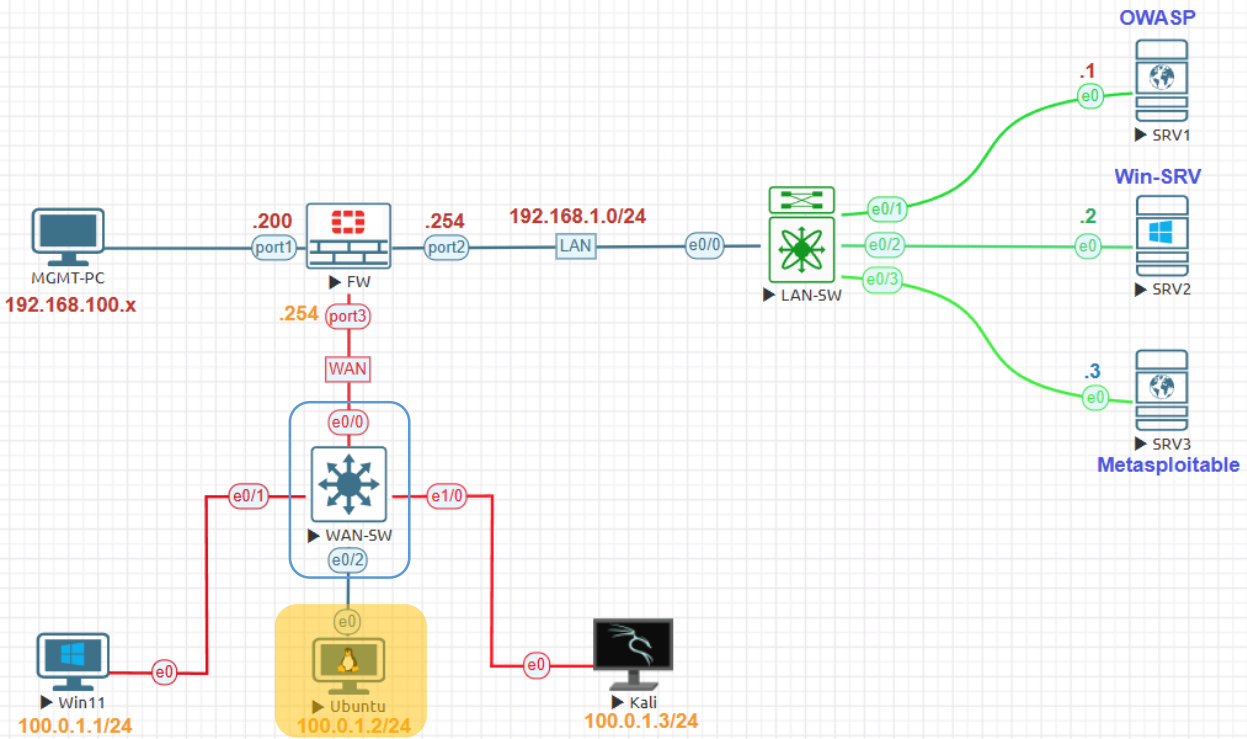
Cisco Switch Vulnerability Scan Lab:



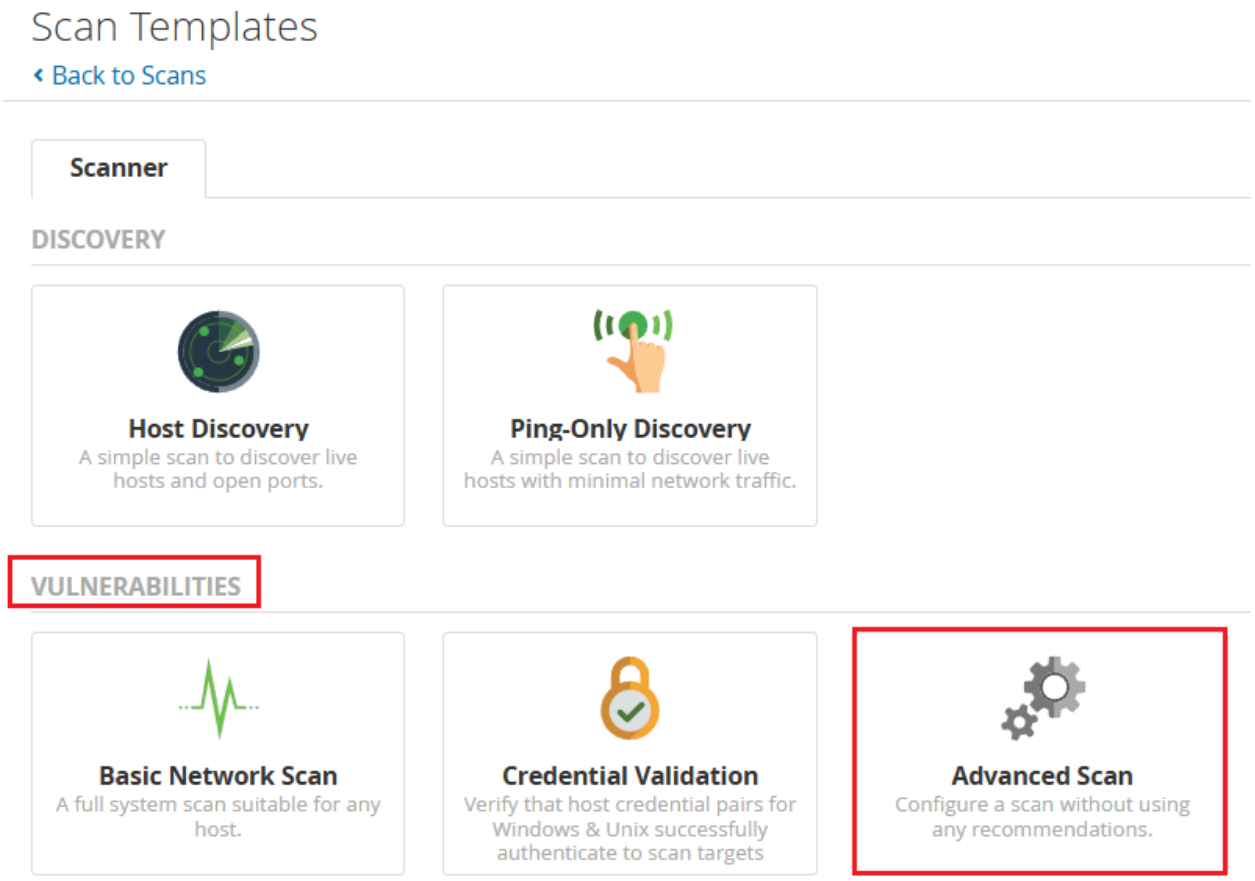
Management Subnet	192.168.100.0/24
FortiGate Management IP	192.168.100.200
Internal Servers Subnet	192.168.1.0/24
FortiGate Firewall External	100.0.1.0/24
FortiGate Firewall Internal IP	192.168.1.254
FortiGate Firewall External IP	100.0.1.254
SRV1 IP Address	192.168.1.1
SRV2 IP Address	192.168.1.2
SRV3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

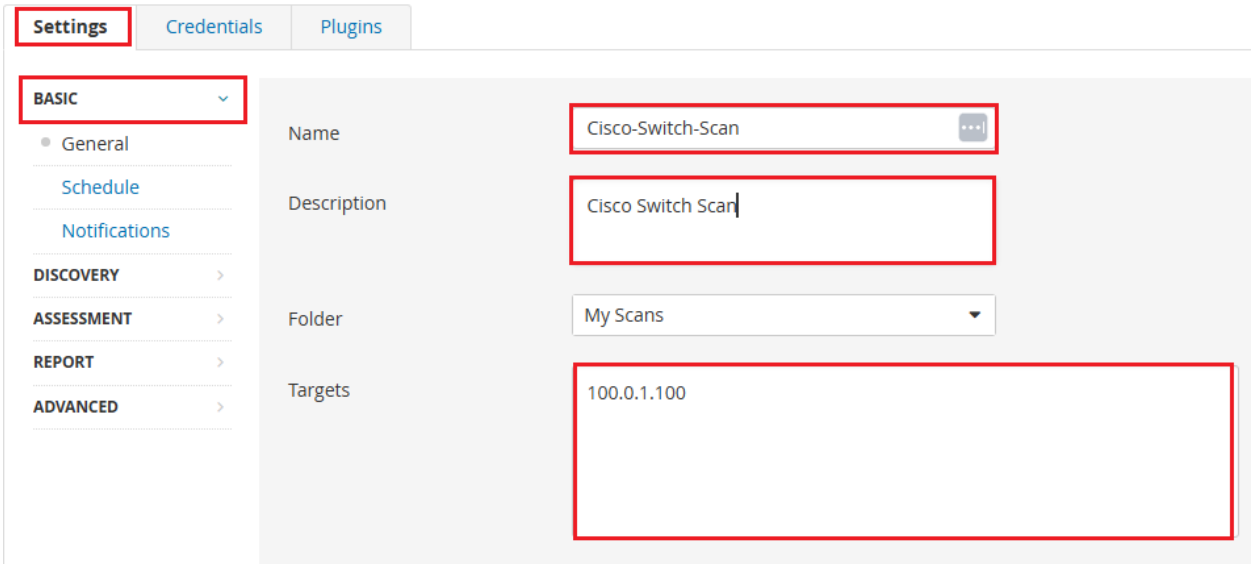
Before Start the scan Cisco Switch Configuation:

Assign IP Address
Switch(config)#interface vlan 1 Switch(config-if)#ip address 100.0.1.100 255.255.255.0 Switch(config-if)#no shutdown
Enable HTTP
Switch(config)#ip http server
Enable Telnet
Switch(config)#username admin privilege 15 password cisco Switch(config)#line vty 0 4 Switch(config-line)#transport input telnet Switch(config-line)#login local
Enable SNMP v1/v2
Switch(config)#snmp-server community public RO Switch(config)#snmp-server community private RW
Enable Mode Password
Switch(config)#enable password cisco
Configure Consol
Switch(config)#line console 0 Switch(config-line)#password cisco Switch(config-line)#login
Enable FTP or TFTP
Switch(config)#ip ftp username ftpuser Switch(config)#ip ftp password ftppass Switch(config)#ip tftp source-interface vlan 1
Expose Unused Services
Switch(config)#service tcp-small-servers Switch(config)#service udp-small-servers

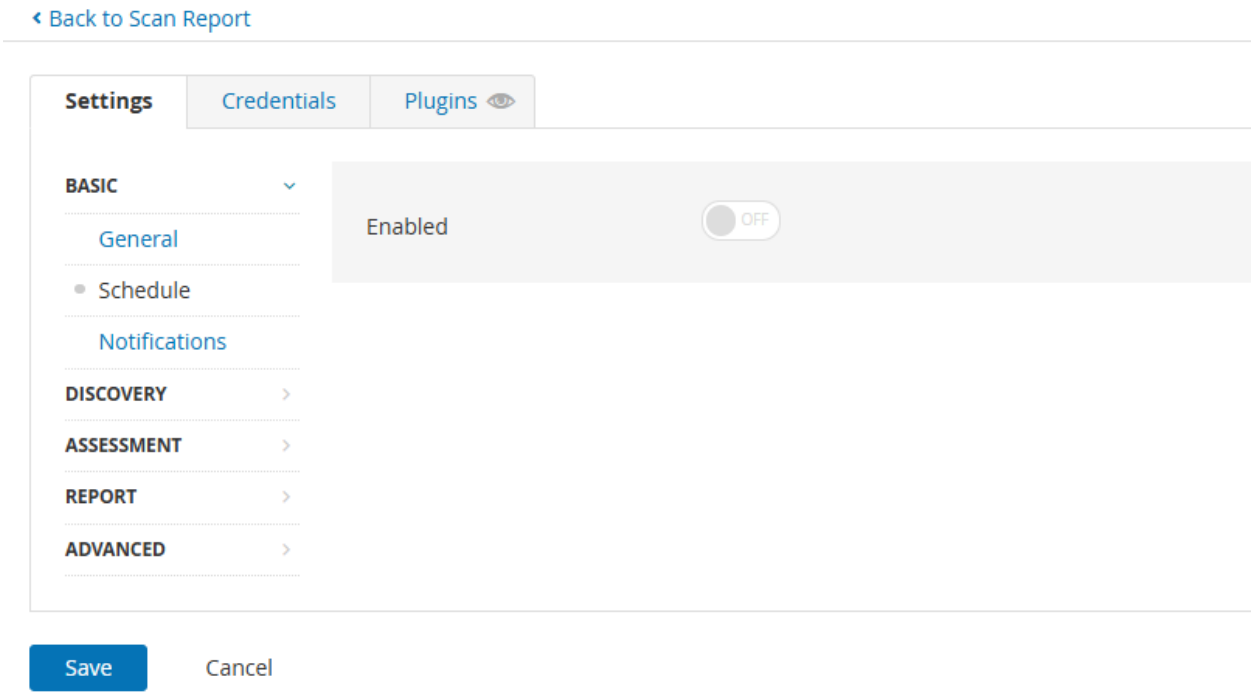
Go to Scans > New Scan. Choose Advanced Scan to open.



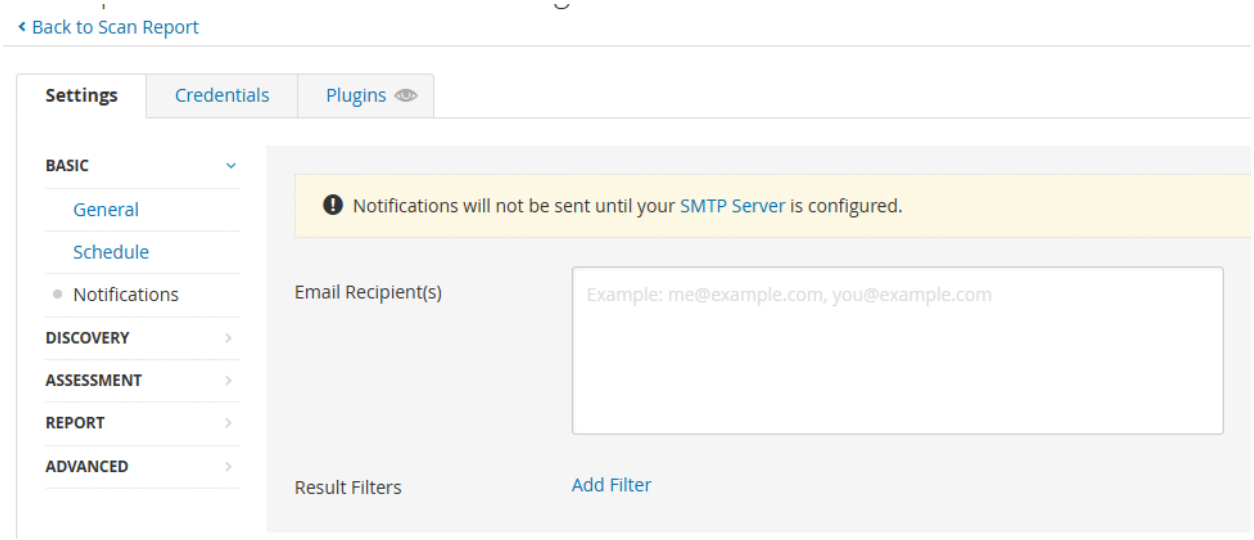
Name: Cisco-Switch-Scan. Targets: IP address of target 100.0.1.100 the IP Address of VLAN Interface of Cisco Switch.



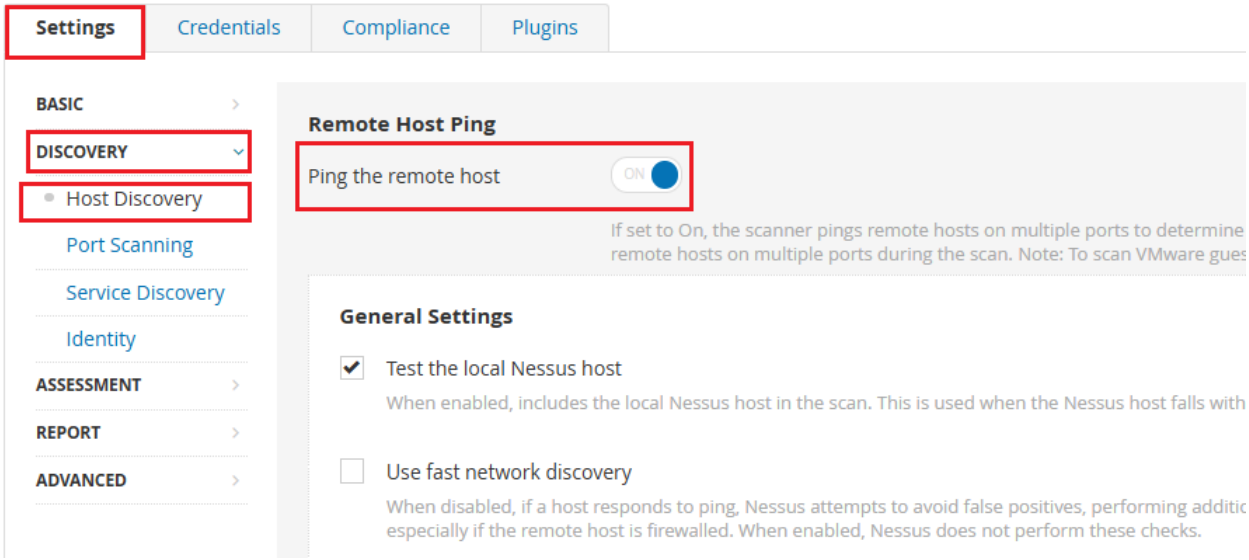
Settings>Basic>Schedule keep default disable.



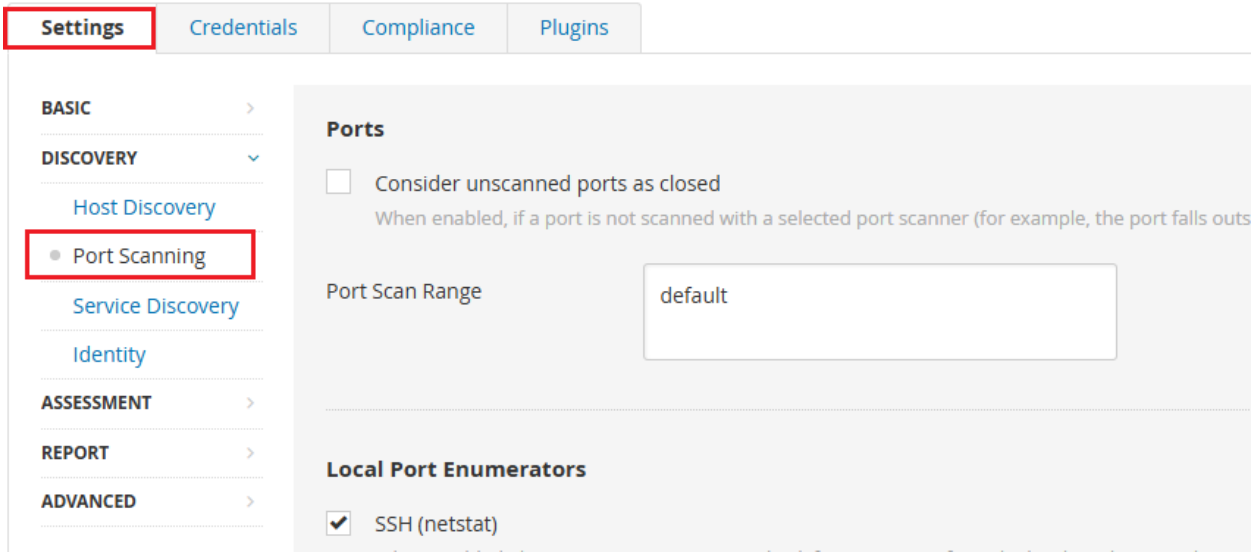
Settings>Basic>Notification keep default disable.



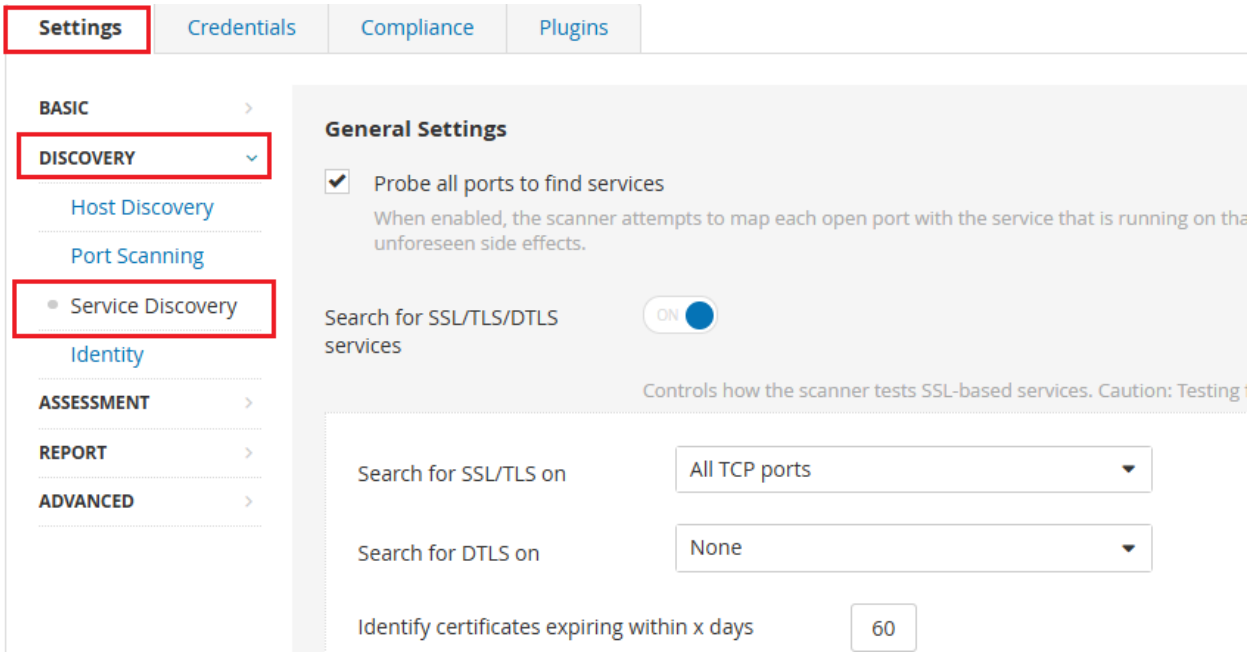
Settings>Discovery>Host Discovery keep default enable.



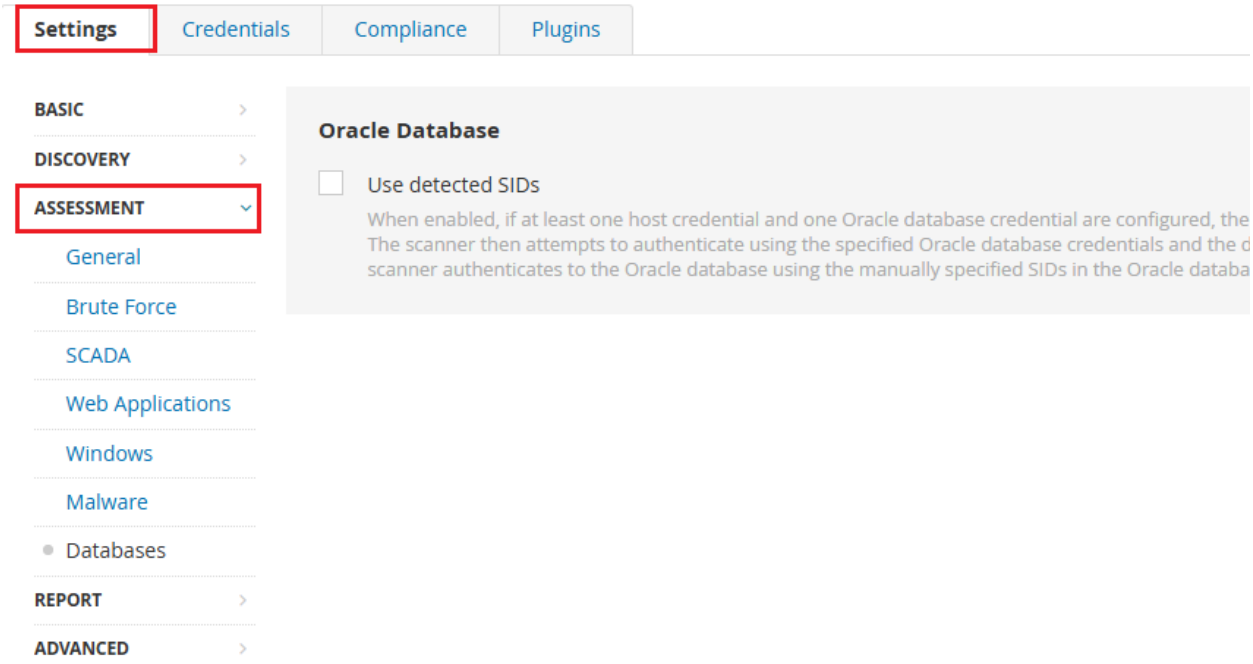
Settings>Discovery>Port Scanning keep default.



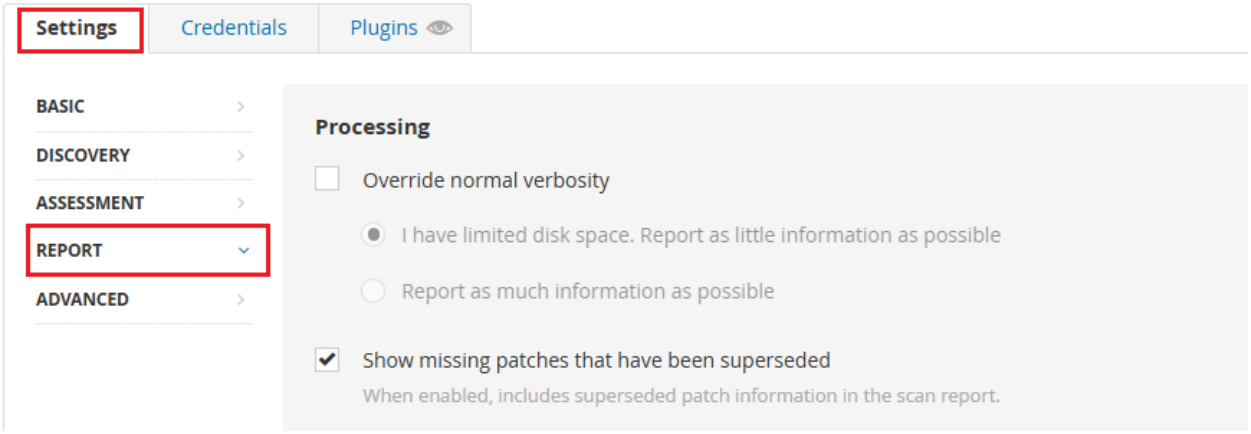
Settings>Discovery>Service Discovery keep default.



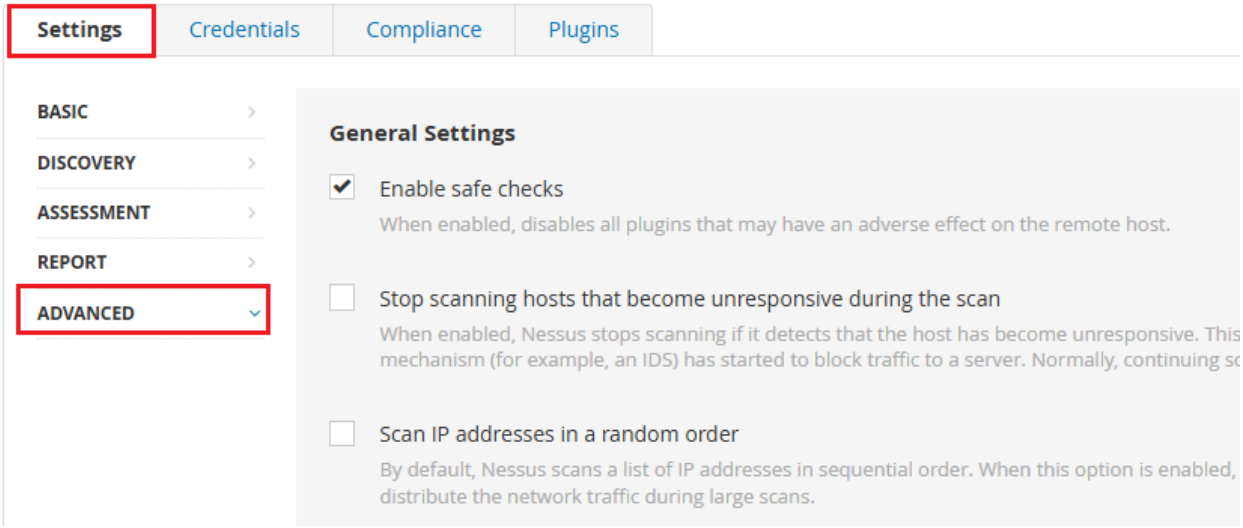
Settings>Assessment keep default.



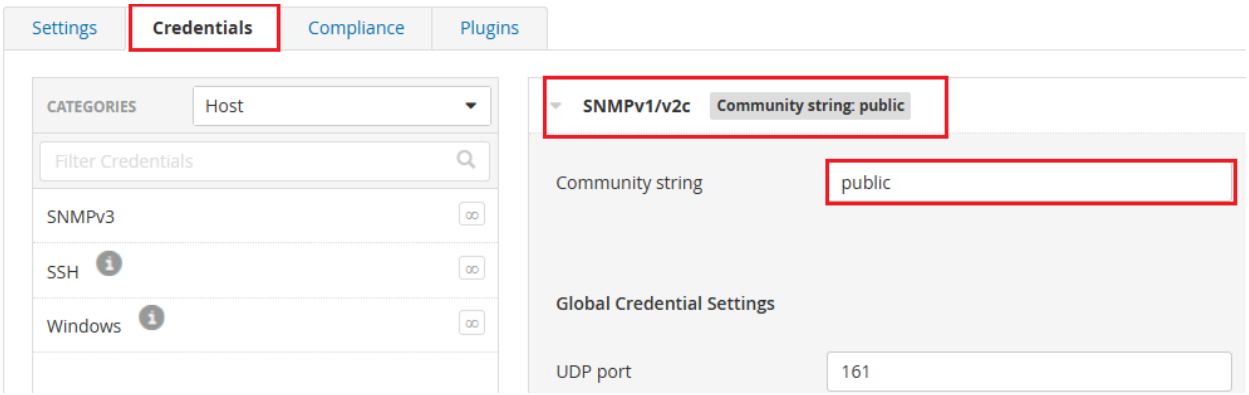
Settings>Reports keep default no changes.



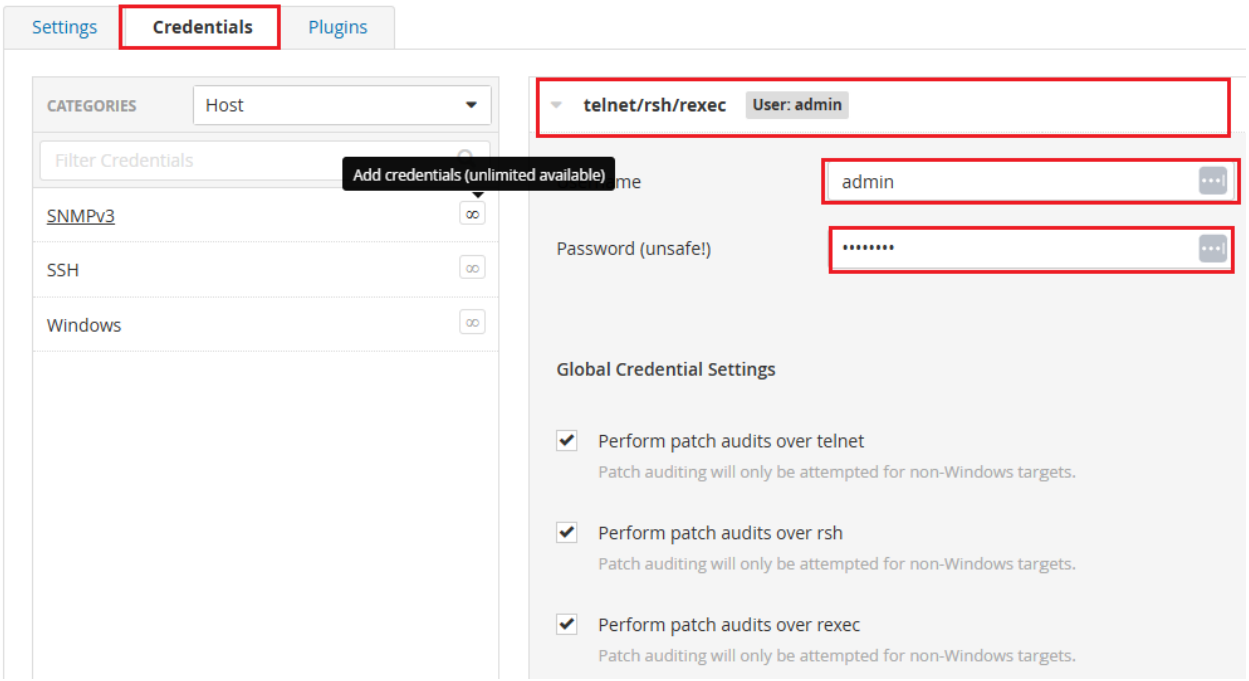
Settings>Advanced keep default no changes.



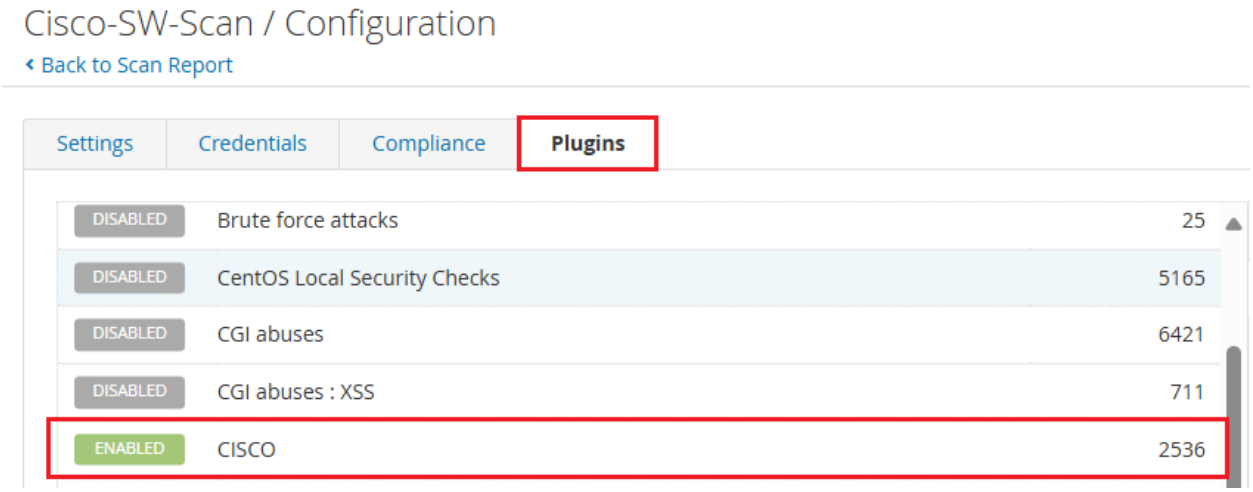
Under Credentials Tab. Choose SSH and SNMPv1/v2c authentication methods. In SNMP enter Community string: public

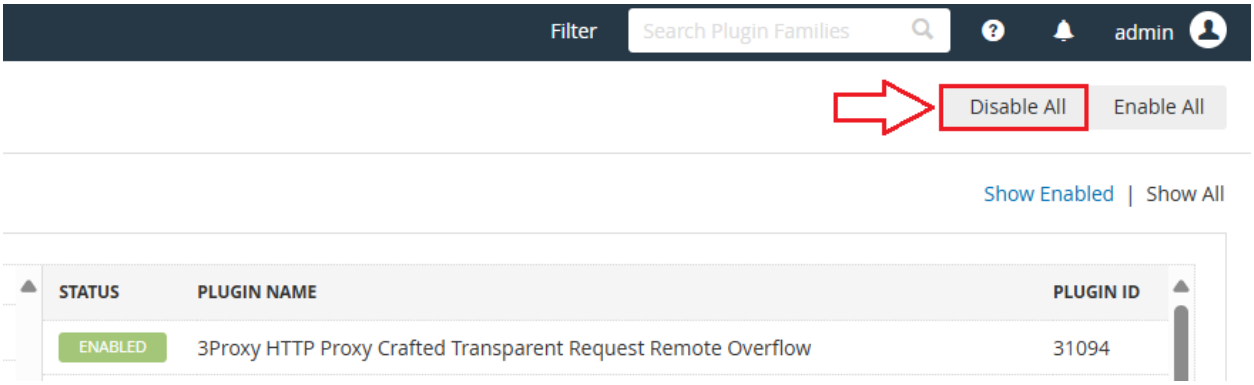


In telnet choose the Authentication method: Password enter username and password of Cisco Switch admin/cisco

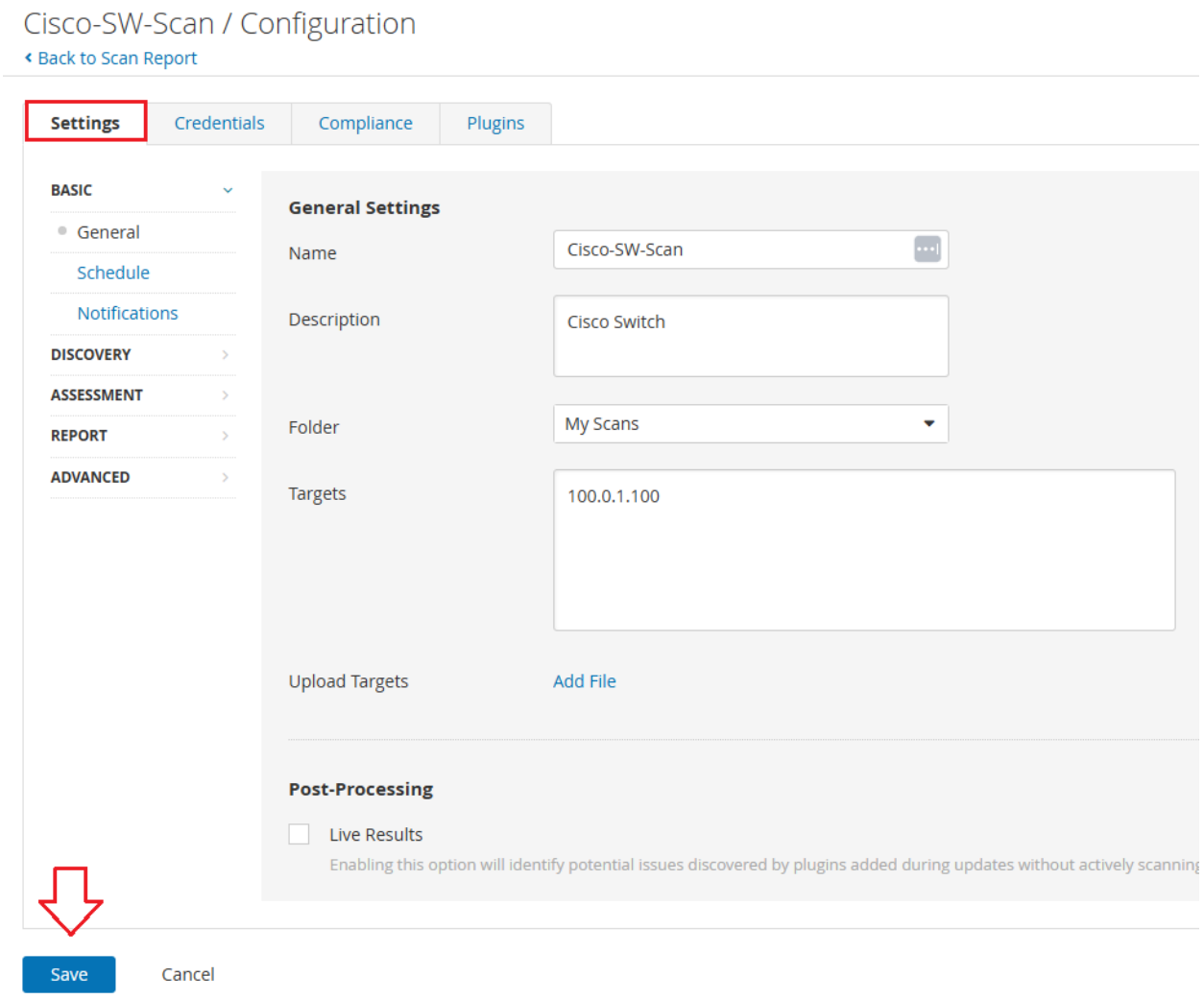


Plugins Tab disable all Plugins only enable Cisco plugin.

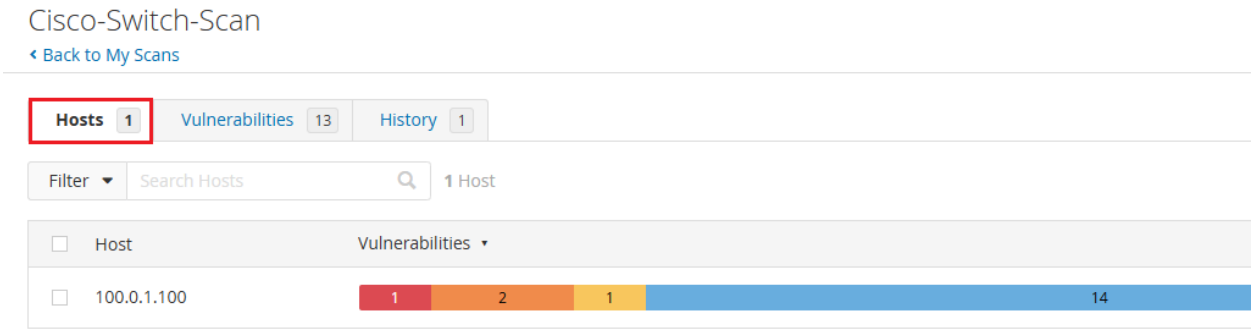




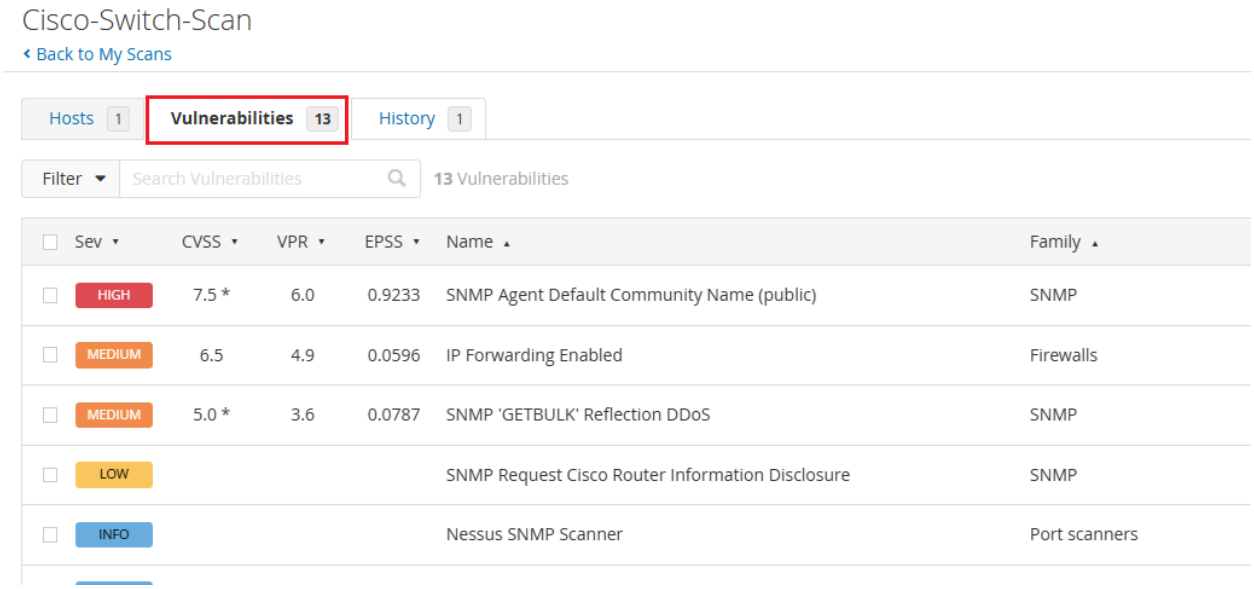
Click Save Then Launch. Wait for the scan to complete.



After complete the scan, in Hosts



Under Vulnerabilities Tab it shows almost 13



Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	May 10 at 4:49 PM
End:	May 10 at 4:53 PM
Elapsed:	3 minutes

Vulnerabilities