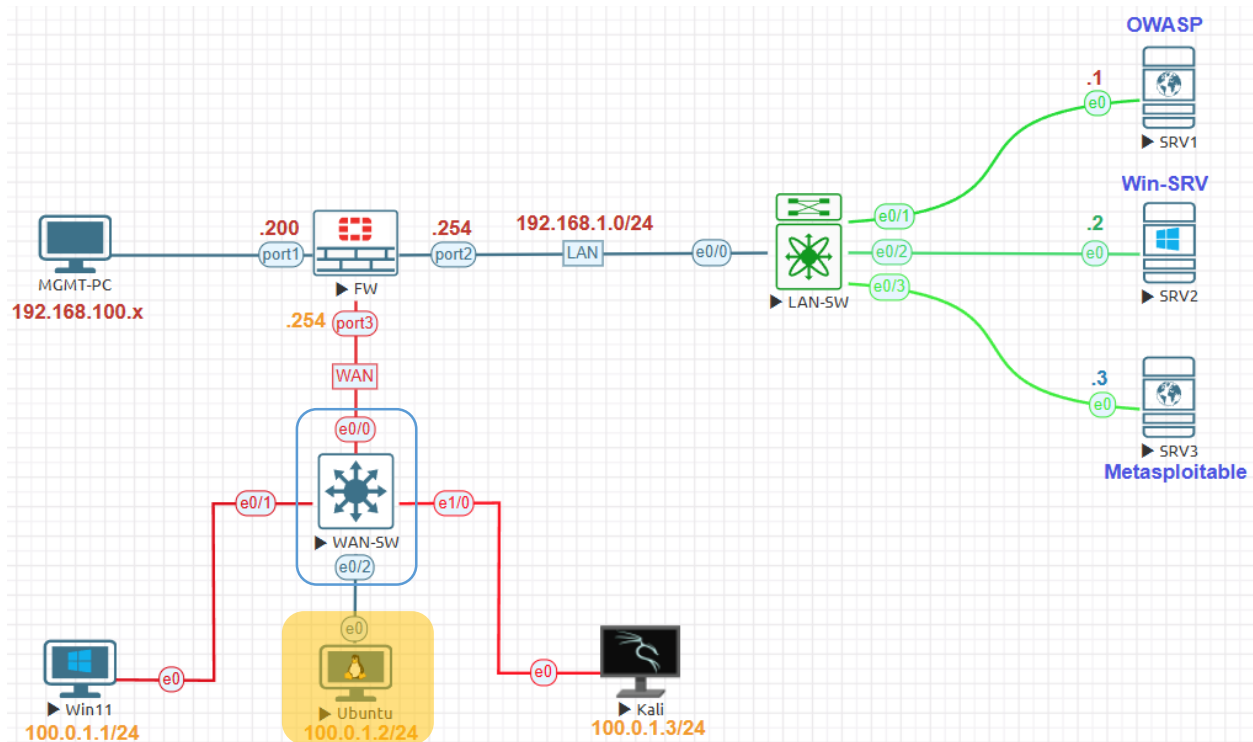


## Cisco Switch Vulnerability Scan Lab:



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

Before Start the scan Cisco Switch Configuration:

<b>Assign IP Address</b>
Switch(config)#interface vlan 1 Switch(config-if)#ip address 100.0.1.100 255.255.255.0 Switch(config-if)#no shutdown
<b>Enable HTTP</b>
Switch(config)#ip http server
<b>Enable Telnet</b>
Switch(config)#username admin privilege 15 password cisco Switch(config)#line vty 0 4 Switch(config-line)#transport input telnet Switch(config-line)#login local
<b>Enable SNMP v1/v2</b>
Switch(config)#snmp-server community public RO Switch(config)#snmp-server community private RW
<b>Enable Mode Password</b>
Switch(config)#enable password cisco
<b>Configure Consol</b>
Switch(config)#line console 0 Switch(config-line)#password cisco Switch(config-line)#login
<b>Enable FTP or TFTP</b>
Switch(config)#ip ftp username ftpuser Switch(config)#ip ftp password ftppass Switch(config)#ip tftp source-interface vlan 1
<b>Expose Unused Services</b>
Switch(config)#service tcp-small-servers Switch(config)#service udp-small-servers

Go to **Scans > New Scan**. Choose **Advanced Scan** to open.

## 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.

#### 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: **Cisco-Switch-Scan**. Targets: IP address of target **100.0.1.100** the IP Address of VLAN Interface of Cisco Switch.

#### Settings

[Credentials](#)

[Plugins](#)

#### BASIC

• General

[Schedule](#)

[Notifications](#)

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name

Cisco-Switch-Scan

Description

Cisco Switch Scan

Folder

My Scans

Targets

100.0.1.100

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>Host Discovery keep default enable.

**Settings** | Credentials | Compliance | Plugins

**BASIC** >  
**DISCOVERY** v  
• Host Discovery  
Port Scanning  
Service Discovery  
Identity

**ASSESSMENT** >  
**REPORT** >  
**ADVANCED** >

**Remote Host Ping**  
Ping the remote host  ON  
If set to On, the scanner pings remote hosts on multiple ports to determine remote hosts on multiple ports during the scan. Note: To scan VMware guests

**General Settings**  
 Test the local Nessus host  
When enabled, includes the local Nessus host in the scan. This is used when the Nessus host falls with  
 Use fast network discovery  
When disabled, if a host responds to ping, Nessus attempts to avoid false positives, performing additional checks especially if the remote host is firewalled. When enabled, Nessus does not perform these checks.

Settings>Discovery>Port Scanning keep default.

**Settings** | Credentials | Compliance | Plugins

**BASIC** >  
**DISCOVERY** v  
Host Discovery  
• Port Scanning  
Service Discovery  
Identity

**ASSESSMENT** >  
**REPORT** >  
**ADVANCED** >

**Ports**  
 Consider unscanned ports as closed  
When enabled, if a port is not scanned with a selected port scanner (for example, the port falls out of the scan range)

Port Scan Range: default

**Local Port Enumerators**  
 SSH (netstat)

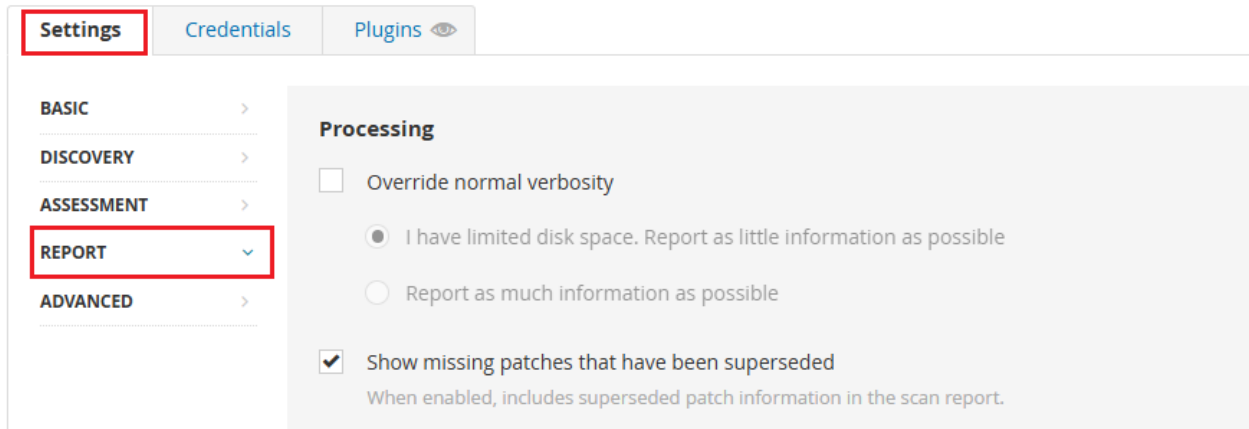
Settings>Discovery>Service Discovery keep default.

The screenshot shows the 'Settings' page with the 'Discovery' section selected. Under 'Discovery', 'Service Discovery' is highlighted. The 'General Settings' for Service Discovery are shown, including a checked box for 'Probe all ports to find services', a toggle for 'Search for SSL/TLS/DTLS services' set to 'ON', and dropdown menus for 'Search for SSL/TLS on' (All TCP ports) and 'Search for DTLS on' (None). A text input field for 'Identify certificates expiring within x days' is set to '60'.

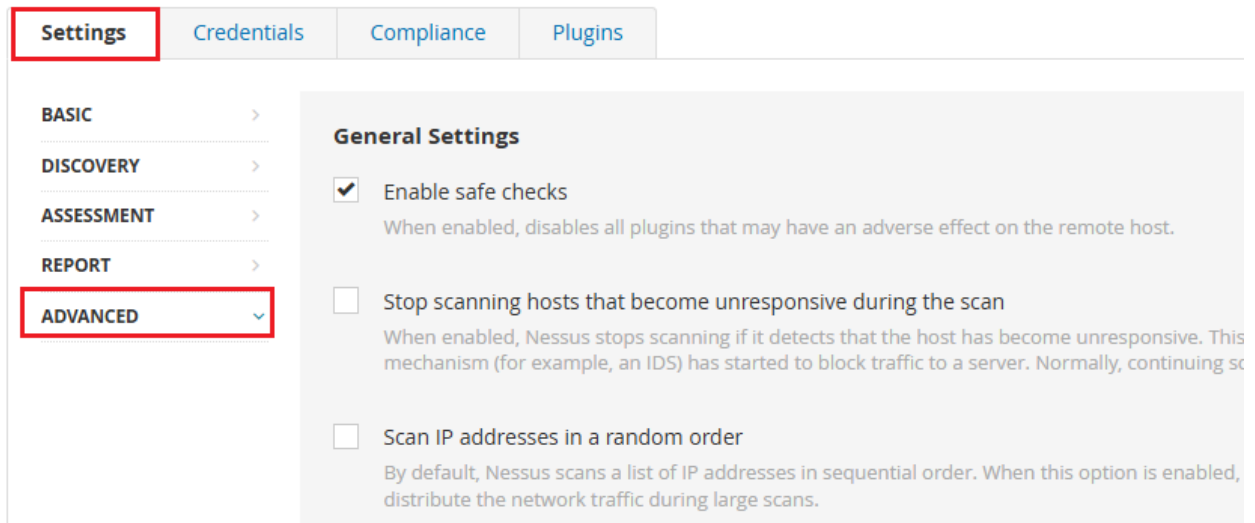
Settings>Assessment keep default.

The screenshot shows the 'Settings' page with the 'Assessment' section selected. Under 'Assessment', 'Oracle Database' is highlighted. The 'Oracle Database' settings are shown, including an unchecked checkbox for 'Use detected SIDs'. The text below the checkbox explains that when enabled, the scanner attempts to authenticate using specified Oracle database credentials and manually specified SIDs.

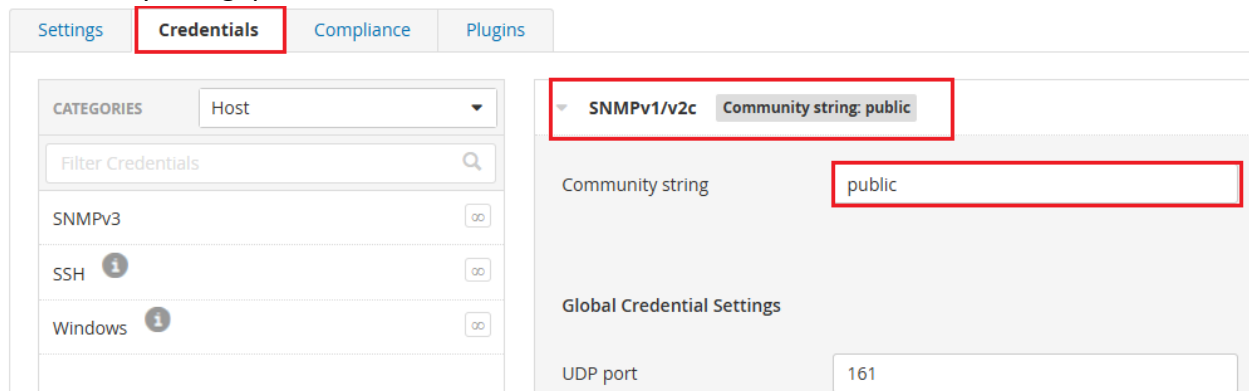
Settings>Reports keep default no changes.



Settings>Advanced keep default no changes.



Under Credentials Tab. Choose SSH and SNMPv1/v2c authentication methods. In SNMP enter Community string: public



In **telnet** choose the Authentication method: **Password** enter username and password of Cisco Switch **admin/cisco**

Settings **Credentials** Plugins

CATEGORIES Host

Filter Credentials

Add credentials (unlimited available)

telnet/rsh/rexec User: admin

admin

Password (unsafe!)

\*\*\*\*\*

Global Credential Settings

- Perform patch audits over telnet  
Patch auditing will only be attempted for non-Windows targets.
- Perform patch audits over rsh  
Patch auditing will only be attempted for non-Windows targets.
- Perform patch audits over rexec  
Patch auditing will only be attempted for non-Windows targets.

**Plugins** Tab **disable** all Plugins only enable **Cisco** plugin.

Cisco-SW-Scan / Configuration

[← Back to Scan Report](#)

Settings Credentials Compliance **Plugins**

DISABLED	Brute force attacks	25
DISABLED	CentOS Local Security Checks	5165
DISABLED	CGI abuses	6421
DISABLED	CGI abuses : XSS	711
ENABLED	CISCO	2536

Disable All Enable All

Show Enabled | Show All

STATUS	PLUGIN NAME	PLUGIN ID
ENABLED	3Proxy HTTP Proxy Crafted Transparent Request Remote Overflow	31094

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

### Cisco-SW-Scan / Configuration

[Back to Scan Report](#)

Settings Credentials Compliance Plugins

**BASIC**

- General
- Schedule
- Notifications

**DISCOVERY**

**ASSESSMENT**

**REPORT**

**ADVANCED**

**General Settings**

Name: Cisco-SW-Scan

Description: Cisco Switch

Folder: My Scans

Targets: 100.0.1.100

Upload Targets: [Add File](#)

**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, in Hosts

Cisco-Switch-Scan

[← Back to My Scans](#)

<b>Hosts</b> 1	Vulnerabilities 13	History 1
Filter	Search Hosts	1 Host
Host	Vulnerabilities	
100.0.1.100	1 2 1	14

## Under Vulnerabilities Tab it shows almost 13

Cisco-Switch-Scan

[← Back to My Scans](#)

Hosts 1	<b>Vulnerabilities</b> 13	History 1			
Filter	Search Vulnerabilities	13 Vulnerabilities			
Sev	CVSS	VPR	EPSS	Name	Family
HIGH	7.5 *	6.0	0.9233	SNMP Agent Default Community Name (public)	SNMP
MEDIUM	6.5	4.9	0.0596	IP Forwarding Enabled	Firewalls
MEDIUM	5.0 *	3.6	0.0787	SNMP 'GETBULK' Reflection DDoS	SNMP
LOW				SNMP Request Cisco Router Information Disclosure	SNMP
INFO				Nessus SNMP Scanner	Port scanners

### Scan Details

Policy: Advanced Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: May 10 at 4:49 PM  
End: May 10 at 4:53 PM  
Elapsed: 3 minutes

### Vulnerabilities

