National Cyber Security Centre

CYBER ESSENTIALS

Cyber Essentials Plus: Illustrative Test Specification

VERSION 2.0

Contents

What's new 2
Audience 2
Purpose 3
Before you begin 3
Success criteria 3
Test results 3
Advisory Notes 4
External testing 5
Test Case 1: Remote vulnerability assessment 5
Internal testing 7
General prerequisites for internal testing 7
Coverage of internal testing 7
Test Case 3: Check malware protection on EUDs 9
Test Case 4: Check effectiveness of EUD defences against malware delivered by email 10
Test Case 5: Check EUD defences against malware delivered through a website 11
Conclude the assessment 12
Appendix A: Vulnerability scanning 13
Appendix B: Types of test file 13

This illustrative test specification exists to help Accreditation Bodies develop their own test specifications for their Certification Bodies to carry out **Cyber Essentials Plus** assessments.

The purpose of this illustration is to encourage a consistent approach, since Applicants should be able to expect the same certification outcome, no matter which Certification Body they ultimately use.

Throughout this illustration we address the Assessor directly, so that all task steps are as clear as possible. We also include some contextual notes for Accreditation Bodies.

What's new

We've reworked this information so that it is easier to understand and use. If you're familiar with the earlier PDF version (entitled 'Common Test Specification') you'll notice lots of changes in sense and structure.

Many statements are now clearer, to reduce ambiguity and potential for misinterpretation. Otherwise, there are few technical changes in this release. The main changes are:

- Aligned content with changes to the Requirements for IT Infrastructure 2017-02-06.
- Reworked throughout to make the flow of tasks clearer and simpler, and to make the interpretation of test results easier and more definite.
- Added contextual notes to help the Assessor understand the intent of this specification.
- Added contextual notes to help Accreditation Bodies understand the thinking behind this illustration, to inform their own design and procedures.
- Fixed the logic of the flow diagram (under current heading Sub-test 1.1) and aligned with the main text.
- Adjusted the CVSS v3 parameters (under the current Sub-test 2.1 heading).

Audience

This document is mostly aimed at personnel who actually conduct **Cyber Essentials Plus** assessments on behalf of Certification Bodies (the 'Assessor', or 'you').

It may also be of interest to the organisation seeking **Cyber Essentials Plus** certification (the 'Applicant') — staff involved in the process may wish to understand the test criteria that make up the assessment.

Purpose

The purpose of this test specification is to facilitate independent testing to check the Applicant's compliance with the technical requirements of the Cyber Essentials scheme, and to:

- ensure this has indeed resulted in adequate defences against the threats in scope
- detail the required tests, and the criteria for 'pass' or 'fail' in assessment for certification

You must agree the boundary of scope with the Applicant, before testing begins. Refer to Requirements for IT Infrastructure (Cyber Essentials scheme).

Before you begin

Before you start testing, you must ensure you have:

- obtained the appropriate written permission from the Applicant
- agreed the details of the system(s) to be tested, and when this testing will occur, with the Applicant
- the correct template for the report you will compile for the Applicant — the format of this report is set by your Accreditation Body

Success criteria

Test results

You must mark the outcome of **each** test case and sub-test with **one** of the following results:

- **Pass**:
  - Before you mark a test case with a Pass result, you must ensure that **every** sub-test in that test case also resulted in Pass — unless a special exception is stated in this test specification.
  - Similarly, before you mark the overall assessment with a Pass result (which would lead to **Cyber Essentials Plus** certification), you must ensure that **every** test case resulted in Pass**.**
- **Fail**:
  - If **any** sub-test within this test specification results in Fail then you must also mark the parent test case — and the overall assessment — Fail.
  - To be clear: Any single Fail means a Fail for the assessment as a whole — unless a special exception is stated in this test specification. In any case, you should

remain diligent and complete the assessment in full, to give the Applicant a complete appraisal.

Advisory Notes

You may include an Advisory Note with any result. Use these to inform the Applicant about relevant improvements they could easily make to improve cyber security, and to explain the rationale for particular test decisions.

External testing

Test Case 1: Remote vulnerability assessment

Test purpose

To test whether an Internet-based opportunist attacker can hack into the Applicant's system wth typical low-skill methods.

Test description

Prerequisites

You will need:

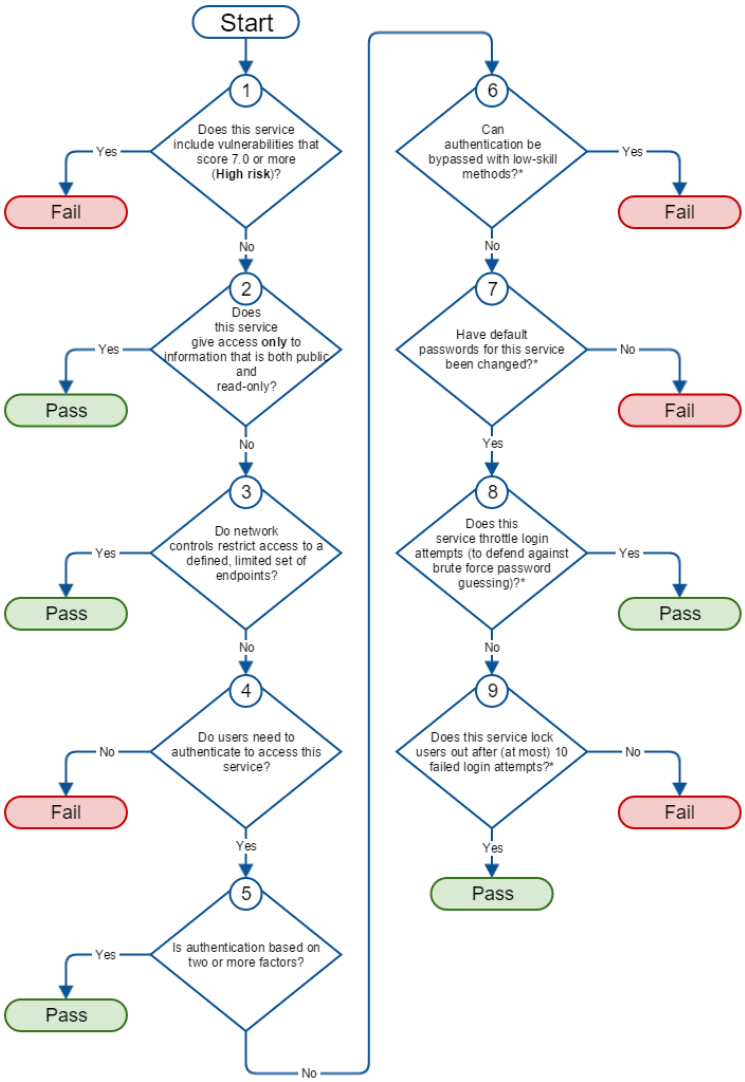
- a vulnerability scanning tool that has been approved by your Accreditation Body — see Appendix A: Vulnerability scanning
- to have identified the IP addresses to be scanned

Where dynamic IP addresses are in use for an Internet connection, the scope may be defined in terms of appropriate DNS entries.

Take care with such addresses to ensure services like carrier-grade NAT do not inadvertently send assessment traffic to the wrong destination.

Sub-test 1.1

1. Identify all of the IP addresses currently in use by the Applicant.
2. Scan all identified IP addresses, on the recommended set of TCP and UDP ports (see Appendix A: Vulnerability scanning).
3. For each Internet-accessible service you discover:
    1. Determine whether any known vulnerabilities exist.
    2. For each vulnerability you find, assess and score the level of risk using the **CVSS v3** standard.
    3. Use the flow diagram and notes below to determine whether to record a Pass or Fail result for the service.



Sub-test flow diagram for assessing services accessible through the firewall.

*6: Low-skill methods for bypassing authentication mechanisms include, for example:

- identifying parameters such as authenticated=true in query strings
- exploiting well-known weaknesses in exposed applications.

*7, *8 and *9: You can check for default passwords and for password throttling/lockout policy by inspecting the relevant configuration for the service, or by practical testing.

Interpreting the test case results

If you determine a Pass result for **every** service tested under Sub-test 1.1, then record a Pass result for this test case. Otherwise, record a Fail result.

Internal testing

These tests assess defence against attacks which originate externally but involve some form of internal user action, or which are difficult to test directly from the Internet.

Internal testing is comprised of four test cases, numbered 2 through 5.

General prerequisites for internal testing

You will need:

- to be able to send arbitrary emails to an account operated by the Applicant — that is, you need an external email system that performs no filtering and is not blacklisted
- test files, hosted on an external website owned by the Certification Body (see Appendix B: Types of test file) — you may need to have the Applicant arrange access to this site, perhaps adding it to their whitelist
- suitable credentials to perform the tests
- working email clients (and associated email addresses) and web browsers on a sample of the end user devices in scope

Coverage of internal testing

General principles

Internal testing applies to all computing devices within the boundary of scope. This includes:

- end user devices (EUDs) such as desktops, tablets, laptops, and smartphones which can connect to internal resources
- servers on which standard (that is, non-administrator) users can obtain an interactive desktop environment

On all but the smallest networks it will be impractical to test every device that is within the agreed boundary of scope. Instead, test a representative sample — but take steps to ensure you can be confident that your sample of devices (including servers and EUDs) is actually representative.

- Many organisations use standardised configurations for their servers and EUDs. In such cases, much of the organisation's equipment can be covered by a small number of representative samples.
- We recommend that you aim to satisfy yourself that, in total, your testing is representative of at least 90% of all the devices in scope. The actual number of representative devices you will need to test to achieve this level of confidence will depend on the amount of variation that exists as a result of the Applicant's particular provisioning processes, and their effectiveness.

Test Case 2: Check patching, by authenticated vulnerability scan of devices

Test purpose

Identify missing patches and security updates that leave vulnerabilities that threats within the scope of the scheme could easily exploit.

Test description

Prerequisites

In addition to the general prerequisites for internal testing, you will need:

- a vulnerability scanning tool that has been approved by your Accreditation Body — see Appendix A: Vulnerability scanning

Sub-test 2.1

For each device to be tested, scan with the approved vulnerability scanning tool.

Using the output of the scan, identify vulnerabilities that are **high risk** or **security critical,** as defined by the following **CVSS v3** parameters:

- attack vector: **network** only
- attack complexity: **low** only
- privileges required: **none** only
- user interaction: **none** only
- exploit code maturity: **functional** or **high**
- report confidence: **confirmed** or **high**

If there are any vulnerabilities which meet the above criteria, **and** for which the vendor-provided patch has been available for more than 14 days prior to testing, record a Fail result for the sub-test. Otherwise, record a Pass result.

The idea here is to assess each vulnerability in context and try to determine if an Internet-based attacker really could exploit it and harm the Applicant.

You may determine that other mitigations for an unpatched vulnerability (such as virtual patching or aggressive sandboxing) are less than ideal, but still adequate for a Pass result.

Interpreting the test case results

If you determine a Pass result for **all** sub-tests, then record a Pass result for this test case. Otherwise, record a Fail result.

Test Case 3: Check malware protection on EUDs

Test purpose

To check that all of the EUDs in scope benefit from at least a basic level of malware protection.

Test description

Prerequisites

Identify what type of malware protection each EUD in the sample set uses — antivirus software, application whitelisting or application sandboxing.

Selecting appropriate sub-tests

Perform the following sub-tests as appropriate for the form of malware protection in use.

Sub-test 3.1 (for EUDs that use antivirus software)

For each EUD in the sample set, check that:

- all antivirus definitions released within the 24 hours prior to testing have been installed
- all antivirus engine updates released within the 30 days prior to testing have been installed

If **both** of these are true, record a Pass result for this sub-test. Otherwise, record a Fail result.

Sub-test 3.2 (for EUDs that use certificate-based application whitelisting)

For each EUD in the sample set, check that:

- the list of trusted root certificates is the standard set as provided by the operating system manufacturer, or a subset thereof
- additional trusted root certificates are added only with the Applicant's explicit agreement
- an unsigned executable, and an executable signed with a certificate that does not chain to a trusted certificate, will not execute on the EUD
- operating system policy settings are appropriate to ensure code signing applies to all executable file formats, as applicable to the EUD

If **all** of these are true, record a Pass result for this sub-test. Otherwise, record a Fail result.

Sub-test 3.3 (for EUDs that use application sandboxing)

For each EUD in the sample set, check that:

- application sandboxing is operational and applies to all user-installed applications

If this is true, record a Pass result for this sub-test. Otherwise, record a Fail result.

Interpreting the test case results

If you determine a Pass result for **all** sub-tests, then record a Pass result for this test case. Otherwise, record a Fail result.

Test Case 4: Check effectiveness of EUD defences against malware delivered by email

Test purpose

To test whether or not EUDs are protected against malware that is delivered via email attachments.

Test description

Prerequisites

See the general prerequisites for internal testing, and especially note Appendix B: Types of test file.

Sub-test 4.1

For each EUD in the sample set:

1. Establish a baseline by sending a simple email from your remote test account, with no attachments. Using the EUD, verify that this email arrives successfully at the test destination.
2. Determine what types of file you should test for and ready your test emails. You'll need one email for every type of file to be tested, given that you'll attach one test file to each email.
3. Attempt to send each test email from your remote test account to the test destination. Using the EUD, attempt to open each attached test file. Note the result.

If any of the malware test files arrive successfully **and** the user is **not** blocked from accessing them then record a Fail result for this sub-test.

If any of the executable test files arrive successfully **and** can be executed without a warning and prompt for the user to decide whether or not to proceed then record a Fail result for this sub-test.

Otherwise, record a Pass result for this sub-test.

Interpreting the test case results

If you determine a Pass result for **all** sub-tests, then record a Pass result for this test case. Otherwise, record a Fail result.

Test Case 5: Check EUD defences against malware delivered through a website

Test purpose

To test whether or not EUDs have protection from malware delivered through a website.

Test description

Prerequisites

See the general prerequisites for internal testing, and especially note Appendix B: Types of test file.

Also, have the Applicant configure the web content filter to provide an amount of filtering for the approved external website that is representative of the filtering performed with most other allowed sites (that is, those that are not specifically blacklisted).

The rationale for this approach is based on the assumption that there probably is a whitelisted site from which files can be downloaded, *somewhere*. Testing for **Cyber Essentials Plus** simulates this by using the approved external website.

Sub-test 5.1

For each EUD in the sample set:

1. Log on with the normal user credentials provided.
2. Using a web browser installed on the EUD, check that you can access the Internet.
3. For **every** web browser installed on the EUD:
    1. Browse to the approved test files and attempt to download and open each in turn.

If any of the malware test files are downloaded successfully **and** the user is **not** blocked from accessing them then record a Fail result for this sub-test.

If any of the executable test files are downloaded successfully **and** can be executed without without a warning and prompt for the user to decide whether or not to proceed then record a Fail result for this sub-test.

Otherwise, record a Pass result for this sub-test.

Interpreting the test case results

If you determine a Pass result for **all** sub-tests, then record a Pass result for this test case. Otherwise, record a Fail result.

Conclude the assessment

Once all tests above have been completed, compile your report.

It may be that you cannot conclude on the appointed day, perhaps because of some particular technical difficulties with testing. In this case, consult with your Accreditation Body — at their discretion, you may defer tests and arrange to complete them at a later date.

Note for Accreditation Bodies

We recommend that you do not allow tests to be deferred for more than one month.

Example

For some temporary reason you cannot obtain the test files you need for Test Case 3: Check existence of malware protection on EUDs. Without these files you cannot complete the sub-tests and confirm either a Pass or a Fail result. So, you should revisit when you can obtain the files and complete the test. Then you can mark with a Pass or Fail result, as appropriate.

If you determine a Pass result for **all** test cases then the Applicant passes the overall assessment and you may proceed to award a **Cyber Essentials Plus** certificate.

If you determine a Fail result for **any** test cases, but these failures result from only a **small** number of minor issues then consult with your Accreditation Body. At their discretion, the Applicant may still pass the overall assessment and then you may proceed to award a **Cyber Essentials Plus** certificate.

Note for Accreditation Bodies

We expect this exception to cover situations where:

1. Only marginal deviation from the standard is found, in less than 5% of performed tests.

2. The evidence does not indicate a wider failure of the Applicant's cyber security processes.

Otherwise, the Applicant fails the overall assessment and you will not award a certificate.

Appendix A: Vulnerability scanning

The most common Internet services are also the most likely to be probed by low-skilled Internet-based attackers. So, the aim of vulnerability scanning for **Cyber Essentials Plus** is to find and review the security of all such services in use by the Applicant.

- Use the vulnerability scanning tool(s) that your Accreditation Body has approved for use in **Cyber Essentials Plus** tests. For information on good practices with such tools see PCI Approved Scanning Vendors Program Guide.
- Scan all IP addresses associated with the Applicant. Rather than scanning all ports associated with all IP addresses, you may scan a more limited range specified by your Accreditation Body.

  Note for Accreditation Bodies

  We suggest you provide a list of TCP and UDP ports that the Assessor should scan. For a good starting point, see nmap.org's Well Known Port List: nmap services.

Appendix B: Types of test file

Your Accreditation Body is responsible for providing a comprehensive set of test files to your Certification Body.

Your Certification Body is responsible for defining and hosting a sub-set for you to test with, appropriate to the particular Applicant. Check with your Certification Body to ensure you will obtain the correct files for each test.

For test result criteria, we distinguish between two broad groups of test files:

- malware test files — anti-malware should detect these and block the user from accessing them
- executable test files — the user should at least see a warning and a prompt that allows them to decide whether or not to proceed

Note for Accreditation Bodies

You must provide the Certification Body with a set of test files that are representative of all the file types that Applicants are likely to encounter, in advance.

You should also encourage the Certification Body to tailor the sub-set of test files that the Assessor will actually use, to suit each Applicant. Each sub-set should reflect the applications and platforms that the particular Applicant is using.

For example, if the Applicant uses only OS X devices then the sub-set need not cover Windows-specific file types. Or, if the Applicant uses a mixed environment then the sub-set should cover a suitably wider set of file types.

The full set of representative test files you provide must include:

- container formats (such as .zip and .gz) which the Applicant's environment is able to process
- a range of file types that are executable by default on common platforms — both native binaries and scripting languages
- files of types which users might regularly receive — such as documents and spreadsheets — but which contain inert malware samples

Also note that:

- executable test files should launch obvious behaviour (such as launching a web browser to a known page, or creating an onscreen dialog) so that the Assessor can detect execution quickly and easily
- malware samples should be specific inert files that are known to be flagged by the majority of common antivirus solutions