TLP:AMBER

MIAUW Security Assessment

[CLIENT NAME]

Author:	User
Project reference:	[Reference project name/number]
Date:	[Date]
Version:	[Version number]

Template by **MIAUW**-team:

Jeroen Diel, Maaike Hielkema, Mischa Rick van Geelen, Brenno de Winter

Document management

Client	[CLIENT NAME]
Classification	**[TLP:]**
Project reference	[Projectnumber] – [Projectname]
Start date	
End date	
Version	
Authors	
Reviewer	
Signature author	

The executive author's relevant accreditations and associated evidence are included below:

Accreditation	**Evidence**
OSCP, OSEP, OSCE, OSCE^3, OSWE, eWPTX	XXX

Version management

Version	Date	Author	Description
0.1			

Distribution list

Version	Name	Organisation	Method
1.0			

Confidentiality

The information contained in this document is considered confidential and proprietary to **[CLIENT NAME]** and is of a sensitive nature. It may contain comprehensive details about vulnerabilities identified within the assessed infrastructure and/or application(s).

The Traffic Light Protocol (TLP) is a globally recognized standard used in information security that employs colors analogous to a traffic light to classify the confidentiality of information in documents, indicating whether it can be shared with other individuals or organizations.

TLP:RED	For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
TLP:AMBER	Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN	Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community.
TLP:CLEAR	Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

The classification of this document is designated as **TLP:AMBER**.

Disclaimer

While efforts have been made to ensure the accuracy and reliability of the information contained in this report, it is provided "as is" and without warranty of any kind, expressed or implied. The findings, conclusions, and recommendations in this report should be used at the reader's own discretion and risk.

It is important to note that security risks and vulnerabilities are dynamic in nature and can evolve over time. New vulnerabilities may be discovered or the security posture of the system may change after the assessment was conducted. Therefore, this report should be considered as a snapshot of the security posture at the time of the assessment and should not be solely relied upon for making security decisions.

Management summary

Client has requested [company] for a security assessment on [environment]. The period of the assessment took place between [start date] and [end date]. During this period the full assessment has been completed/The following parts of the scope could not be tested within this period: [X].

The security assessment has been performed using the following open standard(s): OWASP Web Security Testing Guide (WSTG), OWASP Mobile Security Testing Guide (MSTG) and Penetration Testing Execution Standard (PTES). For auditability, the corresponding checklists with the scope are attached to this report. [Included if applicable] For calculation of the risk scores during the assessment, Client provided information regarding the CIA:

Introduction

The report provides technical details on discovered vulnerabilities, including a thorough explanation of each vulnerability and the mitigation steps. Vulnerability scores for findings are calculated using the Common Vulnerability Scoring System (CVSS) version 4.0, making the risk scores quantifiable from 0 to 10. These scores are categorized as critical, high, medium, low, or informative. It is recommended to take urgent action on critical and high findings. Additionally, a root cause analysis is included to identify underlying issues, aiming to prevent similar vulnerabilities in the future.

Findings

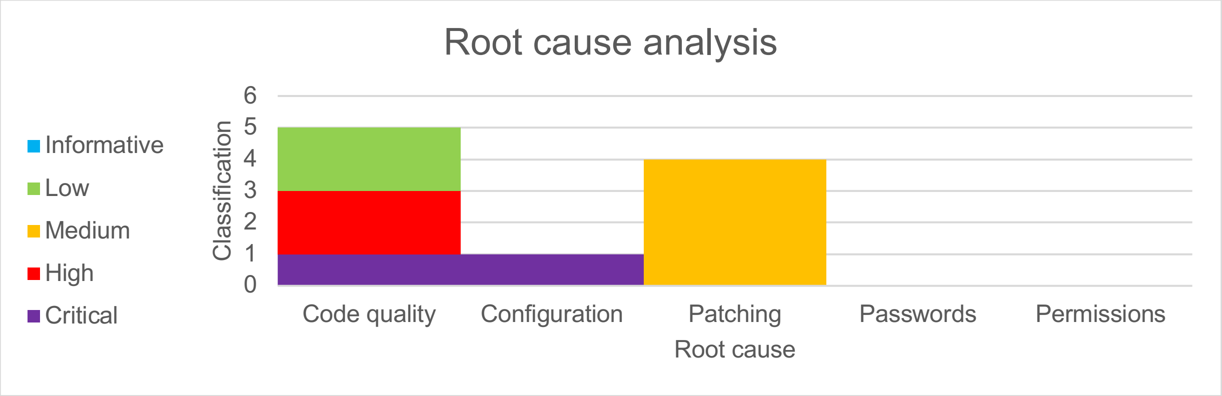
A total of [X] vulnerabilities has been found. In the table below a total of the findings has been summarized and classified based on the severity. The last column states a total of the solved findings per category.

Classification	Score	Findings [scope 1]	Findings [scope 2]	Solved
Critical	9.0 – 10.0	1	1	2
High	7.0 – 8.9	1	1	2
Medium	4.0 – 6.9	1	1	2
Low	0.1 – 3.9	1	1	2
Informative	0.0	1	1	2

[Company] recommends solving the findings as stated above, following a retest to verify if the vulnerabilities have been solved correctly.

Root cause analysis

To categorize the findings, five different root causes have been defined for the analysis: **code quality** (programming errors in software), **configuration** (errors in configuration, settings, which lead to a vulnerability), **patch management** (vulnerability due to out-of-date software), **permissions** (accounts with incorrect permissions, which lead to a vulnerability) and **passwords** (standard- or reuse of passwords or ineffective password policy).



As can be seen in table above, most findings fall under the category [X]. To reduce findings in this category in the future, [recommendation].

Table of Contents

1.Introduction

[Client] engaged [Company] to conduct a security assessment on the relevant scope as outlined in the [Plan of Approach name] document. The security assessment took place from [start date] until [end date].

1.1. Objective

The objective of the security assessment is to evaluate the effectiveness of an organization's information security controls and practices in protecting its assets, data, and operations against potential threats. The assessment aims to identify vulnerabilities, weaknesses, and potential risks in the information technology environment, and provide recommendations for improving the overall security posture.

A penetration test could be performed using three different attack-perspectives, depending on the amount of information provided by client: white box, grey box or black box (see: 1.3 - Approaches for more information). These three different perspectives could be tested using a predefined number of hours, which is known as Timeboxed. Based on the type of scope-objects, different standards are applicable (see: 1.4 - Security standards).

This security assessment is a [Timeboxed?] [Approach], using the applicable standards [standards].

[Include if specific scenarios are requested] Additionally, Client requested the following scenario(s) to be included in the test:

1.2. Scope

The scope objects were defined during the Plan of Approach. A complete overview of the agreed scope is provided below.

[Select applicable tables, or copy from plan of approach]

The following elements are included within the scope:

IP (range)	Hostname	Description

The following user accounts are provided within the scope:

User account	Description

The following hardware is provided in relation to the scope:

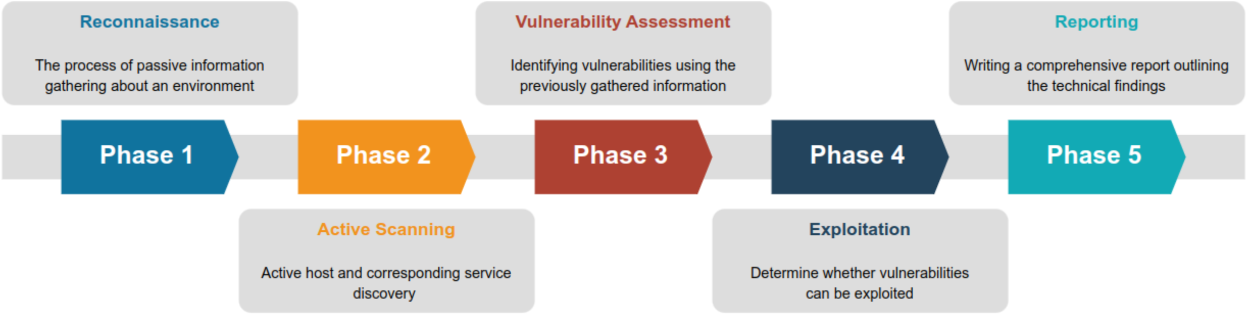
Object	Serial number	Description

[Insert if exclusions are applicable, like such] The infrastructure components, the level of hardening and its controls are explicitly excluded from the scope as the request for access was denied.

Sometimes the penetration test deviates from the plan of approach. If any deviations are applicable, an overview of these are in the appendix (see 1.17).

2.Methodology

The used methodology is a systematic seven-phase process utilized to detect vulnerabilities in an application or system, following the PTES standard.[1]


Reconnaissance
The process of passive information gathering about an environment
Vulnerability Assessment
Identifying vulnerabilities using the previously gathered information
Reporting
Writing a comprehensive report outlining the technical findings
Phase 1
Phase 2
Phase 3
Phase 4
Phase 5
Active Scanning
Active host and corresponding service discovery
Exploitation
Determine whether vulnerabilities can be exploited

Pre-engagement interactions

This stage is performed as a preparation for the penetration test. In this stage an interview with the potential client and planning takes place and agreements on the penetration test are made. This results in a signed estimate and a plan of approach. This stage is reported in the Introduction.

Intelligence Gathering

The reconnaissance phase, also known as information gathering or footprinting, is an initial step in security testing or ethical hacking where an individual or team collects as much information as possible about a target system, network or application.

It involves passive information gathering techniques, such as researching publicly available information, scanning for open ports, analyzing network configurations, and identifying potential vulnerabilities.

The goal of the reconnaissance phase is to gather intelligence about the target system's architecture, design, technologies used, and potential weaknesses, which can be used to plan further steps in the security testing process, including identifying vulnerabilities and planning potential attack vectors.

Threat modeling

During this stage, a threat model is created for Client. A threat model consists of 2 key elements: assets and attacker. Both elements are broken down in business asset and business process and their capabilities. The goal of this stage is to provide clarity of their clients' potential threats and risks. Eventually, this will result in a more accurate relevance and risk score which is specific to the organization.

Vulnerability analysis

This stage consists of the process of actively scanning and probing a system, network, or application for potential vulnerabilities or weaknesses. It involves using various automated tools or manual techniques to identify potential vulnerabilities or misconfigurations that could be exploited by malicious actors to gain unauthorized access or compromise the security of the system. Data collected during reconnaissance and active scanning phases are utilized to identify vulnerabilities and assess their exploitability.

Exploitation

Vulnerabilities are actively exploited or tested for their potential impact. This phase involves attempting to exploit vulnerabilities to gain unauthorized access, escalate privileges, or perform other malicious activities to evaluate the severity and potential consequences of the vulnerabilities discovered during the assessment.

Post exploitation

[1] http://www.pentest-standard.org/index.php/Main_Page

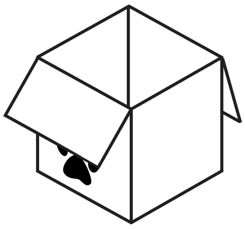
The goal is to assess the importance of the compromised machine and to secure ongoing control for potential future use. This machine's value is judged based on the sensitivity of the data it contains and its potential role in further network breaches. The techniques outlined in this phase aim to assist the tester in identifying and documenting sensitive information, analyzing configuration settings, communication channels, and connections with other network devices that could facilitate deeper network access, and establishing one or more methods for re-accessing the machine later.

Reporting
The consultant prepares a comprehensive report outlining the technical findings, including detailed information for reproducing the exploitation process of identified vulnerabilities.

1.3. Approaches

There are three approaches when performing security assessments:

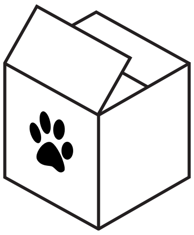
- White Box
- Grey Box
- Black Box



White Box Security Testing

This approach involves testing one or more systems with complete knowledge and access, including architecture and design documents, business flows, and security guidelines such as hardening guidelines and source code. This allows consultants to swiftly identify vulnerabilities compared to other approaches.

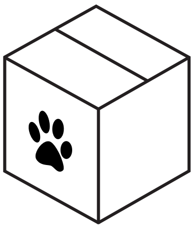
By utilizing this approach, it becomes feasible to determine if each discovered vulnerability could have been exploited from a grey or black box perspective.



Grey Box Security Testing

This approach involves testing one or more systems with restricted knowledge and access. The consultant has limited system access and minimal understanding of internal workings and business processes.

The consultant will attempt various methods to elevate the current privileges granted.



Black Box Security Testing

This approach entails testing one or more systems without any prior knowledge or access. The consultant operates with no system access or internal understanding of the workings and business processes.

Different methods for gaining access to the system will be employed, simulating the tactics an attacker might use over the internet.

1.4. Security standards

Security standards are established guidelines, frameworks, or best practices that define a set of requirements for ensuring the security of information, systems, and processes within an organization. They provide a structured approach to managing security risks and help organizations establish a baseline of security controls to protect their assets and sensitive information from unauthorized access, data breaches, and other security threats. It ensures that assessments are conducted with consistency, follow best practices, meet compliance requirements, and contribute to a more secure and resilient organizational environment.

When conducting a security assessment, the following information security standards are employed:

- Penetration Testing Execution Standard (PTES)
- Open Web Application Security Project (OWASP)
- Web Security Testing Guide (WSTG)
- Center for Internet Security (CIS)

The Penetration Testing Execution Standard (PTES) is a set of guidelines and best practices used in the field of information security to conduct penetration testing or ethical hacking. It provides a structured approach to planning, executing, and documenting penetration testing engagements.

The OWASP top 10 identifies the most critical web application security risks, such as injection attacks, cross-site scripting (XSS), and broken authentication. OWASP also develops guides, tools, and best practices for secure coding, secure authentication, and other web application security topics.

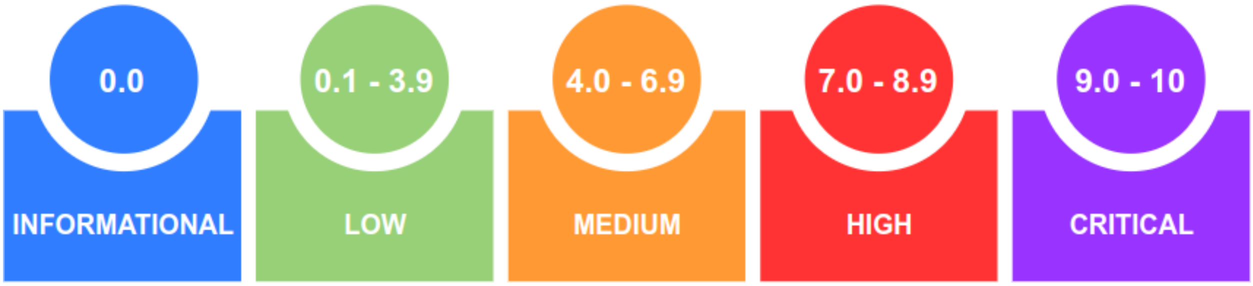
The Web Security Testing Guide (WSTG) is a comprehensive resource developed by the Open Web Application Security Project (OWASP) that provides guidance on how to conduct web application security testing. It is a practical guide that offers techniques, tools, and best practices for identifying and mitigating security vulnerabilities in web applications.

The Center for Internet Security is a set of best practice guidelines and recommendations for securing computer systems and networks. CIS Benchmarks are designed to help organizations improve their security posture by providing specific, actionable recommendations for various operating systems, software, and network devices.

1.5. Technical risk rating

The technical risk rating is the process of evaluating and assigning a level of risk to identified vulnerabilities, weaknesses, or threats in an organization its information technology environment. It involves assessing the likelihood and potential impact of these risks and assigning a rating or score to prioritize them for further action.

The severity rating is determined using the common vulnerability scoring system (CVSS[2] v4.0), which is an open framework that communicates the characteristics and severity of software vulnerabilities.



CVSS is composed of three groups of metrics: *base*, *temporal*, and *environmental*, which collectively produce a score ranging from 0 to 10. This score can be further adjusted by evaluating the temporal and environmental metrics.

[2] https://www.first.org/cvss/calculator/4.0

The CVSS score is commonly represented as a vector string, which is a condensed textual representation of the values used to calculate the score.

1.6. Assume Breach

This penetration test is performed following the assume breach mindset. This is a mindset and approach that operates under the assumption that an attacker has already infiltrated the network or system. Instead of focusing solely on preventing initial access, this principle shifts the focus to detecting, responding to, and mitigating the effects of an ongoing attack.

In practice, penetration testers using the assume breach approach will start their assessment from a position of compromise, such as having access to a user account, an endpoint, or an internal network segment. This allows them to simulate the actions of an attacker who has bypassed perimeter defenses.

In a black box setting, the "assume breach" principle implies that attacks bypass the firewall. The rationale behind using an allowlist is to focus on testing the overall security of the environment, rather than the firewall itself. This ensures that the enhanced security measures will be effective even if the firewall is changed or temporarily weakened due to an incorrect update.

The goal is to evaluate how effectively the organization can detect and respond to this breach, assess the damage that could be done, and identify weaknesses in internal controls that could allow the attacker to escalate privileges, move laterally across the network, and exfiltrate sensitive data.

By assuming that a breach has already occurred, organizations can gain insights into their incident detection and response capabilities, as well as uncover security gaps that might not be evident through traditional perimeter-focused testing. This approach emphasizes the importance of having robust internal security measures, not just strong external defenses.

3. Timeline

The timeline below provides an overview of the events during the penetration test:

Date	Time	Description

4. OSINT

During the intelligence gathering phase of a penetration test, the tester have collected information such as:

- Network details: IP addresses, domain names, network topology, and open ports.
- DNS records: Subdomains and DNS information.
- Organization details: Employee information, company structure, and third-party relationships.
- Systems and technology: Operating systems, software, hardware, and public information about the tech stack.
- Web and application data: Web applications, APIs, and SSL/TLS details.
- Social media and public data: Insights from social media and public documents.
- Historical data: Previous breaches and vulnerabilities.
- WHOIS details: Domain registration information.

Results of the acquired intelligence are included in chapter 7 (Appendix).

5. Security assessment

Vulnerabilities which have been found during the penetration test will be described according to the Methodology (chapter 2). This chapter is categorized per scope subject, and then the vulnerabilities from the highest to the lowest. Each finding will contain information regarding how the vulnerability works, what the impact is and how its mitigated.

1.7. Infrastructure – Part A

The following items in this report will disclose the discovered vulnerabilities and misconfigurations within the assessed infrastructure.

Each vulnerability or misconfiguration will be described with the following details:

- A technical risk rating.
- The functionality where the vulnerability was discovered.
- How the vulnerability could be exploited by an attacker, provided with technical details.
- A recommendation how to mitigate the discovered vulnerability or misconfiguration and how to prevent this from happening in the future.

1.1.1. <Name of the finding>

HOST	CVSS 4.0 SCORE	CVSS VECTOR	CIS-ID	SEVERITY
<hostname>	<CVSS Score>	<Attack vector>	<reference>	MEDIUM

<Introduction explaining what the vulnerability or misconfiguration is about>

<Description where the issue was found within the application>

<Evidence either by a screenshot or an HTTP request / response>

<Mitigation suggestions and recommendations based on security best practices and standards>

1.8. Application – Part B

The following items in this report will disclose the discovered vulnerabilities within the assessed application.

Each vulnerability will be described with the following details:

- A technical risk rating.
- The functionality where the vulnerability was discovered.
- How the vulnerability could be exploited by an attacker, provided with technical details.
- A recommendation how to mitigate the discovered vulnerability or misconfiguration.

1.1.2. <Name of the finding>

HOST	CVSS 4.0 SCORE	CVSS VECTOR	WSTG ID	SEVERITY
<hostname>	<CVSS Score>	<Attack vector>	<reference>	MEDIUM

<Introduction explaining what the vulnerability or misconfiguration is about>

<Description where the issue was found within the application>

<Evidence either by a screenshot or an HTTP request / response>

<Mitigation suggestions and recommendations based on security best practices and standards>

6. Post-exploitation

To assess value of the compromised targets, this chapter will first provide information regarding the accounts and systems which have been gained access to, which path of Privilege Escalation has been taken and finally which likely use cases have been identified. Information from the previous steps will be used to assess the post-exploitation steps.

1.9. Acquired accounts

In the table below an overview of the accounts acquired:

Account	Host	Description

Since the passwords and/or the hashes are known following the penetration tests, it is recommended to reset passwords from the accounts above.

1.10. Privilege Escalation

The table below provides a description of how privilege escalation occurred, mapped to the related vulnerabilities:

Step	ID vulnerability	Host	Action	Result
1				
2				
3				

7. Appendix

1.11. Glossary

Term	Description

1.12. Utilized tools

This section provides a comprehensive overview of the tools employed during the security assessment, along with their respective version numbers. The inclusion of version information is essential for transparency, as it ensures a clear understanding of the technological landscape at the time of the assessment.

Name	Version	Description and URL
BurpSuite Professional	v2023.10.3.6	A web application security testing tool designed for analyzing and identifying vulnerabilities in web applications. https://portswigger.net/burp/communitydownload
Dirbuster	v2.22	A web application scanner that helps identify hidden directories and files by launching dictionary-based attacks against a target web server.
Python3	v310.12	Python 3 is a high-level programming language known for its readability and versatility, widely used for web development, data analysis, artificial intelligence, and scripting.

1.13. Evidence

1.1.3. Documents

In the table below an overview of the documents which have been received from Client:

Filename	Description	SHA1 Hash

1.1.4. Received files

In the table below an overview of the files which have been received from Client:

Filename	Description	SHA1 Hash

1.1.5. Output

In the table below an overview of the source files generated by the penetration test, such as logfiles and scan results:

Filename	Description	SHA1 Hash

1.14. Changes

During the penetration test, some changes might have been made to the environment. Not in all cases it is possible to revert the change after the penetration test. It is always recommended to verify if these changes are undone.

1.1.6.Accounts

The following table contains an overview of received user accounts, per scope object:

Account	Environment	Description

It is recommended to delete or disable these accounts. Alternatively, Client could consider a password reset.

1.1.7.Uploaded files

The following files have been uploaded during the penetration test:

Filename	Description	SHA1 Hash

1.15. Scan results

During the vulnerability analysis stage, network scanning has been performed. In the paragraphs below is an overview of these results. The following ranges have been scanned: [insert ranges].

1.1.8. Port scanning

Port scanning is a technique used to identify and probe open ports to detect services on a system or network and is used during the information gathering phase. As part of the information gathering phase, the following hosts and their associated services were identified:

1	2	3	4
HOSTS UP	OPEN PORTS	CLOSED PORTS	FILTERED PORTS

Port status	Description
open	An application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port.
closed	A closed port is accessible as it receives and responds to port scanning probe packets, but there is no application listening on it.
filtered	The port scanner cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall software.

Host	Protocol	Port	State	Service	Banner
	tcp	80	open	http	
	tcp	443	open	http	

1.1.9.File shares

The following SMB/NFS and ISCSII fileshares have been identified during scanning activity:

Host	IP-address	Share	Permissions

1.16. OSINT

1.1.10. Search engines

1.1.11. Subdomains/DNS

1.1.12. Websites

1.1.13. Certificates

1.1.14. Email addresses

1.1.15. Leaked credentials

1.17. Scope-objects

During the penetration test, the following deviations from the Plan of Approach have been identified:

□ [Describe deviations]

8.Checklists

1.18. Web Application Security Checklist (WSTG)

A web application security checklist is a comprehensive list of security considerations and best practices that developers, security professionals, and organizations should follow to ensure the security of their web applications. This checklist helps identify potential vulnerabilities and risks that can be exploited by attackers.

Test ID	Description	Result
WSTG-INFO-01	Conduct search engine discovery and reconnaissance for information leakage	
WSTG-INFO-02	Fingerprint web server	
WSTG-INFO-03	Review web server meta files for information leakage	
WSTG-INFO-04	Enumerate applications on web server	
WSTG-INFO-0505	Review webpage comments and meta data for information leakage	
WSTG-INFO-06	Identify application entry points	
WSTG-INFO-07	Map execution paths through application	
WSTG-INFO-08	Fingerprint web application framework	
WSTG-INFO-09	Fingerprint web application	
WSTG-INFO-10	Map application architecture	
WSTG-CONF-01	Test Network Infrastructure Configuration	
WSTG-CONF-02	Test Application Platform Configuration	
WSTG-CONF-03	Test File Extensions Handling for Sensitive Information	
WSTG-CONF-04	Review Old Backup and Unreferenced Files for Sensitive Information	
WSTG-CONF-05	Enumerate Infrastructure and Application Admin Interfaces	
WSTG-CONF-06	Test HTTP Methods	
WSTG-CONF-07	Test HTTP Strict Transport Security	
WSTG-CONF-08	Test RIA Cross Domain Policy	
WSTG-CONF-09	Test File Permission	
WSTG-CONF-10	Test for Subdomain Takeover	
WSTG-CONF-11	Test Cloud Storage	
WSTG-CONF-12	Testing for Content Security Policy	

WSTG-CONF-08	Test RIA cross domain policy	
WSTG-IDNT-01	Test Role Definitions	
WSTG-IDNT-02	Test User Registration Process	
WSTG-IDNT-03	Test Account Provisioning Process	
WSTG-IDNT-04	Testing for Account Enumeration and Guessable User Account	
WSTG-IDNT-05	Testing for Weak or Unenforced Username Policy	
WSTG-ATHN-01	Testing for Credentials Transported over an Encrypted Channel	
WSTG-ATHN-02	Testing for Default Credentials	
WSTG-ATHN-03	Testing for Weak Lock Out Mechanism	
WSTG-ATHN-04	Testing for Bypassing Authentication Schema	
WSTG-ATHN-05	Testing for Vulnerable Remember Password	
WSTG-ATHN-06	Testing for Browser Cache Weakness	
WSTG-ATHN-07	Testing for Weak Password Policy	
WSTG-ATHN-08	Testing for Weak Security Question Answer	
WSTG-ATHN-09	Testing for Weak Password Change or Reset Functionalities	
WSTG-ATHN-10	Testing for Weaker Authentication in Alternative Channel	
WSTG-ATHZ-01	Testing Directory Traversal File Include	
WSTG-ATHZ-02	Testing for Bypassing Authorization Schema	
WSTG-ATHZ-03	Testing for Privilege Escalation	
WSTG-ATHZ-04	Testing for Insecure Direct Object References	
WSTG-SESS-01	Testing for Session Management Schema	
WSTG-SESS-02	Testing for Cookies Attributes	
WSTG-SESS-03	Testing for Session Fixation	
WSTG-SESS-04	Testing for Exposed Session Variables	
WSTG-SESS-05	Testing for Cross Site Request Forgery	

WSTG-SESS-06	Testing for Logout Functionality	
WSTG-SESS-07	Testing Session Timeout	
WSTG-SESS-08	Testing for Session Puzzling	
WSTG-SESS-09	Testing for Session Hijacking	
WSTG-SESS-10	Testing JSON Web Tokens	
WSTG-INPV-01	Testing for Reflected Cross Site Scripting	
WSTG-INPV-02	Testing for Stored Cross Site Scripting	
WSTG-INPV-03	Testing for HTTP Verb Tampering	
WSTG-INPV-04	Testing for HTTP Parameter pollution	
WSTG-INPV-05	Testing for SQL Injection	
WSTG-INPV-06	Testing for LDAP Injection	
WSTG-INPV-07	Testing for XML Injection	
WSTG-INPV-08	Testing for SSI Injection	
WSTG-INPV-09	Testing for XPath Injection	
WSTG-INPV-10	Testing for IMAP SMTP Injection	
WSTG-INPV-11	Testing for Code Injection	
WSTG-INPV-12	Testing for Command Injection	
WSTG-INPV-13	Testing for Format String Injection	
WSTG-INPV-14	Testing for Incubated Vulnerabilities	
WSTG-INPV-15	Testing for HTTP Splitting Smuggling	
WSTG-INPV-16	Testing for HTTP Incoming Requests	
WSTG-INPV-17	Testing for Host Header Injection	
WSTG-INPV-18	Testing for Server-Side Template Injection	
WSTG-INPV-19	Testing for Server-Side Request Forgery	
WSTG-ERRH-01	Testing for Improper Error Handling	
WSTG-ERRH-02	Testing for Stack Traces	

WSTG-CRYP-01	Testing for Weak Transport Layer Security	
WSTG-CRYP-02	Testing for Padding Oracle	
WSTG-CRYP-03	Testing for Sensitive Information Sent Via Unencrypted Channels	
WSTG-CRYP-04	Testing for Weak Encryption	
WSTG-BUSL-01	Test Business Logic Data Validation	
WSTG-BUSL-02	Test Ability to Forge Requests	
WSTG-BUSL-03	Test Integrity Checks	
WSTG-BUSL-04	Test for Process Timing	
WSTG-BUSL-05	Test Number of Times a Function Can Be Used Limits	
WSTG-BUSL-06	Testing for the Circumvention of Work Flows	
WSTG-BUSL-07	Test Defenses Against Application Misuse	
WSTG-BUSL-08	Test Upload of Unexpected File Types	
WSTG-BUSL-09	Test Upload of Malicious Files	
WSTG-CLNT-01	Testing for DOM Based Cross Site Scripting	
WSTG-CLNT-02	Testing for JavaScript Execution	
WSTG-CLNT-03	Testing for HTML Injection	
WSTG-CLNT-04	Testing for Client-Side URL Redirect	
WSTG-CLNT-05	Testing for CSS Injection	
WSTG-CLNT-06	Testing for Client-Side Resource Manipulation	
WSTG-CLNT-07	Test Cross Origin Resource Sharing	
WSTG-CLNT-08	Testing for Cross Site Flashing	
WSTG-CLNT-09	Testing for Clickjacking	
WSTG-CLNT-10	Testing WebSockets	
WSTG-CLNT-11	Test Web Messaging	
WSTG-CLNT-12	Test Browser Storage	

WSTG-CLNT-13	Testing for Cross Site Script Inclusion	
WSTG-APIT-01	Testing GraphQL	

1.19. CIS Linux operating system checklist

The Center for Internet Security (CIS) Benchmark is a set of best practice guidelines and recommendations for securing computer systems and networks. These benchmarks are developed and published by the Center for Internet Security, a non-profit organization dedicated to enhancing the cybersecurity of organizations and individuals. CIS Benchmarks are designed to help organizations improve their security posture by providing specific, actionable recommendations for various operating systems, software, and network devices.

1.1.1	Disable unused filesystems	Yes	No	Unknown
1.1.1.1	Ensure mounting of cramfs filesystems is disabled			x
1.1.1.2	Ensure mounting of squashfs filesystems is disabled			x
1.1.1.3	Ensure mounting of udf filesystems is disabled			x
1.1.2	Configure /tmp	Yes	No	Unknown
1.1.2.1	Ensure /tmp is a seperate partition			x
1.1.2.2	Ensure nodev option is set on the /tmp partition			x
1.1.2.3	Ensure noexec option is set on the /tmp partition			x
1.1.2.4	Ensure nosuid option is set on the /tmp partition			x
1.1.3	Configure /var	Yes	No	Unknown
1.1.3.1	Ensure separate partition exists for /var			x
1.1.3.2	Ensure nodev option is set on the /var partition			x
1.1.3.3	Ensure nosuid option is set on the /var partition			x
1.1.4	Configure /var/tmp	Yes	No	Unknown
1.1.4.1	Ensure separate partition exists for /var/tmp			x
1.1.4.2	Ensure noexec option set on the /var/tmp partition			x
1.1.4.3	Ensure nosuid option set on the /var/tmp partition			x
1.1.4.4	Ensure nodev option set on the /var/tmp partition			x
1.1.5	Configure /var/log	Yes	No	Unknown
1.1.5.1	Ensure separate partition exists for /var/log			x

1.1.5.2	Ensure nodev option set on the /var/log partition			x
1.1.5.3	Ensure noexec option set on the /var/log partition			x
1.1.5.4	Ensure nosuid option set on the /var/log partition			x
1.1.6	Configure /var/log/audit	Yes	No	Unknown
1.1.6.1	Ensure separate partition exists for the /var/log/audit partition			x
1.1.6.2	Ensure noexec option set on the /var/log/audit partition			x
1.1.6.3	Ensure nodev option set on the /var/log/audit partition			x
1.1.6.4	Ensure nosuid option set on the /var/log/audit partition			x
1.1.7	Configure /home	Yes	No	Unknown
1.1.7.1	Ensure separate partition exists for /home			x
1.1.7.2	Ensure nodev option set on the /home partition			x
1.1.7.3	Ensure nosuid option set on the /home partition			x
1.1.8	Configure /dev/shm	Yes	No	Unknown
1.1.8.1	Ensure nodev option set on the /dev/shm partition			x
1.1.8.2	Ensure noexec option set on the /dev/shm partition			x
1.1.8.3	Ensure nosuid option set on the /dev/shm partition			x
1.1.9	Disable automounting			x
1.1.10	Disable USB storage			x
1.2	Configure software updates	Yes	No	Unknown
1.2.1	Ensure package manager repositories are configured			x
1.2.2	Ensure GPG keys are configured			x
1.3	File system integrity checking	Yes	No	Unknown

1.3.1	Ensure AIDE is installed			x
1.3.2	Ensure filesystem integrity is regularly checked			x
1.4	Secure boot settings	Yes	No	Unknown
1.4.1	Ensure bootloader password is set			x
1.4.2	Ensure permissions on bootloader config are configured			x
1.4.3	Ensure authentication required for single user mode			x
1.4	Secure boot settings	Yes	No	Unknown
1.4.1	Ensure bootloader password is set			x
1.4.2	Ensure permissions on bootloader config are configured			x
1.4.3	Ensure authentication required for single user mode			x
1.5	Additional process hardening	Yes	No	Unknown
1.5.1	Ensure address space layout randomization (ASLR) is enabled			x
1.5.2	Ensure prelink is not installed			x
1.5.3	Ensure Automatic Error Reporting is not enabled			x
1.5.4	Ensure core dumps are restricted			x
1.6	Mandatory access control	Yes	No	Unknown
1.6.1.1	Ensure AppArmor is installed			x
1.6.1.2	Ensure AppArmor is enabled in the bootloader configuration			x
1.6.1.3	Ensure all AppArmor Profiles are in enforce or complain mode			x
1.6.1.4	Ensure all AppArmor Profiles are enforcing			x
1.7	Command line warning banners	Yes	No	Unknown
1.7.1	Ensure message of the day is configured properly			x
1.7.2	Ensure local login warning banner is configured properly			x

1.7.3	Ensure remote login warning banner is configured			x
1.7.4	Ensure permissions on /etc/motd are configured			x
1.7.5	Ensure permissions on /etc/issue are configured			x
1.7.6	Ensure permissions on /etc/issue.net are configured			x
1.8	Gnome display manager	Yes	No	Unknown
1.8.1	Ensure GNOME Display Manager is removed			x
1.8.2	Ensure GDM login banner is configured			x
1.8.3	Ensure GDM disable-user-list option is enabled			x
1.8.4	Ensure GDM screen locks when the user is idle			x
1.8.5	Ensure GDM screen locks cannot be overridden			x
1.8.6	Ensure GDM automatic mounting of removable media is disabled			x
1.8.7	Ensure GDM disabling automatic mounting of removable media is not overridden			x
1.8.8	Ensure GDM autorun-never is enabled			x
1.8.9	Ensure GDM autorun-never is not overridden			x
1.8.10	Ensure XDCMP is not enabled			x
1.9	Ensure updates, patches, and additional security software are installed			x
2.1.1	Ensure time synchronization is in use	Yes	No	Unknown
2.1.1.1	Ensure a single time synchronization daemon is in use			x
2.1.2	Configure chrony	Yes	No	Unknown
2.1.2.1	Ensure chrony is configured with authorized timeserver			x
2.1.2.2	Ensure chrony is running as user _chrony			x
2.1.2.3	Ensure chrony is enabled and running			x

2.1.3	Configure systemd-timesyncd	Yes	No	Unknown
2.1.3.1	Ensure systemd-timesyncd configured with authorized timeserver			x
2.1.3.2	Ensure systemd-timesyncd is enabled and running			x
2.1.3	Configure ntp	Yes	No	Unknown
2.1.3.1	Ensure ntp access control is configured			x
2.1.3.2	Ensure ntp is configured with authorized timeserver			x
2.1.3.3	Ensure ntp is running as user ntp			x
2.1.3.4	Ensure ntp is enabled and running			x
2.2	Special purpose services	Yes	No	Unknown
2.2.1	Ensure X Window System is not installed			x
2.2.2	Ensure Avahi Server is not installed			x
2.2.3	Ensure CUPS is not installed			x
2.2.4	Ensure DHCP Server is not installed			x
2.2.5	Ensure LDAP server is not installed			x
2.2.6	Ensure NFS is not installed			x
2.2.7	Ensure DNS Server is not installed			x
2.2.8	Ensure FTP Server is not installed			x
2.2.9	Ensure HTTP server is not installed			x
2.2.10	Ensure IMAP and POP3 server are not installed			x
2.2.11	Ensure Samba is not installed			x
2.2.12	Ensure HTTP Proxy Server is not installed			x
2.2.13	Ensure SNMP Server is not installed			x
2.2.14	Ensure NIS Server is not installed			x
2.2.15	Ensure mail transfer agent is configured for local-only mode			x
2.2.16	Ensure rsync service is either not installed or masked			x
2.3	Service clients	Yes	No	Unknown

2.3.1	Ensure NIS Client is not installed			x
2.3.2	Ensure rsh client is not installed			x
2.3.3	Ensure talk client is not installed			x
2.3.4	Ensure telnet client is not installed			x
2.3.5	Ensure LDAP client is not installed			x
2.3.6	Ensure RPC is not installed			x
2.3.7	Ensure nonessential services are removed or masked			x
3.1	Disable unused network protocols and devices	Yes	No	Unknown
3.1.1	Ensure system is checked to determine if IPv6 is enabled			x
3.1.2	Ensure wireless interfaces are disabled			x
3.2	Network parameters (host only)	Yes	No	Unknown
3.2.1	Ensure packet redirect sending is disabled			x
3.2.2	Ensure IP forwarding is disabled			x
3.3	Network parameters (host and router)	Yes	No	Unknown
3.3.1	Ensure source routed packets are not accepted			x
3.3.2	Ensure ICMP redirects are not accepted			x
3.3.3	Ensure secure ICMP redirects are not accepted			x
3.3.4	Ensure suspicious packets are logged			x
3.3.5	Ensure broadcast ICMP requests are ignored			x
3.3.6	Ensure bogus ICMP responses are ignored			x
3.3.7	Ensure Reverse Path Filtering is enabled			x
3.3.8	Ensure TCP SYN Cookies is enabled			x
3.3.9	Ensure IPv6 router advertisements are not accepted			x
3.4	Uncommon network protocols	Yes	No	Unknown
3.4.1	Ensure DCCP is disabled			x

3.4.2	Ensure SCTP is disabled			x
3.4.3	Ensure RDS is disabled			x
3.4.4	Ensure TIPC is disabled			x
3.5.1	Configure uncomplicated firewall	Yes	No	Unknown
3.5.1.1	Ensure ufw is installed			x
3.5.1.2	Ensure iptables-persistent is not installed with ufw			x
3.5.1.3	Ensure ufw service is enabled			x
3.5.1.4	Ensure ufw loopback traffic is configured			x
3.5.1.5	Ensure ufw outbound connections are configured			x
3.5.1.6	Ensure ufw firewall rules exist for all open ports			x
3.5.1.7	Ensure ufw default deny firewall policy			x
3.5.2	Configure nftables	Yes	No	Unknown
3.5.2.1	Ensure nftables is installed			x
3.5.2.2	Ensure ufw is uninstalled or disabled with nftables			x
3.5.2.3	Ensure iptables are flushed with nftables			x
3.5.2.4	Ensure a nftables table exists			x
3.5.2.5	Ensure nftables base chains exist			x
3.5.2.6	Ensure nftables loopback traffic is configured			x
3.5.2.7	Ensure nftables outbound and established connections are configured			x
3.5.2	Configure nftables	Yes	No	Unknown
3.5.2.1	Ensure nftables is installed			x
3.5.2.2	Ensure ufw is uninstalled or disabled with nftables			x
3.5.2.3	Ensure iptables are flushed with nftables			x
3.5.2.4	Ensure iptables are flushed with nftables			x
3.5.2.5	Ensure nftables base chains exist			x

3.5.2.6	Ensure nftables loopback traffic is configured			x
3.5.2.7	Ensure nftables outbound and established connections			x
3.5.2.8	Ensure nftables default deny firewall policy			x
3.5.2.9	Ensure nftables service is enabled			x
3.5.2.10	Ensure nftables rules are permanent			x
3.5.3.1	Configure iptables software	Yes	No	Unknown
3.5.3.1.1	Ensure iptables packages are installed			x
3.5.3.1.2	Ensure nftables is not installed with iptables			x
3.5.3.1.3	Ensure ufw is uninstalled or disabled with iptables			x
3.5.3.2	Configure IPv4 iptables	Yes	No	Unknown
3.5.3.2.1	Ensure iptables default deny firewall policy			x
3.5.3.2.2	Ensure iptables loopback traffic is configured			x
3.5.3.2.3	Ensure iptables outbound and established connections are configured			x
3.5.3.2.4	Ensure iptables firewall rules exist for all open ports			x
3.5.3.3	Configure IPv6 iptables	Yes	No	Unknown
3.5.3.3.1	Ensure ip6tables default deny firewall policy			x
3.5.3.3.2	Ensure ip6tables loopback traffic is configured			x
3.5.3.3.3	Ensure ip6tables outbound and established connections are configured			x
3.5.3.3.4	Ensure ip6tables firewall rules exist for all open ports			x
4.1.1	Ensure auditing is enabled	Yes	No	Unknown
4.1.1.1	Ensure auditd is installed			x
4.1.1.2	Ensure auditd service is enabled and active			x
4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled			x
4.1.1.4	Ensure audit_backlog_limit is sufficient			x

4.1.2	Configure data retention	Yes	No	Unknown
4.1.2.1	Ensure audit log storage size is configured			x
4.1.2.2	Ensure audit logs are not automatically deleted			x
4.1.2.3	Ensure system is disabled when audit logs are full			x
4.1.3	Configure auditd rules	Yes	No	Unknown
4.1.3.1	Ensure audit log storage size is configured			x
4.1.3.2	Ensure audit logs are not automatically deleted			x
4.1.3.3	Ensure system is disabled when audit logs are full			x
4.1.3.4	Ensure events that modify date and time information are collected			x
4.1.3.5	Ensure events that modify the system's network			x
4.1.3.6	Ensure use of privileged commands are collected			x
4.1.3.7	Ensure unsuccessful file access attempts are collected			x
4.1.3.8	Ensure events that modify user/group information are collected			x
4.1.3.9	Ensure discretionary access control permission modification events are collected			x
4.1.3.10	Ensure successful file system mounts are collected			x
4.1.3.11	Ensure session initiation information is collected			x
4.1.3.12	Ensure login and logout events are collected			x
4.1.3.13	Ensure file deletion events by users are collected			x
4.1.3.14	Ensure events that modify the system's Mandatory Access Controls are collected			x
4.1.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded			x
4.1.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded			x
4.1.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded			x
4.1.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded			x
4.1.3.19	Ensure kernel module loading unloading and modification is collected			x

4.1.3.20	Ensure the audit configuration is immutable			x
4.1.3.21	Ensure the running and on disk configuration is the same			x
4.1.4	Configure auditd file access	Yes	No	Unknown
4.1.4.1	Ensure audit log files are mode 0640 or less permissive			x
4.1.4.2	Ensure only authorized users own audit log files			x
4.1.4.3	Ensure only authorized groups are assigned ownership of audit log files			x
4.1.4.4	Ensure the audit log directory is 0750 or more restrictive			x
4.1.4.5	Ensure audit configuration files are 640 or more restrictive			x
4.1.4.6	Ensure audit configuration files are owned by root			x
4.1.4.7	Ensure audit configuration files belong to group root			x
4.1.4.8	Ensure audit tools are 755 or more restrictive			x
4.1.4.9	Ensure audit tools are owned by root			x
4.1.4.10	Ensure audit tools belong to group root			x
4.1.4.11	Ensure cryptographic mechanisms are used to protect the integrity of audit tools			x
4.2.1	Configure journald	Yes	No	Unknown
4.2.1.1	Ensure journald is configured to send logs to a remote log host			x
4.2.1.2	Ensure systemd-journal-remote is installed			x
4.2.1.3	Ensure systemd-journal-remote is configured			x
4.2.1.4	Ensure systemd-journal-remote is enabled			x
4.2.1.5	Ensure journald is not configured to recieve logs from a remote client			x
4.2.1.6	Ensure journald service is enabled			x
4.2.1.7	Ensure journald is configured to compress large log files			x
4.2.1.8	Ensure journald is configured to write logfiles to persistent disk			x
4.2.1.9	Ensure journald is not configured to send logs to rsyslog			x
4.2.1.10	Ensure journald log rotation is configured per site policy			x
4.2.1.11	Ensure journald default file permissions configured			x

4.2.1	Configure rsyslogd	Yes	No	Unknown
4.2.1.1	Ensure rsyslog is installed			x
4.2.1.2	Ensure rsyslog service is enabled			x
4.2.1.3	Ensure journald is configured to send logs to rsyslog			x
4.2.1.4	Ensure rsyslog default file permissions are configured			x
4.2.1.5	Ensure logging is configured			x
4.2.1.6	Ensure rsyslog is configured to send logs to a remote log host			x
4.2.1.7	Ensure rsyslog is not configured to receive logs from a remote client			x
4.2.1.8	Ensure all logfiles have appropriate permissions and ownership			x
5.1	Configure time-based job schedulers	Yes	No	Unknown
5.1.1	Ensure cron daemon is enabled and running			x
5.1.2	Ensure permissions on /etc/crontab are configured			x
5.1.3	Ensure permissions on /etc/cron.hourly are configured			x
5.1.4	Ensure permissions on /etc/cron.daily are configured			x
5.1.5	Ensure permissions on /etc/cron.weekly are configured			x
5.1.6	Ensure permissions on /etc/cron.monthly are configured			x
5.1.7	Ensure permissions on /etc/cron.d are configured			x
5.1.8	Ensure cron is restricted to authorized users			x
5.1.9	Ensure at is restricted to authorized users			x
5.2	Configure SSH server	Yes	No	Unknown
5.2.1	Ensure permissions on /etc/ssh/sshd_config are configured			x
5.2.2	Ensure permissions on SSH private host key files are configured			x
5.2.3	Ensure permissions on SSH public host key files are configured			x
5.2.4	Ensure SSH access is limited			x
5.2.5	Ensure SSH LogLevel is appropriate			x
5.2.6	Ensure SSH PAM is enabled			x

5.2.7	Ensure SSH root login is disabled			x
5.2.8	Ensure SSH HostbasedAuthentication is disabled			x
5.2.9	Ensure SSH PermitEmptyPasswords is disabled			x
5.2.10	Ensure SSH PermitUserEnvironment is disabled			x
5.2.11	Ensure SSH IgnoreRhosts is enabled			x
5.2.12	Ensure SSH X11 forwarding is disabled			x
5.2.13	Ensure only strong Ciphers are used			x
5.2.14	Ensure only strong MAC algorithms are used			x
5.2.15	Ensure only strong Key Exchange algorithms are used			x
5.2.16	Ensure SSH AllowTcpForwarding is disabled			x
5.2.17	Ensure SSH warning banner is configured			x
5.2.18	Ensure SSH MaxAuthTries is set to 4 or less			x
5.2.19	Ensure SSH MaxStartups is configured			x
5.2.20	Ensure SSH MaxSessions is set to 10 or less			x
5.2.21	Ensure SSH LoginGraceTime is set to one minute or less			x
5.2.22	Ensure SSH Idle Timeout Interval is configured			x
5.3	Configure privilege escalation	Yes	No	Unknown
5.3.1	Ensure sudo is installed			x
5.3.2	Ensure sudo commands use pty			x
5.3.3	Ensure sudo log file exists			x
5.3.4	Ensure users must provide password for privilege escalation			x
5.3.5	Ensure re-authentication for privilege escalation is not disabled globally			x
5.3.6	Ensure sudo authentication timeout is configured correctly			x
5.3.7	Ensure access to the su command is restricted			x
5.4	Configure PAM	Yes	No	Unknown
5.4.1	Ensure password creation requirements are configured			x
5.4.2	Ensure lockout for failed password attempts is configured			x

5.4.3	Ensure password reuse is limited			x
5.4.4	Ensure password hashing algorithm is up to date with the latest standards			x
5.4.5	Ensure all current passwords uses the configured hashing algorithm			x
5.5	Set shadow password suite parameters	Yes	No	Unknown
5.5.1	Ensure minimum days between password changes is configured			x
5.5.2	Ensure password expiration is 365 days or less			x
5.5.3	Ensure password expiration warning days is 7 or more			x
5.5.4	Ensure inactive password lock is 30 days or less			x
5.5.5	Ensure all users last password change date is in the past			x
5.5.6	Ensure system accounts are secured			x
5.5.7	Ensure default group for the root account is GID 0			x
5.5.8	Ensure default user umask is 027 or more restrictive			x
5.5.9	Ensure default user shell timeout is 900 seconds or less			x
6.1	System file permissions	Yes	No	Unknown
6.1.1	Ensure permissions on /etc/passwd are configured			x
6.1.2	Ensure permissions on /etc/passwd- are configured			x
6.1.3	Ensure permissions on /etc/group are configured			x
6.1.4	Ensure permissions on /etc/group- are configured			x
6.1.5	Ensure permissions on /etc/shadow are configured			x
6.1.6	Ensure permissions on /etc/shadow- are configured			x
6.1.7	Ensure permissions on /etc/gshadow are configured			x
6.1.8	Ensure permissions on /etc/gshadow- are configured			x
6.1.9	Ensure no world writable files exist			x
6.1.10	Ensure no unowned files or directories exist			x
6.1.11	Ensure no ungrouped files or directories exist			x
6.1.12	Audit SUID executables			x
6.1.13	Audit SGID executables			x

6.2	Local user and group settings	Yes	No	Unknown
6.2.1	Ensure accounts in /etc/passwd use shadowed passwords			x
6.2.2	Ensure /etc/shadow password fields are not empty			x
6.2.3	Ensure all groups in /etc/passwd exist in /etc/group			x
6.2.4	Ensure shadow group is empty			x
6.2.5	Ensure no duplicate UIDs exist			x
6.2.6	Ensure no duplicate GIDs exist			x
6.2.7	Ensure no duplicate user names exist			x
6.2.8	Ensure no duplicate group names exist			x
6.2.9	Ensure root PATH Integrity			x
6.2.10	Ensure root is the only UID 0 account			x
6.2.11	Ensure local interactive user home directories exist			x
6.2.12	Ensure local interactive users own their home directories			x
6.2.13	Ensure local interactive user home directories are mode 750 or more restrictive			x
6.2.14	Ensure no local interactive user has .netrc files			x
6.2.15	Ensure no local interactive user has .forward files			x
6.2.16	Ensure no local interactive user has .rhosts files			x
6.2.17	Ensure local interactive user dot files are not group or world writable			x