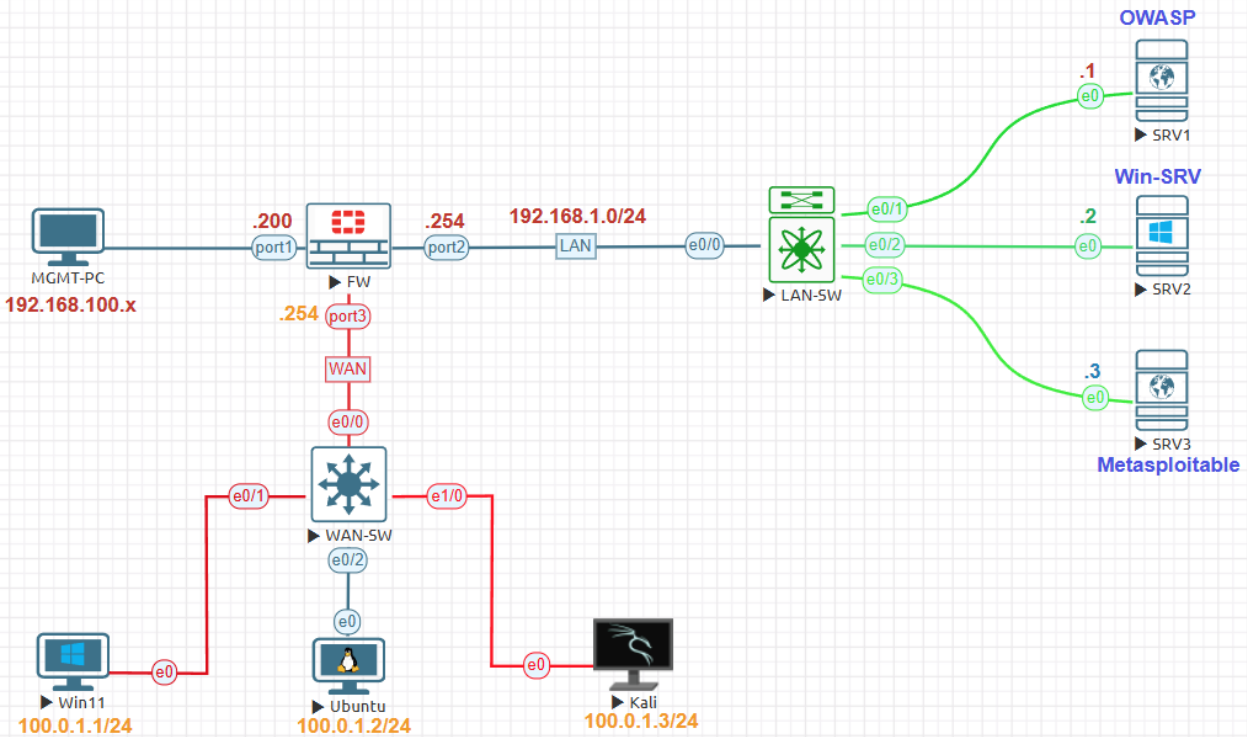
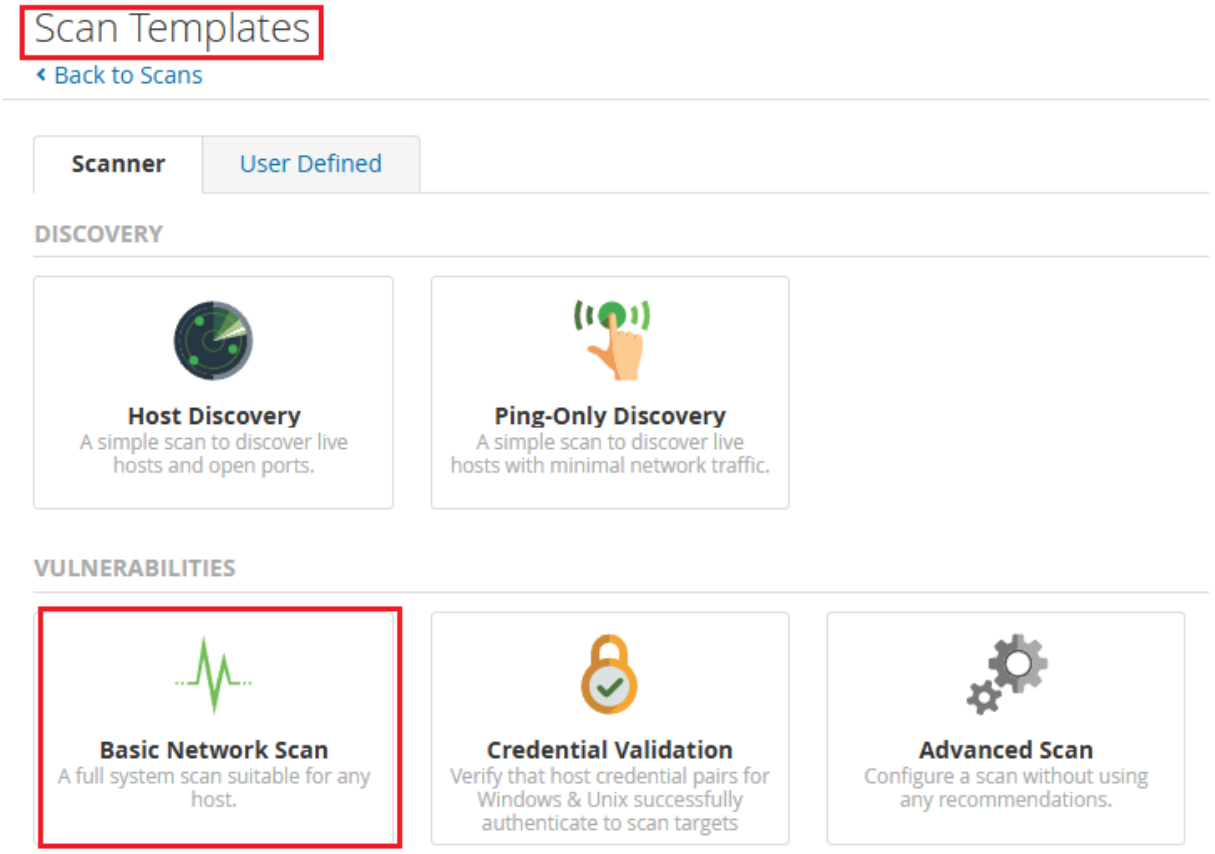
Unauthenticated Scan Lab:



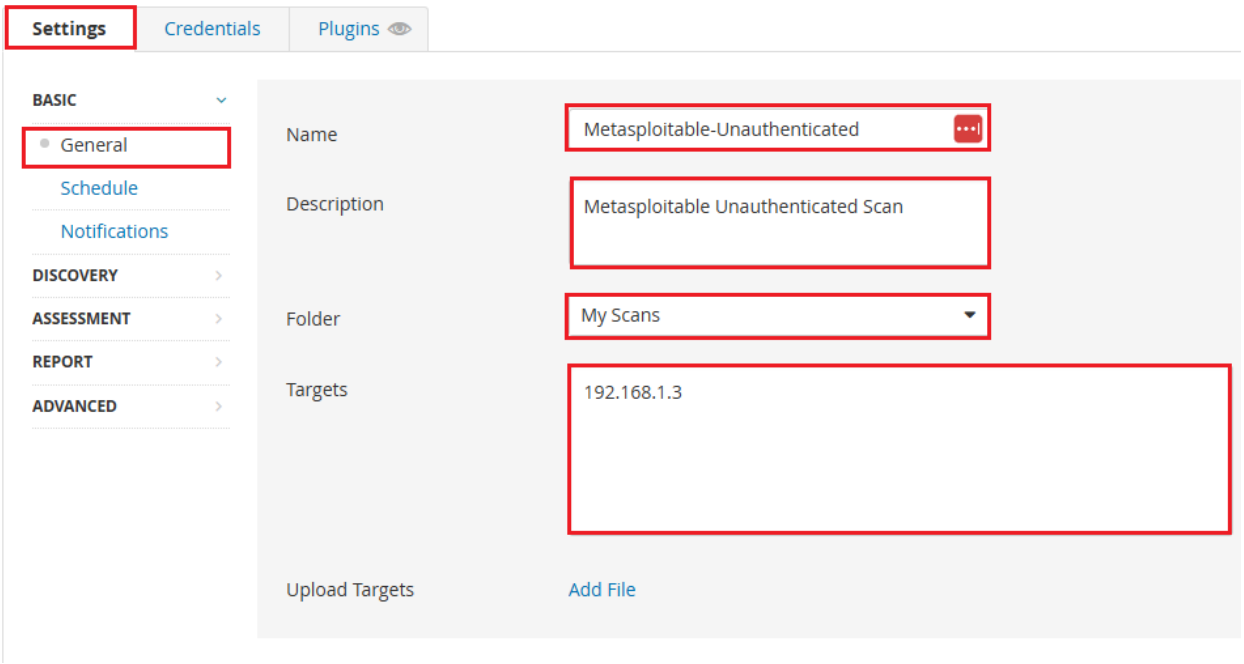
Management Subnet	192.168.100.0/24
FortiGate Management IP	192.168.100.200
Internal Servers Subnet	192.168.1.0/24
FortiGate Firewall External	100.0.1.0/24
FortiGate Firewall Internal IP	192.168.1.254
FortiGate Firewall External IP	100.0.1.254
SRV1 IP Address	192.168.1.1
SRV2 IP Address	192.168.1.2
SRV3 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

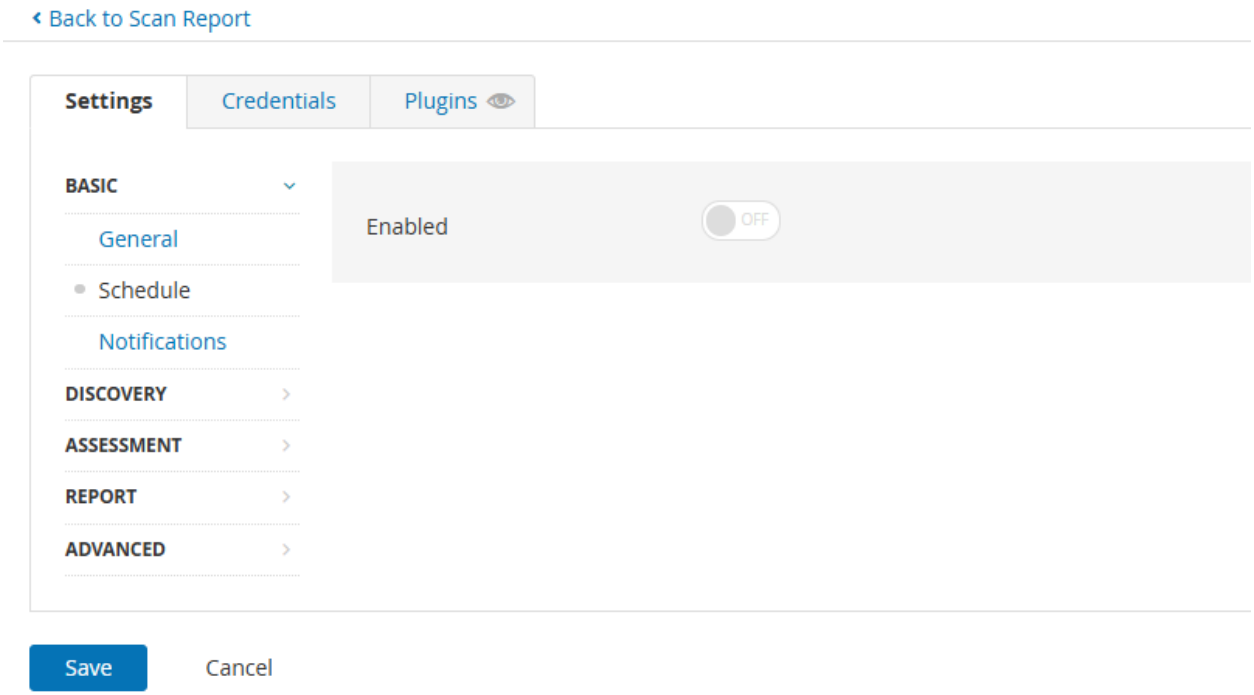
Go to Scans > New Scan. Choose Basic Network Scan to open.



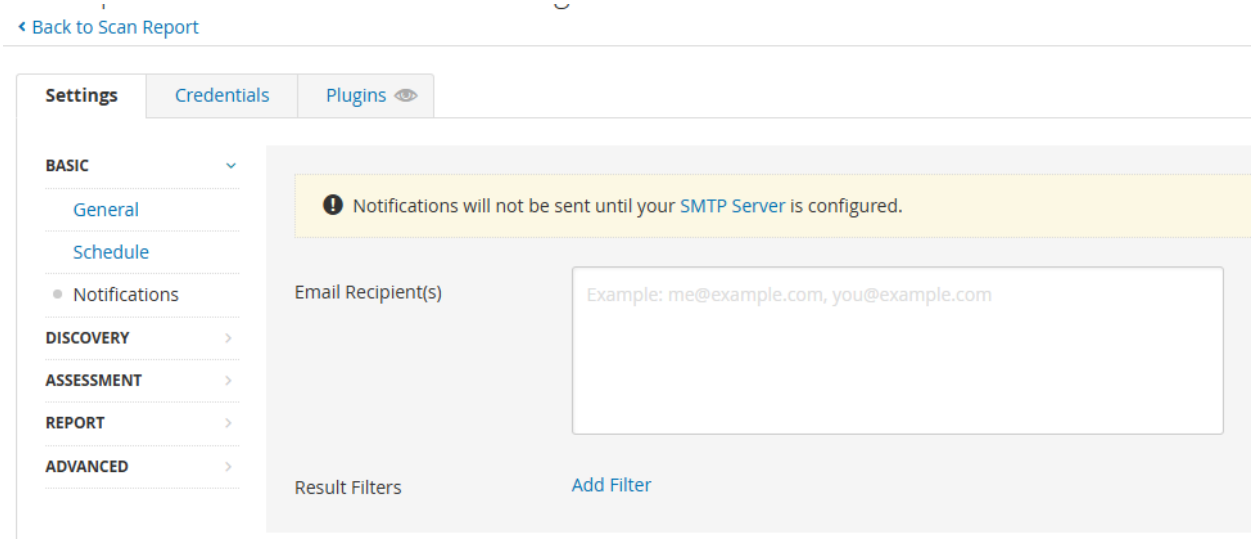
Name: Metasploitable-Unauthenticated. Targets: IP address of target Metasploitable 192.168.1.3.



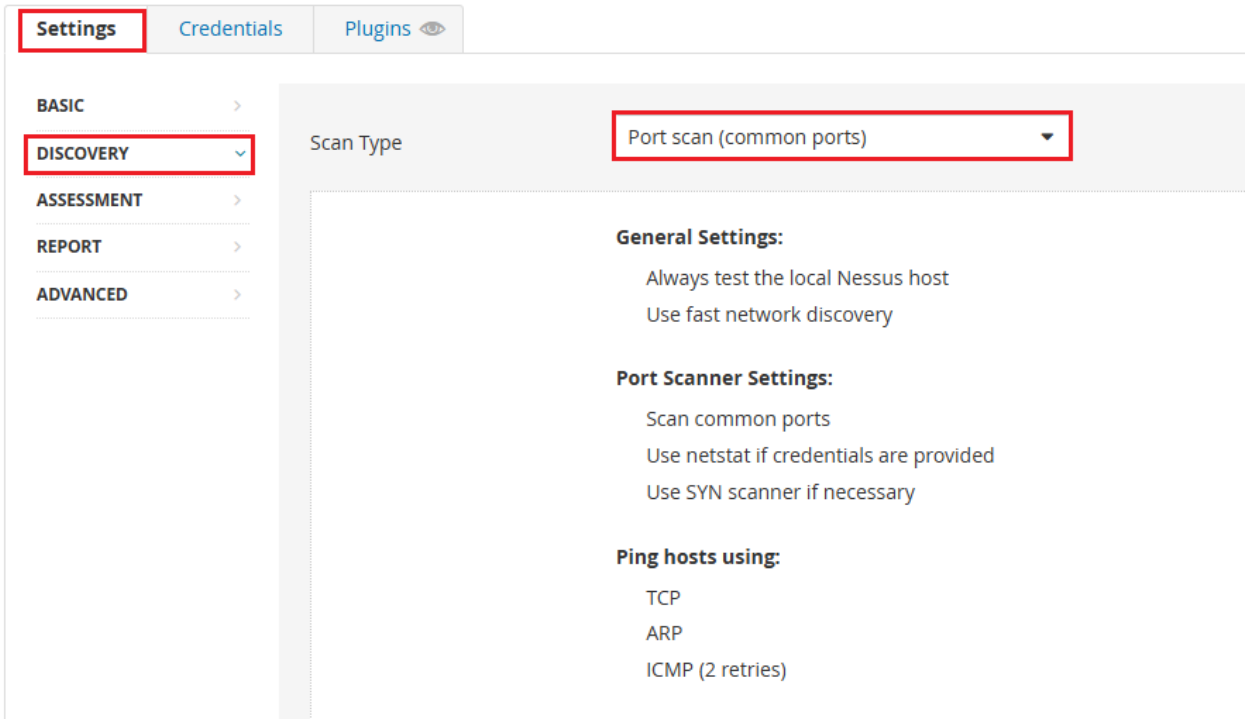
Settings>Basic>Schedule keep default disable.



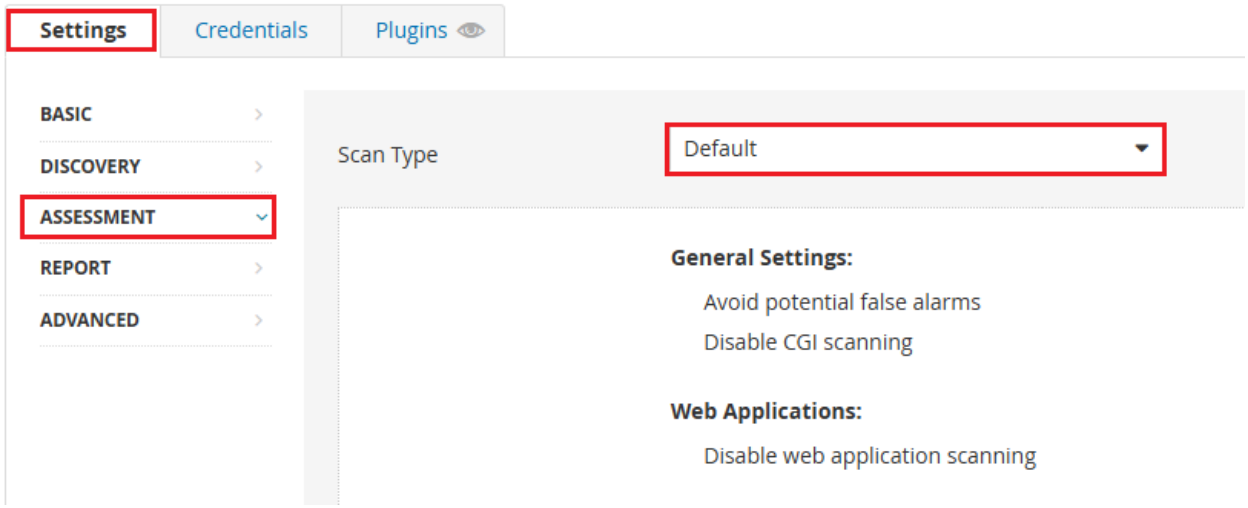
Settings>Basic>Notification keep default disable.



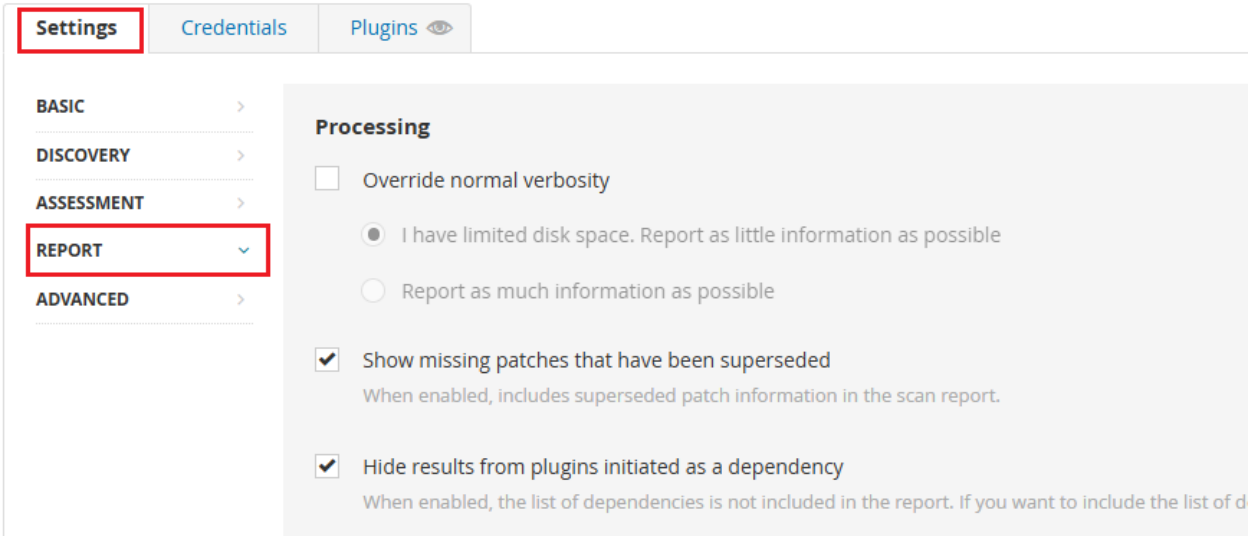
Settings>Discovery keep default Port scan (common ports).



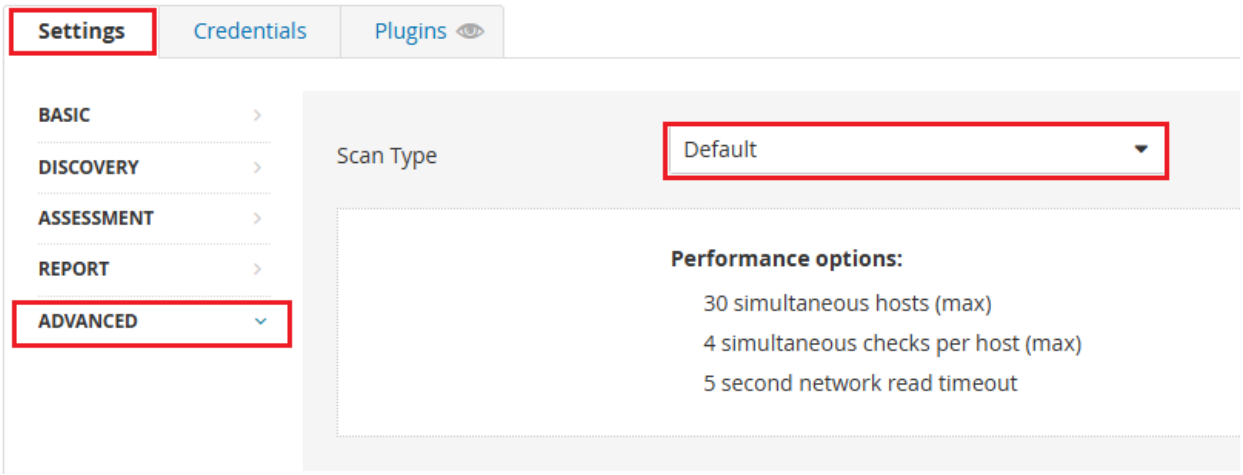
Settings>Assessment keep default



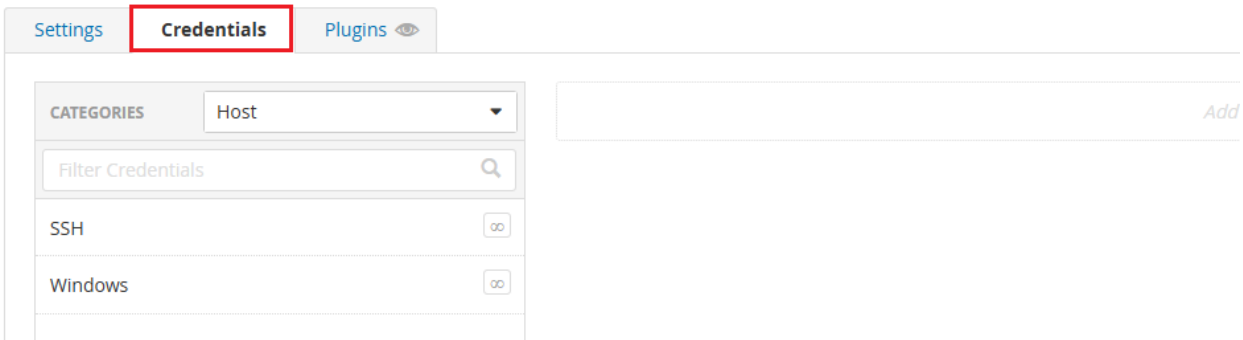
Settings>Reports keep default no changes.



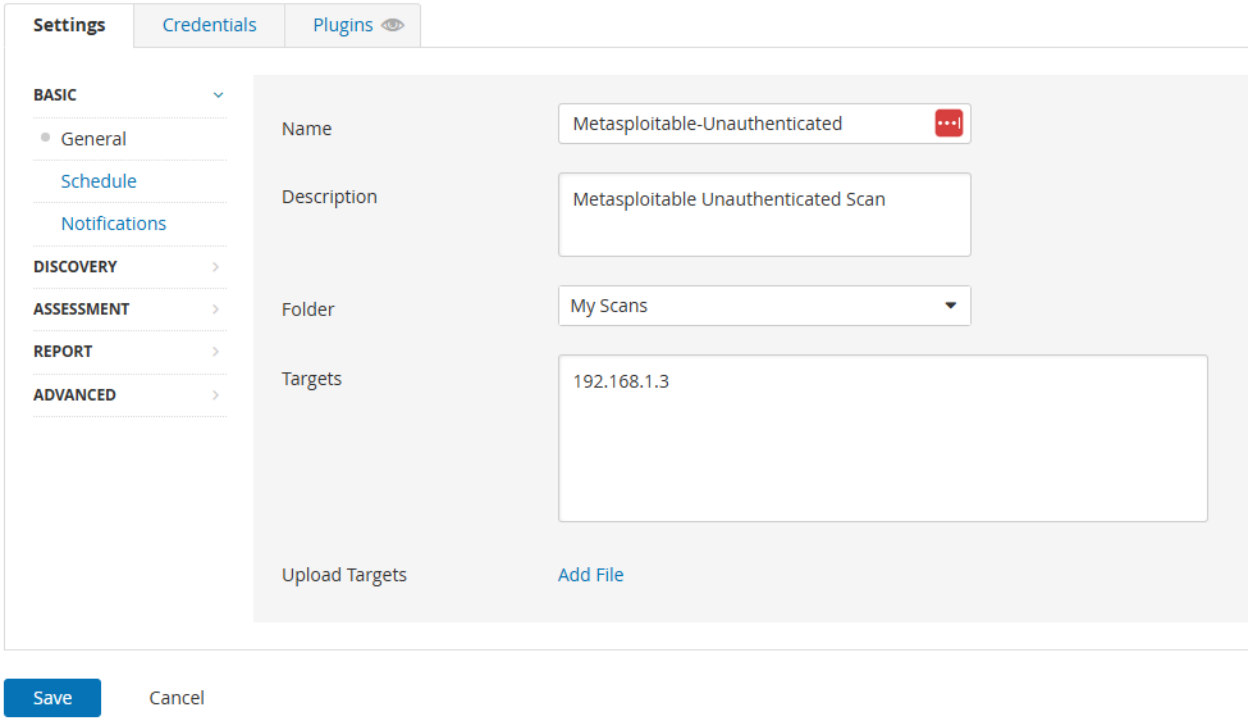
Settings>Advanced keep default no changes.



Under Credentials Tab. Leave all fields empty (unauthenticated)

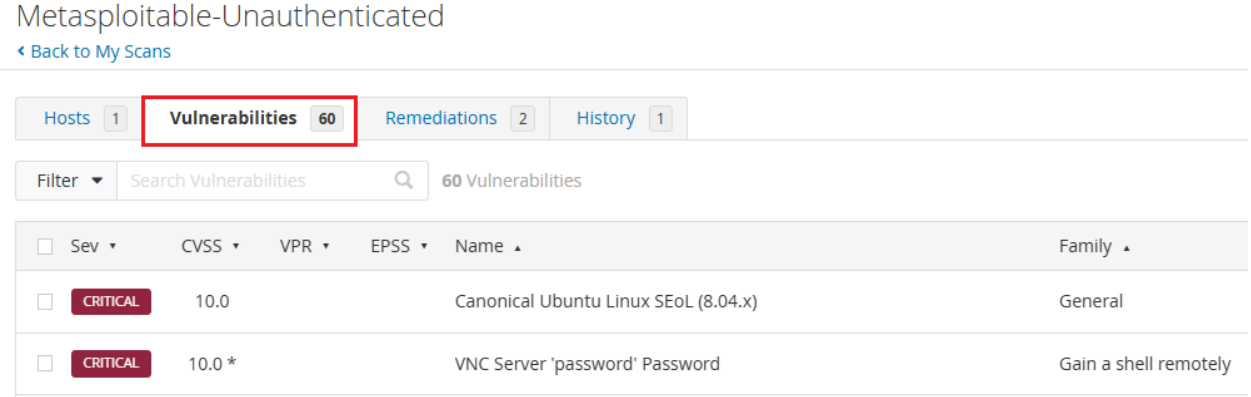


Click Save then Launch. Wait for the scan to complete.



After complete the scan, 9 Critical, 5 High, 22 Medium, 8 Low and 122 info.

Total 60 Vulnerabilities includes 9 Critical, 5 High, 22 Medium, 8 Low and 122 info.



Metasploitable-Unauthenticated

‹ Back to My Scans

Hosts 1 | Vulnerabilities 60 | **Remediations 2** | History 1

Search Actions | 2 Actions

Action
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

192.168.1.3

9	5	22	8	122
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	May 4 at 8:34 PM
End:	May 4 at 8:59 PM
Elapsed:	25 minutes

Vulnerabilities