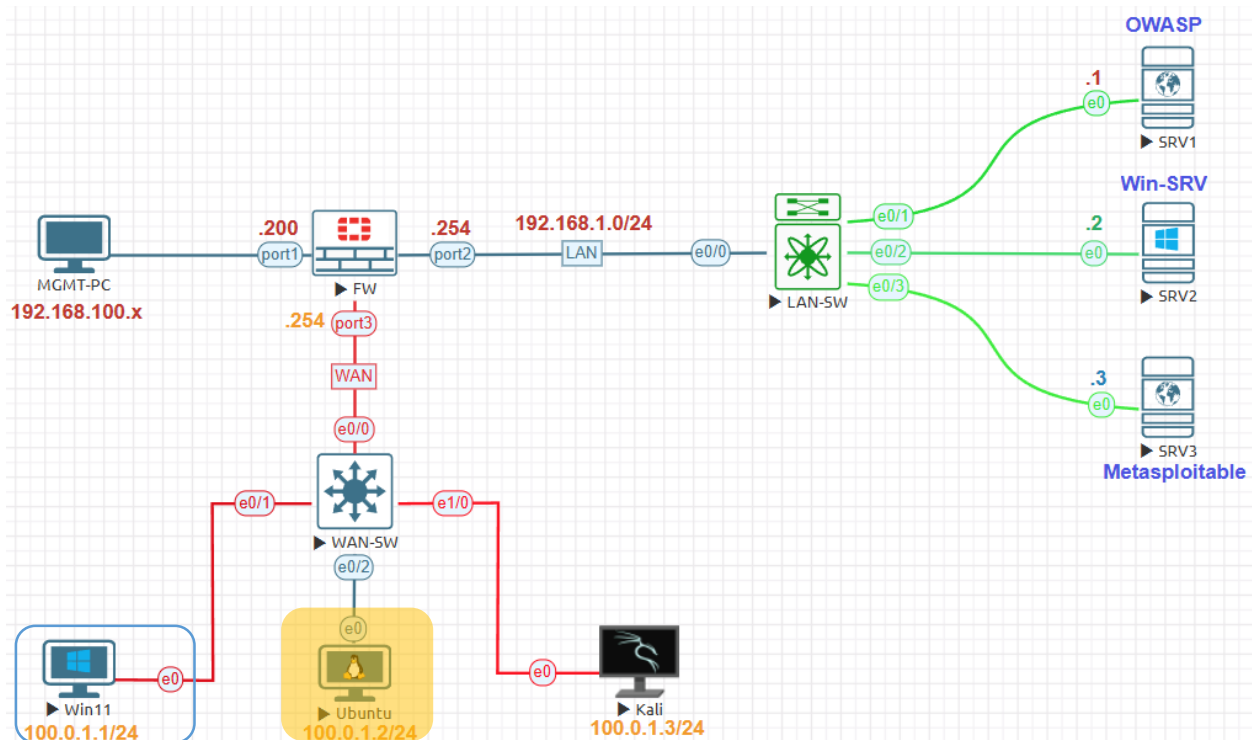


Policy Compliance Auditing Lab:

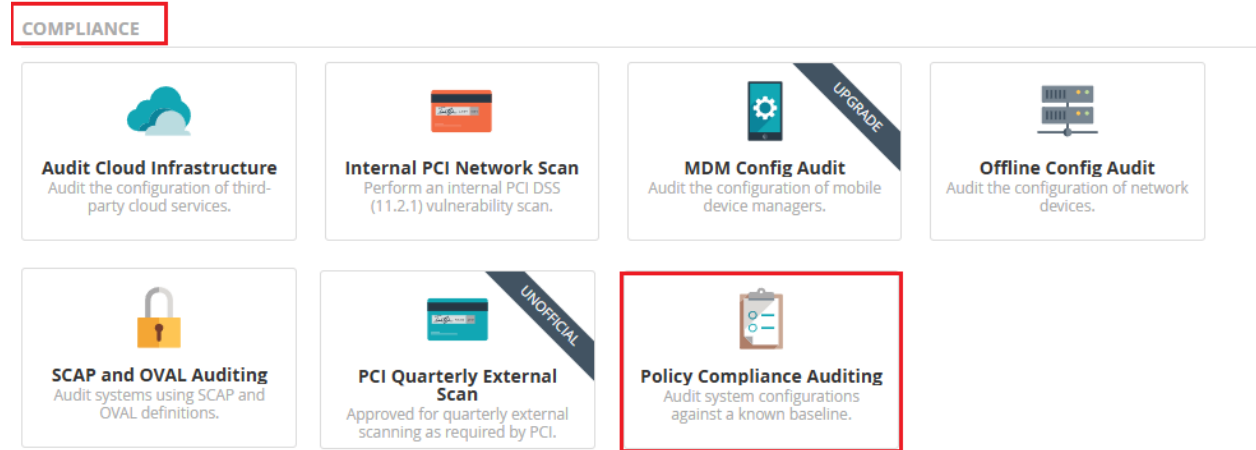


Management Subnet	192.168.100.0/24
FortiGate Management IP	192.168.100.200
Internal Servers Subnet	192.168.1.0/24
FortiGate Firewall External	100.0.1.0/24
FortiGate Firewall Internal IP	192.168.1.254
FortiGate Firewall External IP	100.0.1.254
SRV1 IP Address	192.168.1.1
SRV2 IP Address	192.168.1.2
SRV3 IP Address	192.168.1.3
External Win11 IP Address	100.0.1.1
External Ubuntu IP Address	100.0.1.2
External Kali IP Address	100.0.1.3

Devices	Username	Password
FortiGate 7.0.9	Admin	123
Linux Kali 2025.1c	kali	kali
Linux Ubuntu 22.04 Desktop	user	Test123
Windows 11 x64 SE	user(Administrator)	Test123
Linux Metasploitable 2.0	msfadmin	msfadmin
Linux-OWASP	root	owaspbwa
Windows Server 2012	Administrator	Test123

Go to **Scans > New Scan**. Choose **Policy Compliance Auditing** to open.

COMPLIANCE



- Audit Cloud Infrastructure**
Audit the configuration of third-party cloud services.
- Internal PCI Network Scan**
Perform an internal PCI DSS (11.2.1) vulnerability scan.
- MDM Config Audit** (UPGRADE)
Audit the configuration of mobile device managers.
- Offline Config Audit**
Audit the configuration of network devices.
- SCAP and OVAL Auditing**
Audit systems using SCAP and OVAL definitions.
- PCI Quarterly External Scan** (UNOFFICIAL)
Approved for quarterly external scanning as required by PCI.
- Policy Compliance Auditing** (highlighted)
Audit system configurations against a known baseline.

Name: **Windows11-Policy-Compliance**. Targets: IP address of target **100.0.1.1** which is the IP Address of Windows 11.

Setting>Basic>General

Windows11-Policy-Compliance / Configuration

[Back to Scan Report](#)

Settings | Credentials | Compliance | Plugins

BASIC

- General** (highlighted)
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

General Settings

- Name: Windows11-Policy-Compliance
- Description: Verify Windows 11 CIS Compliance
- Folder: My Scans
- Targets: 100.0.1.1

Settings>Basic>Schedule keep default disable.

[← Back to Scan Report](#)

The screenshot shows the 'Settings' interface with tabs for 'Settings', 'Credentials', and 'Plugins'. Under the 'BASIC' section, there are sub-sections for 'General', 'Schedule', and 'Notifications'. The 'Schedule' sub-section is active, showing a toggle switch labeled 'Enabled' which is currently turned off (OFF). Below the settings are 'Save' and 'Cancel' buttons.

Settings>Basic>Notification keep default disable.

[← Back to Scan Report](#)

The screenshot shows the 'Settings' interface with tabs for 'Settings', 'Credentials', and 'Plugins'. Under the 'BASIC' section, there are sub-sections for 'General', 'Schedule', and 'Notifications'. The 'Notifications' sub-section is active. A yellow warning banner at the top reads: 'Notifications will not be sent until your SMTP Server is configured.' Below this, there is a text input field for 'Email Recipient(s)' with the placeholder text 'Example: me@example.com, you@example.com'. At the bottom, there is a 'Result Filters' section with an 'Add Filter' button.

Settings>Discovery keep scan type Default

Windows11-Policy-Compliance / Configuration

[← Back to Scan Report](#)

The screenshot shows the 'Settings' tab selected in the top navigation bar. On the left, the 'DISCOVERY' category is selected in the sidebar. The main content area is titled 'Scan Type' and features a dropdown menu set to 'Default'. Below this, under 'General Settings', there are two options: 'Ping the remote host' and 'Always test the local Nessus host'. Under 'Scan all devices, including:', there are two options: 'Printers' and 'Novell Netware hosts'.

Settings>Assessment keep default no changes.

Windows11-Policy-Compliance / Configuration

[← Back to Scan Report](#)

The screenshot shows the 'Settings' tab selected in the top navigation bar. On the left, the 'ASSESSMENT' category is selected in the sidebar. The main content area is titled 'Oracle Database' and contains a checkbox labeled 'Use detected SIDs'. Below the checkbox, there is a descriptive paragraph: 'When enabled, if at least one host credential and one Oracle database credential are configured, the scanner authenticates to the Oracle database using the manually specified SIDs in the Oracle database credentials.'

Settings>Reports keep default no changes.

Settings Credentials Compliance Plugins

BASIC >
DISCOVERY >
ASSESSMENT >
REPORT v
ADVANCED >

Output

- Allow users to edit scan results
When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance, this option is required.
- Designate hosts by their DNS name
Uses the host name rather than IP address for report output.
- Display hosts that respond to ping
Reports hosts that successfully respond to a ping.
- Display unreachable hosts
When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts.
- Display Unicode characters
When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and file names. If this issue causes problems with regular expressions in plugins or custom audits, disable this option.

Settings>Advanced keep default no changes.

Settings Credentials Plugins

BASIC >
DISCOVERY >
ASSESSMENT >
REPORT >
ADVANCED v

Scan Type Default v

Performance options:

- 30 simultaneous hosts (max)
- 4 simultaneous checks per host (max)
- 5 second network read timeout

Under **Credentials** Tab. Choose **Windows** authentication methods. In **Windows** choose the Authentication method: **Password** enter username and password of Windows 11 **Administrator/Test123** leave **Domain** empty.

Windows11-Policy-Compliance / Configuration

[Back to Scan Report](#)

Under **Compliance** Tab. Choose Windows 11 related **CIS** Compliances

Plugins Tab leave the default.

PLUGIN FAMILY	TOTAL
General	5
Misc.	1
Policy Compliance	4
Settings	7

Click **Save** Then **Launch**. Wait for the scan to complete.

Windows11-Policy-Compliance / Configuration

[← Back to Scan Report](#)

Settings Credentials Compliance Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

General Settings

Name:

Description:


Folder:

Targets:

Upload Targets [Add File](#)

Post-Processing

Live Results
Enabling this option will identify potential issues discovered by plugins added during updates without actively scanning

 [Save](#) [Cancel](#)

After complete the scan, [Scan Summary Show Authentication / Credential info \(Hosts\)](#) Succeeded.

Scan Summary Hosts 1 Vulnerabilities 4 Compliance 507 History 4

Scan Details

0 Critical Vulnerabilities	0 High Vulnerabilities
0 Medium Vulnerabilities	0 Low Vulnerabilities

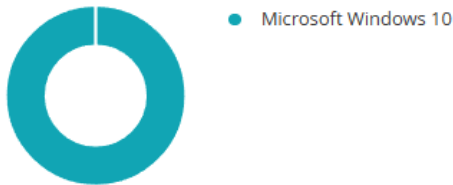
Details

Scan Name: Windows11-Policy-Compliance
Plugin Set: 202505071551
CVSS_Score: CVSS_V3
Scan Template: Policy Compliance Auditing
Scan Start: May 8 at 8:57 PM
Scan End: May 8 at 8:59 PM

Authentication / Credential Info (Hosts)

1 SUCCEEDED	0 FAILED
----------------	-------------

Top 5 Operating Systems Detected During Scan



Scan Durations

00:01:57 SCAN DURATION	00:01:57 MEDIAN SCAN TIME PER HOST	00:01:57 MAX SCAN TIME
---------------------------	---------------------------------------	---------------------------

Under **Vulnerabilities** Tab. It is not Vulnerabilities scan show only info

Windows11-Policy-Compliance

[← Back to My Scans](#)

Scan Summary	Hosts 1	Vulnerabilities 4	Compliance 507	History 4
--------------	---------	--------------------------	----------------	-----------

Filter ▾ Search Vulnerabilities 🔍 4 Vulnerabilities

<input type="checkbox"/>	Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▾	Family ▾
<input type="checkbox"/>	INFO				Netstat Portscanner (WMI)	Port scanners
<input type="checkbox"/>	INFO				Device Hostname	General
<input type="checkbox"/>	INFO				Nessus Scan Information	Settings
<input type="checkbox"/>	INFO				Target Credential Status by Authentication Protocol - Valid Credentials P...	Settings

Under **Compliance** Tab almost **507** issue need to fix the system is not **Compliance**.

Scan Summary	Hosts 1	Vulnerabilities 4	Compliance 507	History 4
--------------	---------	-------------------	-----------------------	-----------

Filter ▾ Search Compliance Checks 🔍 507 Compliance Checks

Sev ▾	Name ▾	Family ▾
FAILED	18.10.9.1.1 (BL) Ensure 'Allow access to BitLocker-protected fixed data drives from earlier versions of Windows' is set t...	Windows Compliance Checks
FAILED	18.10.9.1.10 (BL) Ensure 'Configure use of hardware-based encryption for fixed data drives' is set to 'Disabled'	Windows Compliance Checks
FAILED	18.10.9.1.11 (BL) Ensure 'Configure use of passwords for fixed data drives' is set to 'Disabled'	Windows Compliance Checks
FAILED	18.10.9.1.12 (BL) Ensure 'Configure use of smart cards on fixed data drives' is set to 'Enabled'	Windows Compliance Checks
FAILED	18.10.9.1.13 (BL) Ensure 'Configure use of smart cards on fixed data drives: Require use of smart cards on fixed data ...	Windows Compliance Checks
FAILED	18.10.9.1.2 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered' is set to 'Enabled'	Windows Compliance Checks
FAILED	18.10.9.1.3 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Allow data recovery agent' is ...	Windows Compliance Checks
FAILED	18.10.9.1.4 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Recovery Password' is set to '...	Windows Compliance Checks

Scan Details

Policy: Policy Compliance Auditing
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: May 8 at 8:57 PM
End: May 8 at 8:59 PM
Elapsed: 2 minutes

Compliance



CIS Microsoft Windows 11 Stand Alone Benchmark V2 and V3 Recommendations about Account Policies, Password Policy.

FAILED	1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	Windows Compliance Checks
FAILED	1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'	Windows Compliance Checks
FAILED	1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	Windows Compliance Checks
FAILED	1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'	Windows Compliance Checks
FAILED	1.1.6 (L1) Ensure 'Relax minimum password length limits' is set to 'Enabled'	Windows Compliance Checks
FAILED	18.10.14.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'	Windows Compliance Checks
FAILED	18.10.56.2.3 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'	Windows Compliance Checks
FAILED	18.10.56.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'	Windows Compliance Checks
FAILED	18.10.75.1.3 (L1) Ensure 'Notify Password Reuse' is set to 'Enabled'	Windows Compliance Checks

Can verify and download PDF copy of CIS Benchmarks for Microsoft Windows Desktop from below URL:

<https://www.cisecurity.org/cis-benchmarks>

CIS Benchmarks List

The CIS Benchmarks® are prescriptive configuration recommendations for more than 25+ vendor product families. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.

[DOWNLOAD BENCHMARKS →](#)