Cyber Essentials PLUS

Common Test Specification

V1.2

Version Control

Version	Date	Description	Released by
1.0	07/08/14	Initial Common Test Specification release	SR Smith
1.1	19/08/14	Updated Scope	SR Smith
1.2	20/10/14	Corrected Errors, introduced footer version	SR Smith

Contents

Introduction

The Cyber Essentials scheme 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 not suitable for organisations that may be the target of Advanced Persistent Threat (APT) style attacks.

Scope of the Cyber Essentials Plus Test

The Test Scope is defined in the scheme Assurance Framework document, available on the scheme web site https://www.cyberstreetwise.com/cyberessentials/#downloads

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.

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.

Assumptions

The Assessor has access to an appropriate and sufficient set of test files and a remote web page with links to downloadable test files, to test the implementation of the controls specified in the Framework.

The organisation being evaluated has, or is prepared to, assert that the controls described in the Scheme Requirements document have been properly implemented.

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.

The "two-click rule" is intended to limit the level of nesting under test. If a user is required to undertake multiple steps to execute potential malware (such as for example a file in a zip archive within a zip archive within a zip archive…), then the tester should use experience and initiative to determine what level of nesting is appropriate to test.

Success Criteria

Any organisation that is awarded a “fail” status for ANY test within this specification document is deemed to have failed overall. Otherwise, a pass status should be awarded. Any action points or observations should be detailed in the final report delivered to the customer.

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 the Accreditation Body, 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 IPv4 (and IPv6 where used) addresses within the specified ranges. Ensure scans include a scan for known common UDP services for all IPv4 (and IPv6 where used) addresses within the specified ranges. All risks identified should be scored using the CVSSv2 standard. 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. Results within this section should be split in to three areas for the purposes of reporting in line with the relevant Basic Technical Cyber Protection Controls. **1. Boundary Firewalls and Internet Gateways** **2. Secure Configuration** **3. Patch Management**	Results: **Boundary Firewalls and Internet Gateways** **Secure Configuration** **Patch Management**

Test	Description	Results
	Interpreting Results: 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 any high risks issues are present. The issues (medium and above) identified should be included in the additional information sections of the report. The high level categorisation of issues is described below but the precise classification will not affect the pass/fail result of the test and is instead provided as clarification for the customer. **Boundary Firewalls and Internet Gateways** Unnecessary open ports and services **Secure Configuration** Weak credentials Use of unsupported operating systems **Patch Management** Vulnerabilities in unpatched services	

Internal systems

Tester pre-requisites

- 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 appropriate and sufficient test binaries and payloads;
- Details of a target e-mail account per platform being assessed.

Required tests

The following tests 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** Using your remote test account and desktop/laptop system provided by the customer, send an initial email with no attachments and determine that it arrives successfully in the target inbox. Next, attempt to send multiple emails in from your remote test account, with attached test files. 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** 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 If any of the 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. Note the "two click rule" as per the assumptions section. If no email communications 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.	Results: **Malware Protection** **Secure Configuration**

Test	Description	Results
3)	**Web site page with URLs linking to** binaries Browse to a test page containing links to a downloadable set of test binaries. 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. Boundary Firewalls and Internet Gateways** **2. Malware Protection** **3. Secure Configuration** 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. Note the “two click rule” as per the assumptions section. 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 “Action Point” status for “Secure Configuration”, otherwise record a “Pass” for this element. Note the “two click rule” as per the assumptions section. 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.	Result : **Boundary Firewalls and Internet Gateways** **Malware Protection** **Secure Configuration**

<table>
<tr>
<td>4)</td>
<td>
Authenticated vulnerability scan of host

Using an appropriate industry standard workstation build review tool, 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. Office software suites
4. Adobe Flash
5. Mozilla Firefox
6. Google Chrome
7. Opera
8. Microsoft Internet Explorer

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

All risks identified should be scored using the CVSSv2 standard.

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.

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 should be split in to four areas for the purposes of reporting in line with relevant the Basic Technical Cyber Protection Controls.

1. Patch Management
2. Malware Protection
3. Access Control
4. Secure Configuration

Interpreting Results:

Patch Management
All patches released within 14 days of the date of the audit for any of the applications listed should be installed. If this is true, award a “Pass”.
Otherwise, if all patches released within 30 days of the date of the audit for any of the applications listed are installed award an “Action Point”
Otherwise, award a “Fail”
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.
</td>
<td>
Result:

Patch Management

Malware Protection

Access Control

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

	Malware Protection An AV solution must be in place and all AV definitions released within 7 days of the date of the audit should be installed. Any AV engine updates should be applied within a maximum of 90 days. If both of these are 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". **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 any high risks issues are present. 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 7 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 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.

Weak Credentials

All combination 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 filtering controls.

Files should be either native binaries that launch obvious behaviour to identify execution (eg launching a web browser to a known page, or creating an onscreen dialog) or specific inert files that are 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