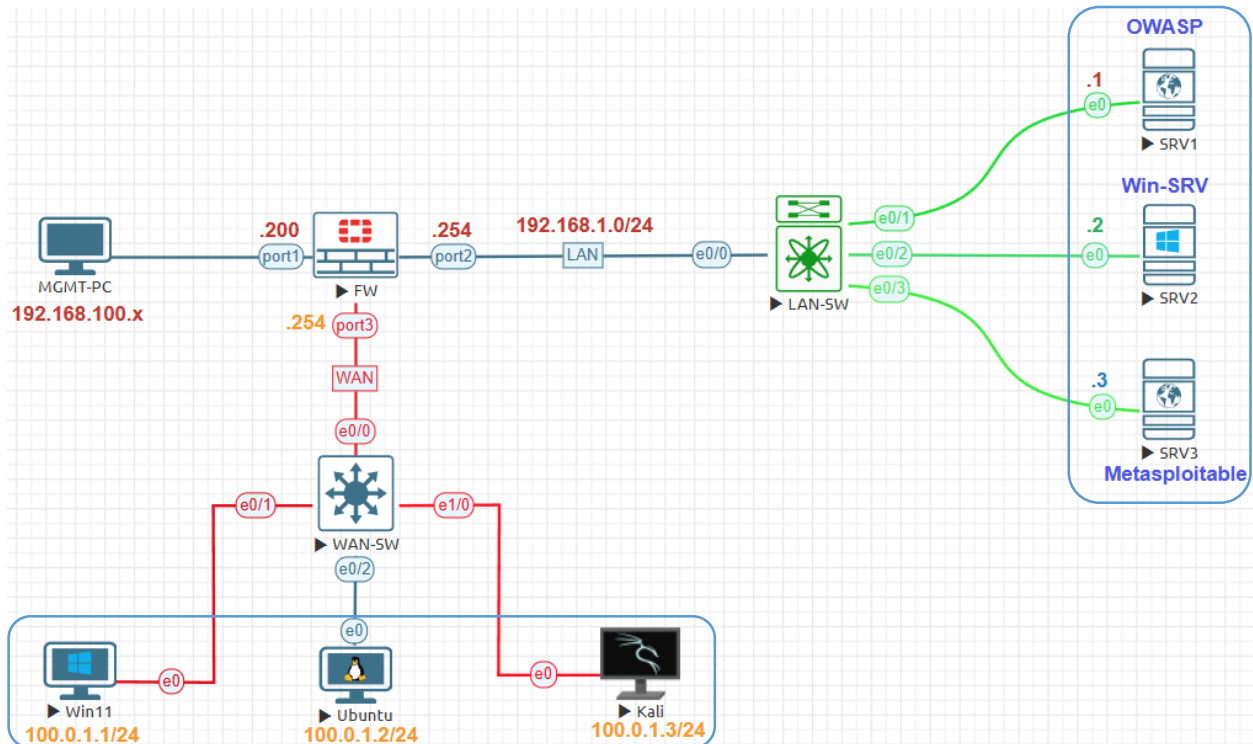


OS Identification Lab:



| | |
|--------------------------------|------------------|
| 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.

tenable Nessus Essentials **Scans** Settings

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

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.

Name: **OS-Identification**. Targets: IP address of targets 192.168.1, 192.168.1.2, 192.168.1.3, 100.0.1.1, 100.0.1.2, 100.0.1.3, 100.0.1.254, 100.0.1.100.

Settings Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

REPORT

ADVANCED

Name: OS-Identification

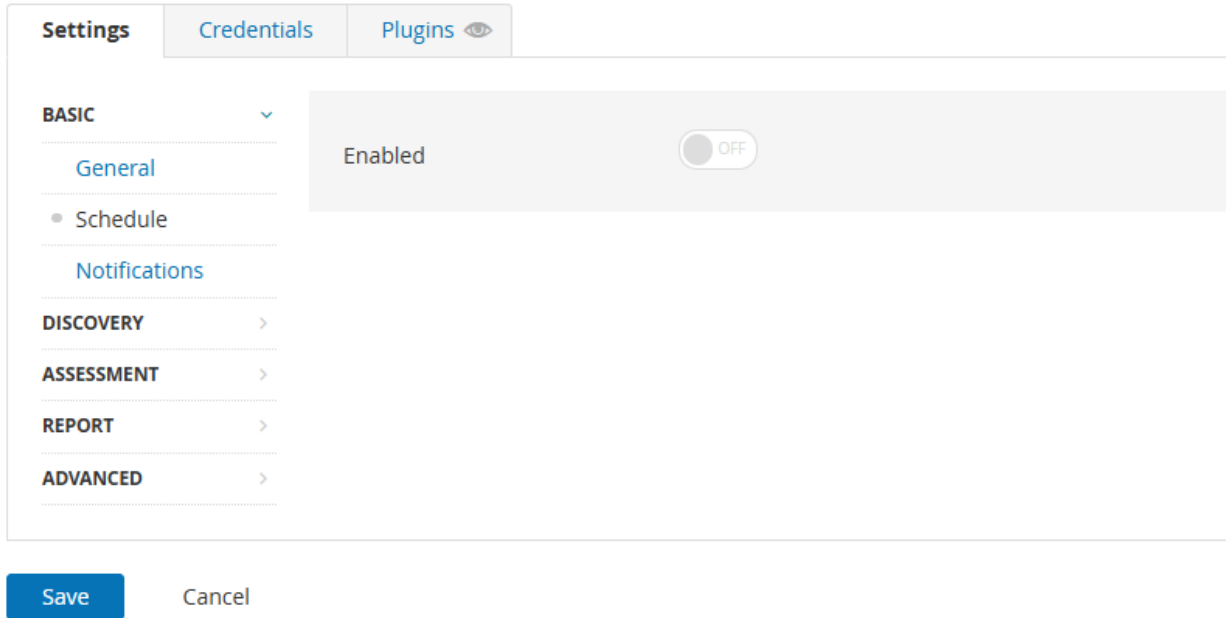
Description: Using Host Discovery scan to Identify Operating System

Folder: My Scans

Targets: 192.168.1.1, 192.168.1.2, 192.168.1.3, 100.0.1.1, 100.0.1.2, 100.0.1.3, 100.0.1.254, 100.0.1.100

Settings>Basic>Schedule keep default disable.

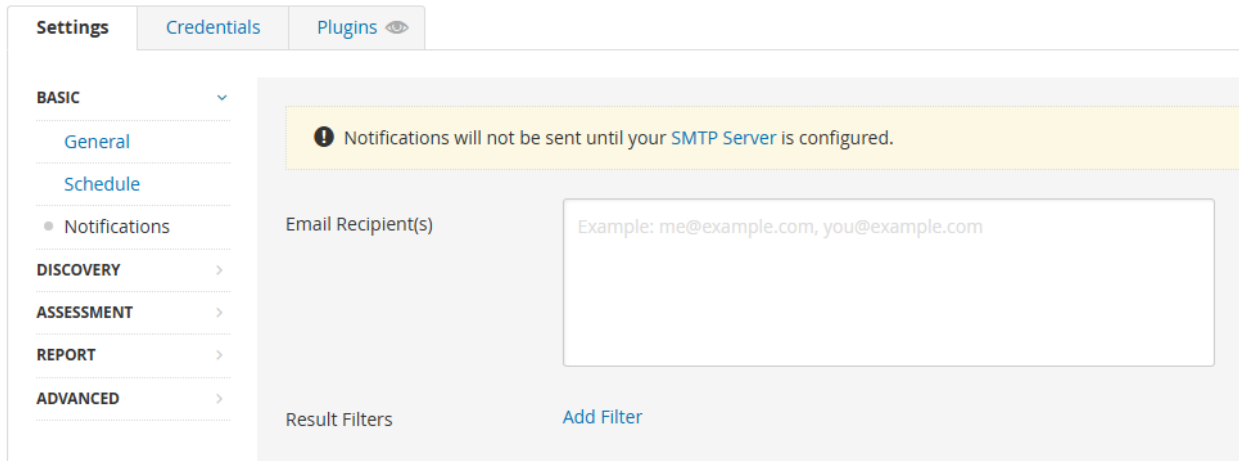
[← Back to Scan Report](#)



The screenshot shows the 'Settings' page with tabs for 'Settings', 'Credentials', and 'Plugins'. The 'BASIC' section is expanded to show 'General', 'Schedule', and 'Notifications'. The 'Schedule' option is selected, and a toggle switch is shown in the 'OFF' position. Below the settings are 'Save' and 'Cancel' buttons.

Settings>Basic>Notification keep default disable.

[← Back to Scan Report](#)



The screenshot shows the 'Settings' page 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>Discovery keep scan type OS Identification

Settings Plugins

BASIC >
DISCOVERY v
REPORT >
ADVANCED >

Scan Type OS Identification

General Settings:
Always test the local Nessus host
Use fast network discovery

Ping hosts using:
TCP
ARP
ICMP

Settings>Reports keep default no changes.

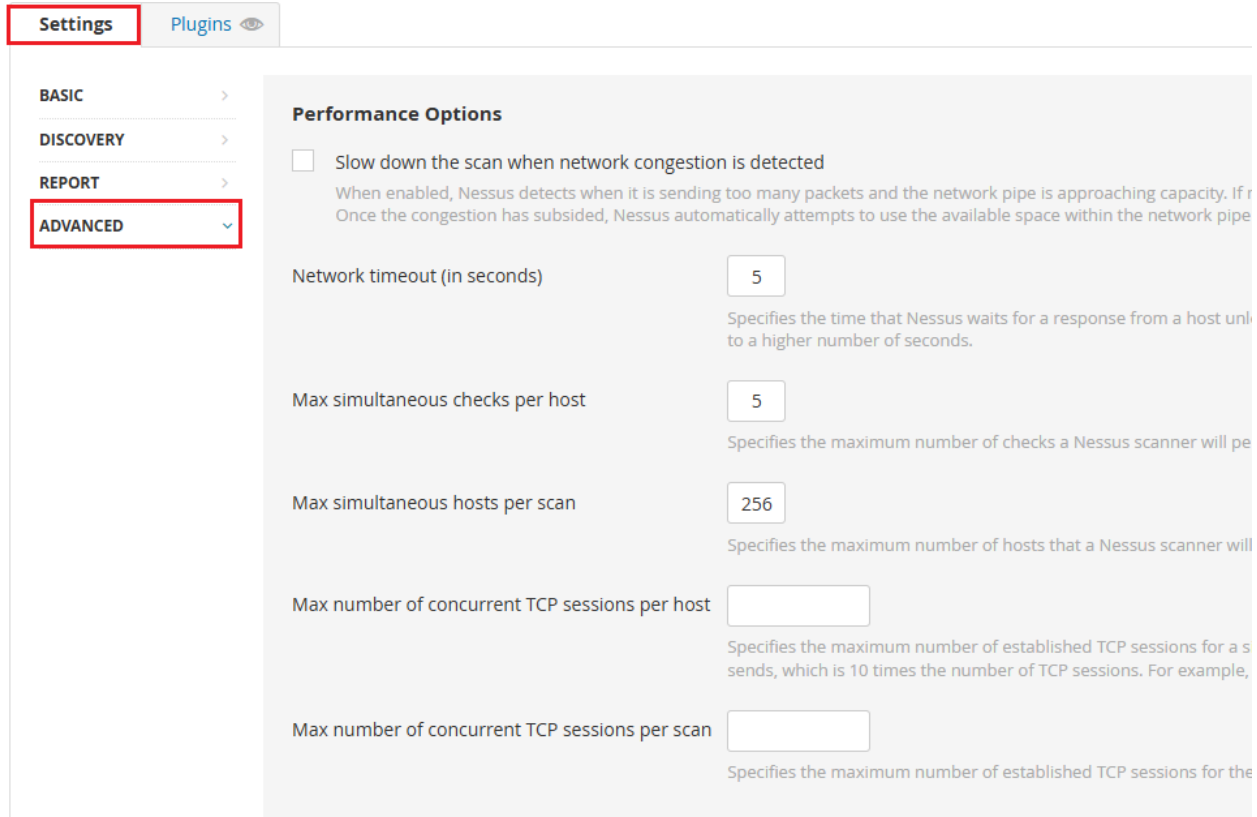
Settings Plugins

BASIC >
DISCOVERY >
REPORT v
ADVANCED >

Output

- 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

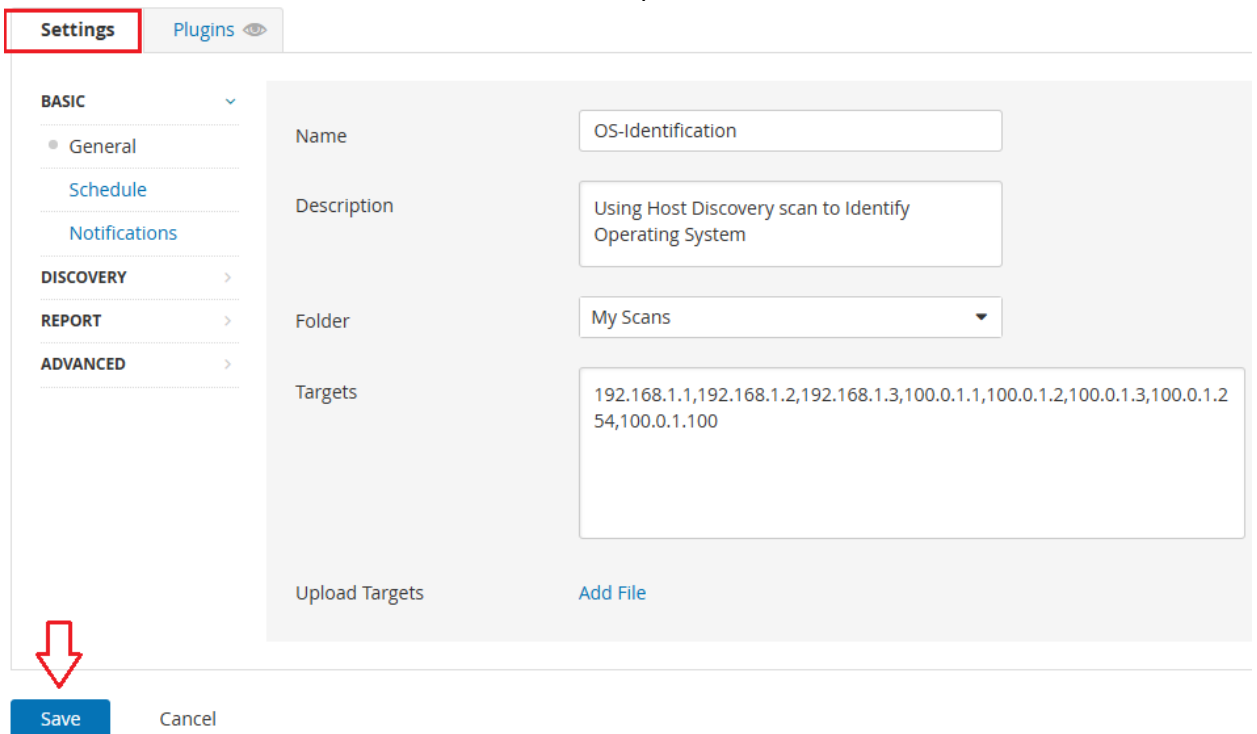
Settings>Advanced keep default no changes.



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

- 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 untl 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 'General' section selected under 'BASIC'. The 'Name' field is 'OS-Identification', the 'Description' is 'Using Host Discovery scan to Identify Operating System', and the 'Folder' is 'My Scans'. The 'Targets' field contains the IP addresses: 192.168.1.1,192.168.1.2,192.168.1.3,100.0.1.1,100.0.1.2,100.0.1.3,100.0.1.254,100.0.1.100. There is an 'Add File' link next to the 'Upload Targets' label. A red arrow points to the 'Save' button at the bottom left.

After complete the scan Hosts Tab 8 host discovered Operating Systems Linux, Microsoft Windows Sever 2019, Microsoft Windows 11.

| Host | FQDN | Operating System | Ports |
|-------------|--|---|--|
| 192.168.1.3 | | Linux Kernel 2.6 on Ubuntu 8.04 (hardy) | 22, 111, 137, 139, 445, 2049, 5432, 41551, 4271... |
| 192.168.1.2 | | Microsoft Windows 10 Enterprise Microsoft Wi... | 123, 135, 139, 445, 3389, 49664, 49665, 49666, ... |
| 192.168.1.1 | | Linux Kernel 2.6 on Ubuntu 10.04 (lucid) | 22, 137, 139, 445 |
| 100.0.1.254 | pool-100-0-1-254.bstnma.fios.verizon.net | | |
| 100.0.1.100 | pool-100-0-1-100.bstnma.fios.verizon.net | | 23 |
| 100.0.1.3 | pool-100-0-1-3.bstnma.fios.verizon.net | Linux Kernel 6.12.13-amd64 | 22, 3389 |
| 100.0.1.2 | pool-100-0-1-2.bstnma.fios.verizon.net | | 5353 |
| 100.0.1.1 | lo0-100.BSTNMA-VFTTP-350.verizon-gni.net | Windows 11 | 135, 137, 139, 445, 49664, 49665, 49666, 49667... |

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 |

INFO OS Identification

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the host. It is also possible sometimes to guess the version of the operating system.

Output

```
Remote operating system : Microsoft Windows 10 Enterprise
Microsoft Windows Server 2019 LTSC
Microsoft Windows Server 2019
Confidence level : 59
Method : SinFP
```