CREST Cyber Essentials Scheme

Test Specification

Version Control

Version	Date	Description	Released by
1.0	12/6/2014	Initial Release to Certification Bodies (CBs)	CREST
2.0	09/01/2015	Updated: Internal Systems Test details No.4)	CREST
2.1	05/10/2017	Draft update to NCSC specifications	CREST
2.2	12/12/2017	Update from review comments issued to CBs for review	CREST
2.3	05/01/2018	Update from CB comments	CREST
3.0	06/02/2018	Release to CBs	CREST
4.0	25.01.2019	Update to application patching list	CREST

Note. It is the responsibility of Certification Bodies to ensure they perform Cyber Essentials assessments using the current CREST version of the Test Specification. Old versions of the Test Specification may only be used for up to 28 days following the release of an updated version.

Contents

Audience

This document is provided by CREST for Certifying Bodies (CBs) operating under the CREST Accreditation Body (AB) Cyber Essentials (CE) and Cyber Essentials Plus (CE+) schemes.

The main focus is for CBs and their assessors, though it is understood that organisations (Applicants) considering being certified may also wish to understand the criteria. Applicants requesting this type of information should in the first instance be directed to the NCSC illustrative test specification: https://www.ncsc.gov.uk/content/files/protected_files/document_files/Cyber_Essentials_PLUS_Illustrative_Test_Spec.pdf

Scope

The scope must be agreed via written permission from the applicant before the test begins. Permission to test without violating the Computer Misuse Act can only be provided by the physical system owner so any project targeting shared systems must be only performed with the express written permission of the third party. This may include third party Internet facing hosted and cloud platforms where they are used to provide critical business functions. This criteria will only apply to dedicated platforms in most cases but shared platforms may also be included by prior discussion with the testing organisation where deemed suitable and permission obtained. When considering the appropriate scope for a test it is advisable to make a list of critical Internet accessible systems from a business perspective and to use this to inform the scoping process.

The scope sets out to cover three critical areas of interest for Cyber Essentials.

1) External Internet accessible systems, including dedicated hosting platforms
2) Internal Systems – Workstations
3) Internal Systems – Mobile devices including tablets

Bring Your Own Device (BYOD) platforms are included within the scope of the test however they are unlikely to be subject to a suitable sampling arrangement as most will have unique configurations. It is the responsibility of the organisation purchasing the test to ensure that suitable written permission has been obtained from all asset owners – this is often done by adding a clause to corporate IT policies and to staff terms and conditions – suitable legal and HR advice should be sought in advance by the organisation purchasing the test.

Mobile device audits (including tablets) will be limited to common functionality and a manual review of software patch levels where appropriate until such time that readily available tools become available to allow a similar level of assessment to that of the desktop.

Wireless networks and attacks against them are excluded from the scope of the audit however this does not exclude testing of devices that make use of a wireless network as a transport layer.

It is acceptable for organisations to specify a limited scope for a test provided robust network segregation / boundary (e.g. a firewall) is in place. In such scenario each remote network should be treated as another untrusted network segment and subject to the same set of tests used for external Internet connections. Where gateways do not make use of NAT connections the IP space to be scanned will be the whole internal IP space of the secure network under review.

Where IPv6 networking is in use (including tunnelling over IPv4) within an organisation this should be included within the scope of an audit.

Where Dynamic IP addresses are in use for the Internet connection, appropriate DNS entries may be defined as the scope and then verified on the day of the testing by the test analyst. Care should be taken with such addresses to ensure services like Carrier Grade NAT (CGNAT) do not inadvertently send audit traffic to the wrong subscriber.

This document details the tests that are required for each element of the system and to provide a means by which to determine whether a pass or fail should be awarded.

Assumptions

It is assumed that organisations are an appropriate size, scale and IT complexity level for an audit within the scope of Cyber Essentials.

The Cyber Essentials test is recommended for organisations looking for a base level Cyber security test where IT is a business enabler rather than a core deliverable. It is mainly applicable where IT systems are primarily based on Common-Off-The-Shelf (COTS) products rather than large, heavily customised, complex solutions.

The aim of the testing is to identify opportunistically 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. 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 specifically not suitable for organisations that may be the target of Advanced Persistent Threat (APT) style attacks.

Only vulnerability analysis and verification rather than full penetration testing is required. Limited exploitation may be included to remove false positive findings following vulnerability scanning.

Complex Application Testing (both thick client and web applications) is beyond the scope of the engagement. Basic web application scanning for common vulnerabilities (notably injection attacks) is included from an unauthenticated user perspective to reflect the common level of capability seen. Database audits and reviews (other than trivial credential checks) are beyond the scope of the engagement. Where more complex services are required these should be delivered as part of a full penetration test, this specification does not prevent suppliers offering to deliver these additional services alongside a Cyber Essentials test.

Where a host has multiple browsers installed, all must be tested.

Denial of Service (DoS) attacks in all forms are specifically excluded from the scope of the Cyber Essentials test.

The final report to the customer MUST be delivered using the Cyber Essentials reporting template as provided by CREST in order to maximise consistency between CBs.

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 a 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.

The assessment must be completed in full, to give the Applicant a complete appraisal and indication of the state of their system.

You may include an Action Point (AP) 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. APs do not affect the overall test result and are provided as information or actions the Applicant can choose to take should they wish to.

External systems

Required tests

The following tests cases are required

1) Vulnerability scan for stated IP range including website scanning;

Test Details

Test	Description	Results
1)	**Vulnerability scan for stated IP range** Using an appropriate industry standard vulnerability scanner that has been approved by CREST, scan the external IP range for all IP addresses within the specified ranges. Note this should also include IPv6 addresses where they are in use. Ensure scans include a full (all 65535 ports) TCP port scan for all IP addresses within the specified ranges. Note this should also include IPv6 addresses where they are in use though only for specified and provided addresses. Ensure scans include a scan for known common UDP services for all IP addresses within the specified ranges. Note this should also include IPv6 addresses where they are in use. Basic web application scanning for common vulnerabilities (notably injection attacks) should be performed from an unauthenticated user perspective. Application testing should be performed in line with the requirements as defined in the Appendix to this document. All risks identified should be scored using the CVSSv3 standard and defined by the following 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** Low risk issues are defined as a score from 0.0 to 3.9 and should not be 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 the obtaining of some piece of specific information enumerated from the system but that could not actually be directly exploited. High risks are defined as a score between 7.0 and 10.0 and will usually be associated with direct compromise of a system or application for the extraction of production data, system passwords or the introduction of malware.	Result: **Boundary Firewalls and Internet Gateways** **Secure Configuration** **Patch Management**

Test	Description	Results
	Where older vulnerabilities are reported by scanning products in v2 then the CB should apply the v3 parameters to check the result. **Reporting:** Results within this section should be 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** 2. **Secure Configuration** 3. **Patch Management** **Interpreting Results:** For identified services use the flow chart in Figure 1 (below) to determine whether to record a “pass” or “fail”. For item 6 within the flow chart 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. For items 7, 8 and 9 then the common username and password list in the appendix should be used and checking of configurations or manual testing for throttling/lockout should be performed. Where vulnerabilities are identified award a “pass” status if only low risk issues are returned. Award an “Action Point” status if the highest risk issues returned are medium. Award a “fail” status if there are any vulnerabilities which meet the CVSSv3 marking criteria (above), and for which the vendor-provided patch has been available for more than 14 days prior to testing. The issues (medium and above) identified should be included in the additional information sections of the report. If you determine a Pass result for every service identified then record a Pass result for this test case. Otherwise, record a Fail result. **Categorisation:** The high level categorisation of issues is described below but the precise classification will not affect the pass/fail result of the audit and is instead provided as clarification for the customer. **Boundary Firewalls and Internet Gateways** Unnecessary open ports and services **Secure Configuration** Weak credentials Poorly implemented web applications Use of unsupported operating systems	

Test	Description	Results
	Patch Management Vulnerabilities in unpatched services	

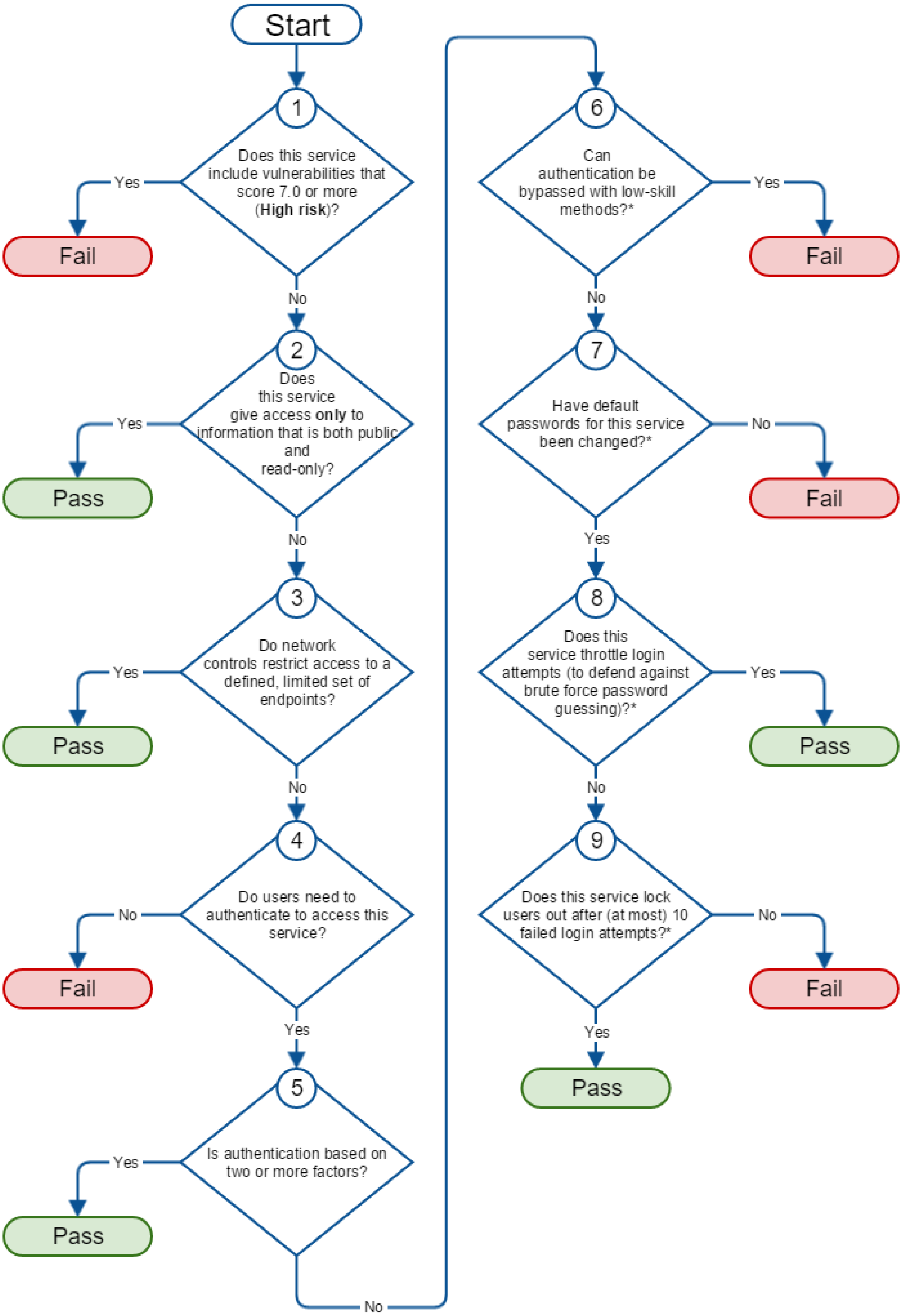

Figure 1 - External Services Flow Chart

Internal systems

Tester pre-requisites

- Access to an End User Device (EUD)
- Access to an external mail system that is not blacklisted and that performs no filtering;
- Access to an Internet host listening on the predefined set of egress test ports;
- Access to test binaries and payloads provided by the AB or CB;
- Details of a target e-mail account per platform being assessed.

Required tests

The following test cases are required

2) Inbound email binaries and payloads
3) Web site page with URLs linking to binaries
4) Authenticated vulnerability scan of host

Test Details

Test	Description	Results
2)	**Inbound email binaries and payloads** For validation purposes send an initial email which has no attachments and check that it arrives successfully at the destination. If the validation test is successful: Using your remote test account and desktop/laptop system provided by the customer, attempt to send multiple emails in from your remote test account, each email containing one of the test files from the provided test set. If the validation test is not successful attempt to troubleshoot with the organisation considering whether the sending address should be added to protection devices or services to facilitate the assessment. **Reporting:** Results within this section should be split in to two areas for the purposes of reporting in line with relevant the Basic Technical Cyber Protection Controls. **1. Malware Protection** **2. Secure Configuration** **Interpreting Results:** If any of the AV test attachments arrive successfully and the user is not blocked from accessing them then record a “Fail” status for “Malware Protection”, otherwise record a “Pass” for this element	Result : **Malware Protection** **Secure Configuration**

Test	Description	Results
	If any of the binary attachments can be run successfully and provide an alert warning of successful execution then record a “Fail” status for “Secure Configuration”, otherwise record a “Pass” for this element. If no email communications at all can be established during the test window (and the client does use email communication) then record a “Fail” status for both elements of this test. Ensure customer’s technical staff are given sufficient information to enable them to attempt to resolve the problem during the test.	
3)	**Web site page with URLs linking to binaries** The applicant must configure any web content filter to provide an amount of filtering representative of other allowed sites (those that are not specifically blacklisted. This approach simulates the fact that there is a whitelisted site somewhere from which files can be downloaded. For every web browser installed on the EUD browse to the Cyber Essentials test page or your local CB copy of this page. Attempt to download and open each of the approved set of test binaries in turn. **Reporting:** Results within this section should be 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** **2. Malware Protection** **3. Secure Configuration** **Interpreting Results:** If any of the executable URL links allow a file to be downloaded and run successfully and provide an alert warning of successful execution then record a “Fail” status for “Boundary Firewalls and Internet Gateways”, otherwise record a “Pass” for this element. If any of the AV test files can be downloaded successfully and the user is not blocked from accessing them then record a “Fail” status for “Malware Protection”, otherwise record a “Pass” for this element. If any of the non AV attachments can be run successfully and provide an alert warning of successful execution then record an “Fail” status for “Secure Configuration”, otherwise record a “Pass” for this element.	Result : **Boundary Firewalls and Internet Gateways** **Malware Protection** **Secure Configuration**

<table>
<tr><th>Test</th><th>Description</th><th>Results</th></tr>
<tr><td></td><td>If no web access at all can be established during the test window then record a “Fail” status for both elements of this test. Ensure customer’s technical staff are given sufficient information to enable them to attempt to resolve the problem during the test.</td><td></td></tr>
<tr><td>4)</td><td>Authenticated vulnerability scan of host

Using an appropriate industry standard workstation build review tool that has been approved by the CREST AB, perform an admin level scan of the host including local checks for each host within sample set.

Ensure scans include a patch check for operating system updates.

Ensure scans include a patch check for the following applications
1. Oracle Java
2. Adobe Acrobat
3. Microsoft Office
4. Adobe Flash
5. Mozilla Firefox
6. Google Chrome
7. Opera
8. Microsoft Internet Explorer
9. Microsoft Edge
10. Microsoft Skype for Business

Ensure scans include a check of any AV solution in use.

All risks identified should be scored using the CVSSv3 standard and defined by the following 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

Award a “fail” status if there are any vulnerabilities which meet the CVSSv3 marking criteria (above), and for which the vendor-provided patch has been available for more than 14 days prior to testing.

Low risk issues are defined as a score from 0.0 to 3.9 and should not be 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.</td><td>Result :

Patch Management

Malware Protection

Access Control

Secure Configuration</td></tr>
</table>

<table>
<tr><th>Test</th><th>Description</th><th>Results</th></tr>
<tr><td></td><td>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.
Where older vulnerabilities are reported by scanning products in v2 then the CB should apply the v3 parameters to check the result.

Identify the type of malware protection the EUD is utilising; antivirus software, application whitelisting or application sandboxing. Then in conjunction with the requesting organisation and the responses on the questionnaire choose the sub test which is most appropriate:

4.1 Antivirus Software
Check the date of update for both the definitions and the antivirus engine.

4.2 Application Whitelisting
Certificate based:
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
Execution arbiter:
An executable which is not in the execution arbiter whitelist will not execute
An executable blacklisted on the host does not execute if copied to an alternate user accessible directory
Whitelisted executables are not the whole operating system and are applications required by users.
4.3 Application Sandboxing
Application sandboxing is operational and applies to all applications
Reporting:

Results within this section should be split in to four areas for the purposes of reporting in line with relevant the Basic Technical Cyber Protection Controls.
Patch Management
Malware Protection
Access Control
Secure Configuration</td><td></td></tr>
</table>

Test	Description	Results
	Interpreting Results: **Patch Management:** Where missing patches are identified award a "pass" status if only low risk issues are returned. Award an "Action Point" status if the highest risk issues returned are medium. Award a "fail" status if there are any vulnerabilities which meet the CVSSv3 marking criteria (above), and for which the vendor-provided patch has been available for more than 14 days prior to testing. If the OS or any application is unsupported and no patches are available then award a "Fail". For an "Action Point" or "Fail" status the issues identified should be included in the additional information sections of the report. **Malware Protection** **4.1 Antivirus Software** An AV solution must be in place and all AV definitions released within 24 hours of the date of the audit should be installed. Any AV engine updates should be applied within a maximum of 30 days. If both of these are true, award a "Pass", otherwise award a "Fail". **4.2 Application Whitelisting** **Certificate** The trusted root certificates are as standard and any additional ones are known and approved by the applicant. Neither of the executables (unsigned, not in chain) execute Policy settings are in place for all executable types applicable to the EUD. If all of the above is true award a "Pass", otherwise award a "Fail". **Execution Arbiter** The non-whitelisted and copied executables fail to execute. The applicant can provide a list of whitelisted executables and applications. Attempts to execute common operating system functions which the user does not require are blocked. If all of the above is true award a "Pass", otherwise award a "Fail". **4.3 Application Sandboxing** All applications operate within a Sandbox and do not provide the user with an option to bypass. If all of the above is true award a "Pass", otherwise award a "Fail". **Access Control** User accounts should be assigned to individuals rather than shared accounts and users should not have admin level access to change system settings and/or install software. If this is true, award a "Pass", otherwise award a "Fail".	

Test	Description	Results
	Secure Configuration Review the output from the build review tool and award a “pass” status if only low risk issues are returned. Award an “Action Point” status if the highest risk issues returned are medium. Award a “fail” status if there are any vulnerabilities which meet the CVSSv3 marking criteria (above), and for which the vendor-provided patch has been available for more than 14 days prior to testing. The issues (medium and above) identified should be included in the additional information sections of the report. **Mobile Devices** Where there is a requirement to audit a mobile device such as a tablet or phone, then only the following platforms are supported and their specific rules should be applied. **Microsoft Surface Tablet Pro** Treat as a standard workstation and apply the rules above. **Microsoft Surface Tablet** **Apple iOS on IPhone or iPad** **Android on Phone or Tablet** **Patch Management** All OS and application store updates released within 14 days of the date of the audit should be installed. If this is true, award a “Pass”, otherwise award a “Fail”. **Access Control** User accounts should be protected by passwords or PINs. If this is true, award a “Pass”, otherwise award a “Fail”.	

Appendix 1 - Tool requirements

Vulnerability scanners

Platforms used to perform scanning must already be approved by PCI for ASV scanning prior to being put forwards for accreditation for the Cyber Essentials scheme. This is to ensure consistency with existing standards but to allow enhancements to be applied where appropriate.

Tools must be able to perform a TCP SYN or FULL CONNECT scan across all 65535 TCP ports for each IP address under review.

Tools must be able to perform a UDP scan across all the first 1024 UDP ports for each IP address under review.

Tools must be able to perform a UDP service scan on commonly used UDP ports. Specifically TFTP, SNMP and NTP ports must be checked due to their common weaknesses.

It is permissible and preferable for scanned ports to be performed in any order.

Vulnerability scanners must be able to identify the following classes of issues:

- Open ports with service identification
- Weak credentials (as defined in the weak credentials list) for the following protocols (and their SSL/TLS variants)
    - SMTP, POP3, IMAP, ActiveSync
    - SSH, TELNET, SMB, LDAP
    - FTP, HTTP
    - SNMP, VNC, RDP, Citrix ICA/CAG
    - VPN including but not limited to SSL, PPTP, OpenVPN, IPSEC
    - MYSQL, MSSQL, POSTGRES, ORACLE
    - Other authenticated services that may allow host compromise or exfiltration of data
- Application level weaknesses within visible services.

Where possible false positives should be removed from reports during the internal review stage and findings with minimal real world risk for a non-targeted attack against the organisation under review should also be removed.

The intent for all Cyber Essentials reporting is to provide customers with meaningful information regarding practical risks to their business and its activities – as such, reporting SSL/TLS issues should only be done by exception when a clear and significant business risk has been identified.

The following tests cases are required for any web applications identified. Note – test cases should only be performed WITHOUT authentication credentials.

- SQL Injection
- Command Injection
- Forced browsing to bypass authentication
- Injection attacks that may allow host compromise or exfiltration of data.

Weak Credentials

All combinations of the following usernames and passwords should be tested for remote services accessible via the Internet.

Usernames	Passwords
adm	<null>
admin	1234
administrator	12345678
cisco	Admin
debug	Administrator
guest	Changeme
manager	changeme2
monitor	Cisco
operator	Letmein
patrol	Manager
public	monitor
recovery	Operator
root	pass
security	password
superuser	Password
support	PASSWORD
sysadm	Password1
sysadmin	Password123
system	Passw0rd
tech	private
test	public
user	recovery
	root
	security
	tech

Ingress file types

The following list of file types should be tested for when evaluating inbound email and web filtering controls.

Files should be used from the Accreditation Body supplied set of test files, it is expected that in most cases these will be accessed for testing from a local CB server.

Files will be either native binaries that launch obvious behaviour to identify execution (eg launching a web browser to a known page) or specific inert files that a known to flag the majority of common AV solutions.

Executables

.com
.bat
.exe
.pif
.scr
.msi
.ps1
.jar
.sh
.py
.dmg

Containers

.zip
.7z
.rar
.tar.gz
.tar
.gz