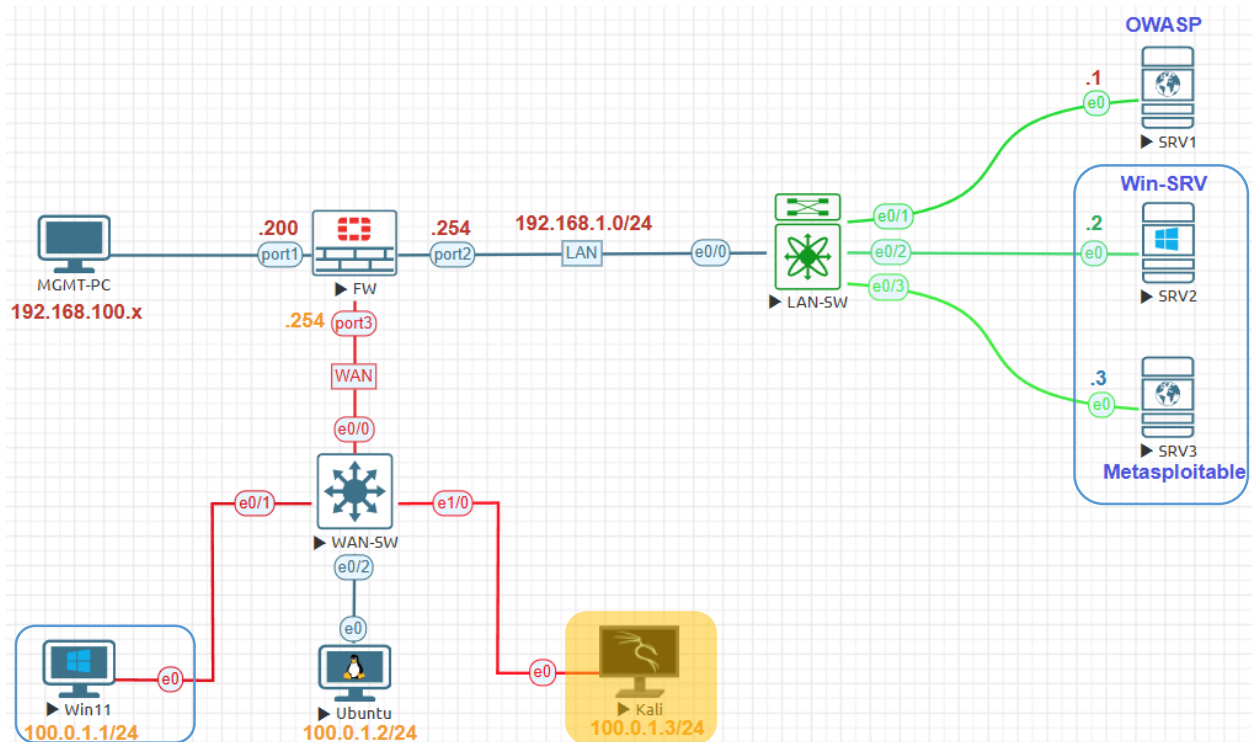


## Credential Validation Lab:



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 **Credential Validation** to open.

**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: **Credential-Validation-Scan**. Targets: IP address of target **100.0.1.1**, **192.168.1.2** and **192.168.1.3** which are Windows 11, Windows Server 2019 and Metasploitable 2.

**Settings** | Credentials | Plugins

**BASIC**

- General**
- Schedule
- Notifications

**REPORT**

**ADVANCED**

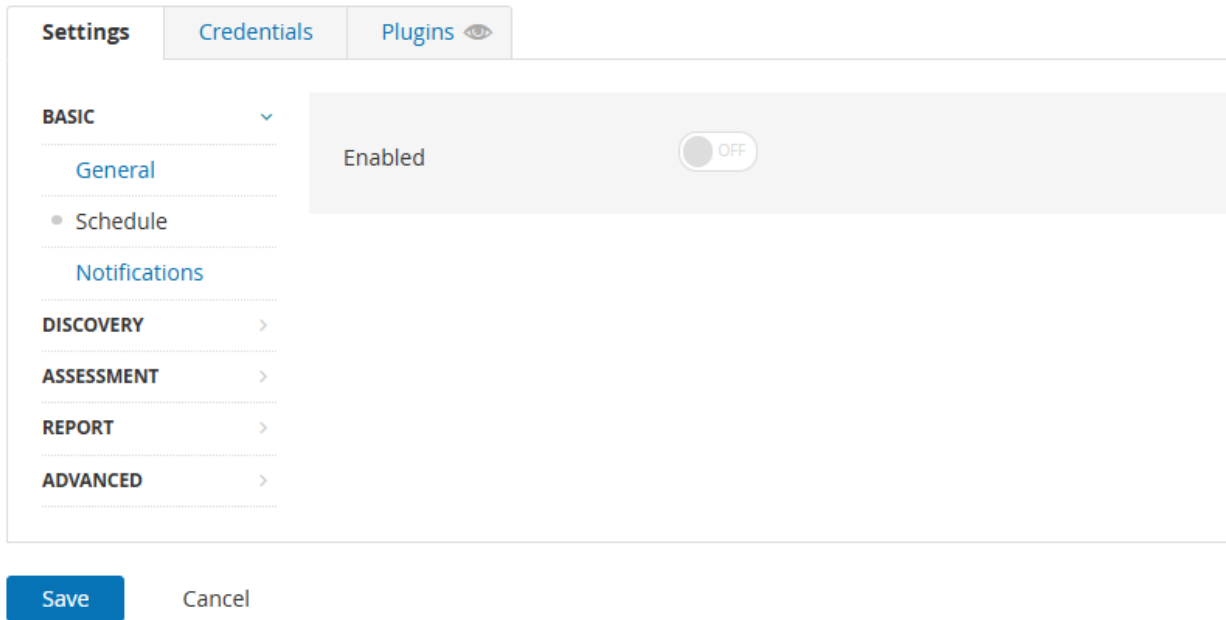
This policy is used to verify that host credential pairs for Windows & Unix are valid.

**General Settings**

- Name: Credential-Validation-Scan
- Description: Windows 11, Server 2019 and Metasploitable
- Folder: My Scans
- Targets: 100.0.1.1, 192.168.1.2, 192.168.1.3,

Settings>Basic>Schedule keep default disable.

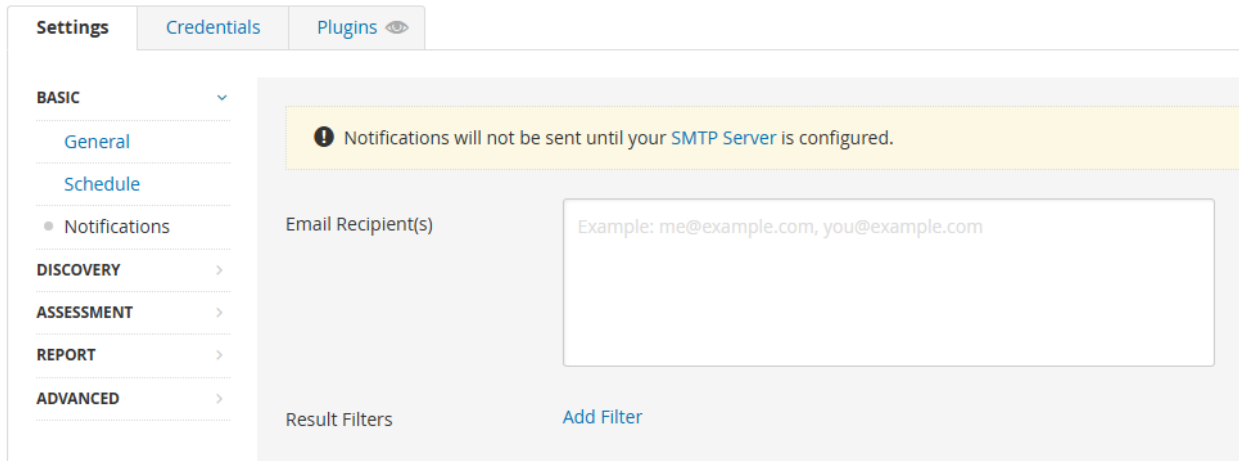
[← Back to Scan Report](#)



The screenshot shows the 'Settings' interface with tabs for 'Settings', 'Credentials', and 'Plugins'. The 'BASIC' section is expanded to show 'General', 'Schedule', and 'Notifications'. The 'Schedule' option is currently disabled, indicated by a greyed-out toggle switch labeled 'OFF'. Below the settings are 'Save' and 'Cancel' buttons.

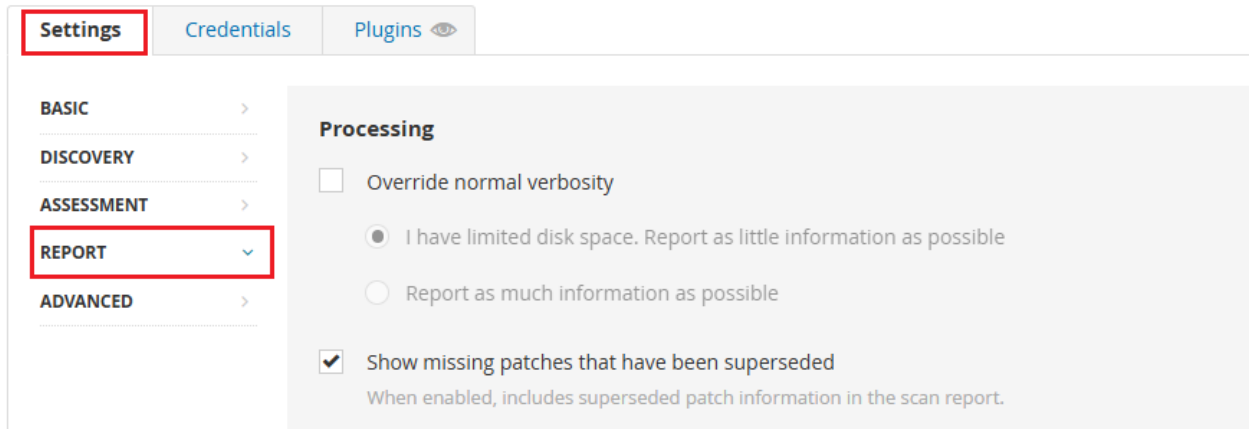
Settings>Basic>Notification keep default disable.

[← Back to Scan Report](#)

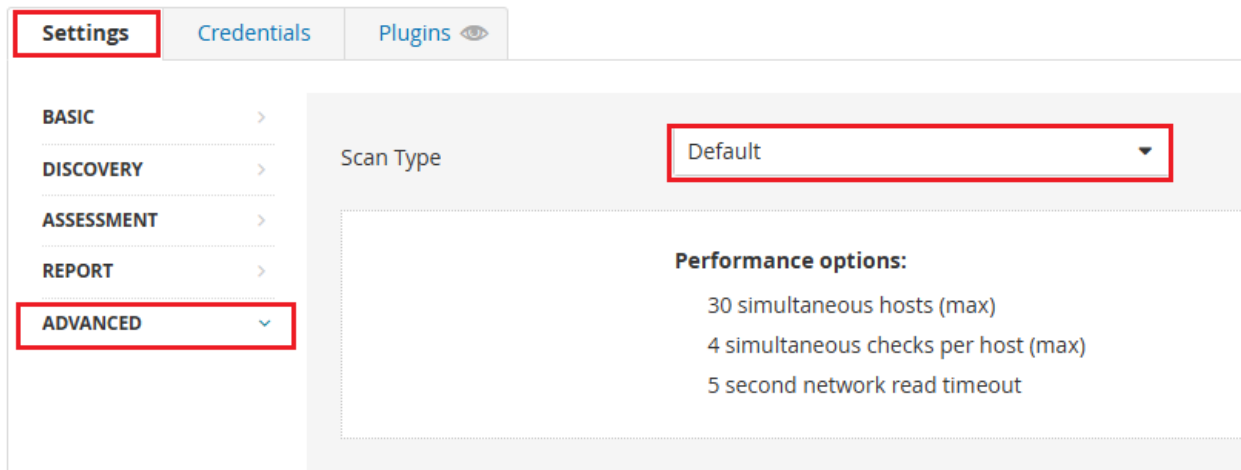


The screenshot shows the 'Settings' interface with tabs for 'Settings', 'Credentials', and 'Plugins'. The 'BASIC' section is expanded to show 'General', 'Schedule', and 'Notifications'. The 'Notifications' option is selected. A yellow warning banner at the top states: 'Notifications will not be sent 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>Reports keep default no changes.



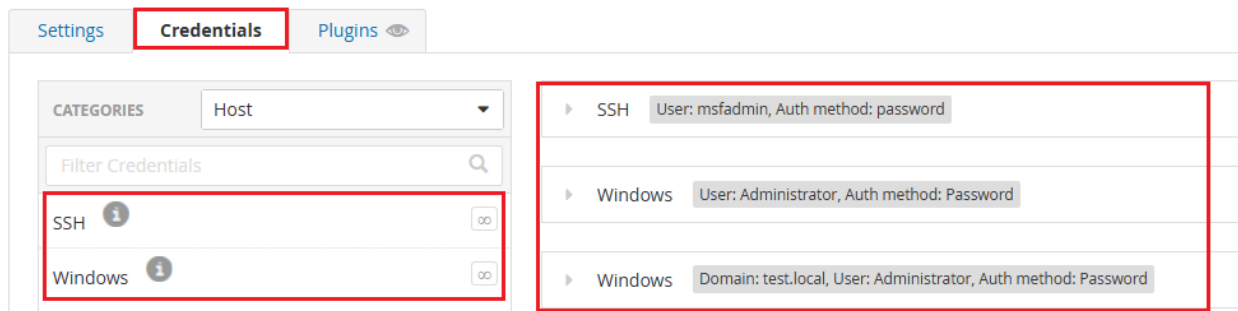
Settings>Advanced keep default no changes.



Under Credentials Tab. Choose SSH and Windows authentication methods.

Credential-Validation-Scan / Configuration

[Back to Scan Report](#)



In **SSH** choose the Authentication method: **Password** enter username and password of Metasploitable 2 **msfadmin/msfadmin**

SSH User: msfadmin, Auth method: password

Authentication method: password

Username: msfadmin

Password (unsafe!): .....

Elevate privileges with: Nothing

This password could be compromised if Nessus connects to a rogue SSH server. This can be mitigated by providing Ne "Global Settings" section below.

In one Windows enter Windows 11 credential Authentication method: password Username/Password **Administrator/Test123** leave the Domain empty.

Windows User: Administrator, Auth method: Password

Authentication method: Password

Username: Administrator

Password: .....

Domain:

In one Windows enter Windows Server 2019 credential Authentication method: password Username/Password **Administrator/Test123** and **Domain: test.local**

Windows Domain: test.local, User: Administrator, Auth method: Pas...

Authentication method: Password

Username: Administrator

Password: .....

Domain: test.local

Plugins Tab leave the default.

## Credential-Validation-Scan / Configuration

[← Back to Scan Report](#)

PLUGIN FAMILY	TOTAL
General	1
Misc.	1
Service detection	1
Settings	12
Windows	4

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

Settings | Credentials | **Plugins**

**BASIC**

- General
- Schedule
- Notifications

**REPORT**

**ADVANCED**

This policy is used to verify that host credential pairs for Windows & Unix are valid.

**General Settings**

Name: Credential-Validation-Scan

Description: Windows 11, Server 2019 and Metaspolitable


Folder: My Scans

Targets: 100.0.1.1, 192.168.1.2, 192.168.1.3,

**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 3 Vulnerabilities 9 History 1

### Scan Details

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

### Details

Scan Name: Credential-Validation-Scan  
Plugin Set: 202505071551  
CVSS\_Score: CVSS\_V3  
Scan Template: Credential Validation  
Scan Start: May 8 at 11:36 AM  
Scan End: May 8 at 11:40 AM

### Authentication / Credential Info (Hosts)

3 SUCCEEDED	0 FAILED
----------------	-------------

### Top 5 Operating Systems Detected During Scan



- Microsoft Windows 11
- Microsoft Windows Server 2019
- Linux (Other)

### Scan Durations

00:03:47 SCAN DURATION	00:02:02 MEDIAN SCAN TIME PER HOST	00:03:47 MAX SCAN TIME
---------------------------	---------------------------------------	---------------------------

# Credential-Validation-Scan

[Back to My Scans](#)

Scan Summary   **Hosts** 3   Vulnerabilities 9   History 1

Filter   Search Hosts   3 Hosts

<input type="checkbox"/>	Host	Vulnerabilities
<input type="checkbox"/>	192.168.1.3	7
<input type="checkbox"/>	100.0.1.1	6
<input type="checkbox"/>	192.168.1.2	6

Scan Summary   Hosts 3   **Vulnerabilities** 9   History 1

Filter   Search Vulnerabilities   9 Vulnerabilities

<input type="checkbox"/>	Sev	CVSS	VPR	EPSS	Name	Family
<input type="checkbox"/>	INFO				Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	Windows
<input type="checkbox"/>	INFO				Nessus Scan Information	Settings
<input type="checkbox"/>	INFO				OS Security Patch Assessment Available	Settings
<input type="checkbox"/>	INFO				Target Credential Status by Authentication Protocol - Valid Credentials P...	Settings
<input type="checkbox"/>	INFO				Target Credential Issues by Authentication Protocol - No Issues Found	Settings
<input type="checkbox"/>	INFO				WMI Available	Windows
<input type="checkbox"/>	INFO				SSH Commands Require Privilege Escalation	Settings
<input type="checkbox"/>	INFO				Target Credential Status by Authentication Protocol - Failure for Provide...	Settings
<input type="checkbox"/>	INFO				WMI Not Available	Windows