[Assessor’s name]

[company name]

Cyber Essentials +

Vulnerability assessment Report V1.0

dd-Month-Year

Contents

[1. Introduction 3](#_Toc417035181)

[1.1 Disclaimer 4](#_Toc417035182)

[2. Certification Body Details 4](#_Toc417035183)

[3. Client Details 4](#_Toc417035184)

[4. Business Scope 6](#_Toc417035185)

[4.1Target systems 6](#_Toc417035186)

[5. Executive summary 7](#_Toc417035187)

[5.1 Value added reporting 7](#_Toc417035188)

[6 Test details and findings 7](#_Toc417035189)

[6.1 Test 1 - External Vulnerability Scan for stated IP range 7](#_Toc417035190)

[6.2 Test 2 – Email Binaries and Payloads 8](#_Toc417035191)

[6.3 Test 3 – Web site page with URLs linking to binaries 9](#_Toc417035192)

[6.4 Test 4 – Authenticated vulnerability scan of host(s) 10](#_Toc417035193)

[6.5 Mobile Devices 11](#_Toc417035194)

[7 Additional Information 13](#_Toc417035195)

[7.1 Test 1 - External Vulnerability Scan for stated IP range 13](#_Toc417035196)

[7.2 Test 2 – Email Binaries and Payloads 13](#_Toc417035197)

[7.3 Test 3 – Web site page with URLs linking to binaries 13](#_Toc417035198)

[7.4 Test 4 – Authenticated vulnerability scan of host(s) 14](#_Toc417035199)

[7.5 Value added checks - internal 16](#_Toc417035200)

[7.6 Value added checks – website (optional) 16](#_Toc417035201)

[8 Summary of Failings, Action Points and Observations. 17](#_Toc417035202)

[8.1 Failings 17](#_Toc417035203)

[8.2 Action Points 17](#_Toc417035204)

[8.3 Observations 17](#_Toc417035205)

[9 Conclusion 18](#_Toc417035206)

Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Comment |
| 1.0 |  |  | Initial Draft |
|  |  |  |  |

# 

# 1. Introduction

Thank you for selecting [COMPANY NAME) to conduct the on-site vulnerability assessment against the *Cyber Essentials Plus Common Test Specification V1.2*

A copy of the test specification can be found at the following web address:

https://www.cesg.gov.uk/servicecatalogue/cyber-essentials/Pages/Scheme-Library.aspx

If the organisation is awarded a “fail” status for ANY test within this specification document, then it is deemed to have failed overall. Otherwise, a pass status is awarded.

**We are pleased to say that the company, within the scope specified in section 4, has been awarded a PASS Status.**

**Unfortunately, on this occasion, the company has been awarded a FAIL status.**

Details of all failings and/or action points or can be found in section 7 of this report and these are summarised along with any observations to improve cyber security in section 8.

The overall conclusion can be found in section 9.

Section 7.5 contains a random sample of tests that do not form part of the *Common Test Specification v1.2* therefore only **passes** and action points are awarded in this section, however, as your company has attested to complying with them in the questionnaire you should quickly address any issues found.

The aim of the onsite vulnerability assessment is to identify easily exploitable vulnerabilities within an organisation’s Internet facing infrastructure and user workstations that provide a high level of exposure to potential attackers with a low level of skill.

Cyber Essentials Plus gives customers, partners and other stakeholders the assurance that the organisation has implemented controls to meet the government’s recommended base level of cyber hygiene and, as such:

* This level of testing assumes no specific threats against an organisation need to be addressed and that the likely level of attack is the broad, untargeted style of unsophisticated attacks.
* This level of testing is not suitable for organisations that may be the target of Advanced Persistent Threat (APT) style attacks.
* Complex Application Testing (both thick client and web applications) is beyond the scope of the engagement.
* Database audits and reviews (other than trivial credential checks) are beyond the scope of the engagement.
* Denial of Service (DoS) attacks in all forms are specifically excluded from the scope of the Cyber Essentials test.

The following test cases have been conducted:

1. External vulnerability scan for stated IP range including website scanning;
2. Inbound email binaries and payloads
3. Web site page with URLs linking to binaries
4. Authenticated vulnerability scan of hosts

Each test is explained in detail along with the “headline” findings in section 6 of this report and additional information can be found in Section 7.

## 1.1 Disclaimer

The customer has accepted that (COMPANY NAME) can perform a security audit of their Internet facing infrastructure.

All information in this document is subject to change without notice and should not be construed as any form of commitment by (COMPANY NAME) .

(COMPANY NAME) takes no responsibility for any errors that may appear in this document.

An audit of a company’s Internet infrastructure should not be construed as a definitive review of the organisation’s security.

(COMPANY NAME) advise that differing security vulnerabilities might be gleaned through using additional scanning and enumeration techniques. (COMPANY NAME) cannot be held liable for any performance issues that occur during or after the audit.

# 2. Certification Body Details

|  |  |
| --- | --- |
| Certifying Body | (COMPANY NAME) |
| Consultant name |  |
| Address | (COMPANY NAME) |
| Phone |  |
| E-mail |  |

# 3. Client Details

|  |  |
| --- | --- |
| Organisation Name (legal entity): |  |
| Sector: |  |
| Parent Organisation name (if any): |  |
| Size of organisation micro, small, medium, large.  (See definition below) |  |
| No of employees |  |
| Point of Contact name:  Salutation (Mr, Mrs, Miss etc)  First  Middle  Surname |  |
| Job Title: |  |
| Email address: |  |
| Telephone Number: |  |
| Building Name/Number  Address 1  Address 2  Address 3  City  County  Postcode |  |
| Certification Body: | **(COMPANY NAME)** |

SME Definition [delete once referenced]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Company category** | **Employees** | **Turnover** | or | | **Balance sheet total** |
| Medium-sized | < 250 | ≤ € 50 m | | ≤ € 43 m | |
| Small | < 50 | ≤ € 10 m | | ≤ € 10 m | |
| Micro | < 10 | ≤ € 2 m | | ≤ € 2 m | |

# 4. Business Scope

[Please identify a diagrammatic scope of the system(s) to be assessed, including locations, network boundaries, management and ownership. Include External IP addresses and/or ranges.]

A system name should be provided that uniquely identifies the systems to be assessed, and which will be used on any certificate awarded. (Note: it is not permissible to provide the company name, unless all systems within the organisation are to be assessed):

|  |
| --- |
|  |

## 4.1Target systems

[AMEND AS REQUIRED]

Whole of the company. [COMPANY X] have around [n] computers at the main office and several servers in the Outsourced Data centre.

Many of the machines and servers have standard build image and are identical therefore a cross section of the devices are tested from each version as detailed below.

|  |  |  |
| --- | --- | --- |
| Device | Description | IP Address |
| Firewall |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 5. Executive summary

This report presents the results of the Cyber Essentials Plus assessment of [COMPANY NAME]. This assessment was performed under the auspices of an (COMPANY NAME) approved vulnerability assessor.

This analysis is based on the technologies and known threats as of the date of this report. (COMPANY NAME) recommends that all recommendations suggested in this document be performed in order to ensure the overall security of the internet facing environment.

(COMPANY NAME) conducted the Cyber Essentials Plus on-site assessment on [DATE] at [Company address]

**Total vulnerabilities found**

|  |  |  |  |
| --- | --- | --- | --- |
| High | Medium | Low | Total |
| 0 | 0 | 0 | 0 |

[EXAMPLE FINDINGS - Please use as a guide.]

The Assessment resulted in a High (fail) for the access control part of the test detailed in section [x] of this report. Users should not have admin level access to change system settings and/or install software. Admin access should be controlled and open to certain small user group instead of network wide unrestricted access.

The external test resulted in [x] medium vulnerabilities therefore an action point for that test has been recorded. Two action points were recorded for the email test.

A number of ports were found to be open on the servers. We understand the need for these ports to access certain services for your business needs but we suggest you review all ports regularly to ensure only the essential services are running on these ports.

## 5.1 Value added reporting

This report includes recommendations where High and Medium vulnerabilities have been found.

Links to appropriate patches have been provided where required. If you would like more information or guidance on how to fix any of the vulnerabilities, then please contact us.

Detailed findings for vulnerabilities that warrant a Low score do not form part of this report.

# 6 Test details and findings

## 6.1 Test 1 - External Vulnerability Scan for stated IP range

Using an appropriate industry standard vulnerability scanner, the assessor scanned the external IP range for all IP addresses within the specified ranges. If applicable, IPv6 addresses were also scanned.

The scans included:

* A full (all 65535 ports) TCP port scan for all IPv4 (and IPv6 where used) addresses within the specified ranges.
* A UDP scan across all the first 1024 UDP ports for each IP address under review.
* A UDP service scan on commonly used UDP ports. Specifically TFTP, SNMP and NTP ports were checked due to their common weaknesses.

All risks identified in this section have been scored using the CVSSv2 standard.

* **Low** risk issues are defined as a score from 0.0 to 3.9 and have not been reported within this document
* **Medium** risks are defined as a score between 4.0 and 6.9 and are usually associated with the obtaining of some piece of specific information enumerated from the system but that could not actually be directly exploited. Details about any such vulnerabilities found are in Section 7 of this report.
* **High** (fail) risks are defined as a score between 7.0 and 10.0 and are usually associated with direct compromise of a system or application for the extraction of production data, system passwords or the introduction of malware.

Results within this section have been split in to three areas in line with the relevant Basic Technical Cyber Protection Controls.

1. **Boundary Firewalls and Internet Gateways**

**PASS – No unnecessary open ports and services were found**

**FAIL - unnecessary open ports and services were found**

1. **Secure Configuration**

**PASS – No Weak credentials were found and no use of unsupported operating systems**

**FAIL - Weak credentials were found and /or unsupported operating systems**

1. **Patch Management**

**PASS – No vulnerabilities in unpatched services were found**

**FAIL - vulnerabilities in unpatched services were found**

## 6.2 Test 2 – Email Binaries and Payloads

**Intent of the test:** To verify that malicious code spread by emails would not run and infect the organisation’s computers

Using a remote test account and desktop/laptop system provided by your company, an email was sent with no attachments and determine that it arrives successfully in the target (employees) inbox.

Then the assessor attempted to send multiple emails in from their remote test account, with attached test files.

The following file types (a selection of binaries and text files) were used in this test:

|  |  |
| --- | --- |
| **Executables**  .com  .bat  .exe  .pif  .scr  .msi  .ps1  .jar  .sh  .py  .dmg | **Containers**  .zip  .7z  .rar  .tar.  gz  .tar  .gz |

No files were sent that would require the user to hunt them out by clicking more than two separate files or locations.

Results within this section have been split in to two areas for the purposes of reporting in line with relevant the Basic Technical Cyber Protection Controls.

1. **Malware Protection**

**PASS – User was prevented from accessing the Test Anti Virus (AV) attachments.**

**FAIL – User was not prevented from accessing the Test Anti Virus files by the Anti Virus Software**

1. **Secure Configuration**

**PASS – None of the attachments (including non AV files) were able to be run successfully.**

**FAIL – At least one of the attachments (including non AV files) was run successfully.**

**Technical issues [delete if no technical issues prevented the test]**

**FAIL - no email communications at all could be established during the test window. We ensured that your technical staff were given sufficient information to enable them to attempt to resolve the problem during the test.**

## 6.3 Test 3 – Web site page with URLs linking to binaries

**Intent:** To verify that sufficient controls are in place to prevent users running malicious code found on websites.

The assessor used a web browser to access the internet and locate a test page containing links to a downloadable set of test binaries.

No files were on the test pagethat would require the user to hunt them out by clicking more than two separate locations or files.

Results within this section have been split in to three areas for the purposes of reporting in line with relevant the Basic Technical Cyber Protection Controls.

1. **Boundary Firewalls and Internet Gateways**

**PASS – None of the executable URL links allow a file to be downloaded (and run) successfully**

**FAIL – Some of the executable URL links allowed a file to be downloaded (and run) successfully**

1. **Malware Protection**

**PASS – None of the Anti Virus (AV) test files were able to be downloaded successfully. The user was blocked from accessing them.**

**FAIL - Some of the Anti Virus (AV) test files were able to be downloaded successfully. The user was not blocked from accessing them.**

1. **Secure Configuration**

**PASS – The Non-Anti Virus (AV) attachments were not able to be run successfully.**

**Action Point – The Non-Anti Virus (AV) attachments that were downloaded were able to be run successfully.**

**Technical issues [delete if no technical issues prevented the test]**

**FAIL - No web access was established during the test. We ensured that your technical staff were given sufficient information to enable them to attempt to resolve the problem during the test.**

## 6.4 Test 4 – Authenticated vulnerability scan of host(s)

**Intent:** To demonstrate that computers have up-to-date applications, Antivirus software and that users cannot install new software or modify system settings.

Mobile devices are not included in these scans (unless they are a Microsoft Surface Tablet Pro).

The Assessor used an appropriate industry standard workstation build review tool and performed an admin level scan of the host including local checks for each host within the sample set.

The scans included a patch check for operating system updates as well for the following applications:

* Oracle Java
* Adobe Acrobat
* Office software suites
* Adobe Flash
* Mozilla Firefox
* Google Chrome
* Opera
* Microsoft Internet Explorer

The scans also included a check of any AV solution in use.

All risks identified were scored using the CVSSv2 standard.

* **Low risk** issues are defined as a score from 0.0 to 3.9 and have not been reported within the Cyber Essentials report.
* **Medium risks** are defined as a score between 4.0 and 6.9 and will usually be associated with a specific weak configuration of the system but that could not actually be directly exploited.

Details about any such vulnerabilities found are in Section 7 of this report.

* **High risks** are defined as a score between 7.0 and 10.0 and will usually be associated with likely direct compromise of a system for the extraction of production data, system passwords or the introduction of malware.

Results within this section have been split in to four areas for the purposes of reporting in line with relevant the Basic Technical Cyber Protection Controls.

1. **Patch Management**

**PASS - All patches that were released within 14 days of the date of the audit for any of the applications listed (above) were installed.**

[Otherwise]

**Action Point – All patches that were released within 30 days of the date of the audit for any of the applications listed (above) were installed.**

**FAIL - Some patches that were released within 30 days of the date of the audit for any of the applications listed (above) were not installed.**

**FAIL - OS or any application is unsupported and no patches are available**

1. **Malware Protection**

**PASS - An AV solution is place on all computers. AV definitions released within 7 days of the date of the audit installed and all AV engine updates were found to have been applied within a maximum of 90 days.**

**FAIL – An AV solution was not in place on one or more computers, or AV definitions released within 7 days of the date of the audit were not installed, or not all AV engine updates were found to have been applied within a maximum of 90 days.**

1. **Access Control**

**PASS - User accounts have been assigned to individuals rather than shared accounts and users do not have admin level access to change system settings and/or install software.**

**FAIL - User accounts have been shared amongst individuals or users do have admin level access to change system settings and/or install software.**

1. **Secure Configuration**

**PASS – The output from the build review tool inspections found only low risk issues**

**Action Point – The output from the build review tool inspections found some medium risk issues.**

**FAIL – The output from the build review tool inspections found one or more high risk issues.**

## 6.5 Mobile Devices

Where there was a requirement to audit a mobile device such as a tablet or phone, then only the following platforms were inspected:

[delete as appropriate]

* **Microsoft Surface Tablet (not PRO – as this handled in section 6.4)**
* **Apple iOS on IPhone or iPad**
* **Android on Phone or Tablet**

Results within this section have been split in to four areas for the purposes of reporting in line with relevant the Basic Technical Cyber Protection Controls.

1. **Patch Management**

**PASS - All OS and application store updates released within 7 days of the date of the audit were installed.**

**FAIL – Not all OS and application store updates released within 7 days of the date of the audit were installed.**

1. **Access Control**

**PASS -** User accounts were found to be protected by passwords or PINs.

**FAIL –** Some user accounts were found not to be protected by passwords or PINs.

# 7 Additional Information

## 7.1 Test 1 - External Vulnerability Scan for stated IP range

1. **Boundary Firewalls and Internet Gateways**

**PASS – No unnecessary open ports and services were found**

**[EVIDENCE]**

**FAIL - unnecessary open ports and services were found**

**[EVIDENCE]**

1. **Secure Configuration**

**PASS – No Weak credentials were found and no use of unsupported operating systems**

**[EVIDENCE]**

**FAIL - Weak credentials were found and /or unsupported operating systems**

**[EVIDENCE]**

1. **Patch Management**

**PASS – No vulnerabilities in unpatched services were found**

**[EVIDENCE]**

**FAIL - vulnerabilities in unpatched services were found**

**[EVIDENCE]**

## 7.2 Test 2 – Email Binaries and Payloads

1. **Malware Protection**

**PASS – User was prevented from accessing the Test Anti Virus (AV) attachments.**

**[EVIDENCE]**

**FAIL – User was not prevented from accessing the Test Anti Virus files by the Anti Virus Software**

**[EVIDENCE]**

1. **Secure Configuration**

**PASS – None of the attachments (including non AV files) were able to be run successfully.**

**[EVIDENCE]**

**FAIL – At least one of the attachments (including non AV files) was run successfully.**

**[EVIDENCE]**

**Technical issues [delete if no technical issues prevented the test]**

**FAIL - no email communications at all could be established during the test window. We ensured that your technical staff were given sufficient information to enable them to attempt to resolve the problem during the test.**

**[DETAIL THE INFORMATION GIVEN TO THE IT DEPARTMENT]**

## 7.3 Test 3 – Web site page with URLs linking to binaries

1. **Boundary Firewalls and Internet Gateways**

**PASS – None of the executable URL links allow a file to be downloaded (and run) successfully**

**[EVIDENCE]**

**FAIL – Some of the executable URL links allowed a file to be downloaded (and run) successfully**

**[EVIDENCE]**

1. **Malware Protection**

**PASS – None of the Anti Virus (AV) test files were able to be downloaded successfully. The user was blocked from accessing them.**

**[EVIDENCE]**

**FAIL - Some of the Anti Virus (AV) test files were able to be downloaded successfully. The user was not blocked from accessing them.**

**[EVIDENCE]**

1. **Secure Configuration**

**PASS – The Non-Anti Virus (AV) attachments were not able to be run successfully.**

**Action Point – The Non-Anti Virus (AV) attachments that were downloaded were able to be run successfully.**

**Technical issues [delete if no technical issues prevented the test]**

**FAIL - No web access was established during the test. We ensured that your technical staff were given sufficient information to enable them to attempt to resolve the problem during the test.**

**[DETAIL THE INFORMATION GIVEN TO THE IT DEPARTMENT]**

## 7.4 Test 4 – Authenticated vulnerability scan of host(s)

[Copy the following table for each device]

|  |
| --- |
| MACHINE NAME:  IP ADDRESS:  OS:  LOCATION:   1. **Patch Management**   **PASS - All patches that were released within 14 days of the date of the audit for any of the applications required applications were installed.**  **[EVIDENCE FOR ALL WITHIN SAMPLE SET]**  [Otherwise]  **Action Point – All patches that were released within 30 days of the date of the audit for any of the required applications were installed.**  **[EVIDENCE]**  **FAIL - Some patches that were released within 30 days of the date of the audit for any of the required applications were not installed.**  **[EVIDENCE]**  **FAIL - OS or any application is unsupported and no patches are available**  **[EVIDENCE]**   1. **Malware Protection**   **PASS - An AV solution is place the computer. AV definitions released within 7 days of the date of the audit installed and all AV engine updates were found to have been applied within a maximum of 90 days.**  **[DESCRIBE/EVIDENCE]**  **FAIL – An AV solution was not in place on one or more computers, or AV definitions released within 7 days of the date of the audit were not installed, or not all AV engine updates were found to have been applied within a maximum of 90 days.**  **[EVIDENCE]**   1. **Access Control**   **PASS - User accounts have been assigned to individuals rather than shared accounts and users do not have admin level access to change system settings and/or install software.**  **FAIL - User accounts have been shared amongst individuals or users do have admin level access to change system settings and/or install software.**  **[DESCRIBE/EVIDENCE]**   1. **Secure Configuration**   **PASS – The output from the build review tool inspections found only low risk issues**  **Action Point – The output from the build review tool inspections found some medium risk issues.**  **[DESCRIBE/EVIDENCE]**  **FAIL – The output from the build review tool inspections found one or more high risk issues.**  **[DESCRIBE/EVIDENCE]** |

7.5 Value added checks - internal

These tests do not form part of the Common Test Specification v1.2 however you have attested to complying with them in the questionnaire. They have been conducted on a random machine

Only passes and action points are awarded in this section.

|  |  |
| --- | --- |
| Test | Result |
| **Unnecessary User Accounts** | [No] unnecessary accounts were identified.  **Pass Action Point** |
| **Weak passwords & Password policy** | OSX Clients has a logical access policy which states:  Maximum Password Age = 30 Day s Expiration  Minimum Password Length = 10 Characters  Password History = Cannot reuse previous 10 passwords  Must contain at least 1 Alpha and 1 Numeric  Windows Client has a logical access policy which states:  Maximum Password Age = 60 Day s Expiration  Minimum Password Length = 10 Characters  Password History = Cannot reuse previous password  Password must meet complexity requirement  **Pass Action Point** |
| **Backup would appear to survive a ransomware attack** | **Pass Action Point** |
| **Unnecessary software** | All devices were found to have [no] Unnecessary software installed.  **Pass Action Point** |
| **Auto run feature Check** | All of the devices have auto run feature disabled as default.  **Pass Action Point** |

7.6 Value added checks – website (optional)

This does not form part of the *Common Test Specification v1.2* however it is useful to be aware of any critical findings on your main website.

[Detail critical findings only]

# 8 Summary of Failings, Action Points and Observations.

## 8.1 Failings

|  |  |  |
| --- | --- | --- |
| Vulnerability | Likely impact | Remediation notes |
| If the vulnerability was found using a scanner, please also put the CVE Code, description and CVSS rating.  Otherwise x-ref the area of the report and include a brief description |  |  |

## 8.2 Action Points

|  |  |  |
| --- | --- | --- |
| Vulnerability | Possible impact | Remediation notes |
| If the vulnerability was found using a scanner, please also put the CVE Code, description and CVSS rating.  Otherwise x-ref the area of the report and include a brief description |  |  |

## 8.3 Observations

|  |  |  |
| --- | --- | --- |
| Observation | Possible impact | Remediation notes |
| Describe any improvement opportunities encountered, such as:   * You may have been handed an out of date policy * You perhaps saw passwords written on desk pads   There may have been an unattended computer left logged in and accessible |  |  |

9 Conclusion