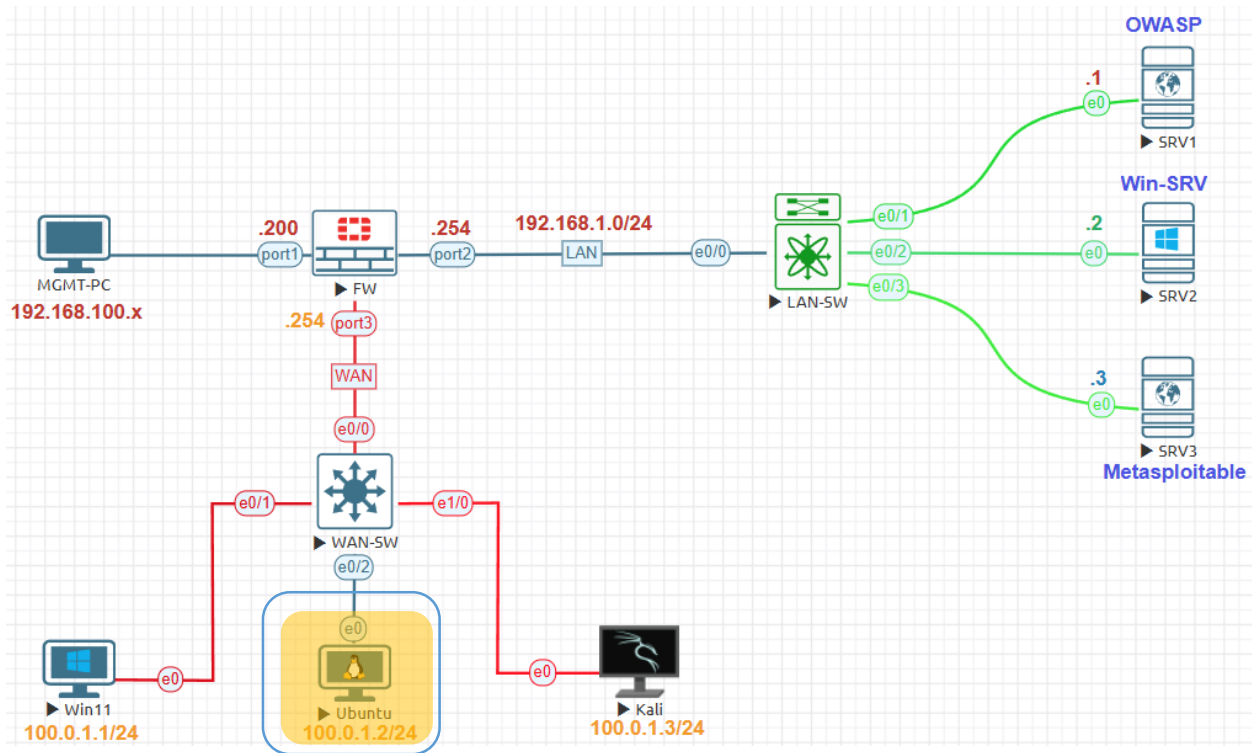


## Advanced Dynamic Scan Lab:



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 **Advanced Dynamic Scan** to open.

**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.
- Advanced Dynamic Scan**  
Configure a dynamic plugin scan without recommendations.

Name: **Ubuntu-DynamicScan**. Targets: IP address of target **100.0.1.2** the IP Address of Ubuntu Linux Machine.

**Settings** Credentials Dynamic Plugins

**BASIC**

- General**
- Schedule
- Notifications

**DISCOVERY** >

**ASSESSMENT** >

**REPORT** >

**ADVANCED** >

**General Settings**

Name: Ubuntu-DynamicScan

Description:

Folder: My Scans

Targets: 100.0.1.2

Setting>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>Basic>Discovery>Host Discovery keep default enable.

The screenshot shows the Nessus configuration interface. At the top, there are tabs for 'Settings', 'Credentials', 'Compliance', and 'Plugins'. The left sidebar has a tree view with 'BASIC' expanded, 'DISCOVERY' selected, and 'Host Discovery' highlighted. The main content area is titled 'Remote Host Ping' and features a toggle switch labeled 'Ping the remote host' which is currently turned ON. Below this, there is a note: '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'. Underneath, the 'General Settings' section includes two options: 'Test the local Nessus host' (checked) and 'Use fast network discovery' (unchecked).

Setting>Discovery>Port Scanning keep default.

The screenshot shows the Nessus configuration interface. At the top, there are tabs for 'Settings', 'Credentials', 'Compliance', and 'Plugins'. The left sidebar has a tree view with 'BASIC' expanded, 'DISCOVERY' selected, and 'Port Scanning' highlighted. The main content area is titled 'Ports' and features a checkbox for 'Consider unscanned ports as closed' which is unchecked. Below this is a text input field for 'Port Scan Range' containing the value 'default'. Underneath, the 'Local Port Enumerators' section includes a checked option for 'SSH (netstat)'.

Setting>Discovery>Service Discovery keep default.

**Settings** | Credentials | Compliance | Plugins

**BASIC** >  
**DISCOVERY** ▾  
Host Discovery  
Port Scanning  
• Service Discovery  
Identity  
**ASSESSMENT** >  
**REPORT** >  
**ADVANCED** >

**General Settings**

Probe all ports to find services  
When enabled, the scanner attempts to map each open port with the service that is running on the unforeseen side effects.

Search for SSL/TLS/DTLS services  ON

Controls how the scanner tests SSL-based services. Caution: Testing !

Search for SSL/TLS on All TCP ports ▾

Search for DTLS on None ▾

Identify certificates expiring within x days 60

Setting> Discovery >Identity Keep default no changes.

**Settings** | Credentials | Dynamic Plugins

**BASIC** >  
**DISCOVERY** ▾  
Host Discovery  
Port Scanning  
Service Discovery  
• Identity  
**ASSESSMENT** >  
**REPORT** >  
**ADVANCED** >

**General Settings**

Collect Identity Data from Active Directory

Checking this box will enable collection of identity information from Active Directory using Domain User credentials.

Setting>Assessment>General keep default.

**Settings** | Credentials | Plugins

**BASIC** >  
**DISCOVERY** >  
**ASSESSMENT** ▾  
• General  
Brute Force  
Web Applications  
Windows  
Malware  
Databases  
**REPORT** >  
**ADVANCED** >

**Accuracy**

- Override normal accuracy
- Avoid potential false alarms
- Show potential false alarms

Perform thorough tests (may disrupt your network or impact scan speed)  
Causes various plugins to work harder. For example, when looking through SMB file shares, a plugin can be more thorough, the scan is more intrusive and is more likely to disrupt the network, while potential

**Antivirus**

Antivirus definition grace period (in days): 0 ▾

Settings>Assessment Keep default.

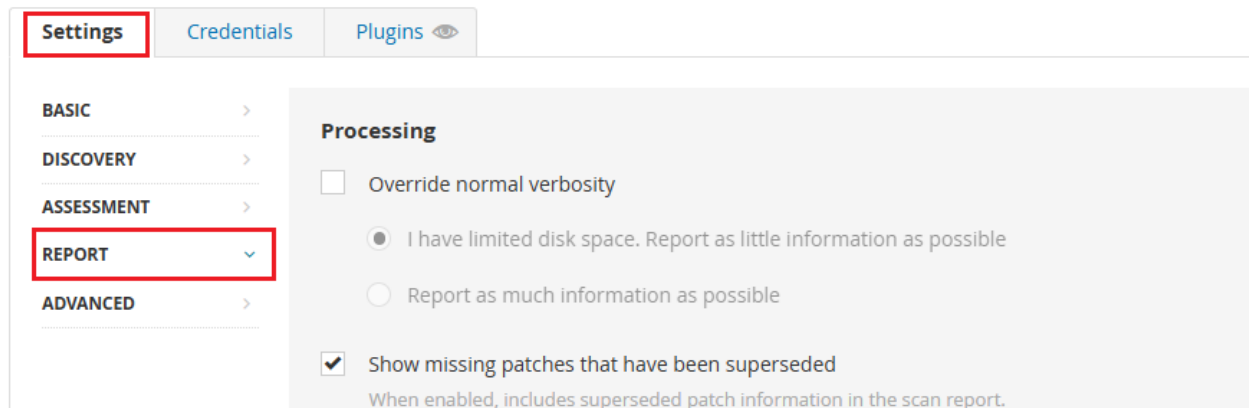
**Settings** | Credentials | Dynamic Plugins

**BASIC** >  
**DISCOVERY** >  
**ASSESSMENT** ▾  
General  
Brute Force  
SCADA  
Web Applications  
Windows  
Malware  
• Databases  
**REPORT** >  
**ADVANCED** >

**Oracle Database**

- Use detected SIDs  
When enabled, if at least one host credential and one Oracle database credential are configured, the scanner then attempts to authenticate using the specified Oracle database credentials and the detected scanner authenticates to the Oracle database using the manually specified SIDs in the Oracle database credentials

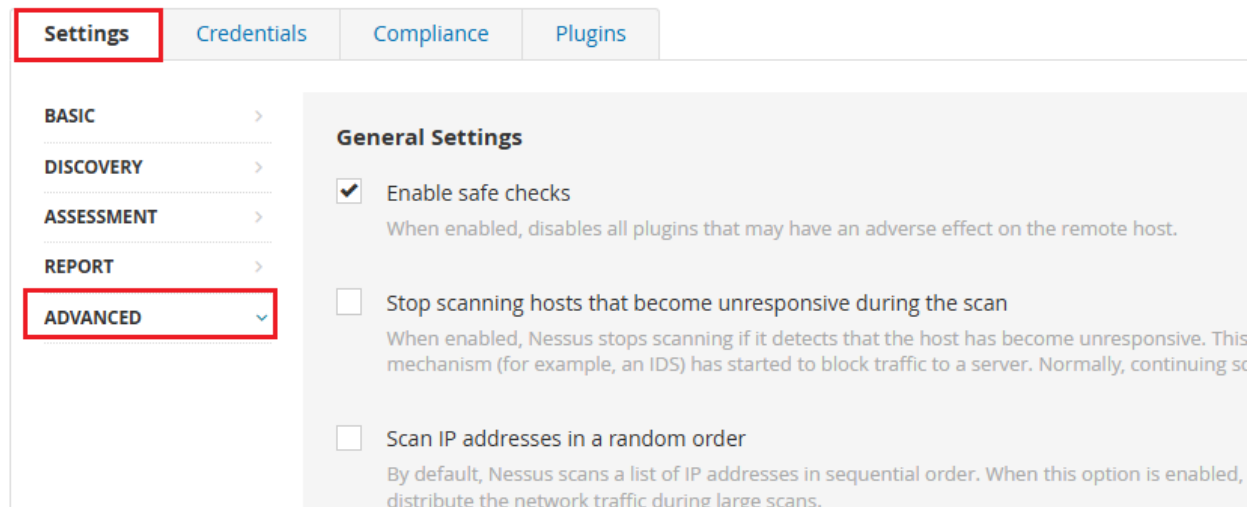
Settings>Report keep the default.



The screenshot shows the 'Settings' tab selected in the top navigation bar. On the left sidebar, the 'REPORT' category is highlighted with a red box. The main content area is titled 'Processing' and contains the following options:

- Override normal verbosity
- I have limited disk space. Report as little information as possible
- Report as much information as possible
- Show missing patches that have been superseded  
When enabled, includes superseded patch information in the scan report.

Settings>Advanced keep default no changes.



The screenshot shows the 'Settings' tab selected in the top navigation bar. On the left sidebar, the 'ADVANCED' category is highlighted with a red box. The main content area is titled 'General Settings' and contains the following options:

- Enable safe checks  
When enabled, disables all plugins that may have an adverse effect on the remote host.
- Stop scanning hosts that become unresponsive during the scan  
When enabled, Nessus stops scanning if it detects that the host has become unresponsive. This mechanism (for example, an IDS) has started to block traffic to a server. Normally, continuing sc
- Scan IP addresses in a random order  
By default, Nessus scans a list of IP addresses in sequential order. When this option is enabled, distribute the network traffic during large scans.

Under **Credentials** Tab. Choose **SSH** Authentication method: **Password**

The screenshot shows the 'Credentials' tab in the Nessus interface. On the left, there is a sidebar with 'CATEGORIES' set to 'Host' and a search box for 'Filter Credentials'. Below this are three categories: 'SNMPv3', 'SSH', and 'Windows', each with an infinity icon. The main area is titled 'SSH User: user, Auth method: password'. It contains several fields: 'Authentication method' is set to 'password'; 'Username' is 'user'; 'Password (unsafe!)' is masked with dots and has a warning note: 'This password could be compromised if Nessus connects to the host. See the "Global Settings" section below.'; 'Elevate privileges with' is set to 'sudo'; 'sudo user' is 'Test123'; 'sudo password' is masked with dots; and 'Location of sudo (directory)' is '/usr/bin'.

**Dynamic Plugins** choose **Plugin Family** is equal to **Ubuntu Local Security Checks** after that click on **Preview Plugins**

The screenshot shows the 'Dynamic Plugins' tab in the Nessus interface. At the top, it says 'Ubuntu-DynamicScan / Configuration' and has a link 'Back to Scan Report'. Below this, there is a 'Match' dropdown set to 'All' and the text 'of the following:'. A configuration rule is shown: 'Plugin Family' is set to 'is equal to' 'Ubuntu Local Security Checks'. A red arrow points from this rule to a blue button labeled 'Preview Plugins'.

Settings | Credentials | **Dynamic Plugins**

Match **All** of the following:

Plugin Family is equal to Ubuntu Local Security Checks

**Preview Plugins** → Ubuntu Local Security Checks (8879)

Plugin Name	Plugin ID
Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : acpid vulnerability	57060
Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : ca-certificates-java	58511
Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : clamav vulnerability	56777
Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : cvs vulnerability (L	58104
Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : empathy vulnerab	56680

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

DISCOVERY >  
 ASSESSMENT >  
 REPORT >  
 ADVANCED >

Folder: My Scans

Targets: 100.0.1.2

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 **Scan Summary** Tab.

### Ubuntu-DynamicScan

[← Back to My Scans](#)

**Scan Summary** Hosts 1 Vulnerabilities 5 Remediations 2 History 1

#### Scan Details

1 Critical Vulnerabilities	1 High Vulnerabilities
0 Medium Vulnerabilities	0 Low Vulnerabilities

#### Details

Scan Name: Ubuntu-DynamicScan  
Plugin Set: 202505170603  
CVSS\_Score: CVSS\_V3  
Scan Template: Advanced Dynamic Scan  
Scan Start: Today at 10:47 AM  
Scan End: Today at 10:47 AM

#### Authentication / Credential Info (Hosts)

1 SUCCEEDED	0 FAILED
----------------	-------------

Under **Vulnerabilities** Tab it shows almost 5

**Scan Summary** Hosts 1 **Vulnerabilities 5** Remediations 2 History 1

Filter Search Vulnerabilities 5 Vulnerabilities

<input type="checkbox"/>	Sev	CVSS	VPR	EPSS	Name	Family
<input type="checkbox"/>	CRITICAL	9.8			Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : xrdp vulnerabi...	Ubuntu Local Security Checks
<input type="checkbox"/>	HIGH	8.1			Ubuntu 20.04 LTS / 22.04 LTS : GRUB2 vulnerabilities (USN-6355-1)	Ubuntu Local Security Checks
<input type="checkbox"/>	INFO				Netstat Portscanner (SSH)	Port scanners
<input type="checkbox"/>	INFO				Nessus Scan Information	Settings
<input type="checkbox"/>	INFO				Patch Report	General

## Under Remediation Tab.

Ubuntu-DynamicScan

[Back to My Scans](#)

Scan Summary | Hosts 1 | Vulnerabilities 5 | **Remediations 2** | History 1

Search Actions  2 Actions

Action
Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : xrdp vulnerabilities (USN-6474-1): Update the affected xorgxrdp, xrdp and / or xrdp-pulse packages.
Ubuntu 20.04 LTS / 22.04 LTS : GRUB2 vulnerabilities (USN-6355-1): Update the affected packages.

## Under Hosts Tab.

Ubuntu-DynamicScan

[Back to My Scans](#)

Scan Summary | **Hosts 1** | Vulnerabilities 5 | Remediations 2 | History 1

Filter  Search Hosts  1 Host

Host	Vulnerabilities
<input type="checkbox"/> 100.0.1.2	<div style="display: flex; align-items: center;"><div style="width: 10px; height: 10px; background-color: #800000; margin-right: 5px;"></div>1</div> <div style="display: flex; align-items: center;"><div style="width: 10px; height: 10px; background-color: #FF0000; margin-right: 5px;"></div>1</div> <div style="display: flex; align-items: center;"><div style="width: 10px; height: 10px; background-color: #0070C0; margin-right: 5px;"></div>7</div>

### Scan Details

Policy: Advanced Dynamic Scan  
Status: Completed  
Severity Base: CVSS v3.0   
Scanner: Local Scanner  
Start: Today at 10:47 AM  
End: Today at 10:47 AM  
Elapsed: a minute

### Vulnerabilities

