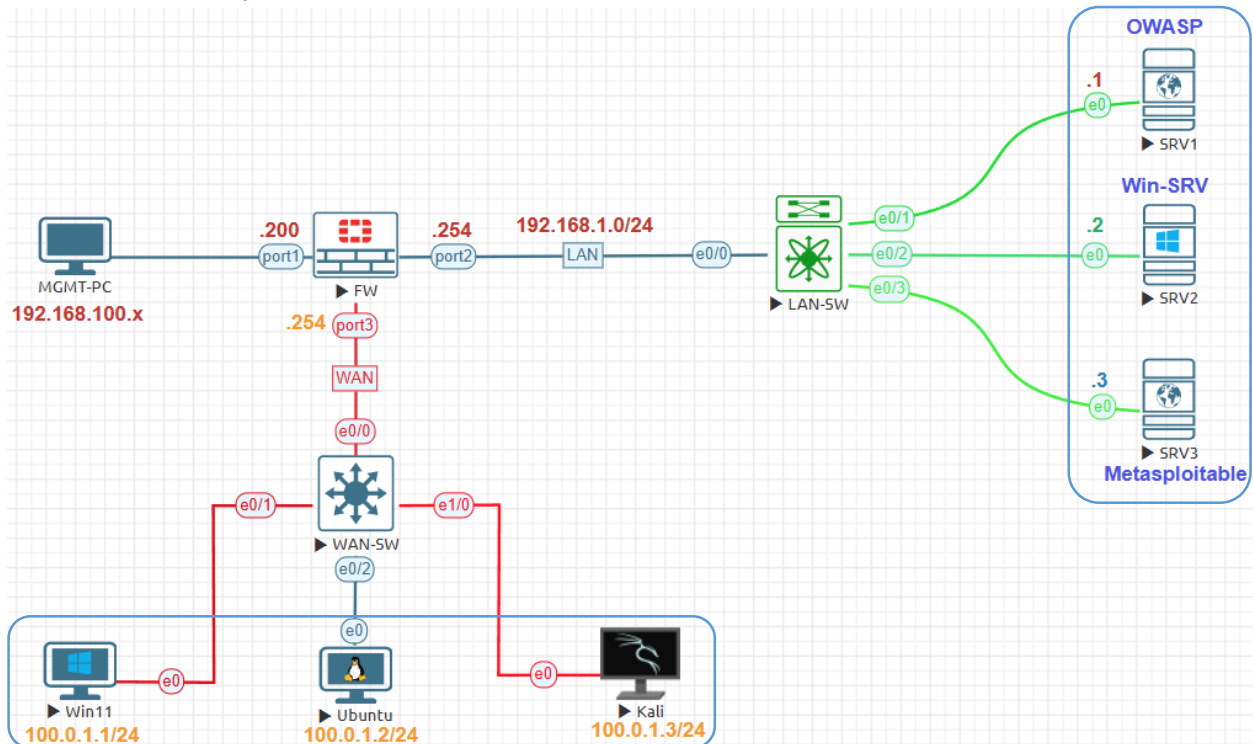


Host Discovery Lab:



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 **Host Discovery** to open.

The screenshot shows the Nessus Essentials interface. At the top, the 'Scans' tab is highlighted. The main content area is titled 'Scan Templates' and includes a 'Back to Scans' link. Below this, there is a 'Scanner' section and a 'DISCOVERY' section. In the 'DISCOVERY' section, the 'Host Discovery' template is highlighted with a red box. It features a circular icon with a green arrow and the text: 'Host Discovery: A simple scan to discover live hosts and open ports.' To its right is the 'Ping-Only Discovery' template, which features a hand icon pointing at a green circle and the text: 'Ping-Only Discovery: A simple scan to discover live hosts with minimal network traffic.'

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

The screenshot shows the 'Settings' page for the 'Host-Discovery' scan. The 'Settings' tab is highlighted. On the left, there is a sidebar with 'BASIC' settings, including 'General' (highlighted), 'Schedule', and 'Notifications'. Below these are 'DISCOVERY', 'REPORT', and 'ADVANCED' sections. The main content area shows the following settings: 'Name' is 'Host-Discovery'; 'Description' is 'Host Discovery scan for the entire network 192.168.1.0/24 and 100.0.1.0/24 subnets'; 'Folder' is 'My Scans'; and 'Targets' is '192.168.1.0/24, 100.0.1.0/24'. The 'Name', 'Description', and 'Targets' fields are highlighted with red boxes.

Settings>Basic>Schedule keep default disable.

[← Back to Scan Report](#)

Settings | Credentials | Plugins

BASIC ▾

- General
- **Schedule**
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Enabled OFF

Save Cancel

Settings>Basic>Notification keep default disable.

[← Back to Scan Report](#)

Settings | Credentials | Plugins

BASIC ▾

- General
- Schedule
- **Notifications**

DISCOVERY >

ASSESSMENT >

REPORT >

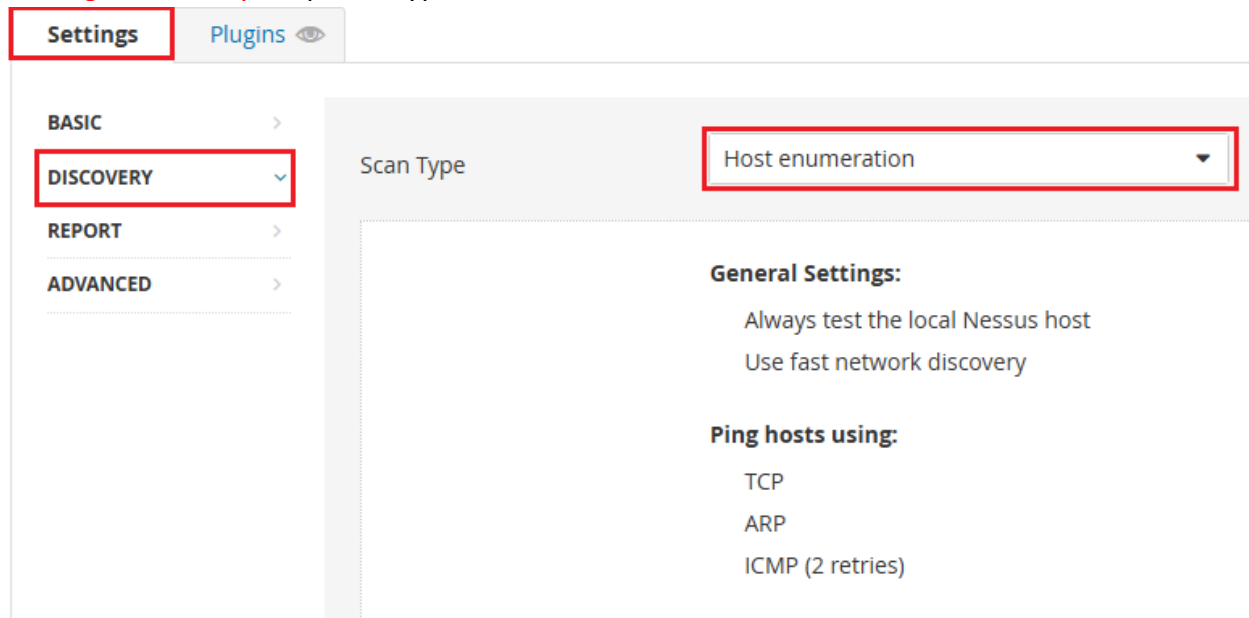
ADVANCED >

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

Email Recipient(s)

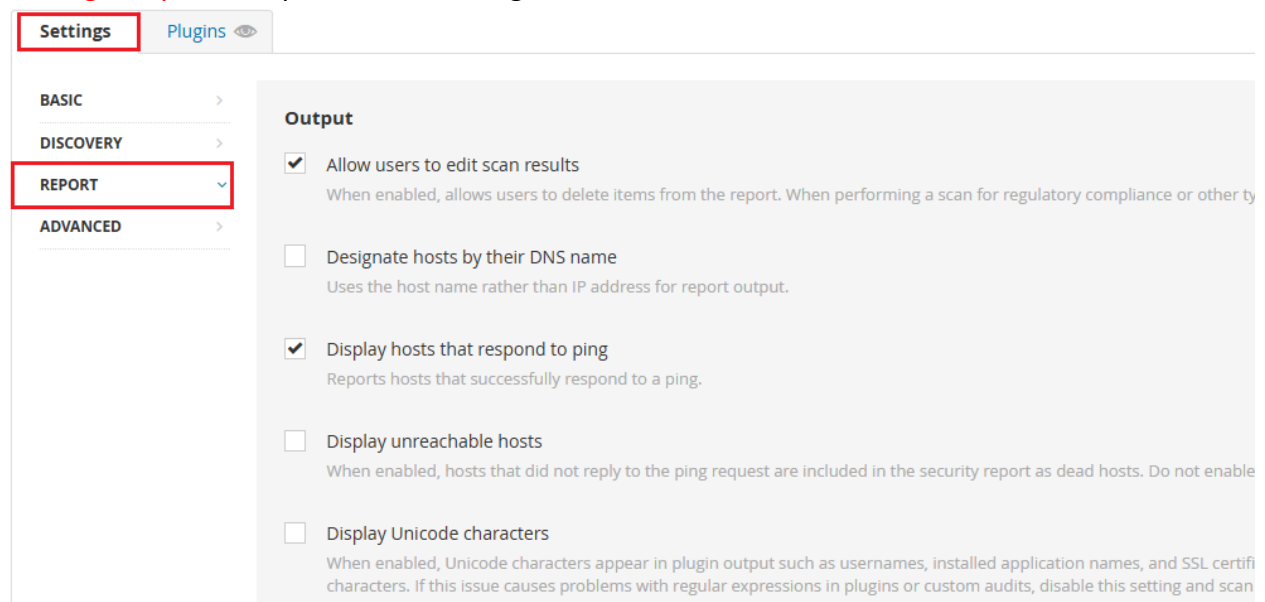
Result Filters [Add Filter](#)

Settings>Discovery keep scan type 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' option is selected and highlighted in red. The main content area shows the 'Scan Type' dropdown menu set to 'Host enumeration', also highlighted in red. Below this, the 'General Settings' section includes two options: 'Always test the local Nessus host' and 'Use fast network discovery'. The 'Ping hosts using:' section lists three options: 'TCP', 'ARP', and 'ICMP (2 retries)'.

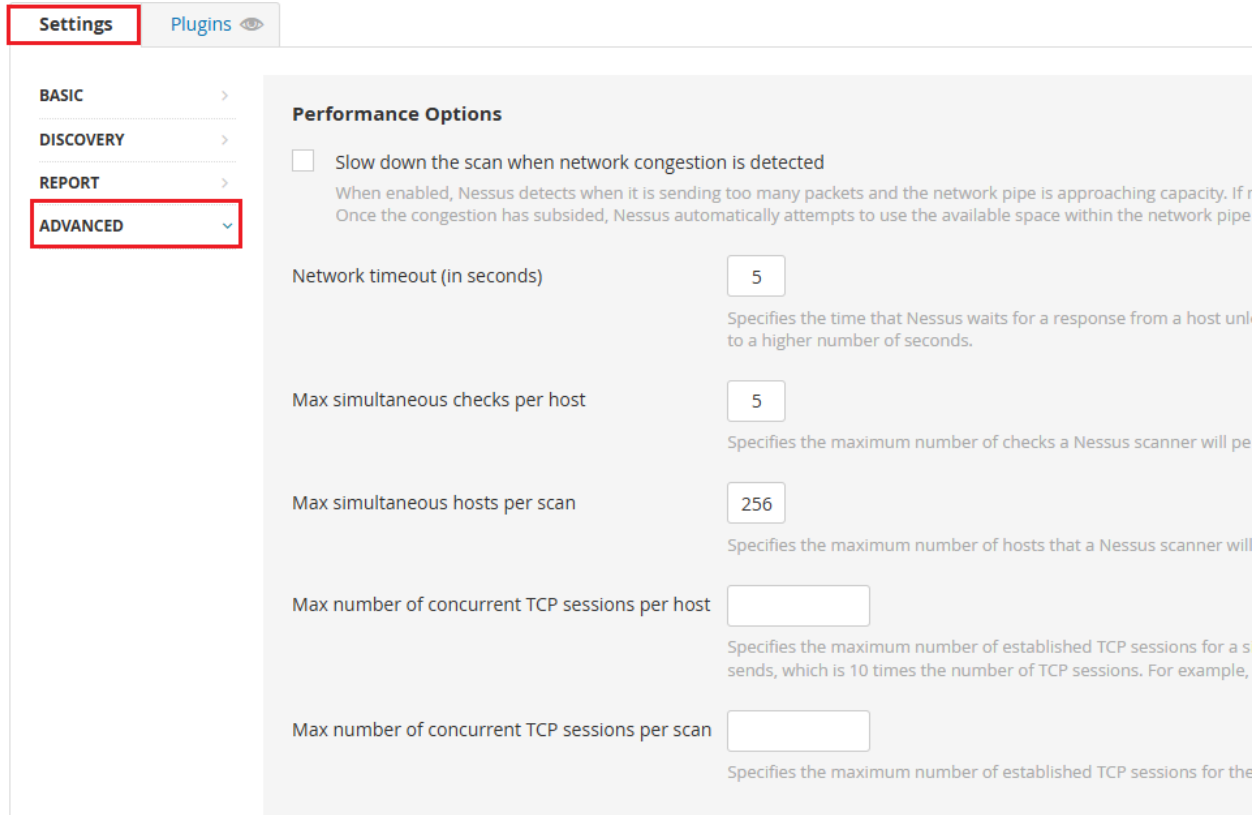
Settings>Reports keep default no changes.



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' option is selected and highlighted in red. The main content area shows the 'Output' section with five settings:

- Allow users to edit scan results
When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other ty
- 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. Do not enable
- Display Unicode characters
When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certifi characters. If this issue causes problems with regular expressions in plugins or custom audits, disable this setting and scan

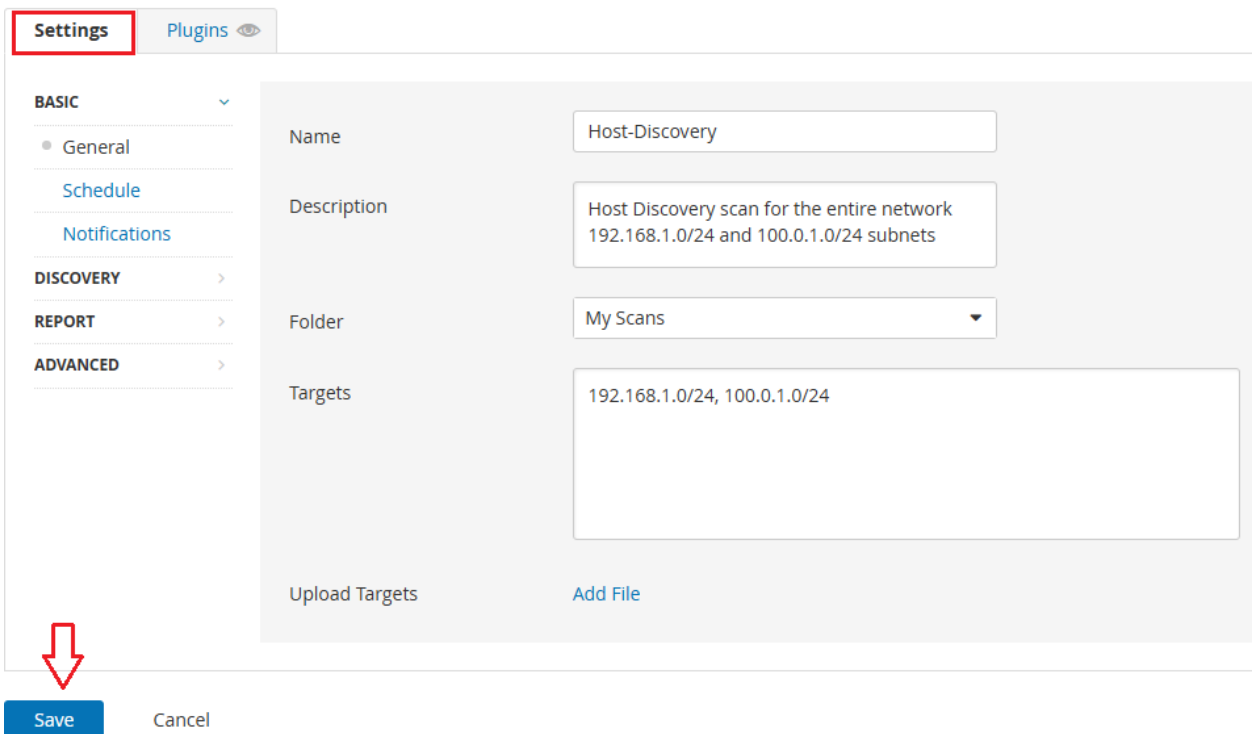
Settings>Advanced keep default no changes.



The screenshot shows the 'Settings' tab in Nessus, with the 'Advanced' section selected. The 'Performance Options' section is expanded, showing several configuration items:

- Slow down the scan when network congestion is detected
When enabled, Nessus detects when it is sending too many packets and the network pipe is approaching capacity. If r Once the congestion has subsided, Nessus automatically attempts to use the available space within the network pipe
- Network timeout (in seconds): 5
Specifies the time that Nessus waits for a response from a host unli to a higher number of seconds.
- Max simultaneous checks per host: 5
Specifies the maximum number of checks a Nessus scanner will pe
- Max simultaneous hosts per scan: 256
Specifies the maximum number of hosts that a Nessus scanner will
- Max number of concurrent TCP sessions per host: [empty field]
Specifies the maximum number of established TCP sessions for a s sends, which is 10 times the number of TCP sessions. For example,
- Max number of concurrent TCP sessions per scan: [empty field]
Specifies the maximum number of established TCP sessions for the

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



The screenshot shows the 'Settings' tab in Nessus, with the 'Host-Discovery' configuration page. The 'Save' button is highlighted with a red arrow.

Configuration details:

- Name: Host-Discovery
- Description: Host Discovery scan for the entire network 192.168.1.0/24 and 100.0.1.0/24 subnets
- Folder: My Scans
- Targets: 192.168.1.0/24, 100.0.1.0/24

Buttons: Save, Cancel

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

Host	FQDN	Ports
192.168.1.254		
192.168.1.3		111, 139, 445, 2049, 41551, 42710, 48364, 48426, 48461, 53842
192.168.1.2		
192.168.1.1		139, 445
100.0.1.254	pool-100-0-1-254.bstnma.fios.verizon.net	
100.0.1.3	pool-100-0-1-3.bstnma.fios.verizon.net	
100.0.1.2	pool-100-0-1-2.bstnma.fios.verizon.net	
100.0.1.1	lo0-100.BSTNMA-VFTTP-350.verizon-gni.net	135, 139, 445, 49664, 49665, 49666, 49667, 49669, 49670

Vulnerabilities Tab provide information about the scan.

Host-Discovery

[Back to My Scans](#)

Sev	CVSS	VPR	EPSS	Name	Family
INFO				Nessus Scan Information	Settings
INFO				Ping the remote host	Port scanners