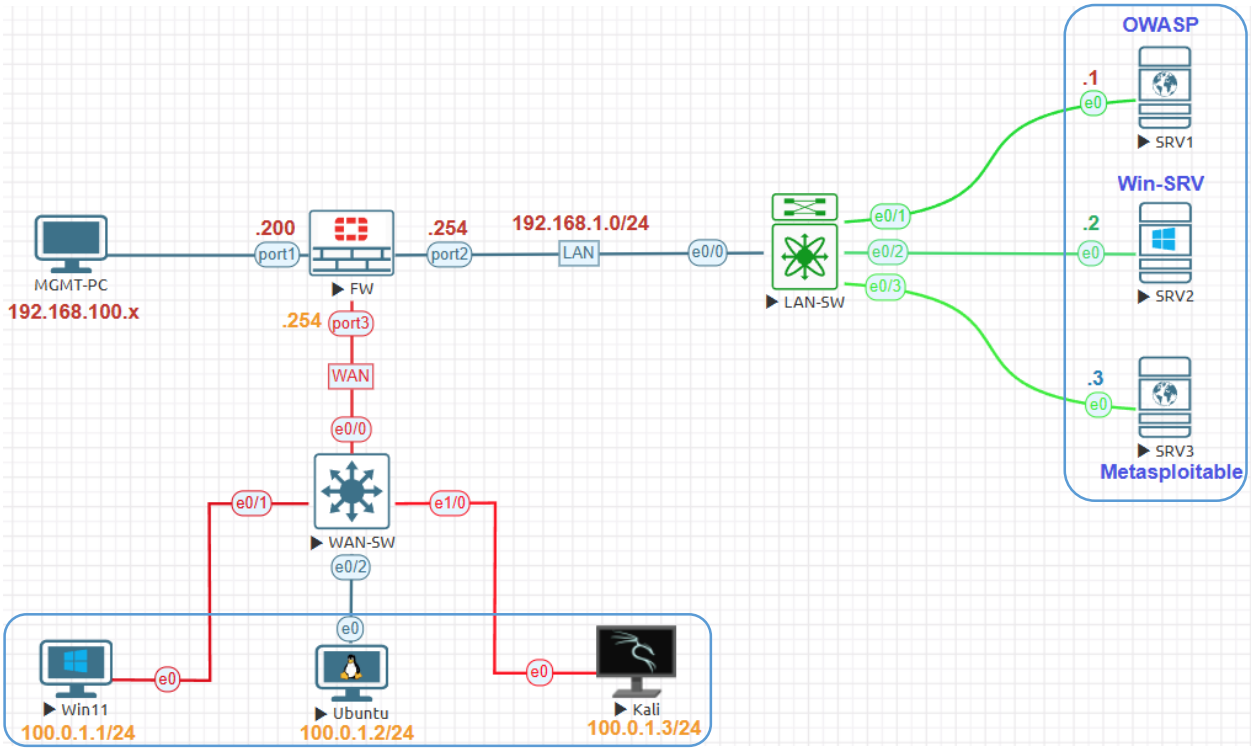
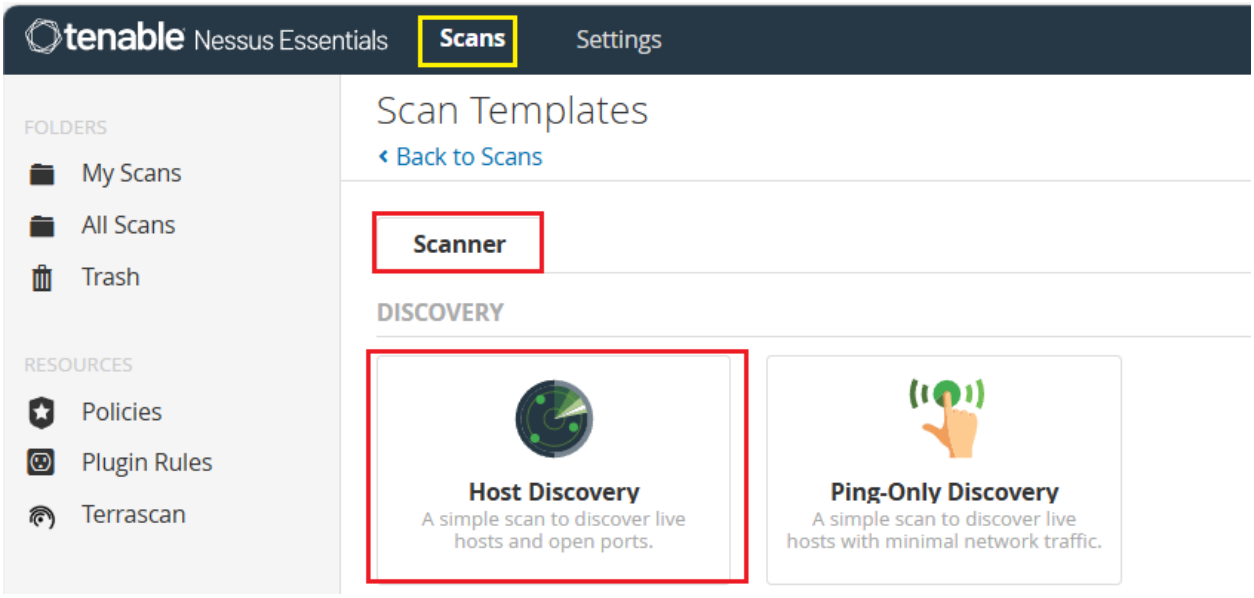
Host Discovery Lab:



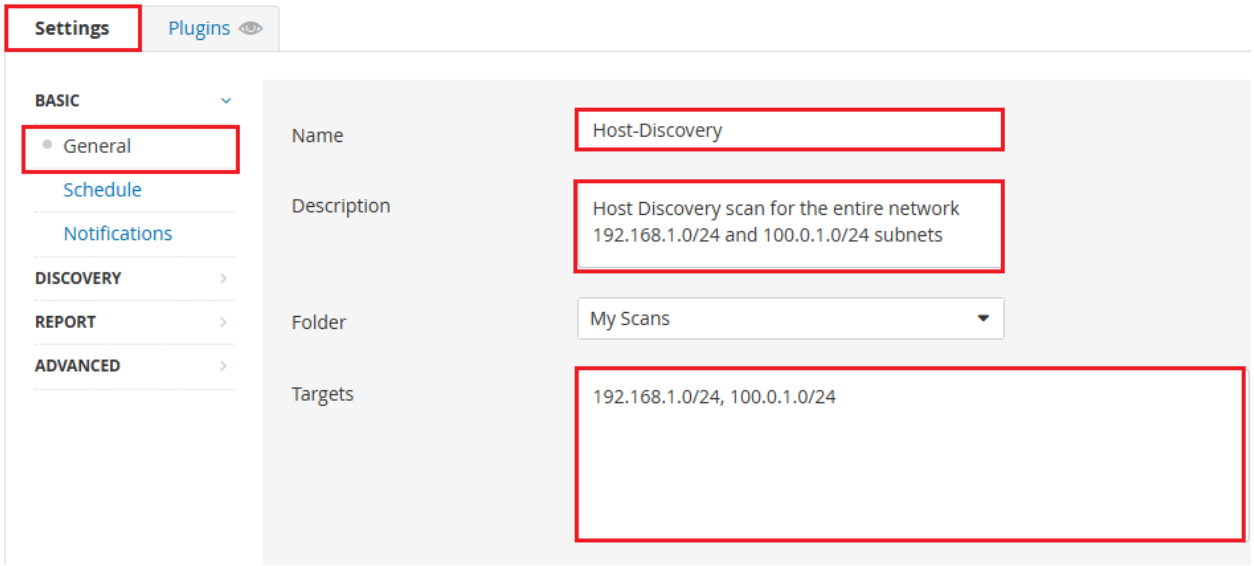
Management Subnet	192.168.100.0/24
FortiGate Management IP	192.168.100.200
Internal Servers Subnet	192.168.1.0/24
FortiGate Firewall External	100.0.1.0/24
FortiGate Firewall Internal IP	192.168.1.254
FortiGate Firewall External IP	100.0.1.254
SRV1 IP Address	192.168.1.1
SRV2 IP Address	192.168.1.2
SRV3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

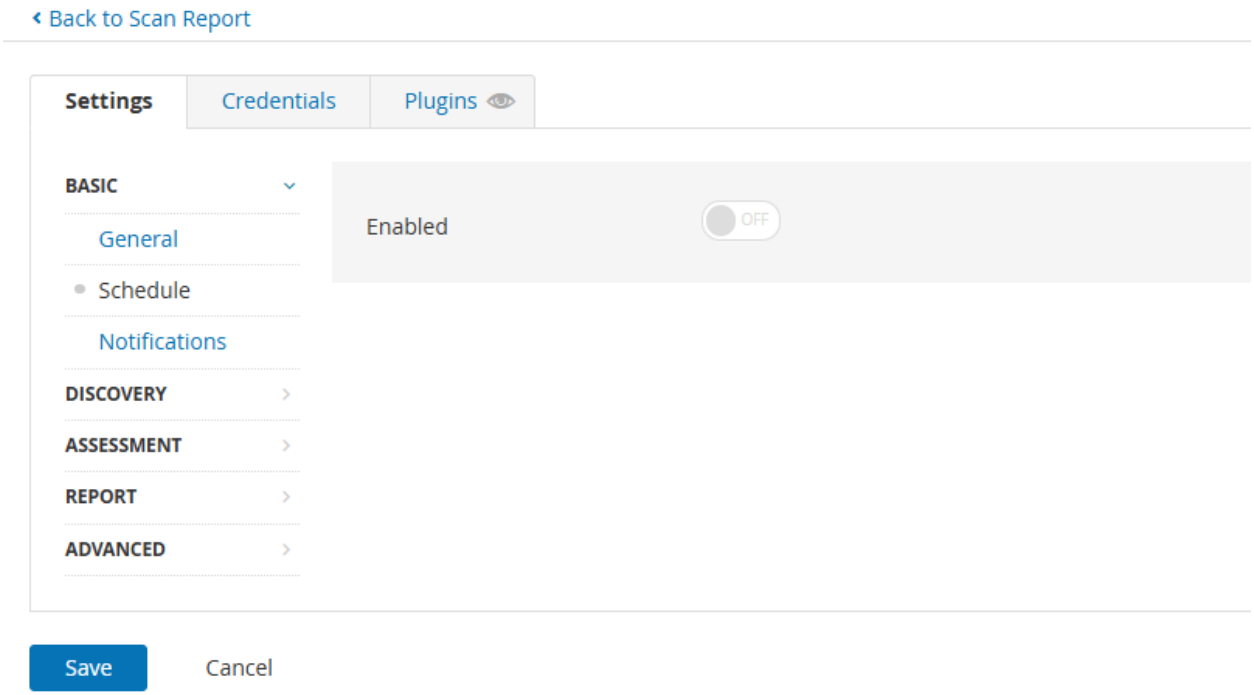
Go to Scans > New Scan. Choose Host Discovery to open.



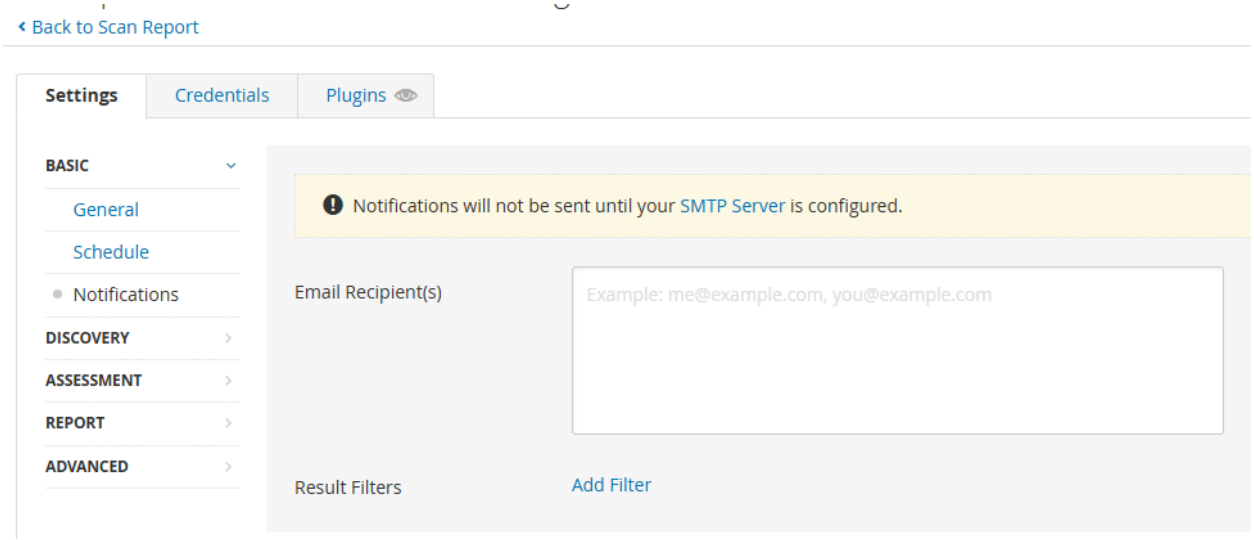
Name: Host-Discovery. Targets: IP address of target subnets 192.168.1.0/24 and 100.0.1.0/24.



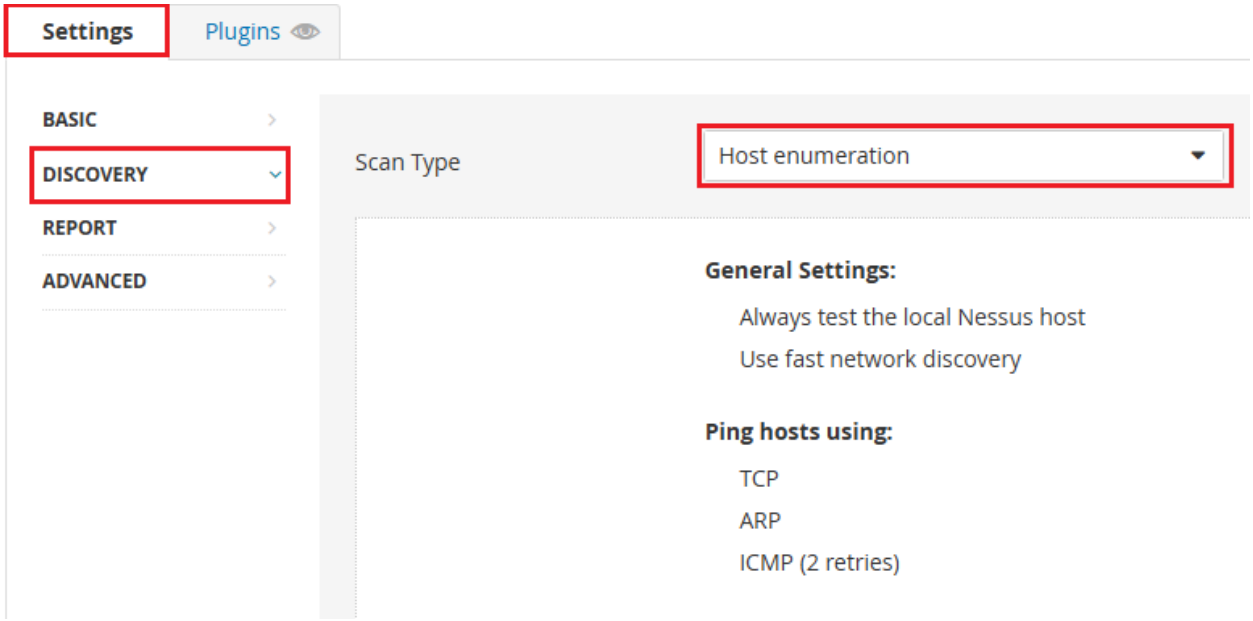
Settings>Basic>Schedule keep default disable.



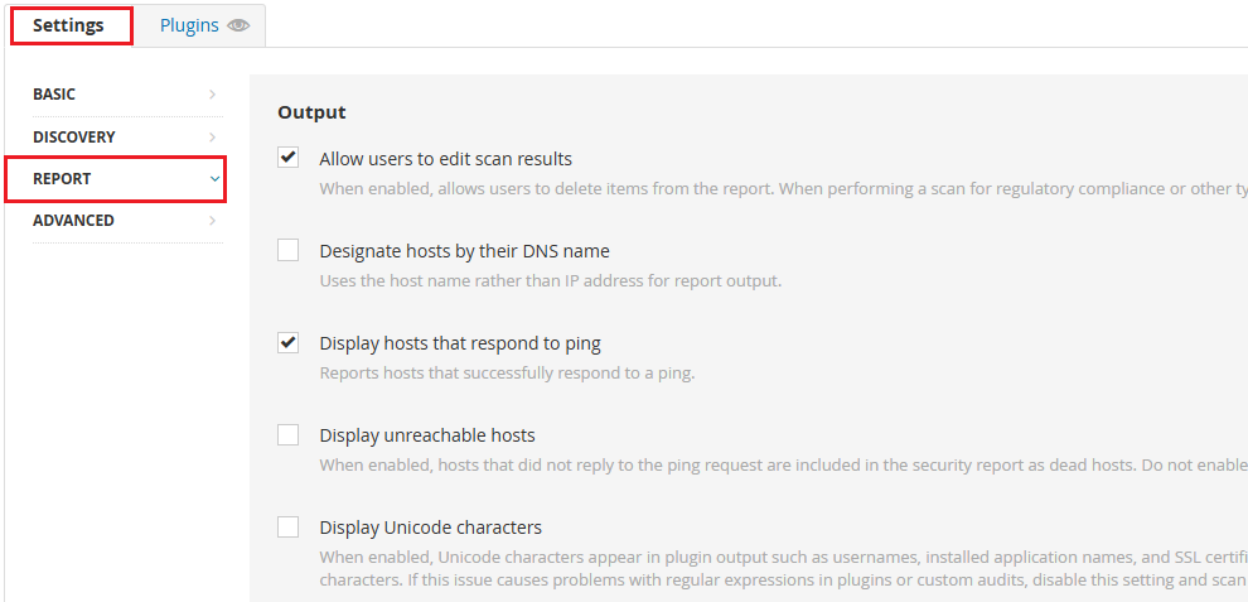
Settings>Basic>Notification keep default disable.



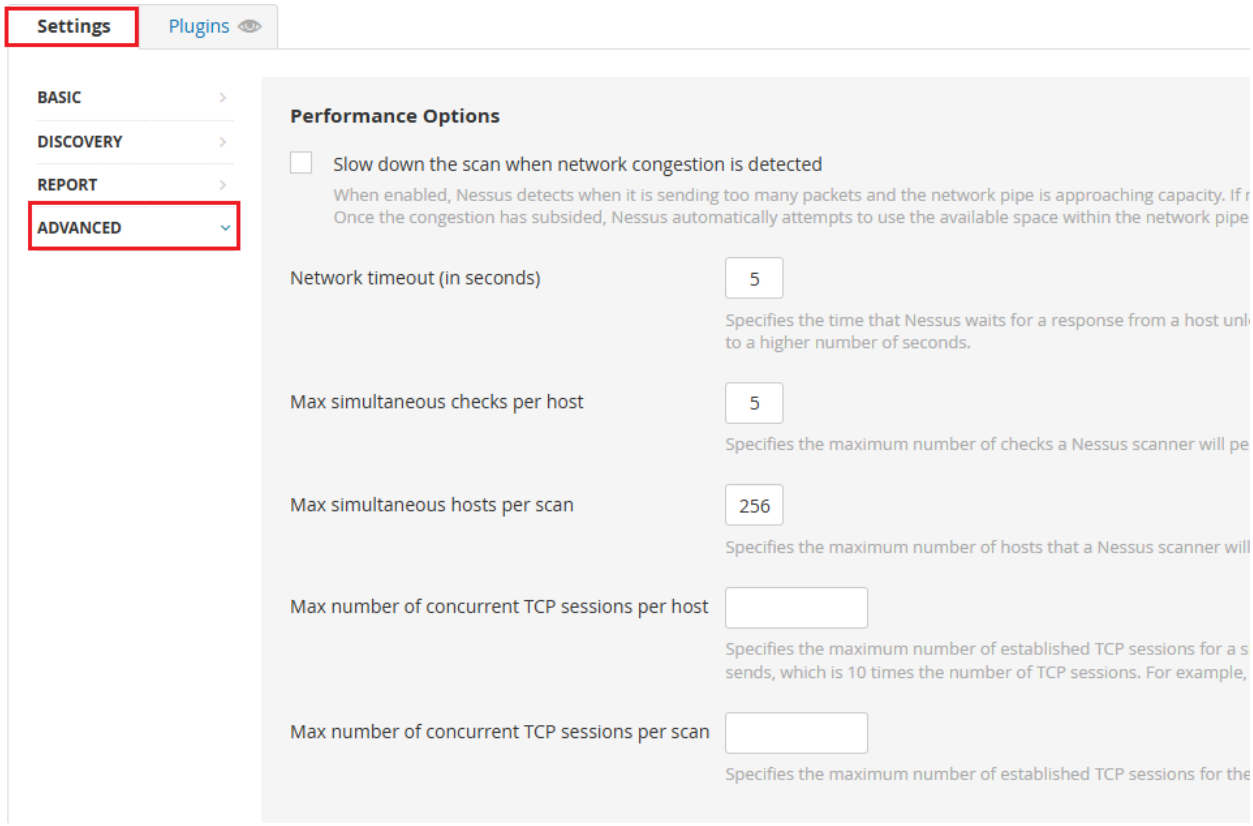
Settings>Discovery keep scan type Host enumeration



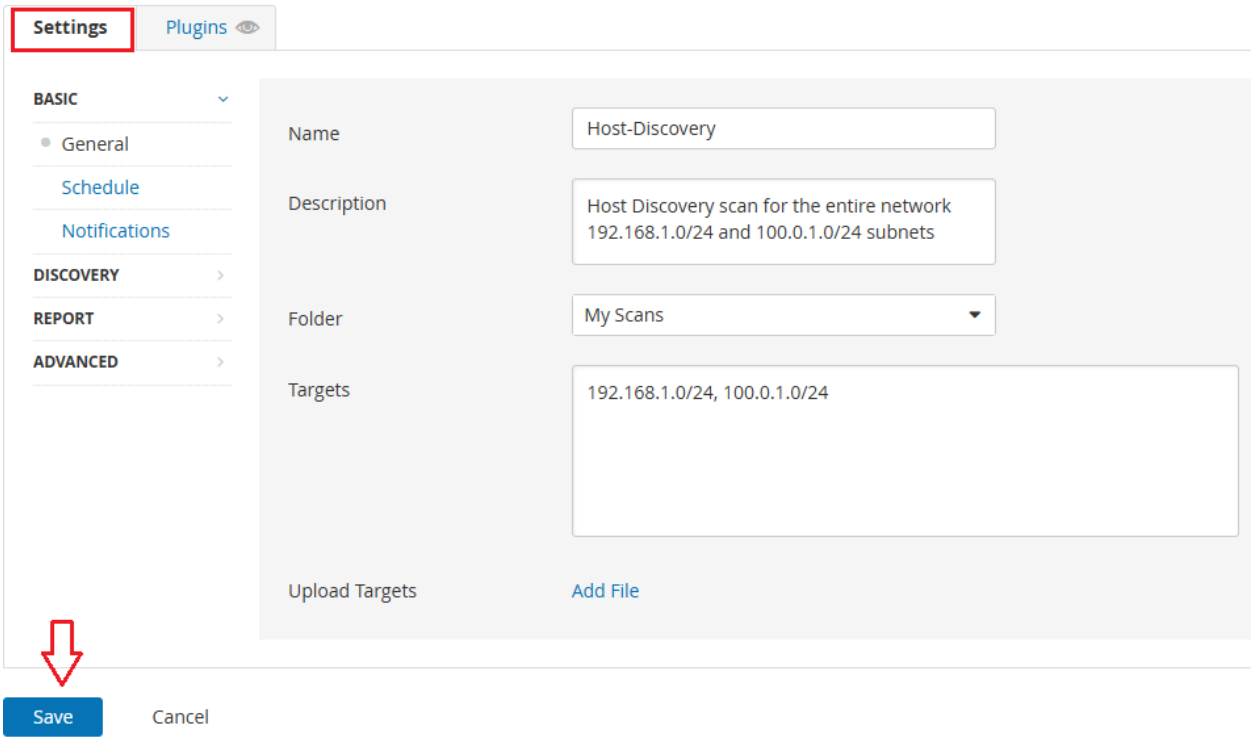
Settings>Reports keep default no changes.



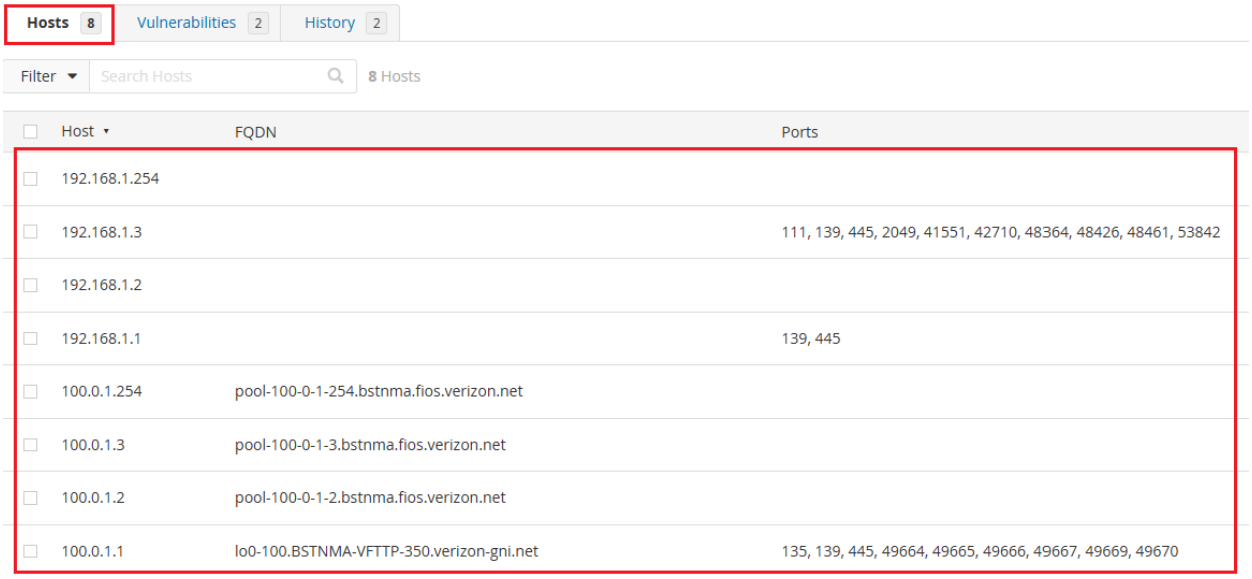
Settings>Advanced keep default no changes.



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



After complete the scan Hosts Tab 8 host discovered FortiGate Firewall, Metasploitable 2, Windows Server 2019, OWASP, Kali Linux, Ubuntu and Windows 11 and open ports.



Vulnerabilities Tab provide information about the scan.