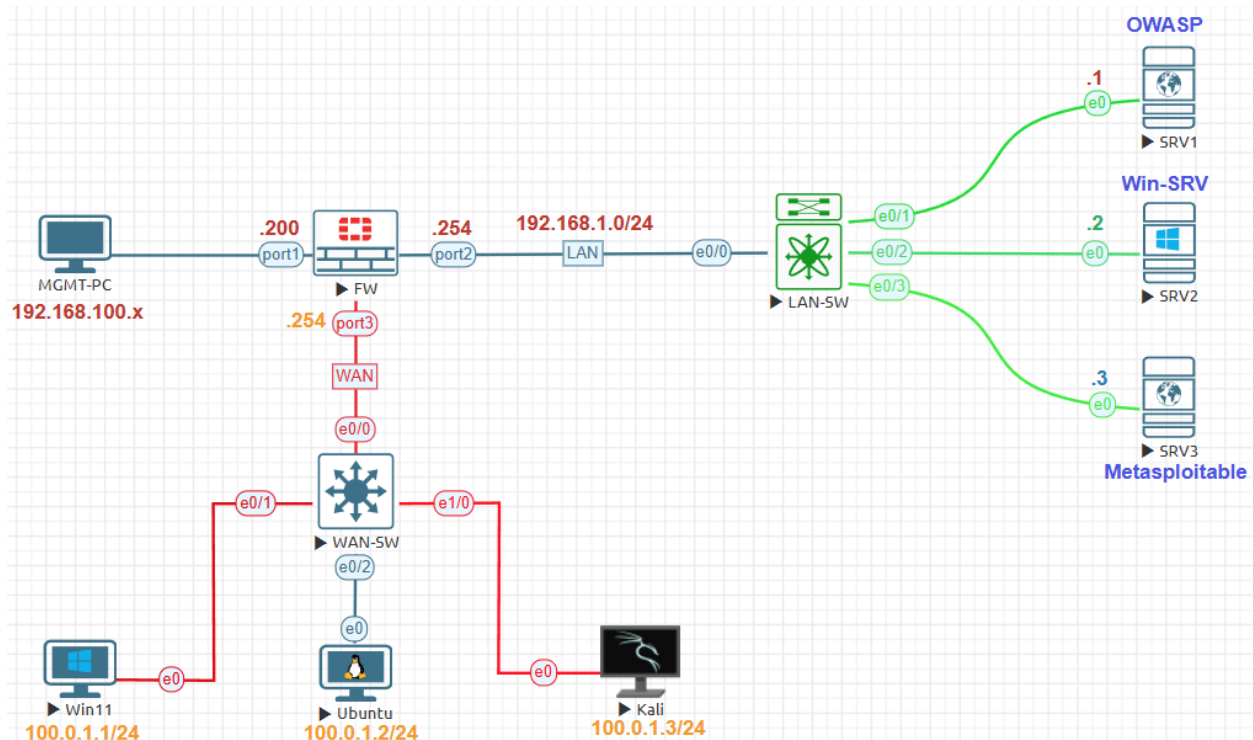


Unauthenticated Scan Lab:



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

Go to **Scans > New Scan**. Choose **Basic Network Scan** to open.

Scan Templates

[← Back to Scans](#)

Scanner

User Defined

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: **Metasploitable-Unauthenticated**. Targets: IP address of target Metasploitable **192.168.1.3**.

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name Metasploitable-Unauthenticated

Description Metasploitable Unauthenticated Scan

Folder My Scans

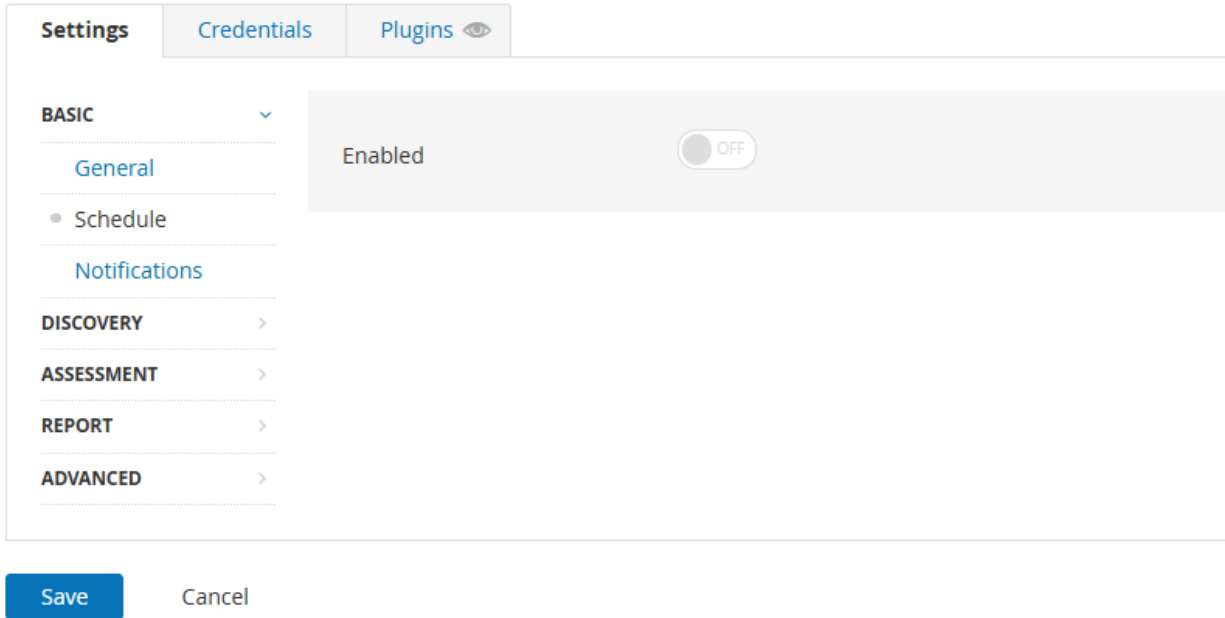
Targets 192.168.1.3

Upload Targets

[Add File](#)

Settings>Basic>Schedule keep default disable.

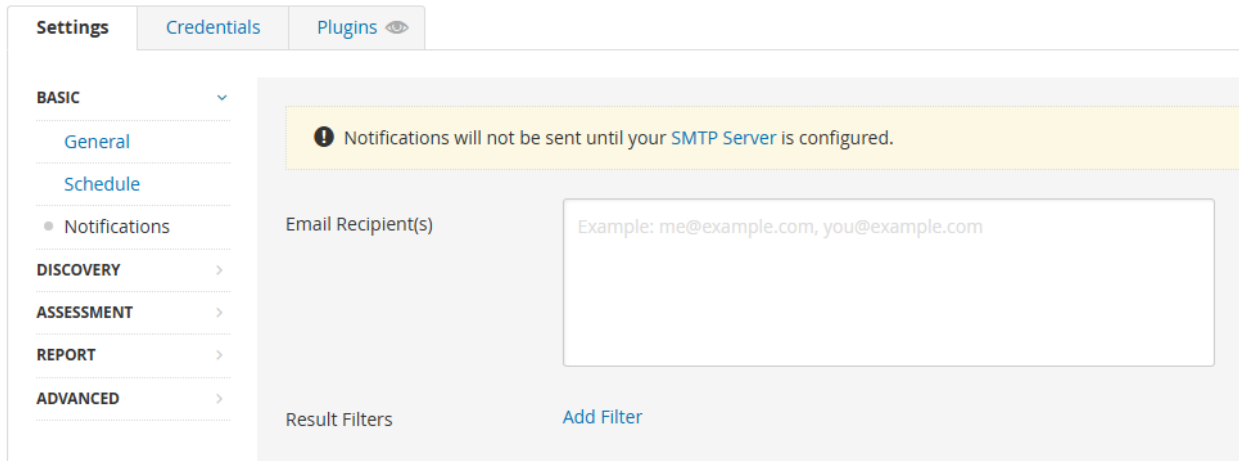
[← Back to Scan Report](#)



The screenshot shows the 'Settings' interface with tabs for 'Settings', 'Credentials', and 'Plugins'. The 'BASIC' section is expanded, showing '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.

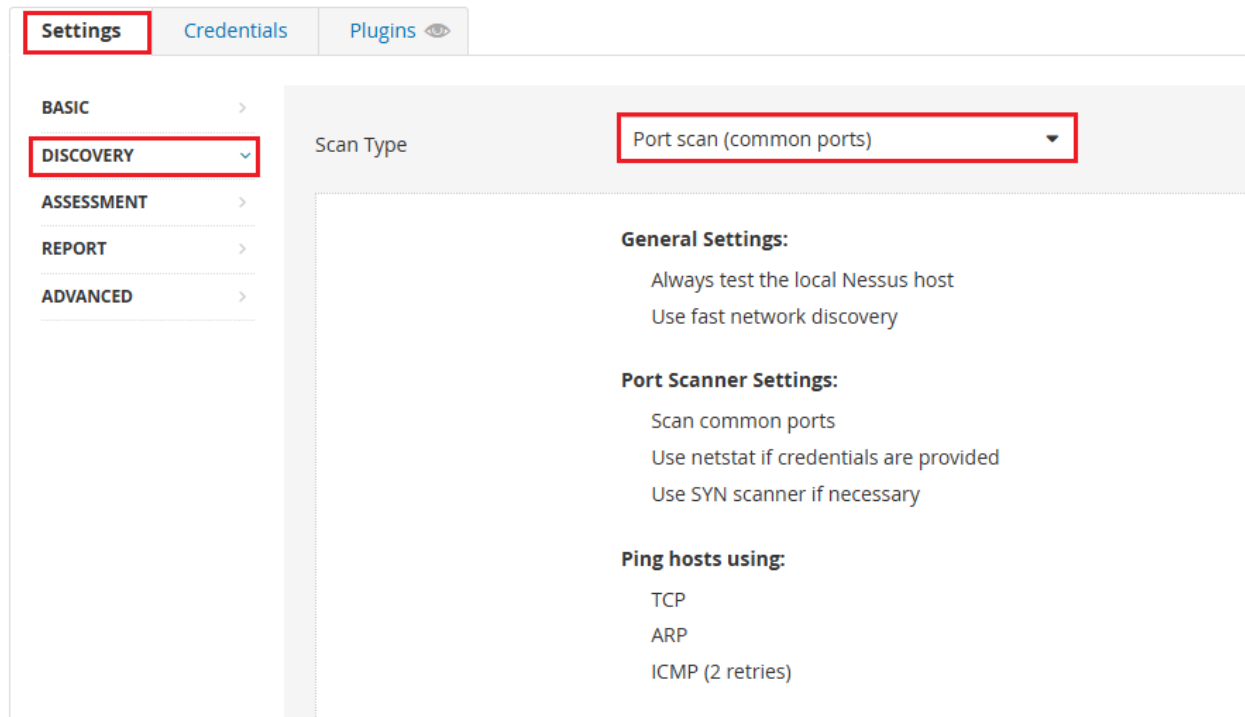
Settings>Basic>Notification keep default disable.

[← Back to Scan Report](#)



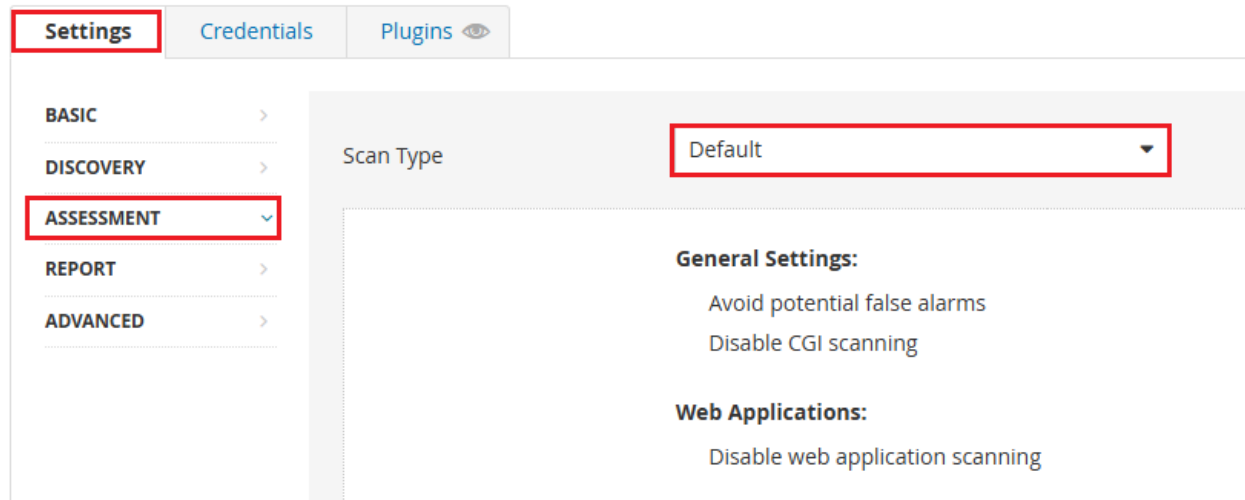
The screenshot shows the 'Settings' interface with tabs for 'Settings', 'Credentials', and 'Plugins'. The 'BASIC' section is expanded, showing 'General', 'Schedule', and 'Notifications'. The 'Notifications' option is selected. A yellow warning banner at the top states: 'Notifications will not be sent 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>Discovery keep default Port scan (common ports).



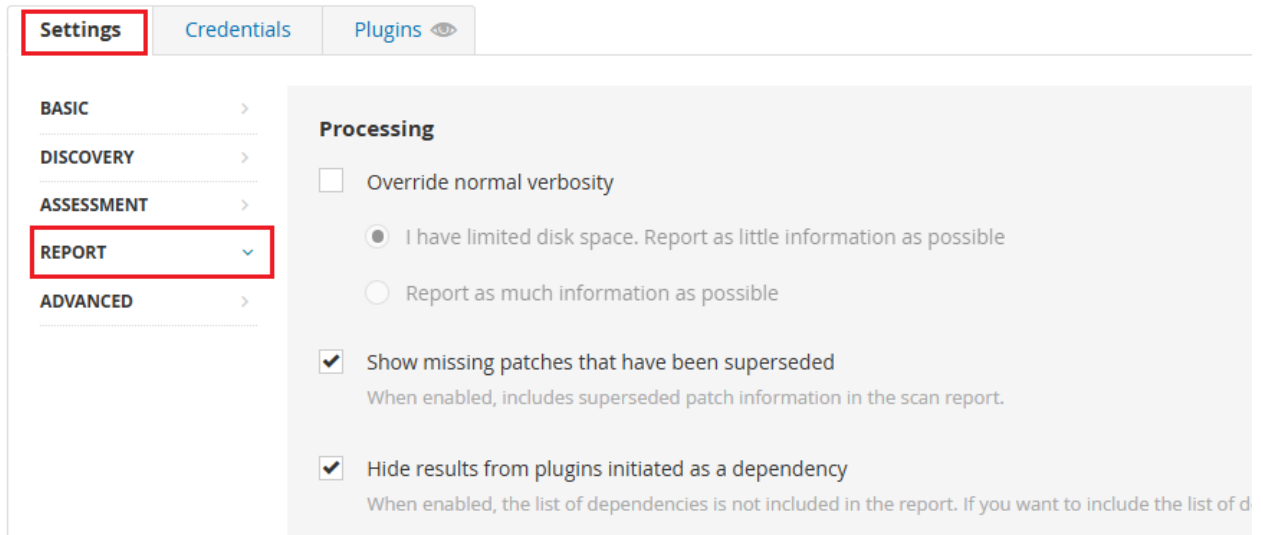
The screenshot shows the 'Settings' tab selected in the top navigation bar. On the left sidebar, the 'DISCOVERY' option is highlighted with a red box. The main content area shows the 'Scan Type' dropdown menu set to 'Port scan (common ports)', also highlighted with a red box. Below this, the settings are organized into three sections: 'General Settings' with options 'Always test the local Nessus host' and 'Use fast network discovery'; 'Port Scanner Settings' with options 'Scan common ports', 'Use netstat if credentials are provided', and 'Use SYN scanner if necessary'; and 'Ping hosts using:' with options 'TCP', 'ARP', and 'ICMP (2 retries)'.

Settings>Assessment keep default

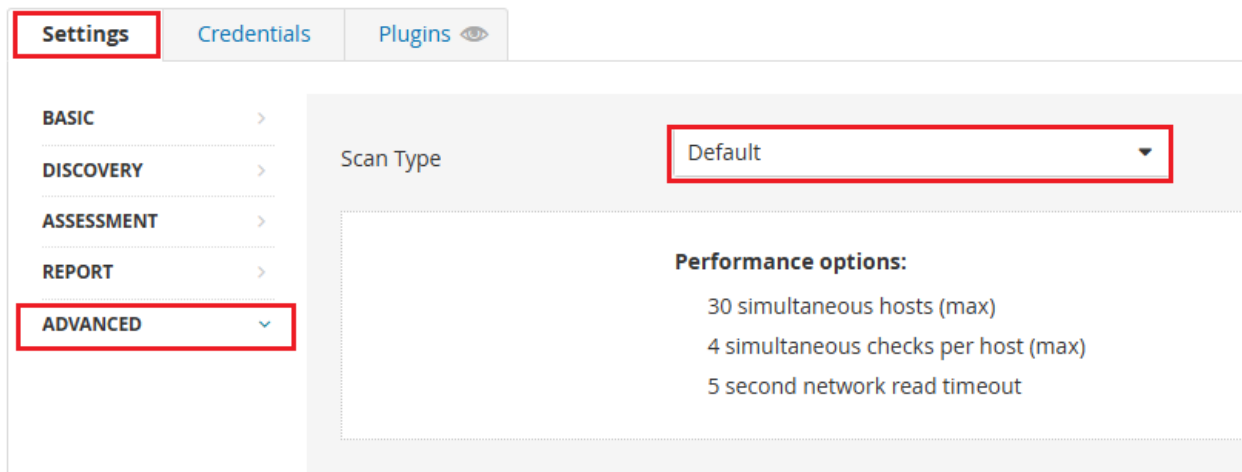


The screenshot shows the 'Settings' tab selected in the top navigation bar. On the left sidebar, the 'ASSESSMENT' option is highlighted with a red box. The main content area shows the 'Scan Type' dropdown menu set to 'Default', also highlighted with a red box. Below this, the settings are organized into two sections: 'General Settings' with options 'Avoid potential false alarms' and 'Disable CGI scanning'; and 'Web Applications:' with the option 'Disable web application scanning'.

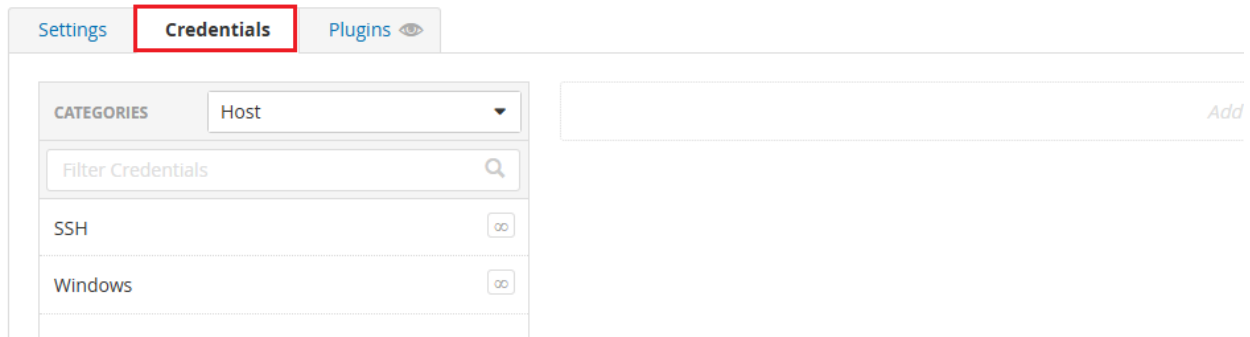
Settings>Reports keep default no changes.



Settings>Advanced keep default no changes.



Under Credentials Tab. Leave all fields empty (unauthenticated)



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

The screenshot shows the 'Settings' page in Metasploit. The 'Credentials' tab is selected. On the left, there is a sidebar with categories: BASIC (General, Schedule, Notifications), DISCOVERY, ASSESSMENT, REPORT, and ADVANCED. The main area shows the configuration for a scan:

- Name: Metasploitable-Unauthenticated
- Description: Metasploitable Unauthenticated Scan
- Folder: My Scans
- Targets: 192.168.1.3

At the bottom, there are buttons for 'Upload Targets' and 'Add File'.

Save Cancel

After complete the scan, 9 Critical, 5 High, 22 Medium, 8 Low and 122 info.

The screenshot shows the 'Hosts' tab with 1 host selected. The host 192.168.1.3 is highlighted with a red box. The results are displayed as a horizontal bar chart:

Host	Critical	High	Medium	Low	Info
192.168.1.3	9	5	22	8	122

Total 60 Vulnerabilities includes 9 Critical, 5 High, 22 Medium, 8 Low and 122 info.

Metasploitable-Unauthenticated

[Back to My Scans](#)

The screenshot shows the 'Vulnerabilities' tab with 60 vulnerabilities listed. The first two are highlighted with a red box:

Sev	CVSS	VPR	EPSS	Name	Family
CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely

Metasploitable-Unauthenticated

[← Back to My Scans](#)

Hosts 1 Vulnerabilities 60 **Remediations 2** History 1

Search Actions 2 Actions

Action
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

192.168.1.3



Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: May 4 at 8:34 PM
End: May 4 at 8:59 PM
Elapsed: 25 minutes

Vulnerabilities

