National Cyber Security Centre
a part of GCHQ

CYBER ESSENTIALS PLUS

Cyber Essentials Plus: Illustrative Test Specification v3.1

April 2023

Contents

What's new

- Added all internally hosted servers to the Sample Testing section
- Updated the sub-test 2.1 criteria to CVSS base score of 7 or above
- Previous tests 4 & 5 removed and included in updated Test 3
- Malware Protection tests updated to align with changes to the technical requirements

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).

This illustrative test specification exists to help the Cyber Essentials Delivery Partner 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 the Delivery Partner.

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 the Delivery Partner

General prerequisites for testing

You will need the following prerequisites for tests 2 to 7:

- 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 deny listed

- 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 allow list
- users with appropriate 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

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 subtest 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.

Test Case 1: Remote vulnerability assessment

Test purpose

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

Test description

Prerequisites

You will need:

- a vulnerability scanning tool that has been approved by the Delivery Partner — 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. This must include IaaS where used.
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 use the flow diagram and notes below to determine whether to record a Pass or Fail result for the service.

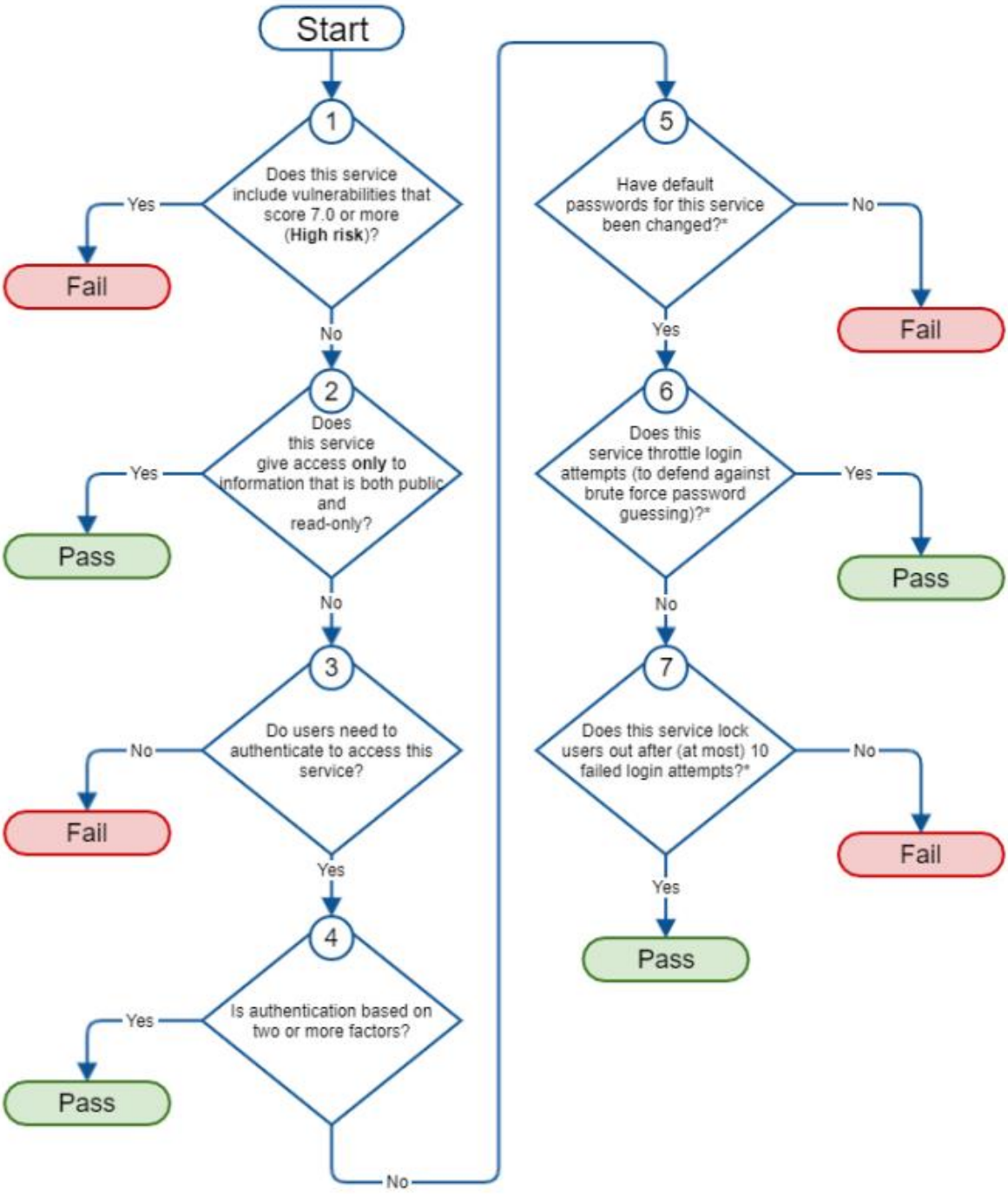

Figure 1: Sub-test flow diagram for assessing services accessible through the firewall.

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.

Sample Testing

The remaining tests apply to all computing devices within the boundary of scope. This includes:

- end user devices (EUDs) that can connect to organisational data or services
- all internally hosted servers
- all types of cloud service (IaaS, Paas, or SaaS)

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, 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 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.

All cloud services must be tested using a representative sample of user accounts. This must consist of at least one normal user and one administrative user for every cloud service used. The same users can be used across multiple cloud services.

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

Perform this test on sampled EUD, servers and IaaS instances.

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 testing, you will need:

- a vulnerability scanning tool that has been approved by the Delivery Partner — 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 meet any of the three following criteria:

- Described by the vendor as ‘critical’ or ‘high risk’
- Has a CVSS v3 base score of 7 or above
- There are no details of the level of vulnerabilities the update fixes provided by the vendor

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.

Virtual patching is not an acceptable mitigation to the security vulnerabilities of legacy unsupported operating systems long term and so will not be recognised as a mechanism for compliance with Cyber Essential requirements.

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

Perform this test on sampled EUD, servers that provide a user-interactive desktop and IaaS instances.

Test purpose

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

Test description

Prerequisites

Identify what type of malware protection each device in the sample set uses (anti-malware software or application allow listing).

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

Selecting appropriate sub-tests

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

Sub-test 3.1 (for devices that use anti-malware software)

For each device in the sample set, check that the anti-malware software is installed, operational and updated in accordance with vendors instructions.

Depending on the software being used, the assessor will determine whether to test the requirement using test files as described in sub-tests 3.1.1, 3.1.2 and the manual check in sub-test 3.1.3 or through manual checks as described in sub-test 3.1.4.

Sub-test 3.1.1 (Check effectiveness of defences against malware delivered by email)

Perform this test on any sampled device or service where a user can receive email.

For each user environment in the sample set:

1. Establish a baseline by sending a simple email from your remote test account, with no attachments. Observe the user to 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. Observe the user attempting 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.

If any of the executable test files arrive successfully **and** can be executed without a prompt that requires additional user interaction then record a Fail.

Otherwise, record a Pass result for this sub-test

Sub-test 3.1.2 (Check effectiveness of defences against malware delivered by browser)

Perform this test on any sampled device or service where a user can browse the web.

The applicant should 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 deny listed).

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

1. Determine the appropriate test files for the Operating System that you are testing;
2. Observe the user access the internet, if they are prevented from accessing the internet record a Pass for this sub-test;
3. Observe the user attempting to download approved test files, if the user is prevented from downloading the approved test files, record a Pass;
4. If the test files are blocked on access record a Pass;

If any of the malware test files download successfully **and** the user is **not** blocked from accessing them record a Fail.

If any of the executable test files download successfully **and** can be executed without a prompt that requires additional user interaction record a Fail.

Sub-test 3.1.3 (Check that the anti-malware software is updated)

The following manual check must take place on all sampled EUD, servers that provide a user-interactive desktop and IaaS instances that use anti-malware software.

- the anti-malware software is updated in accordance with the vendors configuration instructions.

If the check is carried out and confirms the anti-malware software is updated in accordance with the vendors instructions record a Pass for this sub-test, if not record a Fail.

Sub-test 3.1.4 (Manual Checks for devices that use anti-malware software)

The following manual checks must take place on all sampled EUD, servers that provide a user-interactive desktop and IaaS instances that use anti-malware software and the tests files were not used to prove that the software was installed and operational.

- the anti-malware software is installed and operational through investigation of logs.

and

- the anti-malware software is updated in accordance with the vendors configuration instructions.

If both checks are carried out and confirm the anti-malware software is installed, operational and updated in accordance with the vendors instructions record a Pass for this sub-test, if not record a Fail.

Sub-test 3.2 (for devices that use certificate-based application allow listing)

For each device 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 device
- operating system policy settings are appropriate to ensure code signing applies to all executable file formats, as applicable to the device

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

Interpreting the test case results

If you record a Fail for sub-test 3.1 or 3.2 where devices use the corresponding method of anti-malware protection record a Fail for this test case, otherwise record a Pass.

Test case 4: Check Multi-factor authentication configuration

Perform this test on all cloud services.

Test Purpose

To test cloud services declared in scope have been configured for multi factor authentication (MFA).

Test Description

Users of sampled devices to attempt to log into the organisations cloud services using their organisation issued accounts.

All cloud services to be tested for User and Administrator Access. Where multiple cloud services share an authentication service this test only needs to be performed once for each authentication service.

Test Case 4.1

1. Assessor to observe users accessing cloud services using their organisation issued accounts on an untrusted device or from an incognito browser session.
2. If test 1 is not possible, the assessor should share an incognito browser session from their device and then observe the user accessing the cloud services.
3. Repeat the test for each authentication service in use.

If the test results in the user or administrator being prompted for a form of MFA before access is granted, then award a Pass. Otherwise, record a Fail.

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 account separation

Perform this test on any sampled EUD, servers that provide a user-interactive desktop and cloud environments where administrative processes can run.

Test Purpose

To test user accounts don't have administrator privileges assigned.

Test Description

When logged in with a standard user account, they attempt to run a defined administrative process.

All sampled devices need to be tested.

Test case 5.1

1. Observe a user attempting to run an administration process for the particular sampled operating systems with the current logged in account.
2. Repeat the test on every sampled device in the audit.

If the test results in the user being prompted for an additional login and the process does not run using the user account details, then award a Pass. Otherwise, award a Fail.

Interpreting the test case results

If you determine a Pass result for all sub-tests across all sampled devices, 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 the Delivery Partner — at their discretion, you may defer tests and arrange to complete them at a later date.

Note for Delivery Partner

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

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 the Delivery Partner. 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 Delivery Partner

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 the Delivery Partner 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 the Delivery Partner.

Note for Delivery Partner

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

The Delivery Partner 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 Delivery Partner

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