WHBence Limited

ITHC PSN Review

February 2018

Version: 1.0

Report By: Kurtis Baron

Email Kurtis@fidusinfosec.com

Telephone: +447707398088

Table of Content

1 Document Information

Confidentiality and Copyright

Document History

Version Number	Issue Date	Issued By	Change Description
0.1	19/02/2018	Kurtis Baron	Draft for internal review only
0.2	20/02/2018	Andrew Mabbitt	Revised QA
1.0	20/02/2018	Kurtis Baron	Released to Client

Testing Team

Name	Qualifications
Kurtis Baron	CSTM, SST, CISSP

Accreditations and Certifications

2 Management Summary

This report details the findings of a build review assessment carried out on behalf of WHBence Limited on the 16th February. The testing was carried out at WHBence offices in Yate, Bristol. The objective of the assessment was to identity any vulnerabilities or potential issues which could impact the Confidentiality, Integrity or Availability two workstations used to access the Public Services Network (PSN) and any data contained within.

Overall, the workstations were found to be extremely robust and built with security in mind. Multiple protections were identified, such as; removal of the default administrator account, regularly applied software updates, and the use of a firewall and anti-virus product.

A single recommendation has been made for the workstations. Whilst the issue is not exploitable by a malicious attacker, it is recommended as a best practice measurement.

3 Risk Ratings

The table below has been generated to provide an insight into the colours, risk rating and scoring system used throughout this report to help provide a concise and transparent overview.

It should be noted that issues have been rated based on the evidence discovered by the tester and whilst there may be controls in place in the backend of the systems to prevent specific attacks occurring, it may have been known to the tester throughout the assessments.

Colour	Risk Rating	CVSSv2 Score	Explanation
Purple	Critical	9.0-10.0	This requires resolution as quickly as possible.
Red	High	7.0-8.9	This requires resolution in the near future.
Orange	Medium	4.0-6.9	This requires resolution in the medium term.
Blue	Low	1.0-3.9	This requires resolution as part as routine maintenance.
Green	Informational	0-0.9	This requires resolution to be in line with best practices.

4 Summary of Findings

The following table summarises the issues identified throughout testing:

Description	Critical	High	Medium	Low	Total
ITHC	0	0	0	1	1
Total	0	0	0	1	1

All security issues are presented alongside recommendations for mitigating the risks posed. These can be found alongside the related issues in section [5] of this report.

4.1 Key Findings

- The overall security posture of the WHBence PSN workstations were found to be excellent.

4.2 Recommended Next Steps

The goals provided are set out to be suggestions and should be reviewed and fixed according to the risk posed to your business model.

Short Term Goals

- Reconfigure Windows 10 to ensure that it does not cache domain credentials.

5 Vulnerability Findings and Technical Details

The following section details vulnerabilities found throughout the testing phase alongside the technical details associated. The following information is included, where applicable:

- Risk Rating
- Description
- Recommendation
- Affected Hosts
- References

Where possible, enough information to replicate the finding will be included within the vulnerability write up. Additional information, where required, will be added into the Appendices of this report.

5.1 Desktop Build Review

Component	Pass/ Fail	Comments
Host Based Firewall	✓	Windows firewall correctly configured.
Patching Level	✓	The system is fully patched and up-to-date.
Available Shares	✓	No unauthenticated shares available on the system, or protected shares that contain sensitive information.
File System Configuration	✓	File system was suitable configured.
Installed Software	✓	Vulnerable software is not installed on the system.
Anti-Virus Configuration	✓	Anti-Virus is correctly installed and configured. Updates are automatic, and full-system scans are regular.
Active Local Processes	✓	No suspicious processes identified that may significantly affect the performance or security of the system.
Process & Port Association	✓	All networked services are legitimate and required for general operation within a corporate environment.
Routing Table	✓	No suspicious or redundant routes present in the routing table.
Network Connections	✓	All network connections are within the network boundaries.
Local Accounts Review	✓	Default administrative account has been renamed.
Group Policy Configuration	✓	Group Policy correctly applied from the Domain Controller.
Local Services	✓	All local services are necessary and correctly configured.
Start-up Executables	✓	No suspicious executables.
Password Hashes	Low	Password hashes are cached locally.
Password Policy	✓	Password Policy correctly implemented.
Account Lockout	✓	Account Lockout after 3 attempts
BIOS Configuration	✓	BIOS password set.

Fidus performed a build review against two machines due to be connected to the PSN network. These machines were found to be non-domain joined and were separated by use of a dedicated router for outgoing network access. The outcome of this review found the devices to be well configured and fit for purpose.

For this build review, recommendations from NCSC for the setup of a Windows 10 device were considered, as well as a full authenticated vulnerability scan and manual review.

The machines were found to be well configured with all updates installed and further updates to be applied automatically. Anti-Virus was found to be installed and using the latest definition files as can be seen in the image below.

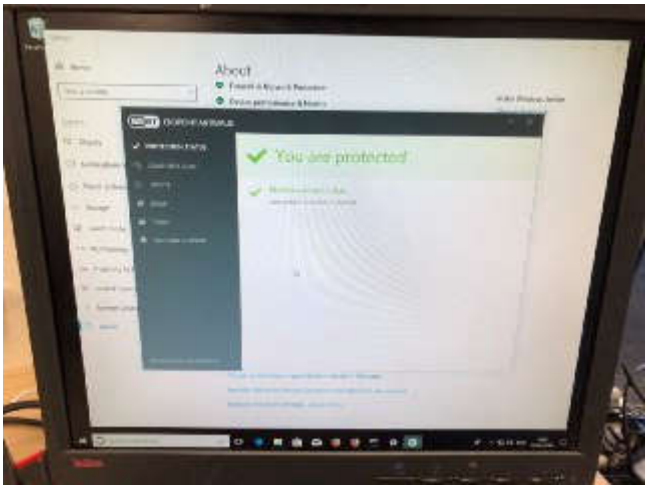

Figure 1: Anti-Virus Updates

Further testing found that the administrator account had been disabled and two further users were in-place, an IT support user who had administrator access and a standard user for general day to day use.

Attempts to access the BIOS were unsuccessful as a password was required to gain access. This meant the tester was unable to boot into any live operating systems other than the installed version of Windows 10.

While onsite, it was noted that the Remote Desktop Protocol (RDP) was enabled, after a discussion with the point of contact it was decided that there was no purpose to this being enabled and was disabled. As such, this is no longer a risk.

Password caching was found to be enabled, but due to the machines in question not being domain joined this finding is found to be a non-issue, even so a recommendation to this feature off has been included below.

Recommendation:

Disable Password Caching

Reconfigure the local security policy and set the following value to 0 –
Security Options - Interactive logon: Number of previous logons to cache (in case domain controller is not available).
Alternatively, the following registry entry can be set to 0 - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount.

Affected Hosts:

IP Address
10.16.201.55
10.16.201.22

6 Tool List

Tool Name & Version	Description
Nessus 7.60 (Professional License)	Vulnerability scanner https://www.tenable.com/products/nessus/nessus-professional
Nmap 7.60	Open source port scanning tool https://nmap.org/download.html
Testssl 2.9.5	Open source SSL/TLS enumeration tool https://testssl.sh/
Metasploit Framework 4.16.39-dev	Exploit framework https://metasploit.com

7 Methodologies

Internal Infrastructure

Fundamentals

An internal infrastructure assessment assesses for the vulnerabilities and weaknesses in the network configuration which are typically leveraged by malicious actors in order to gain full compromise of the internal domain. It provides an insight into an organisation's security posture.

An internal infrastructure assessment can be divided into three stages:

- Discovery
- Assessment
- Exploitation

Test Areas

Fidus utilise a wide range of tools to scan and discover assets. Usually, a target IP range is provided prior to the commencing of testing, albeit some engagements require Fidus to identify ranges in use. Our consultants use the latest scanning tools and techniques to perform a comprehensive audit of all IP ranges. Some of these include:

- TCP and UDP port scanning
- Operating system & service fingerprinting
- Network mapping
- User enumeration (where possible)

Once the discovery phase has ended, Fidus consultants interpret the results and use them to identify possible attack vectors and perform manual attack simulations. Manual assessments focus on:

- Misconfigured hosts and services
- Patch level assessments
- Outdated systems and software
- Insecure protocols
- Weak passwords and default usernames
- LLMNR and NBNS spoofing

If a successful avenue of attack is identified, Fidus will work with you to conduct safe exploitation (where possible) and verification of the issue whilst ensuring there are no disruptions to the daily running of your organisation. All exploitation is conducted under the agreed rules of the engagement.

Should a service be successfully exploited, Fidus will aim to escalate to the highest of privileges and, with your agreement, continue to leverage this access to penetrate as deep as possible in your network to help portray a realistic attack scenario.

Workstation Build Review Assessment

Fundamentals

Poorly and misconfigured servers and workstations can provide an attacker an easy route to domain administrator and full compromise of a corporate network. A build review assessment aims to find these misconfigurations and highlight areas which require improvement.

Test Areas

The following areas are assessed throughout the build review assessment:

- Patch levels, both Operating System and Third Party.
- Management services
- Trust relationships
- Network shares and permissions
- Local shares and permissions
- Password hashing mechanisms
- Group Policy sensitive information
- Antivirus and endpoint protection
- Cached credentials
- Security policy checks
- Service binaries