{{ org\_name }}

Penetration Testing Report

{{ month\_year }}

# Contacts

### {{r org\_name }}

|  |  |
| --- | --- |
| Contact 1 | Contact 2 |
| {{ contact1\_name }} | {{ contact2\_name }} |
| {{ contact1\_role }} | {{ contact2\_role }} |
| **{{ contact1\_email }}** | **{{ contact2\_email }}** |
| {{ contact1\_phone }} | {{ contact2\_phone }} |

### Your Company, Cybersecurity division

|  |  |
| --- | --- |
| Contact 1 | Contact 2 |
| Your Company |  |
| [**s**](mailto:professional.cyberservices@jisc.ac.uk)**ervice@yourcompany.com** |  |
| 0300 300 2212 |  |
|  |  |

### Your Company, Cyber security Penetration Testers

|  |  |
| --- | --- |
| Contact 1 | Contact 2 |
| {{ author\_name }} |  |
| {{ author\_role }} |  |
| **{{ author\_email }}** |  |
| {{ author\_phone }} |  |

# Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. The Penetrating Testing Team prioritised the assessment to identify the weakest security controls an attacker would exploit. We recommend conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

After testing has concluded, you should ensure any test accounts are revoked and any IP whitelist rules added for the test are removed.

# Document Release

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Change | Author (s) |
| 0.1 | {{ date }} | Initial Draft - internal only | {{ author\_name }} |
|  |  |  |  |

# Table of contents

[Contacts 2](#_Toc113022734)

[Disclaimer 4](#_Toc113022735)

[Document Release 4](#_Toc113022736)

[Table of contents 5](#_Toc113022737)

[Executive Summary 6](#_Toc113022738)

[Scope 7](#_Toc113022739)

[Conclusions and Recommendations 8](#_Toc113022740)

[Summary of Findings 9](#_Toc113022741)

[Detailed Findings 10](#_Toc113022742)

[Critical Severity Issues 10](#_Toc113022743)

[High Severity Issues 11](#_Toc113022745)

[Medium Severity Issues 12](#_Toc113022747)

[Low Severity Issues 13](#_Toc113022749)

[Informational Severity Issues 14](#_Toc113022751)

[Appendix A: Methodology 15](#_Toc113022753)

[Appendix B: Tools Used 17](#_Toc113022754)

[Appendix C: Useful resources 18](#_Toc113022755)

[C.1 Scanning 18](#_Toc113022756)

[C.2 SSL and TLS 18](#_Toc113022757)

[C.3 HTTP security headers  18](#_Toc113022758)

[C.4 CIS security benchmarks 19](#_Toc113022759)

# Executive Summary

The Penetration Testing team is pleased to present the Penetration Test Report for {{ org\_name }}.

The testing was conducted between the {{ start\_day }} and {{end\_day}} {{ month\_year }}.

The overarching goal of this engagement was to identify areas for improvement, by highlighting vulnerabilities. Identifying these areas for improvement is also a positive opportunity to commence continuous vulnerability management now that the current security posture has been evaluated.

{%p if num\_total\_ext and num\_total\_int and num\_total\_ad %}

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** **Rating** | **External findings** | **Internal findings** | **AD findings** |
| **Critical** | {{ num\_crit\_ext }} | {{ num\_crit\_int }} | {{ num\_crit\_ad }} |
| **High** | {{ num\_high\_ext }} | {{ num\_high\_int }} | {{ num\_high\_ad }} |
| **Medium** | {{ num\_medium\_ext }} | {{ num\_medium\_int }} | {{ num\_medium\_ad }} |
| **Low** | {{ num\_low\_ext }} | {{ num\_low\_int }} | {{ num\_low\_ad }} |
| **Informational** | {{ num\_info\_ext }} | {{ num\_info\_int }} | {{ num\_info\_ad }} |

{%p elif num\_total\_ext and num\_total\_int %}

|  |  |  |
| --- | --- | --- |
| **Risk** **Rating** | **External findings** | **Internal findings** |
| **Critical** | {{ num\_crit\_ext }} | {{ num\_crit\_int }} |
| **High** | {{ num\_high\_ext }} | {{ num\_high\_int }} |
| **Medium** | {{ num\_medium\_ext }} | {{ num\_medium\_int }} |
| **Low** | {{ num\_low\_ext }} | {{ num\_low\_int }} |
| **Informational** | {{ num\_info\_ext }} | {{ num\_info\_int }} |

{%p elif num\_total\_ext and num\_total\_ad %}

|  |  |  |
| --- | --- | --- |
| **Risk** **Rating** | **External findings** | **AD findings** |
| **Critical** | {{ num\_crit\_ext }} | {{ num\_crit\_ad }} |
| **High** | {{ num\_high\_ext }} | {{ num\_high\_ad }} |
| **Medium** | {{ num\_medium\_ext }} | {{ num\_medium\_ad }} |
| **Low** | {{ num\_low\_ext }} | {{ num\_low\_ad }} |
| **Informational** | {{ num\_info\_ext }} | {{ num\_info\_ad }} |

{%p elif num\_total\_int and num\_total\_ad %}

|  |  |  |
| --- | --- | --- |
| **Risk** **Rating** | **Internal findings** | **AD findings** |
| **Critical** | {{ num\_crit\_int }} | {{ num\_crit\_ad }} |
| **High** | {{ num\_high\_int }} | {{ num\_high\_ad }} |
| **Medium** | {{ num\_medium\_int }} | {{ num\_medium\_ad }} |
| **Low** | {{ num\_low\_int }} | {{ num\_low\_ad }} |
| **Informational** | {{ num\_info\_int }} | {{ num\_info\_ad }} |

{%p elif num\_total\_ext %}

|  |  |
| --- | --- |
| **Risk** **Rating** | **External findings** |
| **Critical** | {{ num\_crit\_ext }} |
| **High** | {{ num\_high\_ext }} |
| **Medium** | {{ num\_medium\_ext }} |
| **Low** | {{ num\_low\_ext }} |
| **Informational** | {{ num\_info\_ext }} |

{%p elif num\_total\_int %}

|  |  |
| --- | --- |
| **Risk** **Rating** | **Internal findings** |
| **Critical** | {{ num\_crit\_int }} |
| **High** | {{ num\_high\_int }} |
| **Medium** | {{ num\_medium\_int }} |
| **Low** | {{ num\_low\_int }} |
| **Informational** | {{ num\_info\_int }} |

{%p elif num\_total\_ad %}

|  |  |
| --- | --- |
| **Risk** **Rating** | **AD findings** |
| **Critical** | {{ num\_crit\_ad }} |
| **High** | {{ num\_high\_ad }} |
| **Medium** | {{ num\_medium\_ad }} |
| **Low** | {{ num\_low\_ad }} |
| **Informational** | {{ num\_info\_ad }} |

{%p endif %}

# Scope

The list of hosts covered by this assessment included:

{%p for item in scope %}

* {{ item }}

{%p endfor %}

# Conclusions and Recommendations

General notes

{%p if num\_total\_ext %}

### External findings

Notes

{%p endif %}

{%p if num\_total\_int %}

### Internal findings

Notes

{%p endif %}

{%p if num\_total\_ad %}

### Active Directory findings

Notes

{%p endif %}

{% if num\_total\_ext %}

# Summary of Findings (external testing)

A total of {{ num\_total\_ext }} findings were identified.

|  |  |  |
| --- | --- | --- |
| **Finding** | **Risk Rating** | **Affected Hosts** |
| {%tr for issue in issues.critical\_ext %} | | |
| {{ issue.title }} | **Critical** | {{ issue.hostlist }} |
| {%tr endfor %} | | |
| {%tr for issue in issues.high\_ext %} | | |
| {{ issue.title }} | **High** | {{ issue.hostlist }} |
| {%tr endfor %} | | |
| {%tr for issue in issues.medium\_ext %} | | |
| {{ issue.title }} | **Medium** | {{ issue.hostlist }} |
| {%tr endfor %} | | |
| {%tr for issue in issues.low\_ext %} | | |
| {{ issue.title }} | **Low** | {{ issue.hostlist }} |
| {%tr endfor %} | | |
| {%tr for issue in issues.info\_ext %} | | |
| {{ issue.title }} | **Informational** | {{ issue.hostlist }} |
| {%tr endfor %} | | |

{% endif %}

{% if num\_total\_int %}

# Summary of Findings (internal testing)

A total of {{ num\_total\_int }} findings were identified.

|  |  |  |
| --- | --- | --- |
| **Finding** | **Risk Rating** | **Affected Hosts** |
| {%tr for issue in issues.critical\_int %} | | |
| {{ issue.title }} | **Critical** | {{ issue.hostlist }} |
| {%tr endfor %} | | |
| {%tr for issue in issues.high\_int %} | | |
| {{ issue.title }} | **High** | {{ issue.hostlist }} |
| {%tr endfor %} | | |
| {%tr for issue in issues.medium\_int %} | | |
| {{ issue.title }} | **Medium** | {{ issue.hostlist }} |
| {%tr endfor %} | | |
| {%tr for issue in issues.low\_int %} | | |
| {{ issue.title }} | **Low** | {{ issue.hostlist }} |
| {%tr endfor %} | | |
| {%tr for issue in issues.info\_int %} | | |
| {{ issue.title }} | **Informational** | {{ issue.hostlist }} |
| {%tr endfor %} | | |

{% endif %}

{% if num\_total\_ad %}

# Summary of Findings (**AD** testing)

A total of {{ num\_total\_ad }} findings were identified.

|  |  |  |
| --- | --- | --- |
| **Finding** | **Risk Rating** | **Affected Hosts** |
| {%tr for issue in issues.critical\_ad %} | | |
| {{ issue.title }} | **Critical** | {{ issue.hostlist }} |
| {%tr endfor %} | | |
| {%tr for issue in issues.high\_ad %} | | |
| {{ issue.title }} | **High** | {{ issue.hostlist }} |
| {%tr endfor %} | | |
| {%tr for issue in issues.medium\_ad %} | | |
| {{ issue.title }} | **Medium** | {{ issue.hostlist }} |
| {%tr endfor %} | | |
| {%tr for issue in issues.low\_ad %} | | |
| {{ issue.title }} | **Low** | {{ issue.hostlist }} |
| {%tr endfor %} | | |
| {%tr for issue in issues.info\_ad %} | | |
| {{ issue.title }} | **Informational** | {{ issue.hostlist }} |
| {%tr endfor %} | | |

{% endif %}

{% if num\_total\_ext %}

# Detailed Findings

# External Critical Severity Issues

{% for issue in issues.critical\_ext %}

## {{ issue.title }}

|  |  |  |
| --- | --- | --- |
| {%tr for host in issue.hosts %} | | |
|  | {{ host.label }} | {{ host.ports }} |
| {%tr endfor %} | | |

{% if issue.cvss3 and issue.cvss3|length %}

### CVSSv3

Score: {{ issue.cvss3 }}{% if issue.cvss3\_vector and issue.cvss3\_vector|length%} ({{ issue.cvss3\_vector }}){% endif %}{% endif %}

### Issue Description

{{r issue.description }}

{%p if issue.discoverability %}

### Issue Discoverability

{{r issue.discoverability }}

{%p endif %}

{%p if issue.exploitability %}

### Issue Exploitability

{{r issue.exploitability }}

{%p endif %}

{%p if issue.impact %}

### Issue Impact

{{r issue.impact }}

{%p endif %}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

# External High Severity Issues

{% for issue in issues.high\_ext %}

## {{ issue.title }}

|  |  |  |
| --- | --- | --- |
| {%tr for host in issue.hosts %} | | |
|  | {{ host.label }} | {{ host.ports }} |
| {%tr endfor %} | | |

{% if issue.cvss3 and issue.cvss3|length %}

### CVSSv3

Score: {{ issue.cvss3 }}{% if issue.cvss3\_vector and issue.cvss3\_vector|length%} ({{ issue.cvss3\_vector }}){% endif %}{% endif %}

### Issue Description

{{r issue.description }}

{%p if issue.discoverability %}

### Issue Discoverability

{{r issue.discoverability }}

{%p endif %}

{%p if issue.exploitability %}

### Issue Exploitability

{{r issue.exploitability }}

{%p endif %}

{%p if issue.impact %}

### Issue Impact

{{r issue.impact }}

{%p endif %}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

# External Medium Severity Issues

{% for issue in issues.medium\_ext %}

## {{ issue.title }}

|  |  |  |
| --- | --- | --- |
| {%tr for host in issue.hosts %} | | |
|  | {{ host.label }} | {{ host.ports }} |
| {%tr endfor %} | | |

{% if issue.cvss3 and issue.cvss3|length %}

### CVSSv3

Score: {{ issue.cvss3 }}{% if issue.cvss3\_vector and issue.cvss3\_vector|length%} ({{ issue.cvss3\_vector }}){% endif %}{% endif %}

### Issue Description

{{r issue.description }}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

# External Low Severity Issues

{% for issue in issues.low\_ext %}

## {{ issue.title }}

|  |  |  |
| --- | --- | --- |
| {%tr for host in issue.hosts %} | | |
|  | {{ host.label }} | {{ host.ports }} |
| {%tr endfor %} | | |

{% if issue.cvss3 and issue.cvss3|length %}

### CVSSv3

Score: {{ issue.cvss3 }}{% if issue.cvss3\_vector and issue.cvss3\_vector|length%} ({{ issue.cvss3\_vector }}){% endif %}{% endif %}

### Issue Description

{{r issue.description }}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

# External Informational Severity Issues

{% for issue in issues.info\_ext %}

## {{ issue.title }}

|  |  |  |
| --- | --- | --- |
| {%tr for host in issue.hosts %} | | |
|  | {{ host.label }} | {{ host.ports }} |
| {%tr endfor %} | | |

{% if issue.cvss3 and issue.cvss3|length %}

### CVSSv3

Score: {{ issue.cvss3 }}{% if issue.cvss3\_vector and issue.cvss3\_vector|length%} ({{ issue.cvss3\_vector }}){% endif %}{% endif %}

### Issue Description

{{r issue.description }}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

{% endif %}

{% if num\_total\_int %}

{% if not num\_total\_ext %}

# Detailed Findings

{% endif %}

# Internal Critical Severity Issues

{% for issue in issues.critical\_int %}

## {{ issue.title }}

|  |  |  |
| --- | --- | --- |
| {%tr for host in issue.hosts %} | | |
|  | {{ host.label }} | {{ host.ports }} |
| {%tr endfor %} | | |

### Issue Description

{{r issue.description }}

{%p if issue.discoverability %}

### Issue Discoverability

{{r issue.discoverability }}

{%p endif %}

{%p if issue.exploitability %}

### Issue Exploitability

{{r issue.exploitability }}

{%p endif %}

{%p if issue.impact %}

### Issue Impact

{{r issue.impact }}

{%p endif %}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

# Internal High Severity Issues

{% for issue in issues.high\_int %}

## {{ issue.title }}

|  |  |  |
| --- | --- | --- |
| {%tr for host in issue.hosts %} | | |
|  | {{ host.label }} | {{ host.ports }} |
| {%tr endfor %} | | |

### Issue Description

{{r issue.description }}

{%p if issue.discoverability %}

### Issue Discoverability

{{r issue.discoverability }}

{%p endif %}

{%p if issue.exploitability %}

### Issue Exploitability

{{r issue.exploitability }}

{%p endif %}

{%p if issue.impact %}

### Issue Impact

{{r issue.impact }}

{%p endif %}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

# Internal Medium Severity Issues

{% for issue in issues.medium\_int %}

## {{ issue.title }}

|  |  |  |
| --- | --- | --- |
| {%tr for host in issue.hosts %} | | |
|  | {{ host.label }} | {{ host.ports }} |
| {%tr endfor %} | | |

### Issue Description

{{r issue.description }}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

# Internal Low Severity Issues

{% for issue in issues.low\_int %}

## {{ issue.title }}

|  |  |  |
| --- | --- | --- |
| {%tr for host in issue.hosts %} | | |
|  | {{ host.label }} | {{ host.ports }} |
| {%tr endfor %} | | |

### Issue Description

{{r issue.description }}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

# Internal Informational Severity Issues

{% for issue in issues.info\_int %}

## {{ issue.title }}

|  |  |  |
| --- | --- | --- |
| {%tr for host in issue.hosts %} | | |
|  | {{ host.label }} | {{ host.ports }} |
| {%tr endfor %} | | |

### Issue Description

{{r issue.description }}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

{% endif %}

{% if num\_total\_ad %}

{% if not num\_total\_ext and not num\_total\_int %}

# Detailed Findings

{% endif %}

# AD Critical Severity Issues

{% for issue in issues.critical\_ad %}

## {{ issue.title }}

|  |  |
| --- | --- |
| {%tr for host in issue.hosts %} | |
|  | {{ host.label }} |
| {%tr endfor %} | |

### Issue Description

{{r issue.description }}

{%p if issue.discoverability %}

### Issue Discoverability

{{r issue.discoverability }}

{%p endif %}

{%p if issue.exploitability %}

### Issue Exploitability

{{r issue.exploitability }}

{%p endif %}

{%p if issue.impact %}

### Issue Impact

{{r issue.impact }}

{%p endif %}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

# AD High Severity Issues

{% for issue in issues.high\_ad %}

## {{ issue.title }}

|  |  |
| --- | --- |
| {%tr for host in issue.hosts %} | |
|  | {{ host.label }} |
| {%tr endfor %} | |

### Issue Description

{{r issue.description }}

{%p if issue.discoverability %}

### Issue Discoverability

{{r issue.discoverability }}

{%p endif %}

{%p if issue.exploitability %}

### Issue Exploitability

{{r issue.exploitability }}

{%p endif %}

{%p if issue.impact %}

### Issue Impact

{{r issue.impact }}

{%p endif %}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

# AD Medium Severity Issues

{% for issue in issues.medium\_ad %}

## {{ issue.title }}

|  |  |
| --- | --- |
| {%tr for host in issue.hosts %} | |
|  | {{ host.label }} |
| {%tr endfor %} | |

### Issue Description

{{r issue.description }}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

# AD Low Severity Issues

{% for issue in issues.low\_ad %}

## {{ issue.title }}

|  |  |
| --- | --- |
| {%tr for host in issue.hosts %} | |
|  | {{ host.label }} |
| {%tr endfor %} | |

### Issue Description

{{r issue.description }}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

# AD Informational Severity Issues

{% for issue in issues.info\_ad %}

## {{ issue.title }}

|  |  |
| --- | --- |
| {%tr for host in issue.hosts %} | |
|  | {{ host.label }} |
| {%tr endfor %} | |

### Issue Description

{{r issue.description }}

### Issue Remediation

{{r issue.remediation }}

{% endfor %}

{% endif %}

# Appendix A: Methodology

|  |  |
| --- | --- |
| **Task Completed** | **Details** |
| **Information Gathering** | * Conduct Search Engine Discovery and Reconnaissance for Information Leakage (OTG-INFO-001) * Fingerprint Web Server (OTG-INFO-002) * Review Webserver Metafiles for Information Leakage (OTG-INFO-003) * Enumerate Applications on Webserver (OTG-INFO-004) * Review Webpage Comments and Metadata for Information Leakage (OTG-INFO-005) * Identify application entry points (OTG-INFO-006) * Map execution paths through application (OTG-INFO-007) * Fingerprint Web Application Framework (OTG-INFO-008) * Fingerprint Web Application (OTG-INFO-009) * Map Application Architecture (OTG-INFO-010) |
| **Configuration and Deployment Management Testing** | * Test Network/Infrastructure Configuration (OTG-CONFIG-001) * Test Application Platform Configuration (OTG-CONFIG-002) * Test File Extensions Handling for Sensitive Information (OTG-CONFIG-003) * Review Old, Backup and Unreferenced Files for Sensitive Information (OTG-CONFIG-004) * Enumerate Infrastructure and Application Admin Interfaces (OTG-CONFIG-005) * Test HTTP Methods (OTG-CONFIG-006) * Test HTTP Strict Transport Security (OTG-CONFIG-007) * Test RIA cross domain policy (OTG-CONFIG-008) |
| **Identity Management Testing** | * Test Role Definitions (OTG-IDENT-001) * Test User Registration Process (OTG-IDENT-002) * Test Account Provisioning Process (OTG-IDENT-003) * Testing for Account Enumeration and Guessable User Account (OTG-IDENT-004) * Testing for Weak or unenforced username policy (OTG-IDENT-005) |
| **Authentication Testing** | * Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001) * Testing for default credentials (OTG-AUTHN-002) * Testing for Weak lock out mechanism (OTG-AUTHN-003) * Testing for bypassing authentication schema (OTG-AUTHN-004) * Test remember password functionality (OTG-AUTHN-005) * Testing for Browser cache weakness (OTG-AUTHN-006) * Testing for Weak password policy (OTG-AUTHN-007) * Testing for Weak security question/answer (OTG-AUTHN-008) * Testing for weak password change or reset functionalities (OTG-AUTHN-009) * Testing for Weaker authentication in alternative channel (OTG-AUTHN-010) |
| **Authorization Testing** | * Testing Directory traversal/file include (OTG-AUTHZ-001) * Testing for bypassing authorization schema (OTG-AUTHZ-002) * Testing for Privilege Escalation (OTG-AUTHZ-003) * Testing for Insecure Direct Object References (OTG-AUTHZ-004) |
| **Session Management Testing** | * Testing for Bypassing Session Management Schema (OTG-SESS-001) * Testing for Cookies attributes (OTG-SESS-002) * Testing for Session Fixation (OTG-SESS-003) * Testing for Exposed Session Variables (OTG-SESS-004) * Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005) * Testing for logout functionality (OTG-SESS-006) * Test Session Timeout (OTG-SESS-007) * Testing for Session puzzling (OTG-SESS-008) |
| **Testing for Error Handling** | * Analysis of Error Codes (OTG-ERR-001) * Analysis of Stack Traces (OTG-ERR-002) |

# Appendix B: Tools Used

|  |  |
| --- | --- |
| **Tool** | **Description** |
| **Acunetix** | Acunetix is an application security testing solution for securing your websites, web applications, and APIs |
| **Burp Suite** | Burp Suite is an integrated platform for attacking web applications.  <http://portswigger.net/burp/> |
| **Metasploit** | Metasploit is a penetration testing software created through a collaboration between the open source community and Rapid7.  <http://www.metasploit.com/> |
| **Nessus** | Nessus is one of the most popular and capable vulnerability scanners, particularly for UNIX systems.  http://www.tenable.com/products/nessus-vulnerability-scanner |
| **Nikto** | Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items.  <https://cirt.net/Nikto2> |
| **Nmap** | Nmap is a free and open source utility for network discovery and security auditing.  <http://nmap.org/> |
| **PingCastle** | PingCastle is a free Active Directory auditting tool. Recommendations must be actioned within a change control process.  https://www.pingcastle.com |

# **Appendix C: Useful resources**

## C.1 Scanning

* OpenVAS is a free vulnerability scanner that can be deployed for use internally and externally:
  + <http://openvas.org/>
* Tenable Nessus and Rapid7 Nexpose are paid products that both offer similar functionality and a free trial, which would be suitable for occasional use (eg: quarterly):
  + [tenable.com/](https://www.tenable.com/) and [rapid7.com/products/nexpose/](https://www.rapid7.com/products/nexpose/)
* PingCastle is a free-to-use Active Directory audit tool that can quickly identify issues in the AD configuration and group policy: [pingcastle.com/](https://www.pingcastle.com/)

## C.2 SSL and TLS

* For SSL maintenance, Qualys’ online SSL test can provide clear and detailed information about an internet-facing site’s SSL configuration:
  + [ssllabs.com/ssltest/analyze.html](https://www.ssllabs.com/ssltest/analyze.html)
* Similarly, the tool sslscan can be run locally to identify the configuration of SSL services:
  + <https://github.com/rbsec/sslscan>
* The following article contains practical information on configuring SSL/TLS on a variety of servers:
  + <https://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/>
* The SSL Labs “SSL and TLS Deployment Best Practices” guide contains information about which cipher suites and configurations to use:
  + <https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices>
* The OWASP Transport Layer Protection Cheat Sheet provides a variety of high level information about designing and using TLS and SSL:
  + <https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.md>
* IISCrypto is a free tool that can be used to centrally manage SSL/TLS cipher suites, which can greatly reduce the burden of keeping configurations and in line with best practices:
  + [nartac.com/Products/IISCrypto/](https://www.nartac.com/Products/IISCrypto/)

## C.3 HTTP security headers

* It is considered best practice to send specific HTTP security headers, which can help control a browser’s behaviour in order to protect users against common attacks. The following resource details these headers and their possible values: [keycdn.com/blog/http-security-headers](https://www.keycdn.com/blog/http-security-headers)

## C.4 CIS security benchmarks

### Operating System Benchmarks (Hardening)

* [CIS Microsoft Windows Desktop Benchmarks (cisecurity.org)](https://www.cisecurity.org/benchmark/microsoft_windows_desktop/)
* [CIS Microsoft Windows Server Benchmarks (cisecurity.org)](https://www.cisecurity.org/benchmark/microsoft_windows_server/)
* [Debian Family Linux (cisecurity.org)](https://www.cisecurity.org/benchmark/debian_family/)
* [Fedora Family Linux (cisecurity.org)](https://www.cisecurity.org/benchmark/fedora_family_linux/)

### Database Benchmarks (Hardening)

* [PostgreSQL (cisecurity.org)](https://www.cisecurity.org/benchmark/postgresql/)
* [CIS Microsoft SQL Server Benchmarks (cisecurity.org)](https://www.cisecurity.org/benchmark/microsoft_sql_server/)

### Application Benchmarks (Hardening)

* [CIS Microsoft IIS Benchmarks (cisecurity.org)](https://www.cisecurity.org/benchmark/microsoft_iis/)
* [CIS Microsoft Exchange Server Benchmarks (cisecurity.org)](https://www.cisecurity.org/benchmark/microsoft_exchange_server/)

{% for appx in appendices %}

# **Appendix {{ appx.letter }}: {{ appx.issue\_name }} - affected hosts**

{{appx.content}}

{% endfor %}