CYBER ESSENTIALS

CREST

Cyber Essentials

Test Specification

Contents

Scope of the Audit

The audit scope sets out to cover three critical areas of interest for the 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 exploits 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.

The audit scope will be agreed before the test begins and may include third party Internet facing hosted 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. 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. 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.

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 sets out to specify precisely what tests 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.

When attempting to exploit the client workstations through potential user interaction, no more than two clicks in the sequence of pop-ups per file or URL should be accepted. If more than two clicks are required then the test is deemed not to have exploited the platform and that individual test case should be discontinued.

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 the accreditation body in order to maximise consistency between testing providers.

Success Criteria

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

External systems

Required tests

The following tests cases are required

1. Review of customer questionnaire information on open ports;
2. Sanity check with RIPE of stated IP range;
3. External full TCP port and UDP service scan for stated IP range;
4. Vulnerability scan for stated IP range;
5. Basic web application scanning for common vulnerabilities.

Test Details

Test	Description	Results
1.	**Review of customer questionnaire information on open ports** Review the list of services that the customer questionnaire states are accessible from the Internet. Accept VPN, mail and web ports and award a pass status unless the following criteria are met. Award a "minor fail" for any database ports or remote access technologies unless it is stated that they are protected by source IP address filters. Award a "major fail" for remote administration services unless it is stated that they are protected by source IP address filters or other form of strong authentication.	Result :

Test	Description	Results
2.	**Sanity check with RIPE of stated IP range** Go to www.ripe.net and use the IP lookup functionality to query for the IP ranges specified as being in use by the customer. Where multiple IP addresses are in use and they do not fall within the subnet boundaries specified by the mask information, check all IP addresses. In this case award at least a minor fail status. If any of the IP addresses clearly belong to the organisation in question then award a pass status. If ANY of the IP addresses clearly belong to a different organisation (other than an ISP or hosting company) then award a major fail status and refer to the customer for investigation. If it is unclear then award an observation status.	Result :
3.	**External full TCP port and UDP service scan for stated IP range** Ensure the customer does not have any specific firewall rules in place for your test source IP addresses. Perform a full (all 65535 ports) TCP port scan for all IP addresses within the specified ranges except for those that caused a "major fail" in test 2. Note this should also include IPv6 addresses where they are in use. Perform a scan for known common UDP services for all IP addresses within the specified ranges except for those that caused a "major fail" in test 2. Note this should also include IPv6 addresses where they are in use. If the port scan output agrees with the information provided by the customer then award a pass status for this test. If the port scan does not match then at least a minor fail must be awarded.	Result :

Test	Description	Results
4.	**Vulnerability scan for stated IP range** Using an appropriate industry standard vulnerability scanner (see Appendix 1 - **Tool requirements**) scan the external IP range for all IP addresses within the specified ranges except for those that caused a "major fail" in test 2. Note this should also include IPv6 addresses where they are in use. Medium risks 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 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. Award a pass status if only low risk issues are returned. Award a minor fail status if the highest risk found is medium. Award a major fail status if the highest risk found is high or critical.	Result:
5.	**Basic web application scanning for common vulnerabilities.** Basic web application scanning for common vulnerabilities (notably injection attacks) should be performed from an unauthenticated user perspective. Application testing should be performed using common tools that cover the requirements as defined in the Appendix to this document. Award a pass if no trivially exploitable injection or forced browsing vulnerabilities are discovered. Award a major fail if trivially exploitable injection or forced browsing vulnerabilities attacks are discovered.	Result:
	Overall Result (Worst Case result of this section)	Result:

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 test binaries and payloads provided by the Certification Body;
- Details of a target e-mail account per platform being assessed.

Required tests

The following tests cases are required

6. Inbound email binaries and payloads
7. Inbound emails containing URLs linking to binaries and browser exploitation payloads

Test Details

Test	Description	Results
6.	**Inbound email binaries and payloads** 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. Ensure your initial email has no attachments and that it arrives successfully at the destination. If any of the emails with the file attachments are successfully delivered to your test platform then a minor fail should be recorded as the test status result (with the exception of the initial test e-mail). If no emails with attachments are received then record a pass status. If any of the executable files or vulnerability payloads can be run successfully and provide an alert warning of successful execution either through a popup window or via a pingback to an external server, then record a major fail. External pingback connections should be attempted on TCP ports 53, 80, 443 and 8080. Vulnerability exploit files and binaries must attempt to connect to hosts by both IP address and URL and SSL sites must have a valid certificate. 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 major fail. Ensure customer's technical staff are given sufficient information to enable them to attempt to resolve the problem during the testing window.	Result:

Test	Description	Results
7.	**Inbound emails containing URLs linking to binaries and browser exploitation payloads** 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 URLs. Ensure your initial email has no URLs and that it arrives successfully at the destination. If any of the executable files or vulnerability payloads can be run successfully and provide an alert warning of successful execution via a pingback to an external server then record a major fail. External pingback connections should be attempted on TCP ports 53, 80, 443 and 8080. Vulnerability exploit files and binaries must attempt to connect to hosts by both IP address and URL and SSL sites must have a valid certificate. 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 major fail. Ensure customer's technical staff are given sufficient information to enable them to attempt to resolve the problem during the testing window.	Result:
	Overall Result (Worst Case result of this section)	Result:

Appendix 1 - Tool requirements

Port scanners

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 service scan on commonly used UDP ports. Specifically SNMP and NTP ports must be checked due to their common weaknesses.

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

Common tools that can perform some of these functions included in the Backtrack and Kali distributions.

Definitions

"Additional major services" – hosts running databases, web servers or management systems that are not listed in their description

Common tools that can perform some of these functions are included in the Backtrack and Kali distributions.

Vulnerability scanners

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.

Common commercial tools that can be used to perform some of these tests include Nessus and Qualysguard. CREST is not aware of any free alternatives that offer a complete solution at the time of writing. However, customisation of existing platforms to cover the test specifications in this document could be considered.

Weak Credentials

Any 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 used from the Certification Body supplied set of test files and will be either native binaries or will be targeted to exploit versions of common applications to ping back (beacon) to a consultancy configured test server.

Executables

.com

.bat

.exe

.pif

.scr

.msi

.ps1

.jar

.sh

.py

.dmg

Exploit targeting extensions

.pdf

.doc

.docx

.ppt

.pptx

.xls

.xlsx

.png

.jpg

.mp4

.avi

.mov

Containers

.zip

.7z

.rar

.tar.gz

.tar

.gz

CYBER ESSENTIALS

CREST

Abbey House | 18-24 Stoke Road | Slough | Berkshire | SL2 5AG

T: 0845 686 5542
E: admin@crest-approved.org
W: crest-approved.org