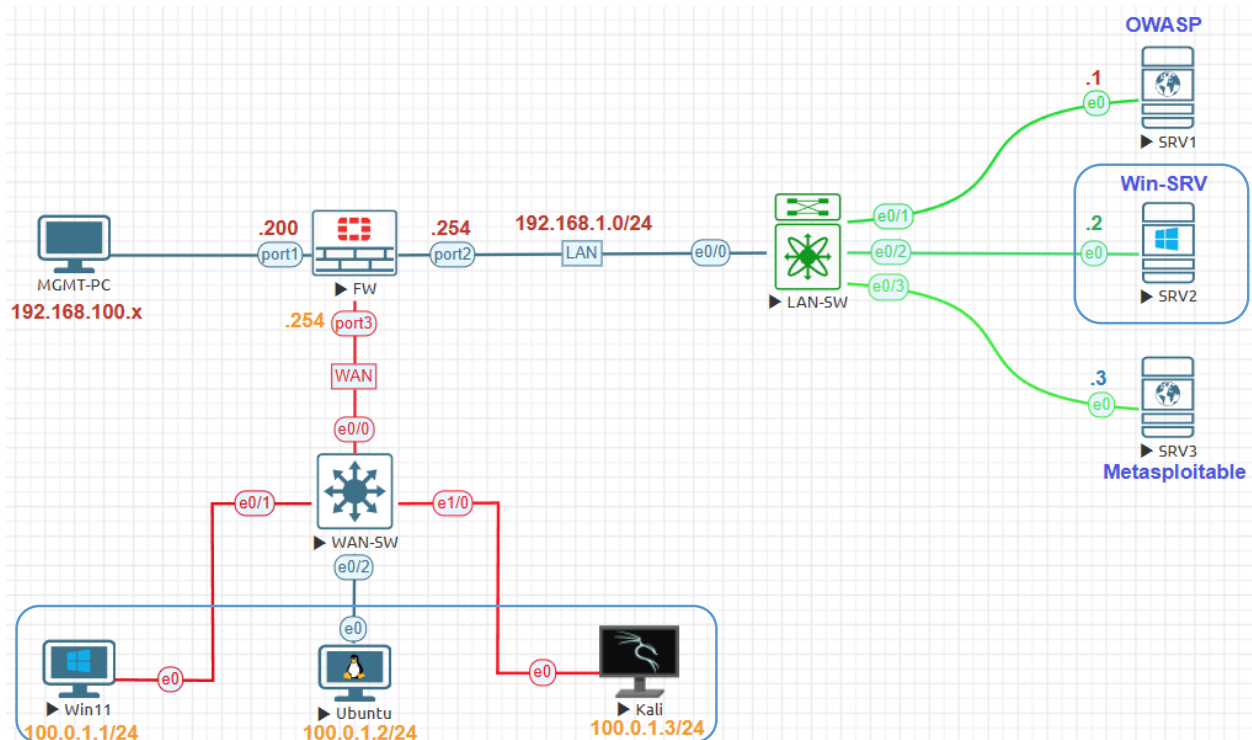


Basic Network Scan Lab:




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.

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: **Win-SRV19-Vul-Scan**. Targets: IP address of target **192.168.1.2** Windows Server 2019

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Win-SRV19-Vul-Scan

Description: Windows Server 2019 with IP address 192.168.1.2 Vulnerability scan

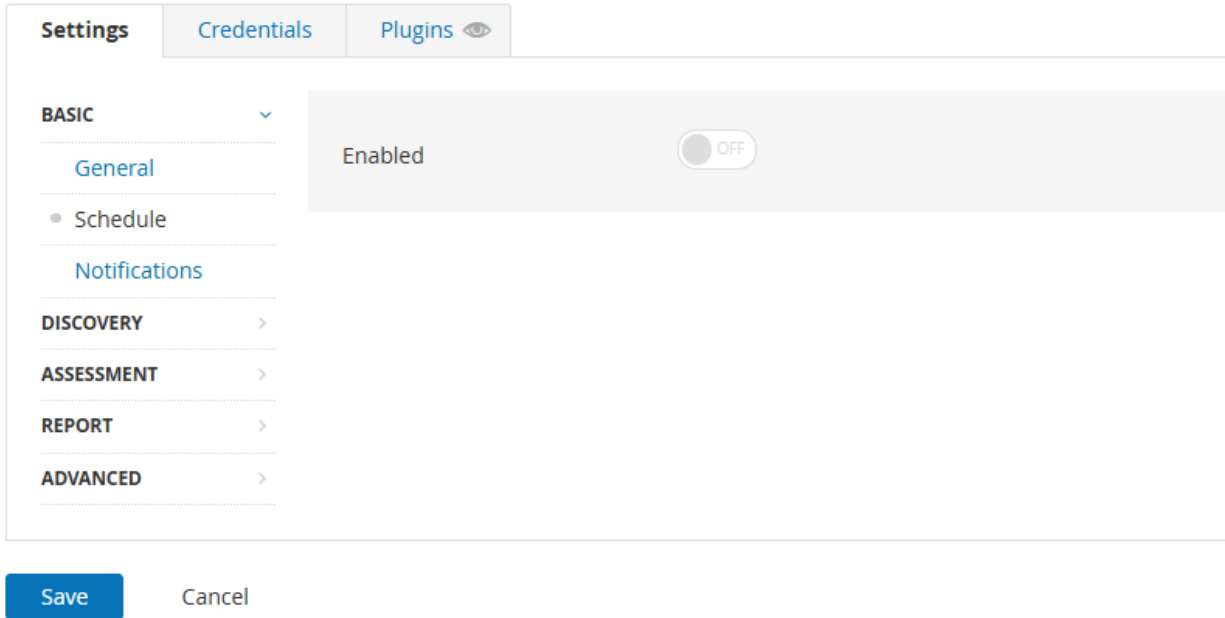
Folder: My Scans

Targets: 192.168.1.2

Upload Targets [Add File](#)

Settings>Basic>Schedule keep default disable.

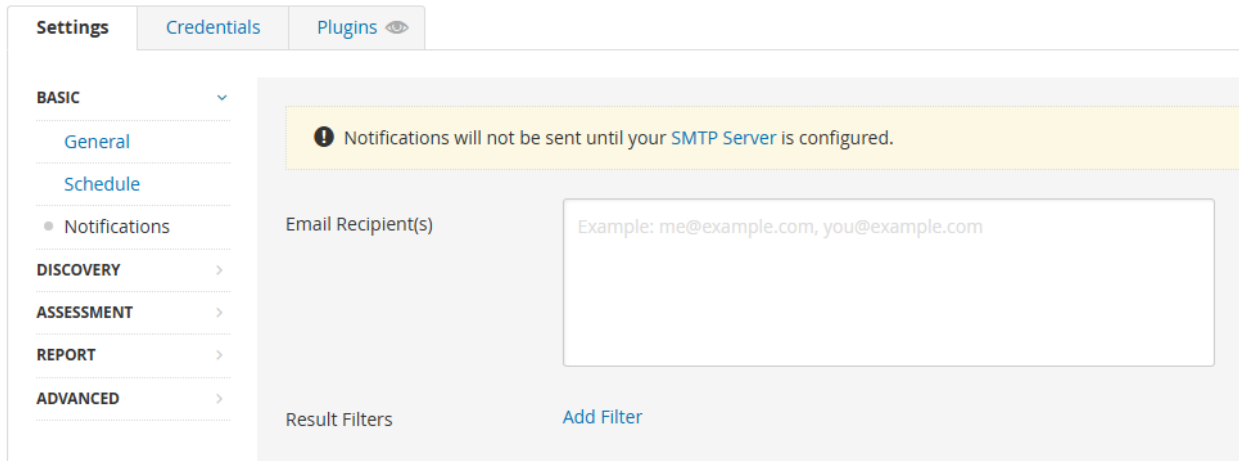
[← Back to Scan Report](#)



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 currently disabled, indicated by a greyed-out toggle switch labeled 'OFF'. 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 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 default no changes.

[← Back to Scan Report](#)

The screenshot shows the 'Settings' tab selected in the top navigation bar. On the left sidebar, the 'DISCOVERY' menu item is highlighted with a red box. The main content area shows the 'Scan Type' dropdown menu set to 'Port scan (all ports)', also highlighted with a red box. Below this, the configuration is organized into sections: 'General Settings' with options 'Always test the local Nessus host' and 'Use fast network discovery'; 'Port Scanner Settings' with options 'Scan all ports (1-65535)', 'Use netstat if credentials are provided', and 'Use SYN scanner if necessary'; and 'Ping hosts using:' with options 'TCP', 'ARP', and 'ICMP (2 retries)'.

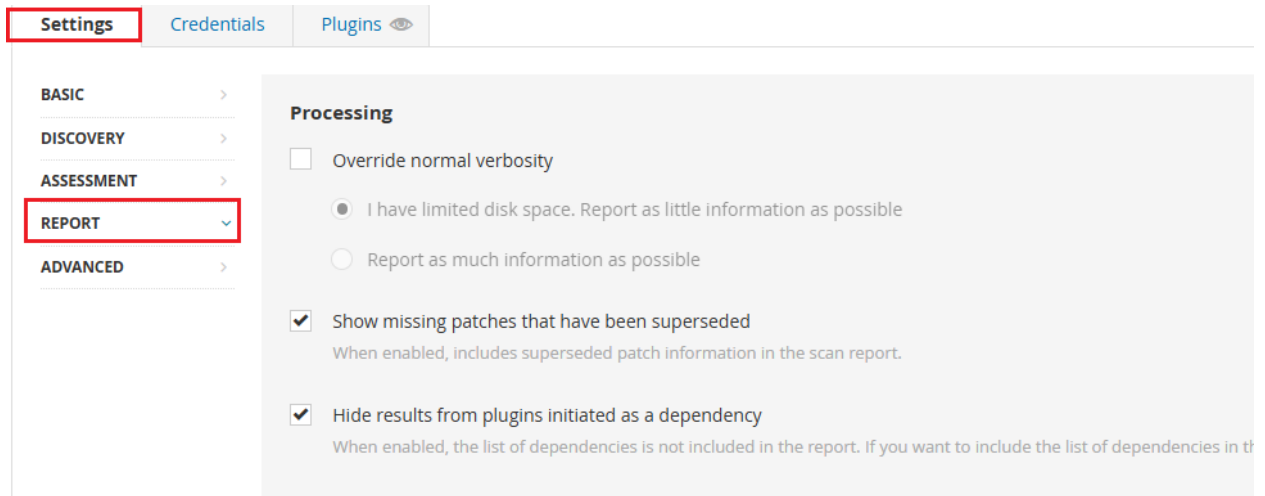
Settings>Assessment keep default no changes.

Win-SRV19-Vul-Scan / Configuration

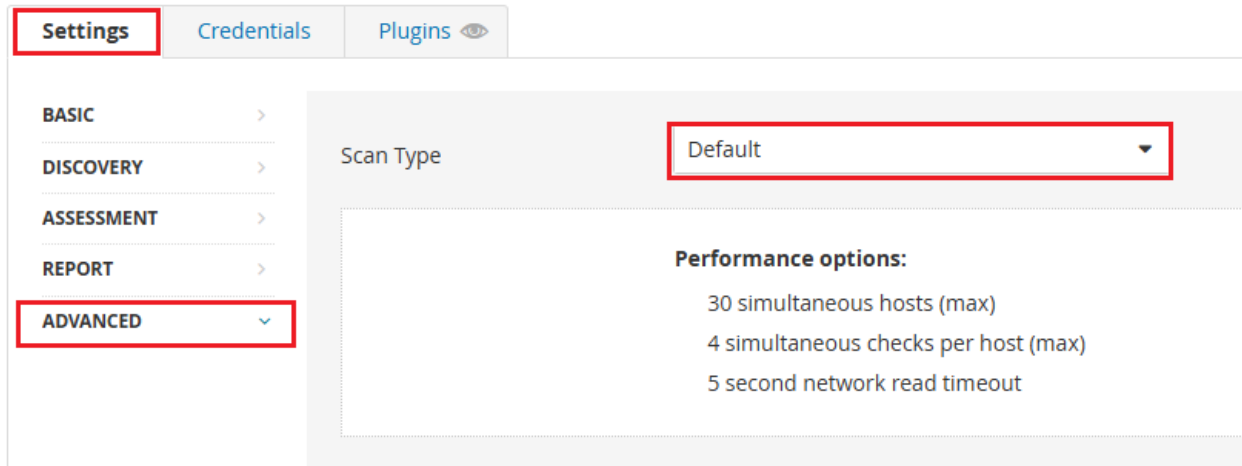
[← Back to Scan Report](#)

The screenshot shows the 'Settings' tab selected in the top navigation bar. On the left sidebar, the 'ASSESSMENT' menu item 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 configuration is organized into sections: 'General Settings' with options 'Avoid potential false alarms' and 'Disable CGI scanning'; and 'Web Applications:' with the option 'Disable web application scanning'.

Settings>Reports keep default no changes.



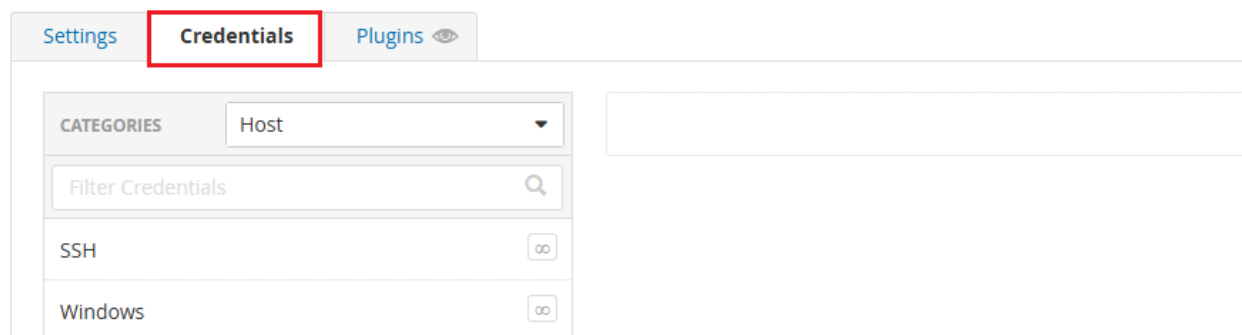
Settings>Advanced keep default no changes.



Under Credentials Tab. Default do not use any credentials.

Win-SRV19-Vul-Scan / Configuration

[← Back to Scan Report](#)



Plugins Tab leave the default we cannot change anything.

PLUGIN FAMILY	TOTAL	PLUGIN NAME
Alibaba Cloud Linux Local Security Checks	804	No plugin family sele
Alma Linux Local Security Checks	9	
Amazon Linux Local Security Checks	55	
Artificial Intelligence	3	
Azure Linux Local Security Checks	3	
Backdoors	1	
CentOS Local Security Checks	1	
CGI abuses	745	
CGI abuses : XSS	121	
CISCO	15	
Databases	11	
Debian Local Security Checks	11	
Denial of Service	2	
DNS	1	

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

Win-SRV19-Vul-Scan / Configuration

[← Back to Scan Report](#)

Settings	Credentials	Plugins
BASIC > DISCOVERY > ASSESSMENT > REPORT > ADVANCED v		<p>Scan Type: Default</p> <p>Performance options:</p> <ul style="list-style-type: none">30 simultaneous hosts (max)4 simultaneous checks per host (max)5 second network read timeout
Save	Cancel	

After complete the scan, Hosts Tab show below

Win-SRV19-Vul-Scan

[Back to My Scans](#)

Hosts 1 Vulnerabilities 31 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.1.2	4

Vulnerabilities Tab show total 31 and details.

Win-SRV19-Vul-Scan

[Back to My Scans](#)

Hosts 1 Vulnerabilities 31 History 1

Filter Search Vulnerabilities 31 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family
MIXED	9 SSL (Multiple Issues)	General
MIXED	3 Microsoft Windows (Multiple Issues)	Windows
MIXED	4 TLS (Multiple Issues)	Service detection
LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General
INFO	3 HTTP (Multiple Issues)	Web Servers
INFO	6 SMB (Multiple Issues)	Windows
INFO	2 TLS (Multiple Issues)	General
INFO	Nessus SYN scanner	Port scanners

Scan Details under Vulnerabilities Tab.

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: May 3 at 4:41 PM
End: May 3 at 5:15 PM
Elapsed: 34 minutes

Vulnerabilities

