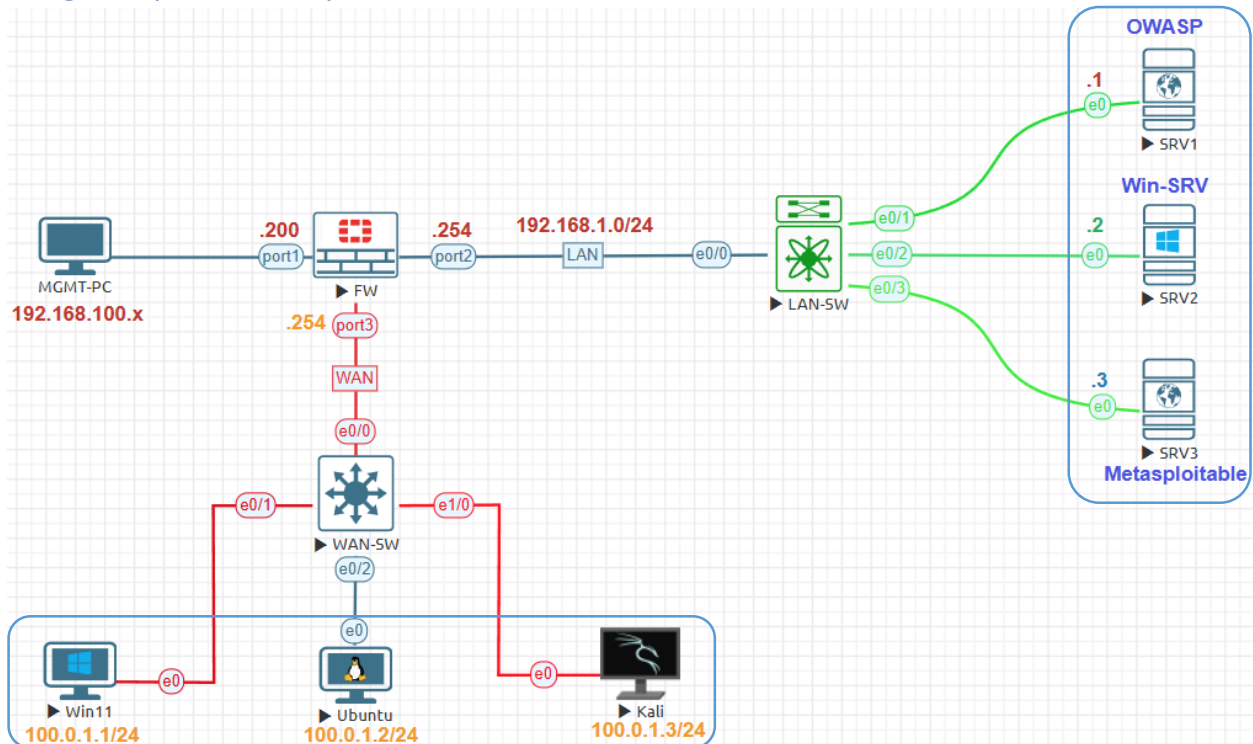


Ping-Only Discovery Lab:



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 **Ping-Only Discovery** to open.

Name: **Ping-Only-Discovery**. Targets: IP address of target subnets **192.168.1.0/24** and **100.0.1.0/24**.

Settings>Basic>Schedule keep default disable.

[← Back to Scan Report](#)

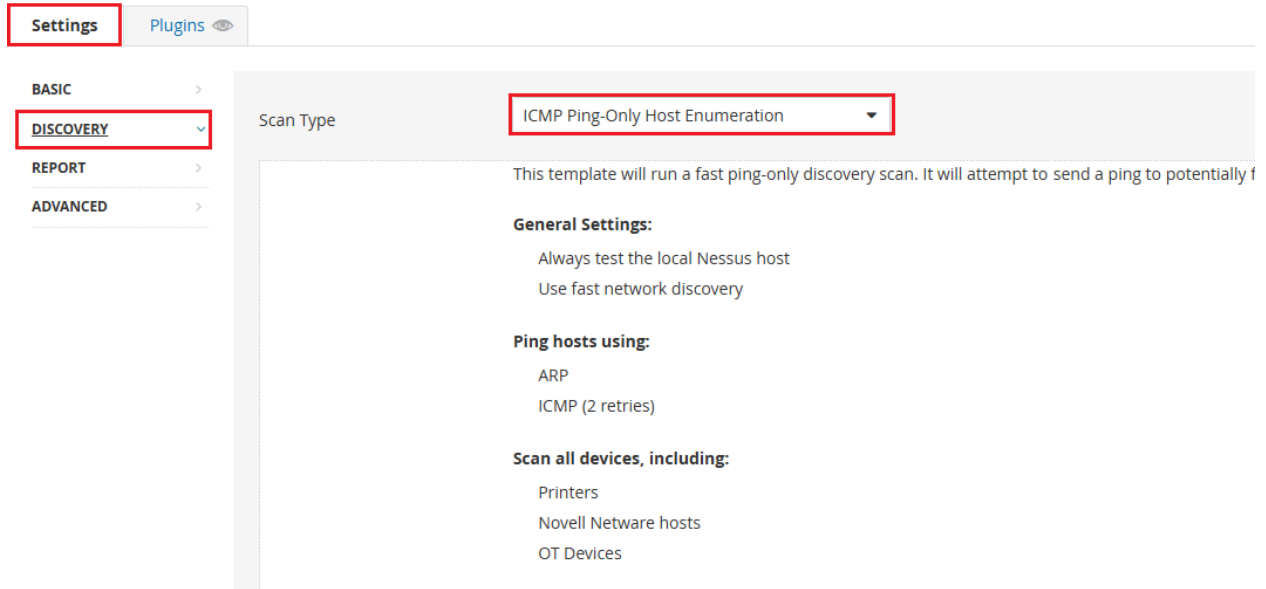
The screenshot shows the 'Settings' interface with tabs for 'Settings', 'Credentials', and 'Plugins'. Under the 'BASIC' section, there are sub-sections for 'General', 'Schedule', and 'Notifications'. The 'Schedule' sub-section is active, showing a toggle switch labeled 'Enabled' which is currently turned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

Settings>Basic>Notification keep default disable.

[← Back to Scan Report](#)

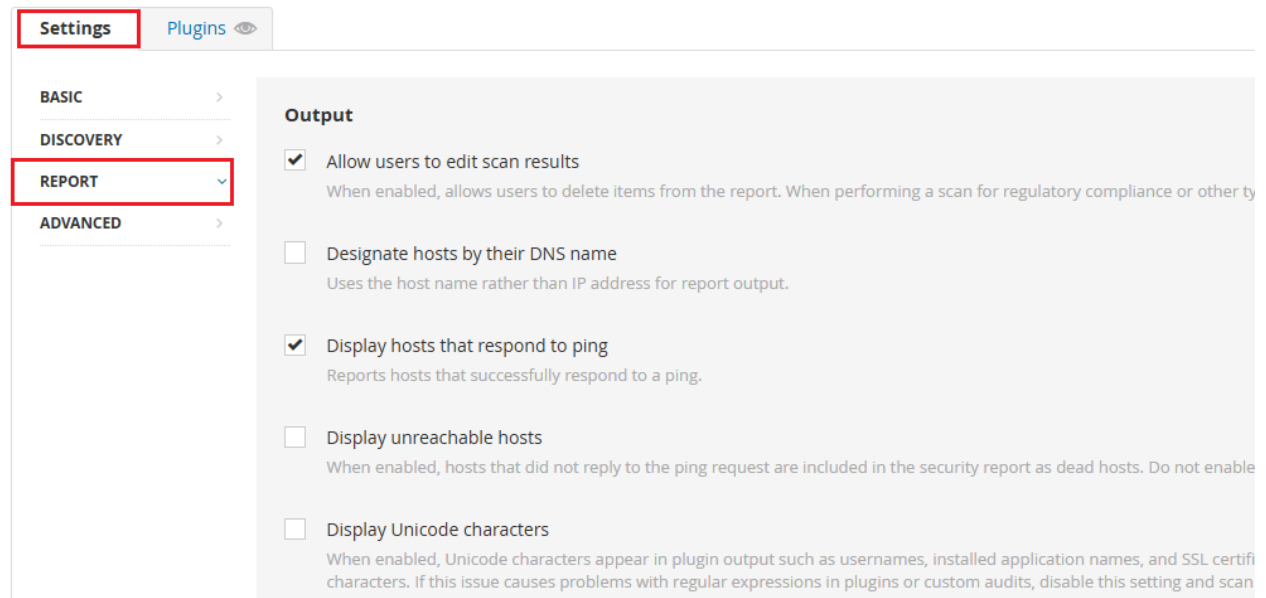
The screenshot shows the 'Settings' interface with tabs for 'Settings', 'Credentials', and 'Plugins'. Under the 'BASIC' section, there are sub-sections for 'General', 'Schedule', and 'Notifications'. The 'Notifications' sub-section is active, displaying a yellow warning message: 'Notifications will not be sent until your SMTP Server is configured.' Below the warning, 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 ICMP Ping-Only Host Enumeration



The screenshot shows the 'Settings' page in Nessus, specifically the 'Discovery' section. The 'Settings' tab is highlighted in red. On the left sidebar, the 'DISCOVERY' menu item is also highlighted in red. The main content area shows the 'Scan Type' dropdown menu set to 'ICMP Ping-Only Host Enumeration', which is also highlighted in red. Below this, there is a description of the scan type and several configuration sections: 'General Settings' (Always test the local Nessus host, Use fast network discovery), 'Ping hosts using:' (ARP, ICMP (2 retries)), and 'Scan all devices, including:' (Printers, Novell Netware hosts, OT Devices).

Settings>Reports keep default no changes.

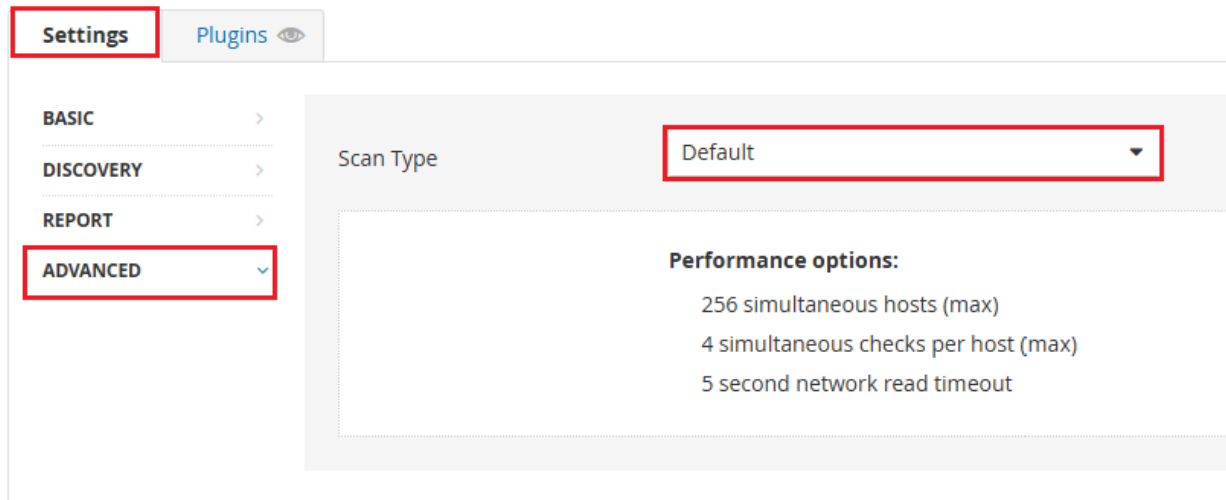


The screenshot shows the 'Settings' page in Nessus, specifically the 'Reports' section. The 'Settings' tab is highlighted in red. On the left sidebar, the 'REPORT' menu item is highlighted in red. The main content area shows the 'Output' section with several checkboxes: 'Allow users to edit scan results' (checked), 'Designate hosts by their DNS name' (unchecked), 'Display hosts that respond to ping' (checked), 'Display unreachable hosts' (unchecked), and 'Display Unicode characters' (unchecked). Each checkbox has a brief description of its function.

Settings>Advanced keep default no changes.

Ping-Only-Discovery / Configuration

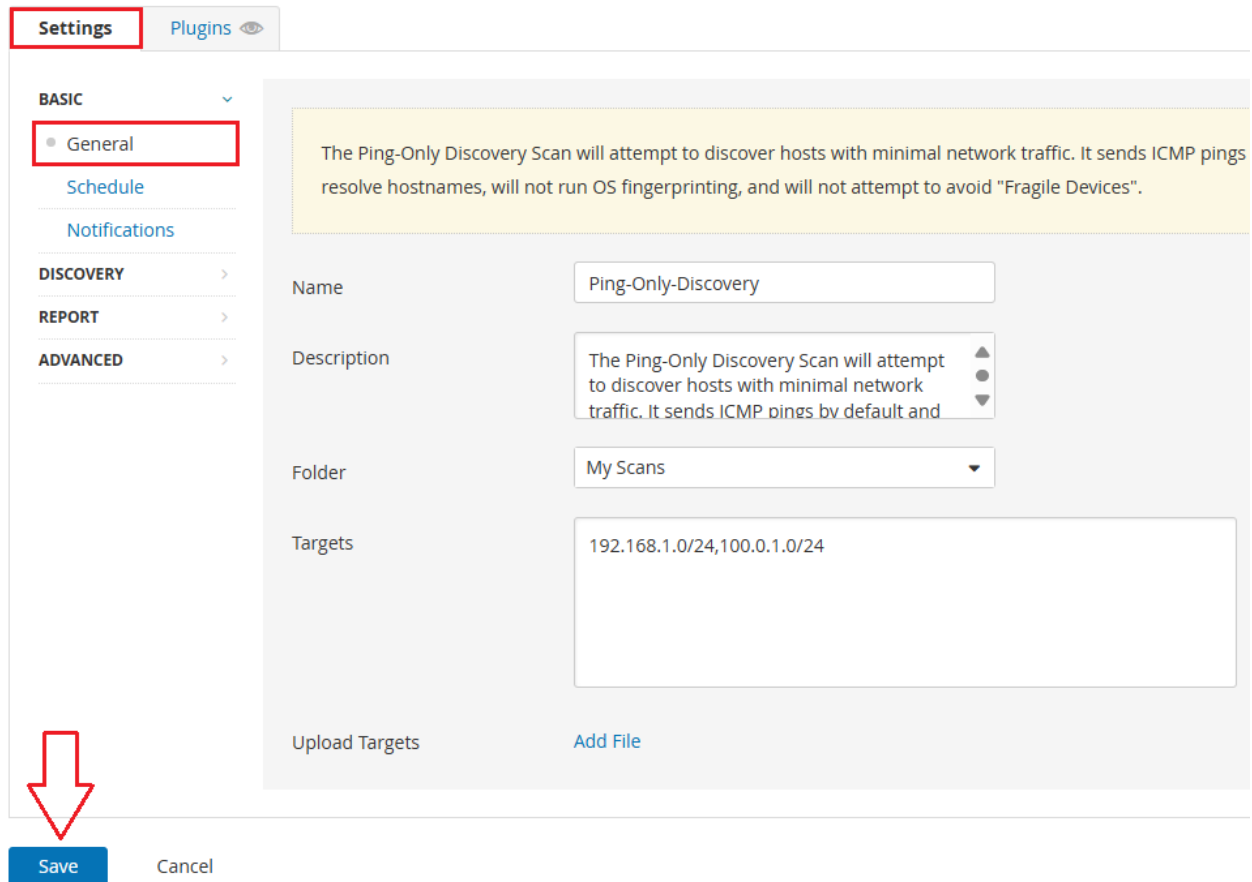
[← Back to Scan Report](#)



The screenshot shows the 'Settings' page with the 'ADVANCED' tab selected. The 'Scan Type' dropdown is set to 'Default'. Under 'Performance options', the following settings are listed:

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

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



The screenshot shows the configuration page for 'Ping-Only-Discovery'. The 'General' tab is selected. The configuration details are as follows:

- Name:** Ping-Only-Discovery
- Description:** The Ping-Only Discovery Scan will attempt to discover hosts with minimal network traffic. It sends ICMP pings by default and resolve hostnames, will not run OS fingerprinting, and will not attempt to avoid "Fragile Devices".
- Folder:** My Scans
- Targets:** 192.168.1.0/24,100.0.1.0/24

At the bottom, there is an 'Upload Targets' section with an 'Add File' button. A red arrow points to the 'Save' button.

After complete the scan Hosts Tab 8 host discovered FortiGate Firewall, Metasploitable 2, Windows Server 2019, OWASP, Kali Linux, Ubuntu and Windows 11.

Hosts 8 Vulnerabilities 2 History 1

Filter Search Hosts 8 Hosts

Host	Vulnerabilities
<input type="checkbox"/> 100.0.1.1	2
<input type="checkbox"/> 100.0.1.2	2
<input type="checkbox"/> 100.0.1.3	2
<input type="checkbox"/> 100.0.1.254	2
<input type="checkbox"/> 192.168.1.1	2
<input type="checkbox"/> 192.168.1.2	2
<input type="checkbox"/> 192.168.1.3	2
<input type="checkbox"/> 192.168.1.254	2

Vulnerabilities Tab provide information about the scan.

Host-Discovery

[Back to My Scans](#)

Hosts 8 Vulnerabilities 2 History 2

Filter Search Vulnerabilities 2 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family
<input type="checkbox"/> INFO				Nessus Scan Information	Settings
<input type="checkbox"/> INFO				Ping the remote host	Port scanners