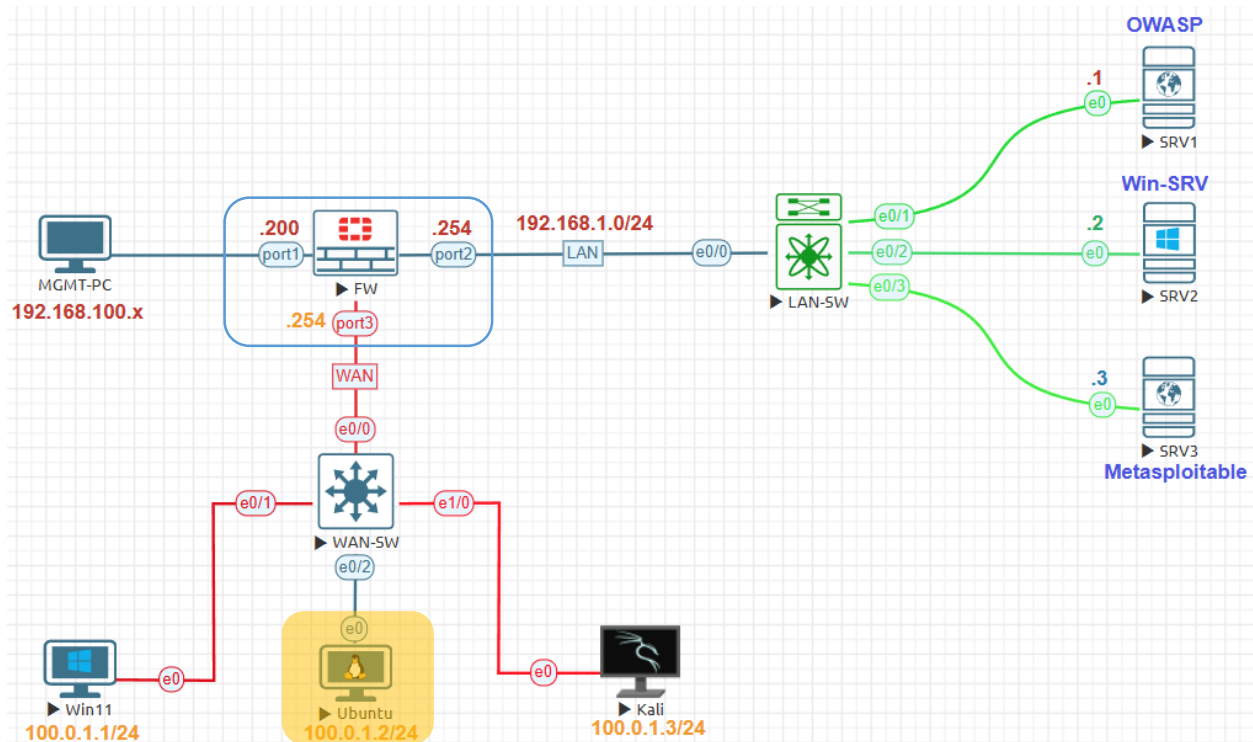


## FortiGate Firewall Vulnerability Scan Lab:



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

Before Start the scan enable **PING,SNMP** and **SSH** on WAN Interface of FortiGate Firewall.

Address

Addressing mode **Manual** DHCP

IP/Netmask 100.0.1.254/255.255.255.0

Secondary IP address

---

Administrative Access

IPv4

HTTPS  SSH  PING  SNMP  FMG-Access  FTM  Speed Test

RADIUS Accounting  Security Fabric Connection ⓘ

Receive LLDP ⓘ Use VDOM Setting **Enable** Disable

Transmit LLDP ⓘ Use VDOM Setting **Enable** Disable

Enable **SNMP Agent**.

Dashboard > Network > Policy & Objects > Security Profiles > VPN > User & Authentication > **System** <sup>1</sup> > **SNMP** ☆

SNMP

Download FortiGate MIB File Download Fortinet Core MIB File

System Information

**SNMP Agent**

Description FW

Location DC

Contact Info Ahmad

SNMP v1/v2c

+ Create New Edit Delete Status ▾

Name ▾	Queries ▾	Traps ▾	Hosts ▾	Events ▾	Status ▾

SNMP v3

+ Create New Edit Delete Status ▾

Name ▾	Security Level ▾	Queries ▾	Traps ▾	Hosts ▾	Events ▾	Status ▾
admin	No Authentication No Private	✓ Enable	✓ Enable	100.0.1.2	37	✓ Enable

0 Security Rating Issues <sup>1</sup>

Go to **Scans > New Scan**. Choose **Advanced Scan** to open.

## Scan Templates

[← Back to Scans](#)

### Scanner

#### DISCOVERY



##### Host Discovery

A simple scan to discover live hosts and open ports.



##### Ping-Only Discovery

A simple scan to discover live hosts with minimal network traffic.

#### VULNERABILITIES



##### Basic Network Scan

A full system scan suitable for any host.



##### Credential Validation

Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets



##### Advanced Scan

Configure a scan without using any recommendations.

Name: **FortiGate-FW-Scan**. Targets: IP address of target **100.0.1.254** the IP Address of WAN Interface of FortiGate Firewall.

### Settings

[Credentials](#)

[Compliance](#)

[Plugins](#)

#### BASIC

General

[Schedule](#)

[Notifications](#)

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

#### General Settings

Name: FortiGate-FW-Scan

Description: FortiGate-FW

Folder: My Scans

Targets: 100.0.1.254

Basic>Schedule keep default disable.

[← Back to Scan Report](#)

**Settings** | Credentials | Plugins

**BASIC** ▾

- General
- Schedule
- Notifications

**DISCOVERY** >

**ASSESSMENT** >

**REPORT** >

**ADVANCED** >

Enabled  OFF

**Save** Cancel

Basic>Notification keep default disable.

[← Back to Scan Report](#)

**Settings** | Credentials | Plugins

**BASIC** ▾

- General
- Schedule
- Notifications

**DISCOVERY** >

**ASSESSMENT** >

**REPORT** >

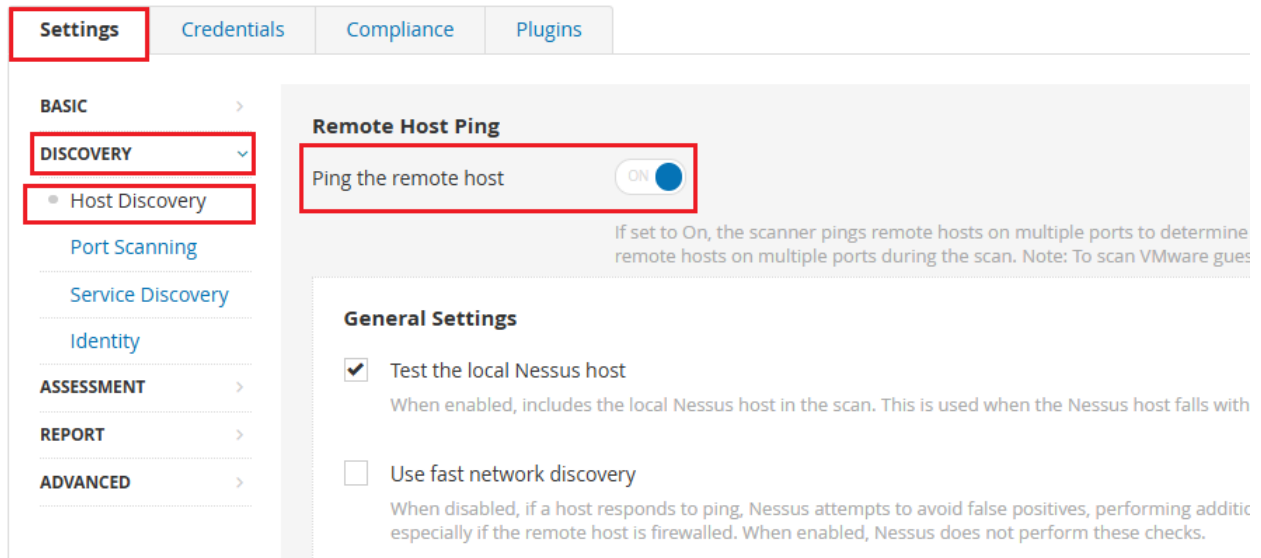
**ADVANCED** >

Notifications will not be sent until your SMTP Server is configured.

Email Recipient(s)

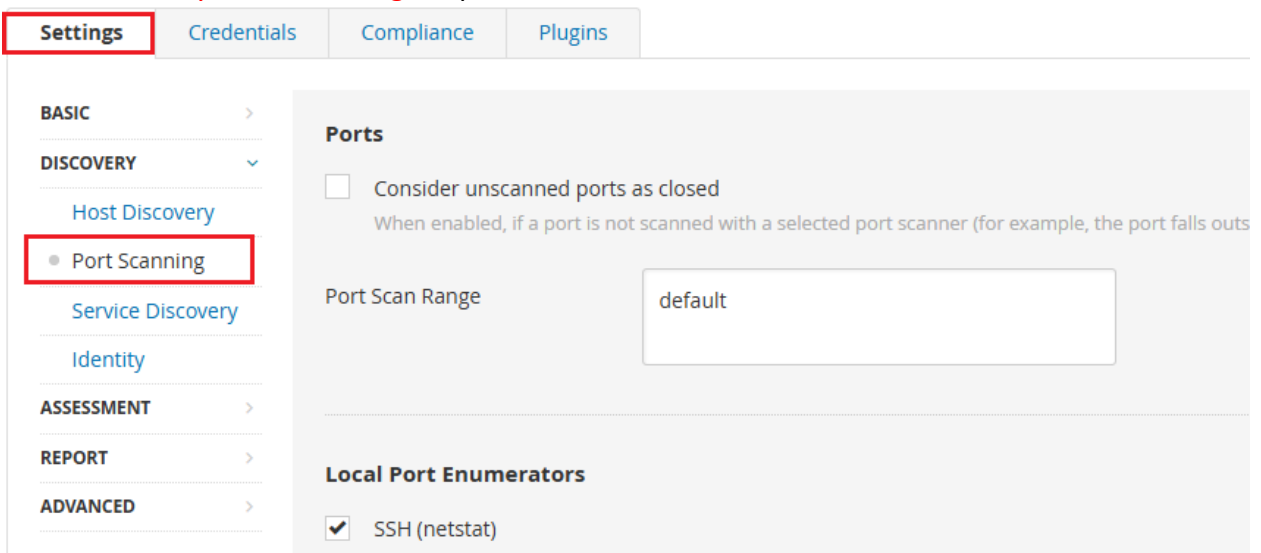
Result Filters [Add Filter](#)

Basic>Discovery>Host Discovery keep default enable.



The screenshot shows the 'Settings' page in Nessus, with the 'Settings' tab highlighted. The left sidebar shows the navigation menu with 'DISCOVERY' and 'Host Discovery' highlighted. The main content area is titled 'Remote Host Ping' and features a toggle switch for 'Ping the remote host' which is currently turned 'ON'. Below this, there is a note: 'If set to On, the scanner pings remote hosts on multiple ports to determine remote hosts on multiple ports during the scan. Note: To scan VMware guests'. Under the 'General Settings' section, there are two options: 'Test the local Nessus host' (checked) and 'Use fast network discovery' (unchecked). The 'Test the local Nessus host' option has a description: 'When enabled, includes the local Nessus host in the scan. This is used when the Nessus host falls with'. The 'Use fast network discovery' option has a description: 'When disabled, if a host responds to ping, Nessus attempts to avoid false positives, performing additional checks especially if the remote host is firewalled. When enabled, Nessus does not perform these checks.'

Basic>Discovery>Port Scanning keep default.



The screenshot shows the 'Settings' page in Nessus, with the 'Settings' tab highlighted. The left sidebar shows the navigation menu with 'DISCOVERY' and 'Port Scanning' highlighted. The main content area is titled 'Ports' and features a checkbox for 'Consider unscanned ports as closed' which is currently unchecked. Below this, there is a note: 'When enabled, if a port is not scanned with a selected port scanner (for example, the port falls out'. The 'Port Scan Range' is set to 'default'. Under the 'Local Port Enumerators' section, there is one option: 'SSH (netstat)' which is checked.

Basic>Discovery>Service Discovery keep default.

**Settings** | Credentials | Compliance | Plugins

**BASIC** >  
**DISCOVERY** ▾  
Host Discovery  
Port Scanning  
• Service Discovery  
Identity  
**ASSESSMENT** >  
**REPORT** >  
**ADVANCED** >

**General Settings**

Probe all ports to find services  
When enabled, the scanner attempts to map each open port with the service that is running on the unforeseen side effects.

Search for SSL/TLS/DTLS services  ON

Controls how the scanner tests SSL-based services. Caution: Testing !

Search for SSL/TLS on

Search for DTLS on

Identify certificates expiring within x days

Basic>Assessment keep default.

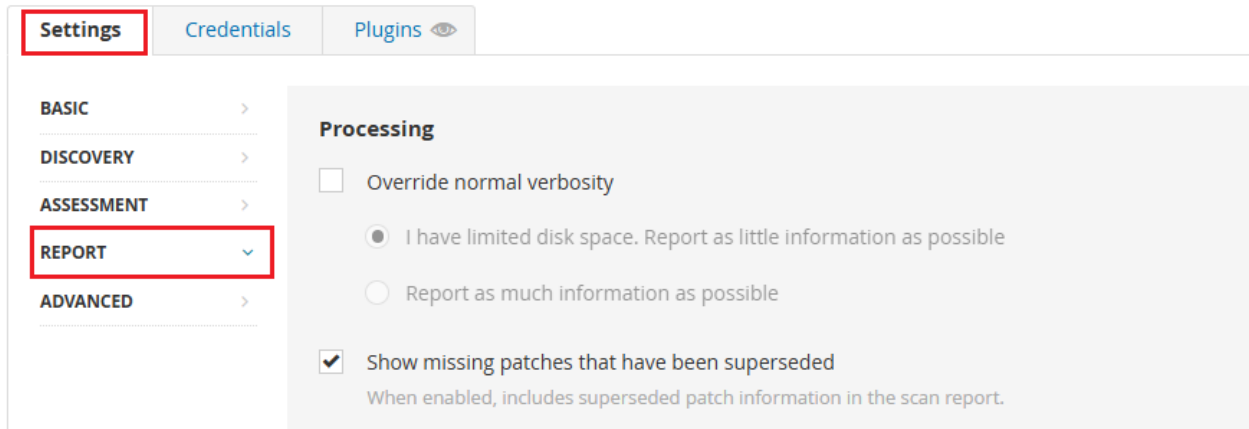
**Settings** | Credentials | Compliance | Plugins

**BASIC** >  
**DISCOVERY** >  
**ASSESSMENT** ▾  
General  
Brute Force  
SCADA  
Web Applications  
Windows  
Malware  
• Databases  
**REPORT** >  
**ADVANCED** >

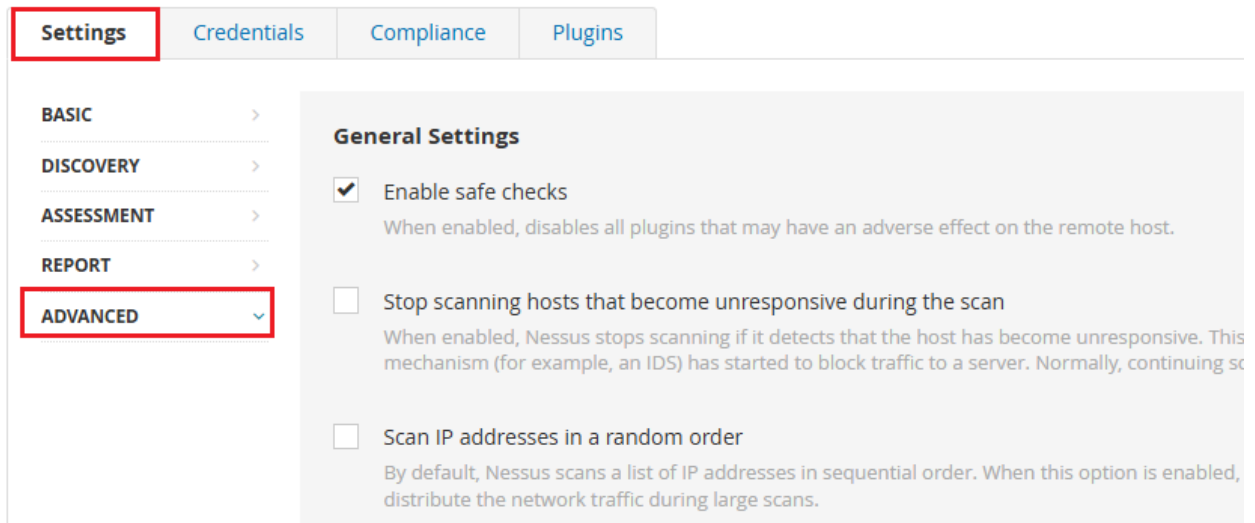
**Oracle Database**

Use detected SIDs  
When enabled, if at least one host credential and one Oracle database credential are configured, the scanner then attempts to authenticate using the specified Oracle database credentials and the scanner authenticates to the Oracle database using the manually specified SIDs in the Oracle databa

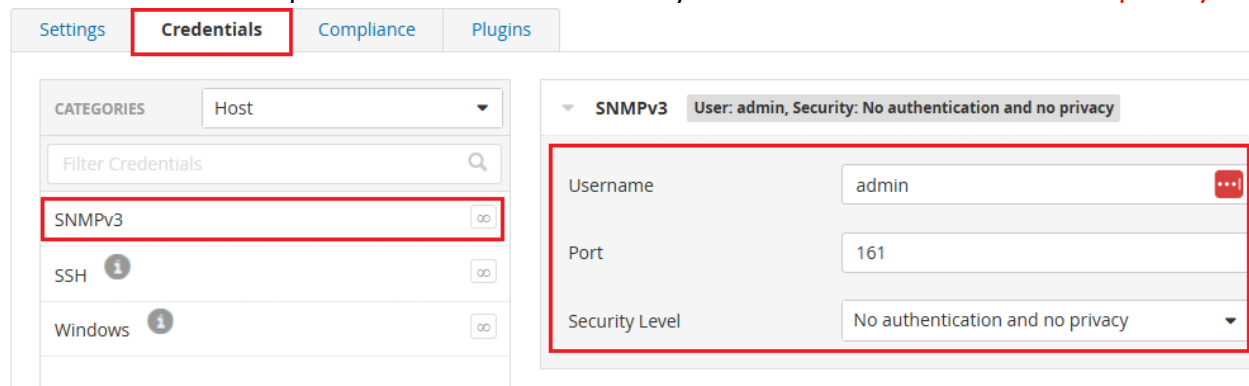
Settings>Reports keep default no changes.



Settings>Advanced keep default no changes.



Under Credentials Tab. Choose SSH and SNMP3 authentication methods. In SNMP enter Username: admin keep the default Port:161 Security Level: No authentication and no privacy



In **SSH** choose the Authentication method: **Password** enter username and password of FortiGate Firewall **admin/123**

Settings | **Credentials** | Compliance | Plugins

CATEGORIES: Host

Filter Credentials

SNMPv3

**SSH** ⓘ ∞

Windows ⓘ ∞

SNMPv3 User: admin, Security: No authentication and no privacy

**SSH** User: admin, Auth method: password

Authentication method: password

Username: admin

Password (unsafe!): 123

Elevate privileges with: Nothing

This password could be compromised if Nessus connect "Global Settings" section below.

**Plugins** Tab **disable** all Plugins only enable Firewalls plugin.

FortiGate-FW-Scan / Configuration

[Back to Scan Report](#)

Settings | Credentials | Compliance | **Plugins**

STATUS	Plugin Name	Count	STATUS
ENABLED	Firewalls	600	ENABLED
DISABLED	FreeBSD Local Security Checks	5904	ENABLED
DISABLED	FTP	289	ENABLED
DISABLED	Gain a shell remotely	282	ENABLED
DISABLED	General	588	ENABLED
DISABLED	Gentoo Local Security Checks	3734	ENABLED

Filter Search Plugin Families ? admin

Disable All Enable All

Show Enabled | Show All

STATUS	PLUGIN NAME	PLUGIN ID
ENABLED	3Proxy HTTP Proxy Crafted Transparent Request Remote Overflow	31094

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

The screenshot shows the FortiGate configuration interface for a scan. The 'Settings' tab is selected, and the 'General' sub-tab is highlighted with a red box. The 'General Settings' section contains the following fields:

- Name: FortiGate-FW-Scan
- Description: FortiGate-FW
- Folder: My Scans
- Targets: 100.0.1.254

Below the 'Targets' field, there is an 'Upload Targets' section with an 'Add File' button. The 'Post-Processing' section has a checkbox for 'Live Results' which is currently unchecked. A red arrow points to the 'Save' button at the bottom left.

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

**Scan Summary**

Hosts 1

Vulnerabilities 57

Remediations 1

History 1

**Scan Details**

4

Critical Vulnerabilities

19

High Vulnerabilities

28

Medium Vulnerabilities

2

Low Vulnerabilities

**Details**

Scan Name: FortiGate-FW-Scan

Plugin Set: 202505071551

CVSS\_Score: CVSS\_V3

Scan Template: Advanced Scan

Scan Start: May 8 at 2:08 PM

Scan End: May 8 at 2:22 PM



Authentication / Credential Info (Hosts)

1

SUCCEEDED

0

FAILED

Top 5 Operating Systems Detected During Scan



● FortiOS 7.0.9, Build 0444, 221121 On FortiGate-VM64-KVM

Scan Durations

00:13:54

SCAN DURATION

00:13:54

MEDIAN SCAN TIME PER HOST

00:13:54

MAX SCAN TIME

Under **Vulnerabilities** Tab it shows almost 57

Scan Summary	Hosts 1	<b>Vulnerabilities 57</b>	Remediations 1	History 1
--------------	---------	---------------------------	----------------	-----------

Filter Search Vulnerabilities 57 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family
<input type="checkbox"/> CRITICAL	9.8	7.4	0.1801	Fortinet Fortigate Curl and libcurl CVE-2023-38545 and CVE-2023-385...	Firewalls
<input type="checkbox"/> CRITICAL	9.8	5.9	0.0013	Fortinet Fortigate Weak Authentication in csfd daemon (FG-IR-24-221)	Firewalls
<input type="checkbox"/> CRITICAL	9.8	5.9	0.0004	Fortinet Fortigate - Improper authentication in fgfmd (FG-IR-24-032)	Firewalls
<input type="checkbox"/> CRITICAL	9.0	7.3	0.0291	Fortinet Fortigate RADIUS Protocol CVE-2024-3596 (FG-IR-24-255)	Firewalls
<input type="checkbox"/> HIGH	8.8	5.9	0.004	Fortinet Fortigate Format String Bug in Fcllicense daemon (FG-IR-23-1...	Firewalls
<input type="checkbox"/> HIGH	8.8	5.9	0.0029	Fortinet Fortigate Improper authorization via prof-admin profile (FG-I...	Firewalls
<input type="checkbox"/> HIGH	8.8	5.9	0.002	Fortinet Fortigate Administrator cookie leakage (FG-IR-23-493)	Firewalls
<input type="checkbox"/> HIGH	8.8	5.9	0.0014	Fortinet Fortigate - SSLVPN session hijacking using SAML authenticati...	Firewalls
<input type="checkbox"/> HIGH	8.8	5.9	0.0009	Fortinet Fortigate (FG-IR-22-444)	Firewalls

### Scan Details

Policy: Advanced Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: May 8 at 2:08 PM  
End: May 8 at 2:22 PM  
Elapsed: 14 minutes

### Vulnerabilities



Under **Remediation** Tab

FortiGate-FW-Scan

[Back to My Scans](#)

Scan Summary	Hosts 1	Vulnerabilities 57	<b>Remediations 1</b>	History 1
--------------	---------	--------------------	-----------------------	-----------

Search Actions 1 Action

Action
Fortinet Fortigate - SMTP password ciphertext exposure in Log (FG-IR-22-455): Please upgrade to FortiOS version 7.2.6, 7.4.0 or above.