceeded. Account lockouts occur most commonly when automated attacks are performed against domain users on a Windows domain when a low lockout threshold is configured. However, this situation can also occur on local Windows server and workstation accounts, database accounts, and Web applications. The current password policies across systems within scope is typically discussed during the initial briefing sessions with the consultant.

6.3 Unpredictable Exploitation Code

Pentest People's consultants will only use tried, tested and trusted exploitation code, and only ever when doing so is necessary to fully confirm the existence of a vulnerability. Pentest People's consultants will not use untested exploitation code obtained from online resources during the assessment. If publicly available untested exploitation code exists for a specific software version, then this will be highlighted in a report.

6.4 Dangerous Application Attacks

Some critically rated vulnerabilities in Web applications can be leveraged to cause significant business disruption or to affect the integrity of sensitive business information. For example, should SQL Injection be possible, then an attacker could modify database information via the affected application, or if contact forms are not protected with a CAPTCHA, then an automated attack could flood the business with emails. Pentest People's consultants take steps to mitigate the risks of these issues by de-scoping dangerous application functionality, and avoiding attacks widely known to cause issues.

6.5 Layer 2 Traffic Manipulation

Pentest People's consultants aim to identify vulnerabilities with the network infrastructure, such as insecure routing, lack of segmentation, and vulnerable broadcast traffic. However, the consultants will not aim to exploit these issues and manipulate layer 2 network traffic, such as poisoning ARP, STP, or routing tables, or attacking Cisco specific protocols such as CDP.

7. Presentation

Will the results of the assessment be discussed?

Pentest People's consultants encourage clients to be involved throughout the assessment process, discussing each stage in detail. This approach helps clients to better understand the tests and what the results mean from both a technical and business impact perspective. This allows remediation efforts to be better prioritised and for management to better understand the current state of security.

7.1 Assessment Shadowing

When performing onsite testing, Pentest People's consultants encourage clients to sit and observe the testing throughout the day. Each stage can be explained, stepping through exploitation methods and discussing potentially options for remediation.

7.2 End of Test Debrief Session

The standard policy is to include a debrief session on the last day of testing. The consultant will walk the client through the most significant findings in chronological order, and discuss at length the most suitable options to resolve each issue. It is recommended that a representative from each relevant department be present at this meeting. The timing for this debrief is typically confirmed during the initial briefing on the morning of the first day of testing.

At a minimum, the end of assessment debrief will include the following:

- Chronological walk-through of the steps taken to breach security (if applicable)
- Discussion of the most significant vulnerabilities from a technical and business impact perspective
- Discussion of remediation options
- Confirmation that all required testing has been completed
- Discussion around report structure and delivery times
- Discussion around secure transport and storage of client data

7.3 Awareness Training Presentations and Workshops

If desired, the client's assigned Pentest People account manager can discuss options for the consultant (or consultants) to return to site and present the findings of the assessment to a non-technical audience. This is commonly aimed at upper management, or used as a way to provide impact to general awareness training for all employees.

8. Reporting

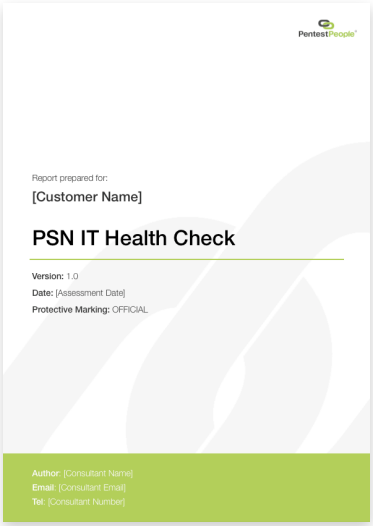
What can I expect from the assessment report?

The results of the PSN IT Health Check assessment are delivered as a PDF report, containing the information required for both management and technical staff to understand and remediate vulnerabilities. However, given the relatively large quantity of tests included within an ITHC, and the depth to which these tests are performed, a series of supplemental reports are often included. These additional reports are provided in .xlsx or .csv format, to present the large quantity of results in a manageable way.

The main ITHC report includes the following sections:

8.1 Overview

This section includes a list of the individual tests that were performed, the background to the testing, compliance drivers, assessment context, assessment purpose, information about sample testing, and information about any caveats that the consultants adhered to. Additionally, the numerical references for sections of the report that provide evidence for each specific PSN requirement are also included.


Report prepared for:
[Customer Name]
PSN IT Health Check
Version: 1.0
Date: [Assessment Date]
Protective Marking: OFFICIAL
Author: [Consultant Name]
Email: [Consultant Email]
Tel: [Consultant Number]

8.2 Assessment Scope

This section lists the IP addresses, hostnames, URLs, wireless SSIDs, handset makes, and firewall devices that were included in the scope of testing. Any systems that were de-scoped by the client, consultant, or PSN assessor are also listed here.

8.3 About This Report

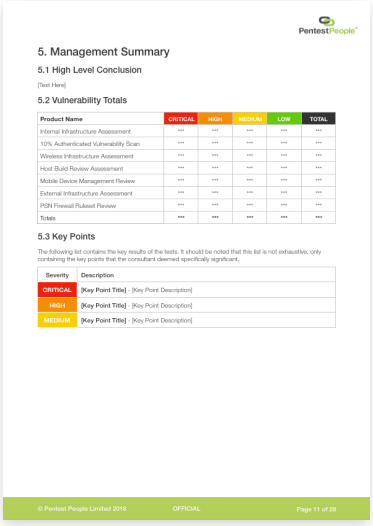
This section briefly explains the content of the four core sections of the overall report, ‘Management Summary’, ‘Detailed Technical Results’, ‘Additional Information’, and ‘Appendices’.

8.4 Management Summary

This section includes a high-level paragraph summarising the overall results of the assessment, allowing readers with little time to gain an understanding of the ‘bottom line’. The key findings with a short description and level of risk are included. This section also includes the consultant’s comments to further explain the results of each test, their business impact and the recommended remediation steps specific to the client.

8.5 Detailed Technical Results

This section constitutes the main body of the report and includes the detailed findings of each test. All identified vulnerabilities are listed with a description, proof of concept screenshot where applicable, relevant tool output, risk rating, remediation advice, external references and affected target hosts. All issues identified as part of automated and manual testing techniques are included. Non-issues (or informational issues) may also be included to highlight certain areas that do not necessarily present a security concern.


5. Management Summary
5.1 High Level Conclusion
[Text Here]
5.2 Vulnerability Totals
Product Name	CRITICAL	HIGH	MEDIUM	LOW	TOTAL
Internal Infrastructure Assessment	***	***	***	***	***
10% Authenticated Vulnerability Scan	***	***	***	***	***
Wireless Infrastructure Assessment	***	***	***	***	***
Host Build Review Assessment	***	***	***	***	***
Mobile Device Management Review	***	***	***	***	***
External Infrastructure Assessment	***	***	***	***	***
PSN Firewall Ruleset Review	***	***	***	***	***
Totals	***	***	***	***	***
5.3 Key Points
The following list contains the key results of the tests. It should be noted that this list is not exhaustive, only containing the key points that the consultant deemed specifically significant.
Severity	Description
CRITICAL	[Key Point Title] - [Key Point Description]
HIGH	[Key Point Title] - [Key Point Description]
MEDIUM	[Key Point Title] - [Key Point Description]
© Pentest People Limited 2018 OFFICIAL Page 11 of 28

8.6 Additional Information

Any testing data (such as tool output or gathered evidence) considered too large (or not relevant enough) to include in the main body of the report will be placed in this section. For example, this section may include large lists of email addresses enumerated through OSINT techniques, large port scanning tool output or extensive lists of firewall rules deemed overly permissive. Where appropriate, the main body will provide links to the relevant additional information section.

9. Remediation

What remediation support will I receive?

Penetration Testing is a well-utilised service with many organisations undertaking such a service either for risk management or compliance purposes.

Fixing the issues identified in a Penetration Test is referred to as Remediation. In our experience, Remediation after a Penetration Test can be an onerous task that can burden the organisation's technical teams.

Pentest People offer a Remediation Consultancy Service as part of their Penetration Testing as a Service (PTaaS) offering. This service offering completes the Penetration Testing process by engaging with a consultant to provide a tailored prioritised approach to remediating any security issues identified from the testing engagement.

9.1 What are the risks?

Fixing identified security issues is a technical task that has to be performed by competent technical consultants who are adept with dealing with such matters. Pentest People specialise in identifying and remediating security issues on all common platforms and applications. It is important that you assign proper priorities to the identified issues and fix them in a timely manner. Once these issues have been fixed, they have to be retested to ensure that the fix has mitigated the risk.

9.2 How can we help?

This Remediation Consultancy Service provided by Pentest People is a two-stage process. The initial phase involves one of our specialised consultants reviewing the findings of the Penetration Test report and aligning this with your business requirements to create a prioritised approach document that contains remediation advice for all of the identified issues ranked in order of risk.

Once this report is created, the next step is to look at the implementation of this plan to mitigate the risks identified.

This prioritised approach document can be implemented either by your own internal IT staff, your incumbent IT provider or Pentest People as part of the engagement, therefore, taking away the time pressures of ensuring your infrastructure is secure and free from security issues.

The service would be delivered as part of the Pentest People Penetration Testing as a Service (PTaaS) and full access to the SecurePortal and other complementary tools would be provided.

10. Further Testing

What other services would Pentest People recommend?

The PSN IT Health Check assessment covers a large range of systems, both from an internal and external perspective. However, the guidance for IT Health Checks is not exhaustive, and does not include certain tests that would greatly reduce the overall risk to the client's infrastructure.

The following assessments are recommended to compliment a PSN IT Health Check, providing additional assurance that sensitive business data is sufficiently secured.

10.1 Social Engineering Assessment

Pentest People can perform a wide variety of social engineering associated assessments, such as broad scale email phishing, targeted spear phishing, business/employee OSINT, vishing, and onsite physical access assessments. These tests can identify weaknesses in the business policies, procedures, and awareness training that an attacker could leverage to gain remote access.

10.2 Web Application Assessment

Web technologies have advanced in recent years and so have the Web Applications that we all use daily. With this advancement and reliance upon web technologies, we have also been exposed to security risks associated with these applications. In either case, these applications are a common target for attackers. External facing Web Applications used by businesses are by nature available to all via the public Internet. The complexity and availability of these applications have made them an ideal target for attackers and there have been many publicised data breaches that have been caused by insecure web applications. Protecting these applications from new threats is a constant challenge, especially for developers who may not be security aware and who are working towards a performance deadline.

Please contact your Pentest People account manger If you would like any further information on the above assessments.

11. Appendices

11.1 About Pentest People

Pentest People are a UK-based boutique security consultancy focussing on bringing the benefits of Penetration Testing as a Service (PTaaS) to all its clients. This innovative approach to security testing combines the benefits of a consultant-led penetration test and vulnerability assurance through a technologically advanced SecurePortal, providing a living threat system to its clients and benefit through the life of the contract rather than just a single point in time.

Pentest People are a CREST accredited company for its Penetration Testing services and have also attained the NCSC Cyber Essentials and Cyber Essentials Plus. Pentest People are also accredited to ISO:9001 and ISO:27001.

Our specialised team of security consultants hold industry qualifications such as CHECK Team Leader, CCIE, CISSP and CEH and combine this with many years of industry experience at the highest level working across all industry sectors. It is the aim of our consultants to work with organisations to ensure that their security investment is fully optimised on a 24/7/365 basis.

By building on our front-line network security experience and listening to the day-to-day challenges of our customers we aim to deliver world-class, integrated security risk management solutions that turn security data into security intelligence; simplifies and automates regulatory compliance processes and provides peace of mind for network managers that their IT environment is fully protected.

Pentest People is a part of the Storm Technology Group that also includes The Data Protection Consultancy company Data Protection People, The Malware Protection company InfoSecurity People and the Digital Experience Monitoring company, RapidSpike.

Company Details

Pentest People Limited
Round Foundry Media Centre, Foundry Street, Leeds, LS11 5QB 0113 394 4630
info@pentestpeople.com
www.pentestpeople.com
Company Number: 10661715
VAT Number: P283 8433 75