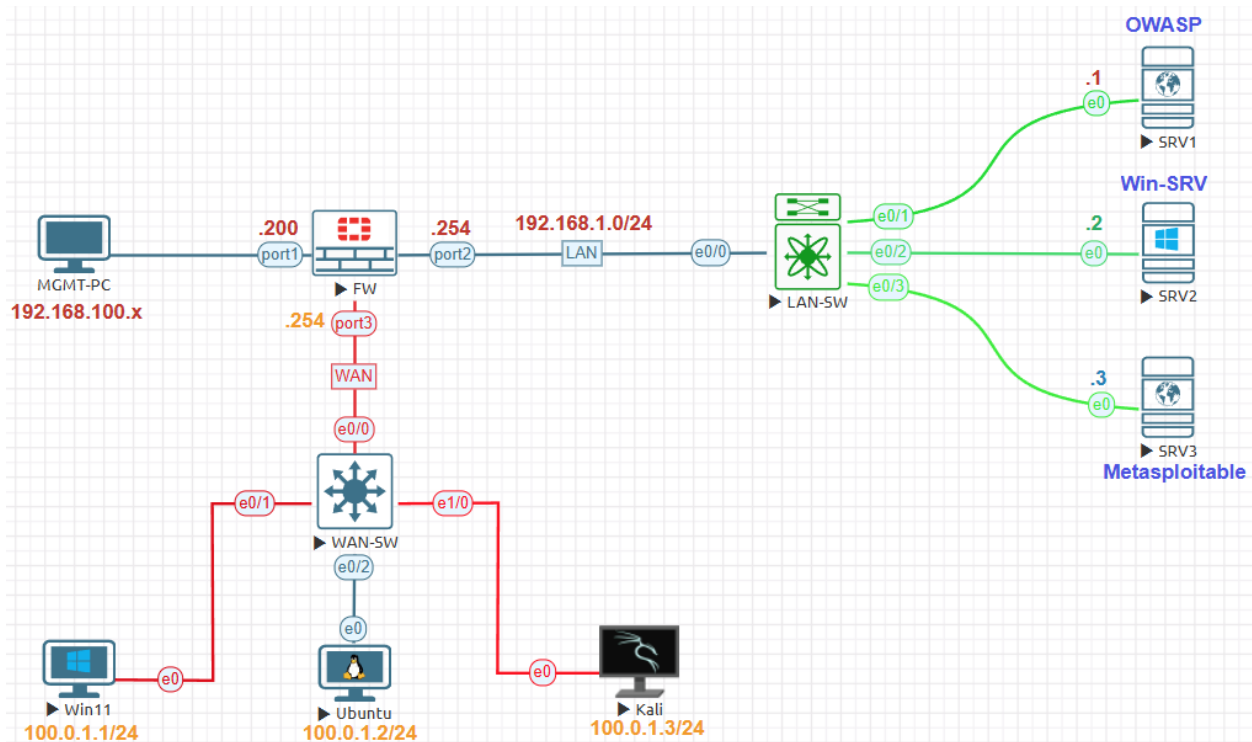


Authenticated Scan Lab:



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 **Basic Network Scan** to open.

Scan Templates

[← Back to Scans](#)

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.

Name: **Metasploitable-Authenticated**. Targets: IP address of target Metasploitable **192.168.1.3**.

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Metasploitable-Authenticated

Description

Metasploitable - Authenticated Scan

Folder

My Scans

Targets

192.168.1.3

Upload Targets

[Add File](#)

Settings>Basic>Schedule keep default disable.

[← Back to Scan Report](#)

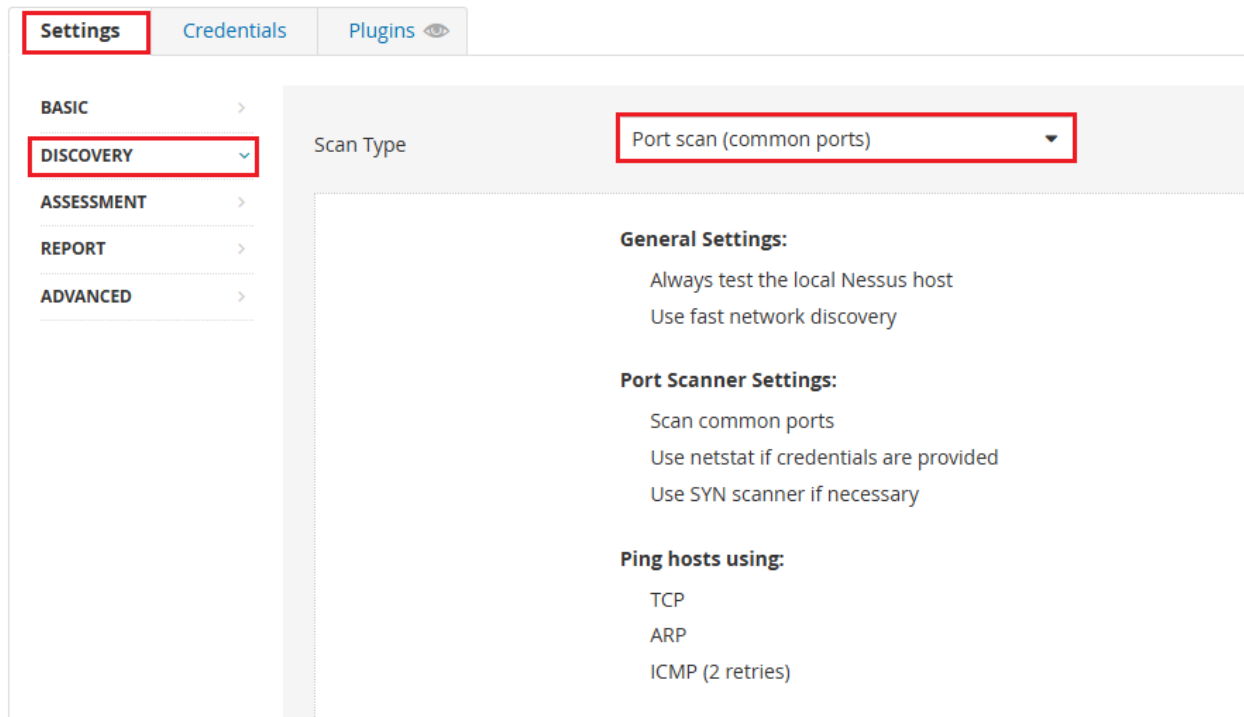
The screenshot shows the 'Settings' interface with tabs for 'Settings', 'Credentials', and 'Plugins'. The 'BASIC' section is expanded to show 'General', 'Schedule', and 'Notifications'. The 'Schedule' option is selected, and a toggle switch is shown in the 'OFF' position. Below the settings are 'Save'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

Settings>Basic>Notification keep default disable.

[← Back to Scan Report](#)

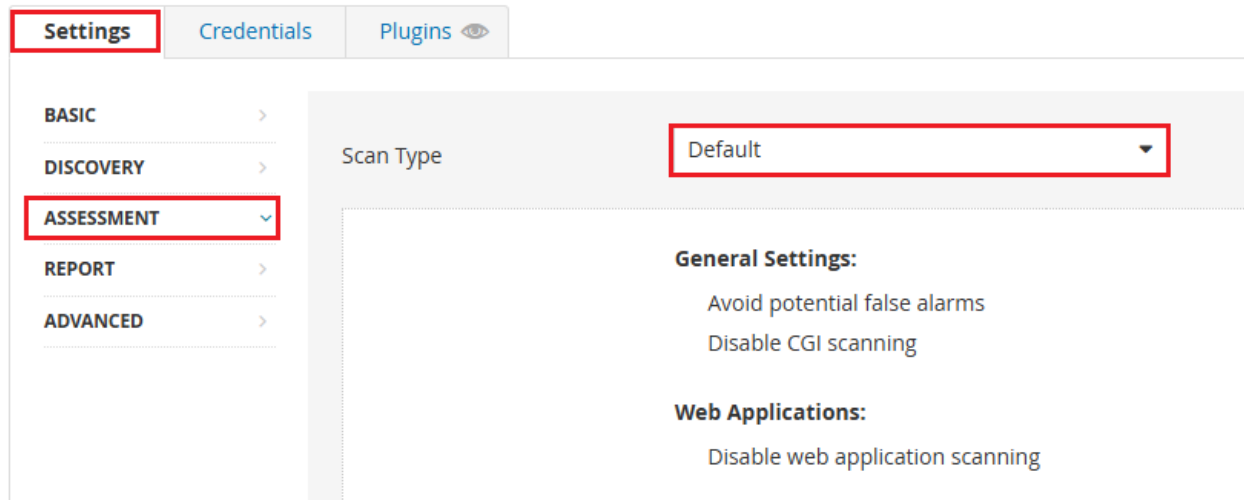
The screenshot shows the 'Settings' interface with tabs for 'Settings', 'Credentials', and 'Plugins'. The 'BASIC' section is expanded to show 'General', 'Schedule', and 'Notifications'. The 'Notifications' option is selected. A yellow warning banner at the top reads: 'Notifications will not be sent until 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 default Port scan (common ports).



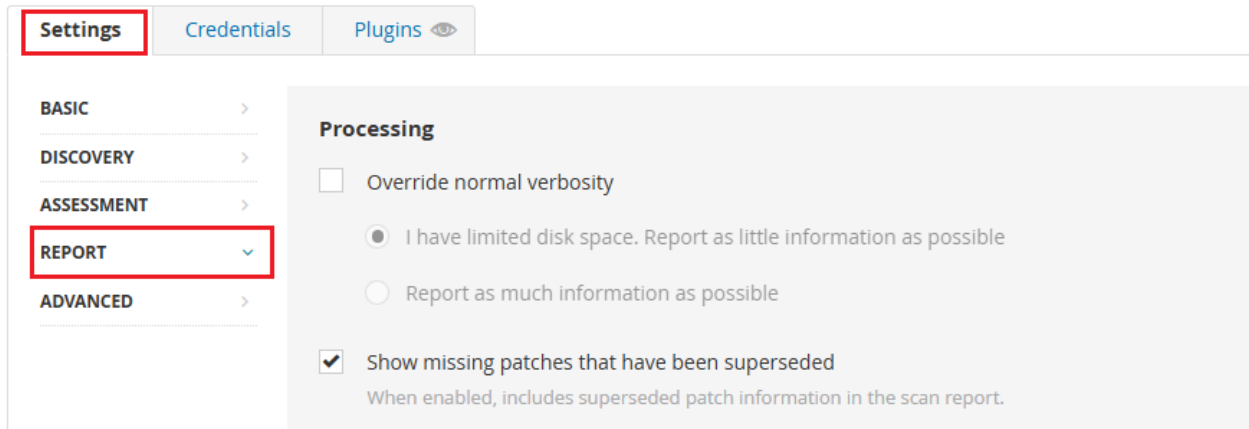
The screenshot shows the 'Settings' tab selected in the top navigation bar. On the left sidebar, the 'DISCOVERY' option is highlighted with a red box. The main content area shows the 'Scan Type' dropdown menu set to 'Port scan (common ports)', also highlighted with a red box. Below this, the settings are organized into sections: 'General Settings' (Always test the local Nessus host, Use fast network discovery), 'Port Scanner Settings' (Scan common ports, Use netstat if credentials are provided, Use SYN scanner if necessary), and 'Ping hosts using:' (TCP, ARP, ICMP (2 retries)).

Settings>Assessment keep default

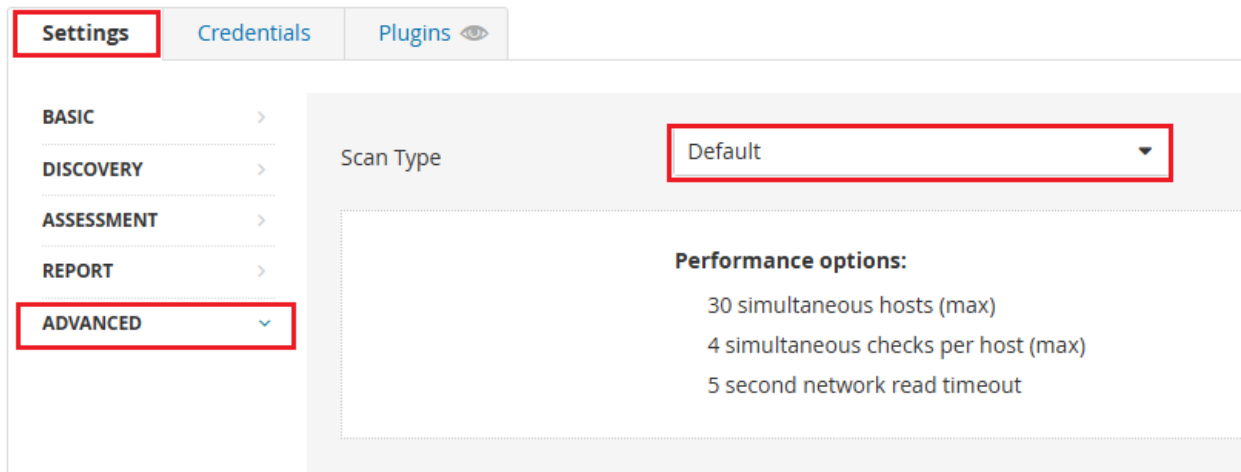


The screenshot shows the 'Settings' tab selected in the top navigation bar. On the left sidebar, the 'ASSESSMENT' option is highlighted with a red box. The main content area shows the 'Scan Type' dropdown menu set to 'Default', also highlighted with a red box. Below this, the settings are organized into sections: 'General Settings' (Avoid potential false alarms, Disable CGI scanning) and 'Web Applications:' (Disable web application scanning).

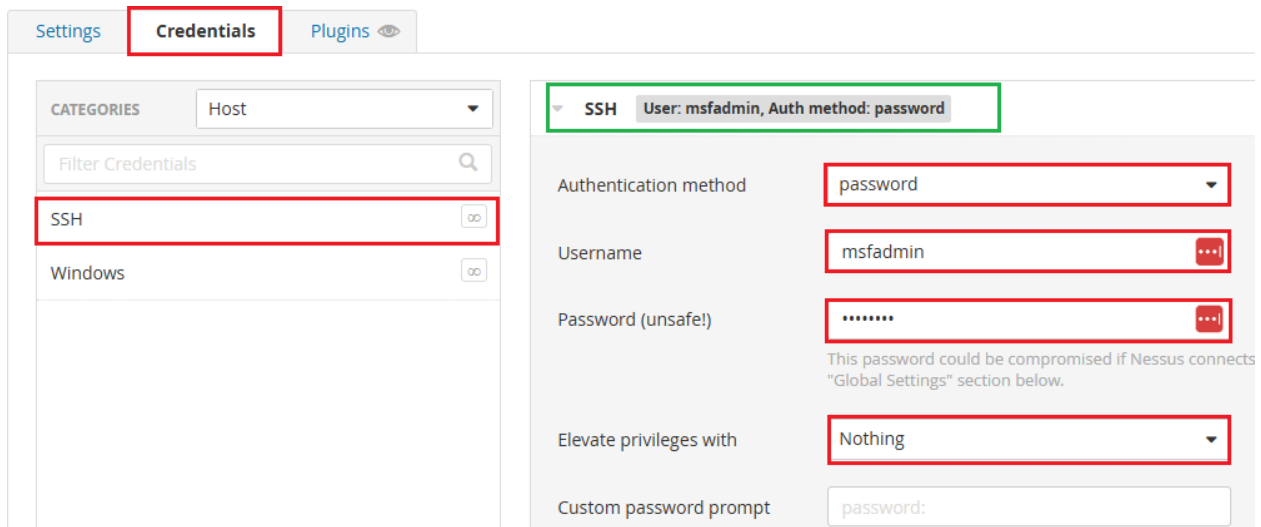
Settings>Reports keep default no changes.



Settings>Advanced keep default no changes.



Under Credentials Tab. Choose SSH authentication method password, enter username and password msfadmin/msfadmin



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

Settings | Credentials | Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Metasploitable-Authenticated

Description: Metasploitable - Authenticated Scan

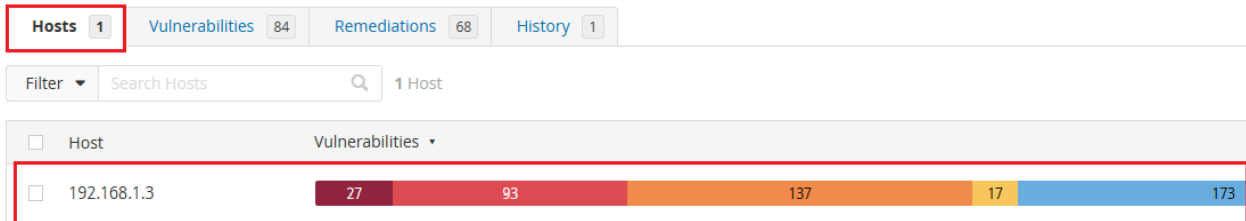
Folder: My Scans

Targets: 192.168.1.3

Upload Targets: Add File

Save | Cancel

After complete the scan, 27 Critical, 93 High, 137 Medium, 17 Low and 173 info.



Total 84 Vulnerabilities includes 27 Critical, 93 High, 137 Medium, 17 Low and 173 info.

Hosts 1 | **Vulnerabilities** 84 | Remediations 68 | History 1

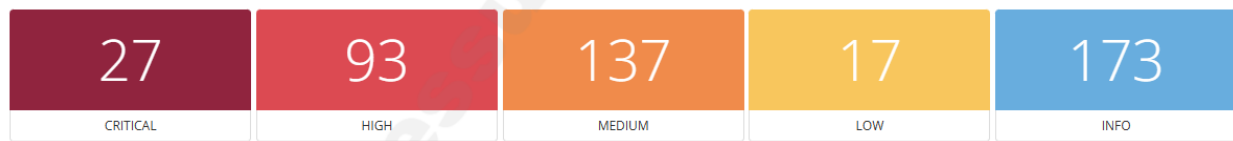
Filter Search Vulnerabilities 84 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely
CRITICAL	9.8	9.5	0.9414	Bash Remote Code Execution (Shellshock)	Gain a shell remotely
CRITICAL	9.8	8.9	0.9447	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers
CRITICAL	9.8	5.1	0.0165	Weak Debian OpenSSH Keys in ~/.ssh/authorized_keys	Gain a shell remotely

Search Actions 68 Actions

Action
Ubuntu 8.04 LTS : linux vulnerabilities (USN-1105-1): Update the affected packages.
Ubuntu 8.04 LTS : linux vulnerability (USN-1660-1): Update the affected packages.
Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : mysql-5.1, mysql-5.5, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-1467-1): Update the affected mysql-server-5.0, mysql-server-5.1 and / or mysql-server-5.5 packages.
Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : php5 regression (USN-1358-2): Update the affected packages.
Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : apache2 vulnerabilities (USN-1765-1): Update the affected apache2.2-common package.
Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : openssl vulnerabilities (USN-1732-1): Update the affected libssl0.9.8 and / or libssl1.0.0 packages.

192.168.1.3



Scan Details

Policy: Basic Network Scan
 Status: Completed
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: May 4 at 8:35 PM
 End: May 4 at 9:30 PM
 Elapsed: an hour

Vulnerabilities

