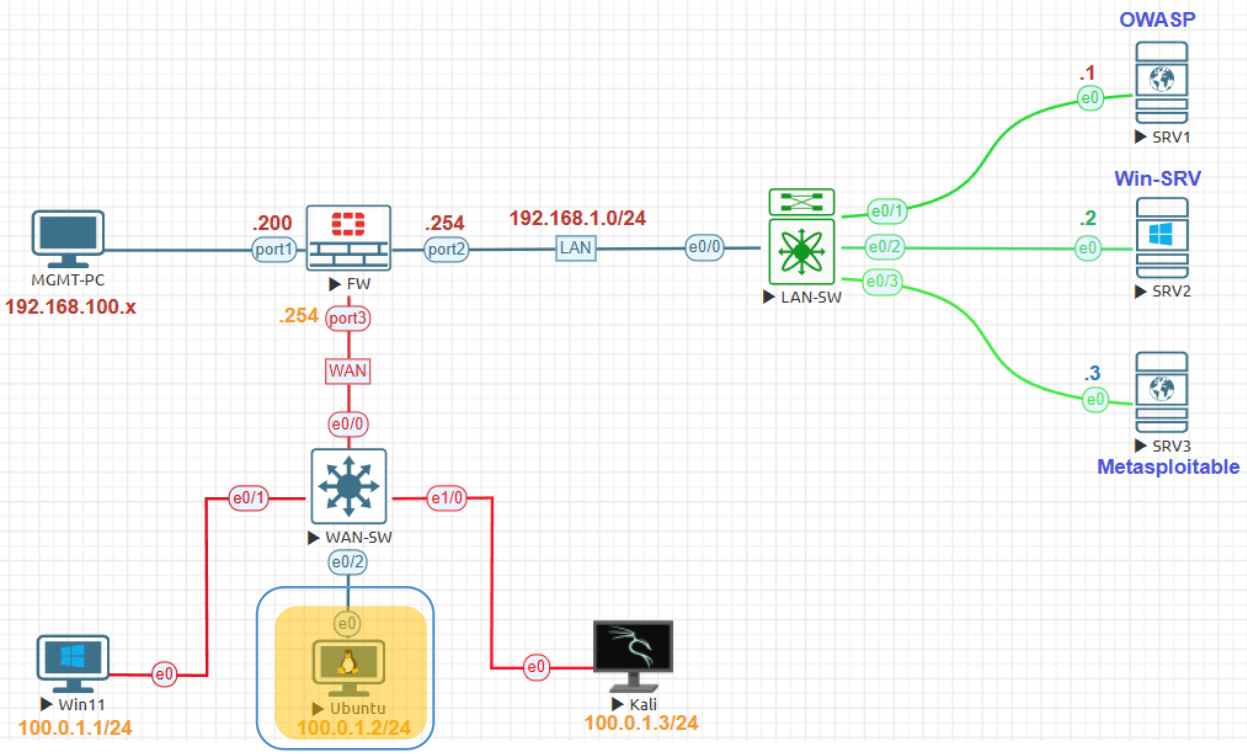
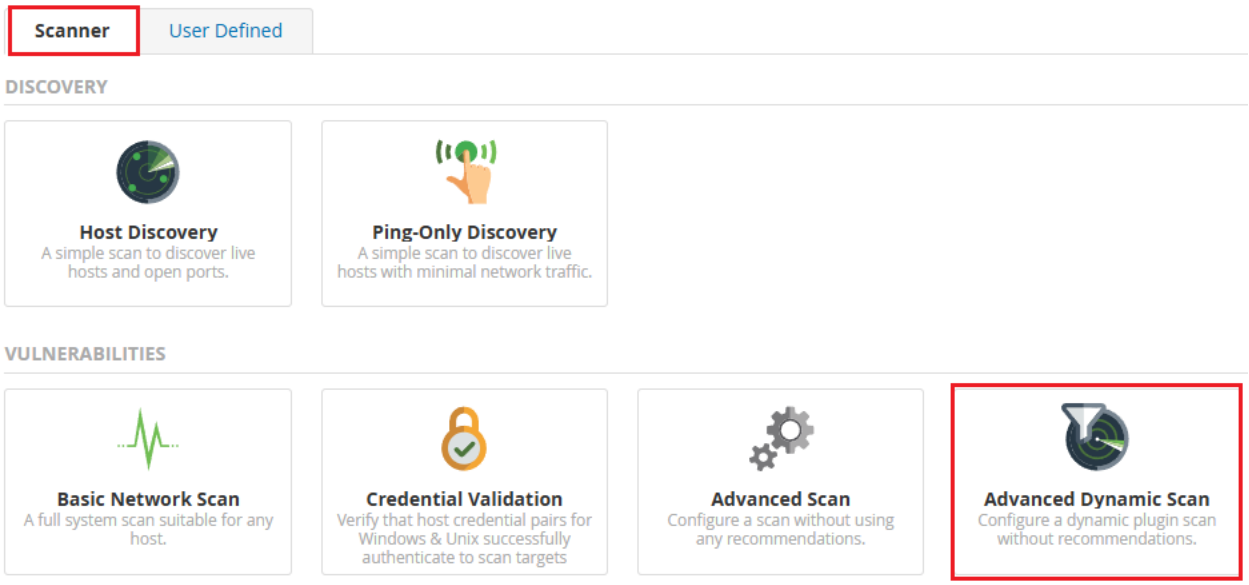
Advanced Dynamic Scan Lab:



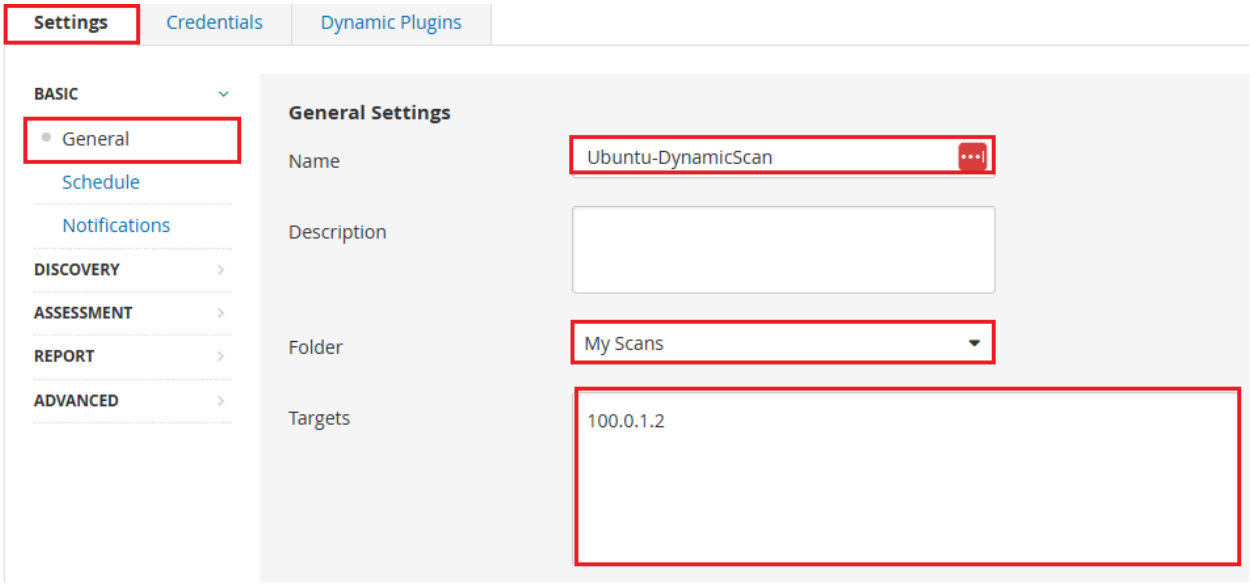
Management Subnet	192.168.100.0/24
FortiGate Management IP	192.168.100.200
Internal Servers Subnet	192.168.1.0/24
FortiGate Firewall External	100.0.1.0/24
FortiGate Firewall Internal IP	192.168.1.254
FortiGate Firewall External IP	100.0.1.254
SRV1 IP Address	192.168.1.1
SRV2 IP Address	192.168.1.2
SRV3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

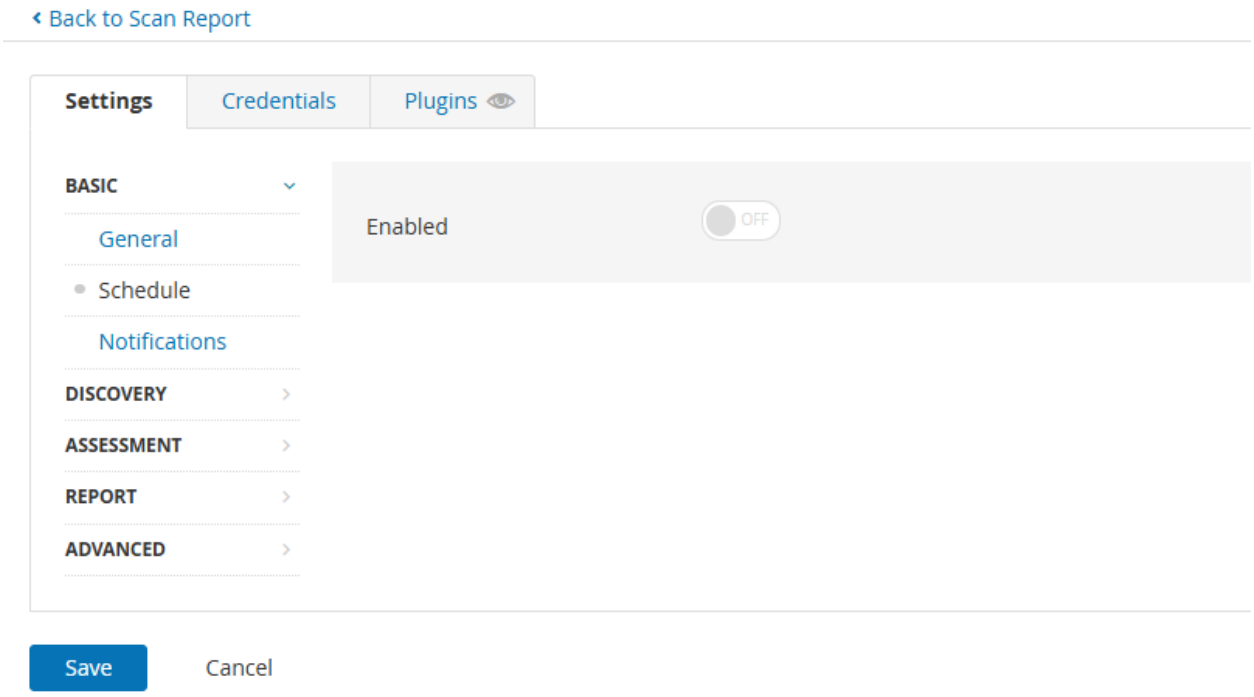
Go to Scans > New Scan. Choose Advanced Dynamic Scan to open.



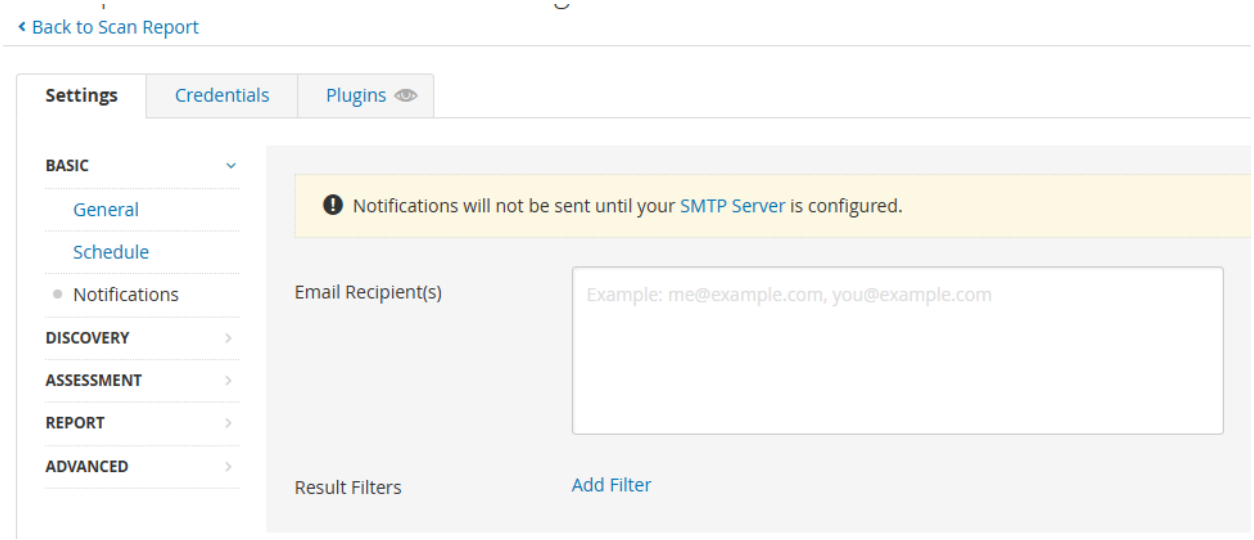
Name: Ubuntu-DynamicScan. Targets: IP address of target 100.0.1.2 the IP Address of Ubuntu Linux Machine.



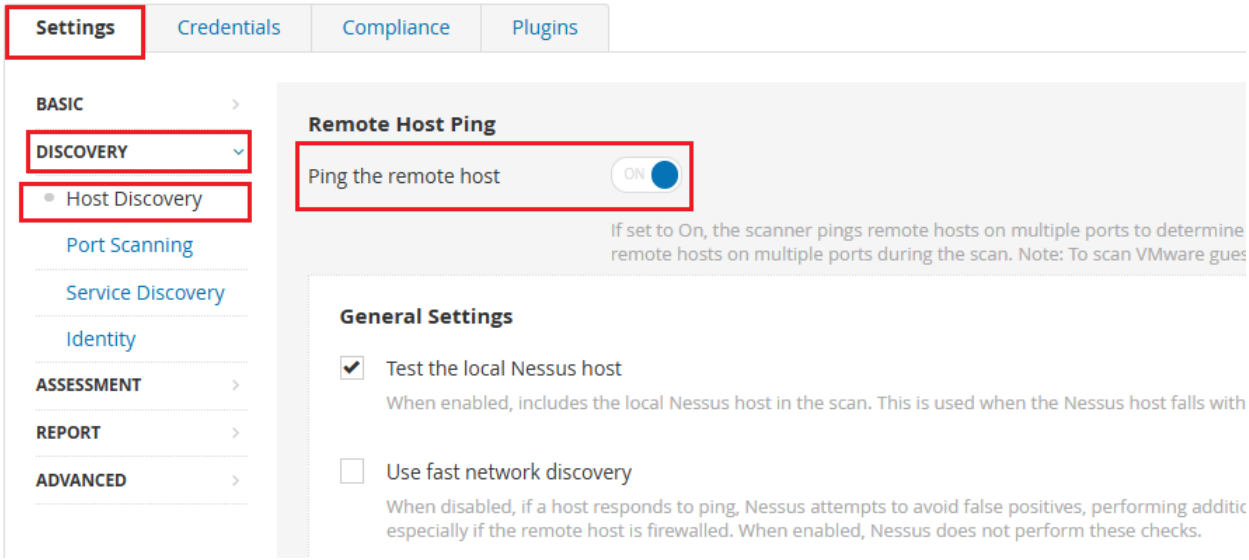
Setting>Basic>Schedule keep default disable.



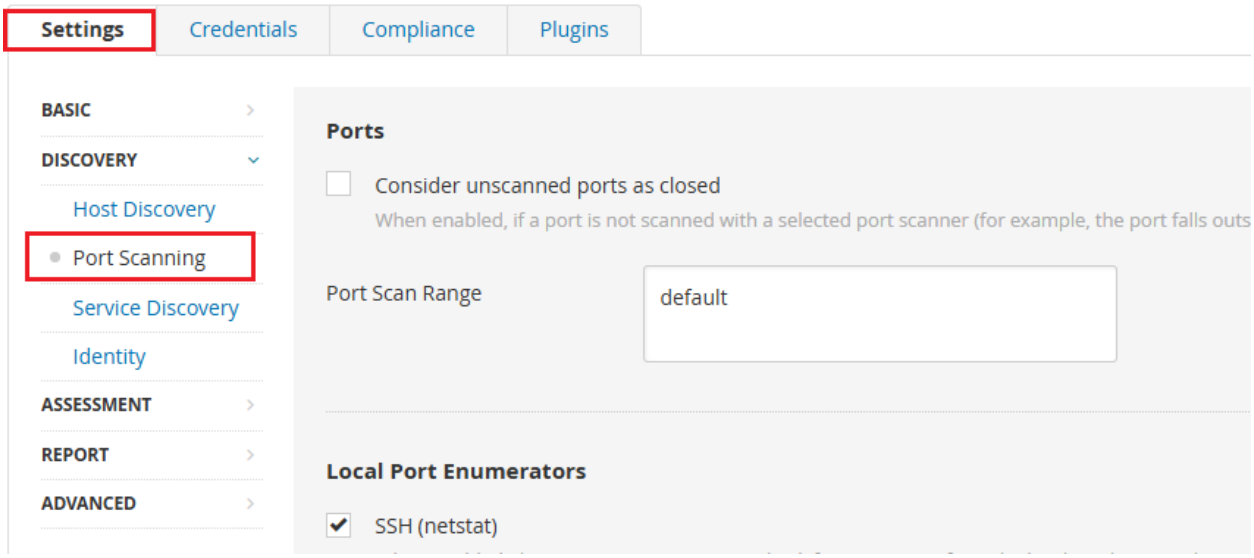
Settings>Basic>Notification keep default disable.



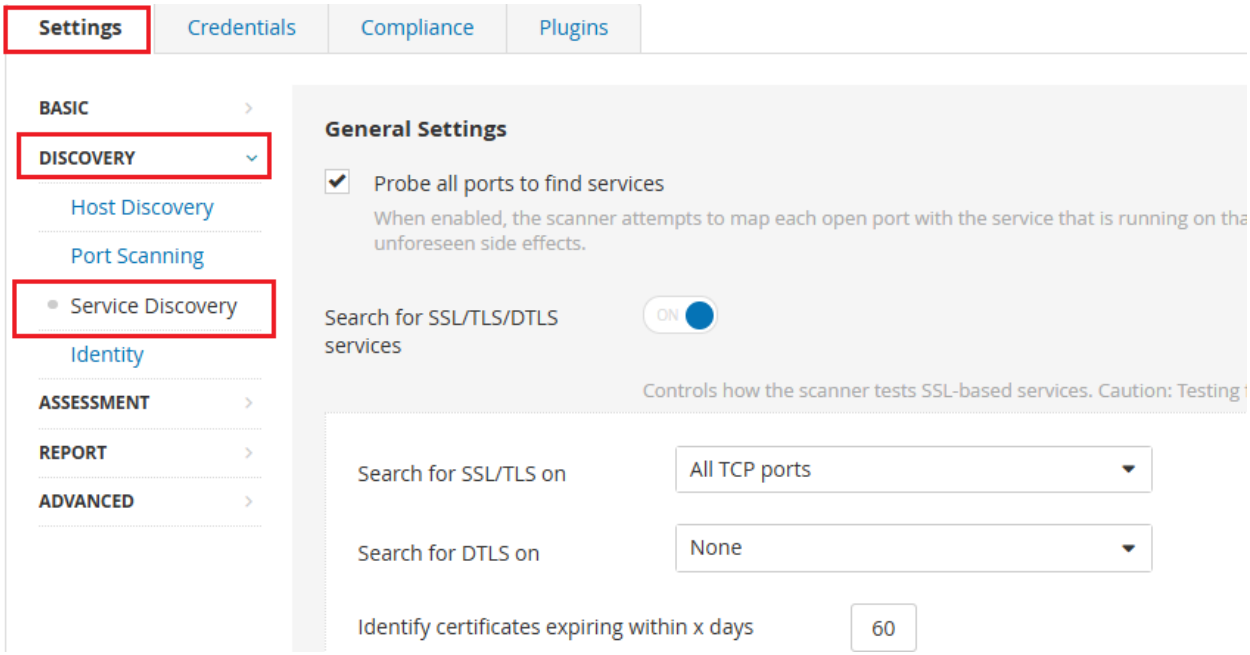
Settings>Basic>Discovery>Host Discovery keep default enable.



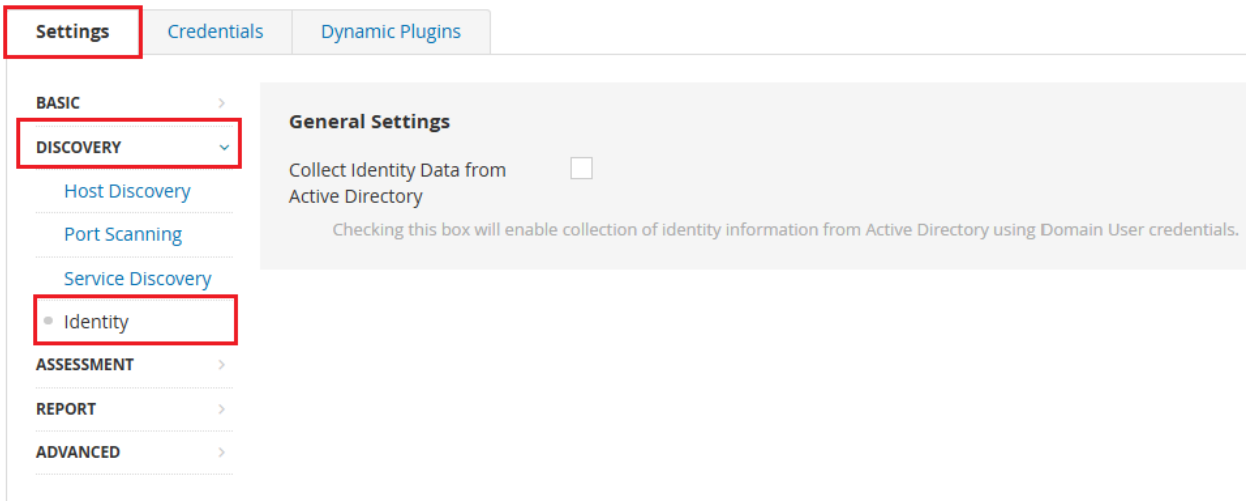
Setting>Discovery>Port Scanning keep default.



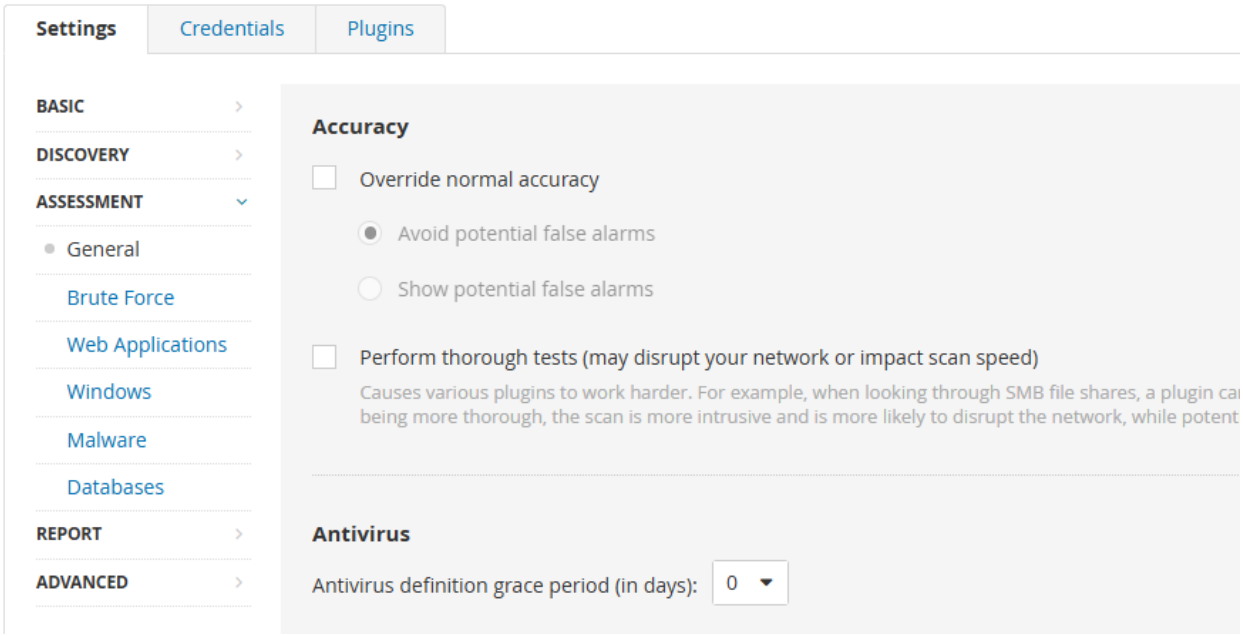
Setting>Discovery>Service Discovery keep default.



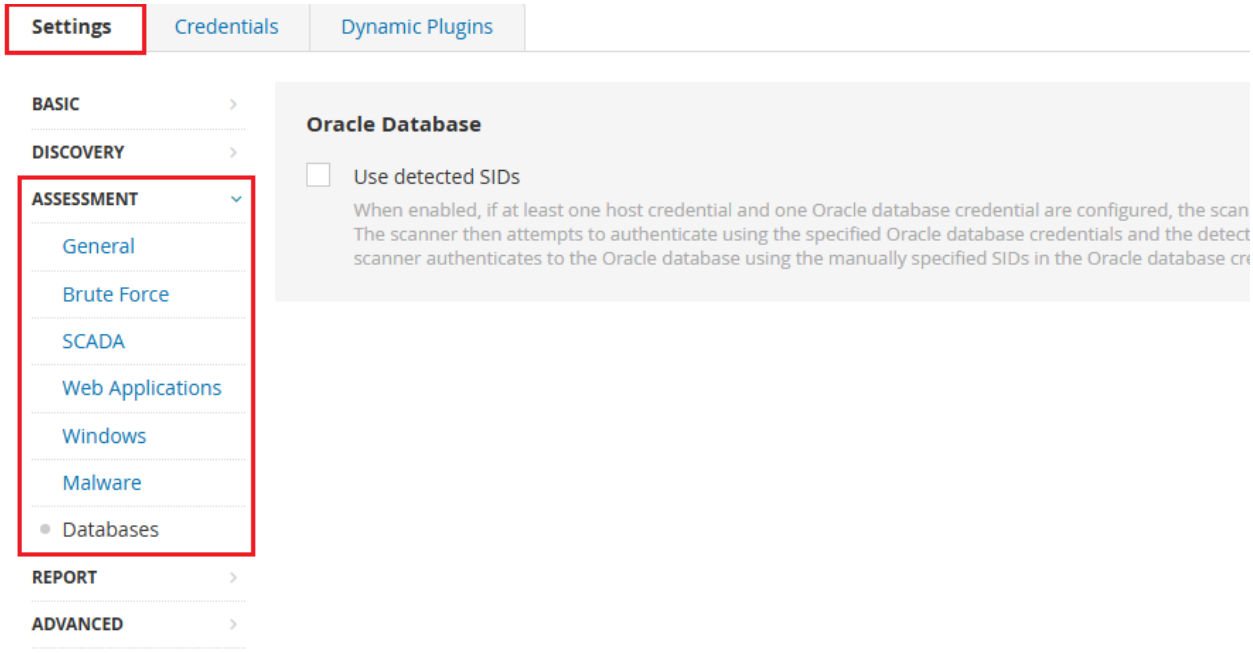
Setting> Discovery >Identity Keep default no changes.



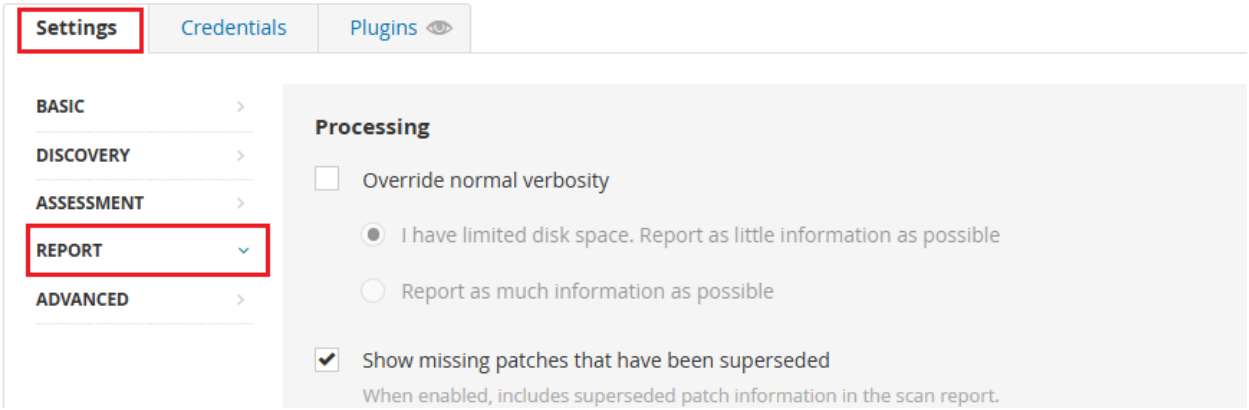
Setting>Assessment>General keep default.



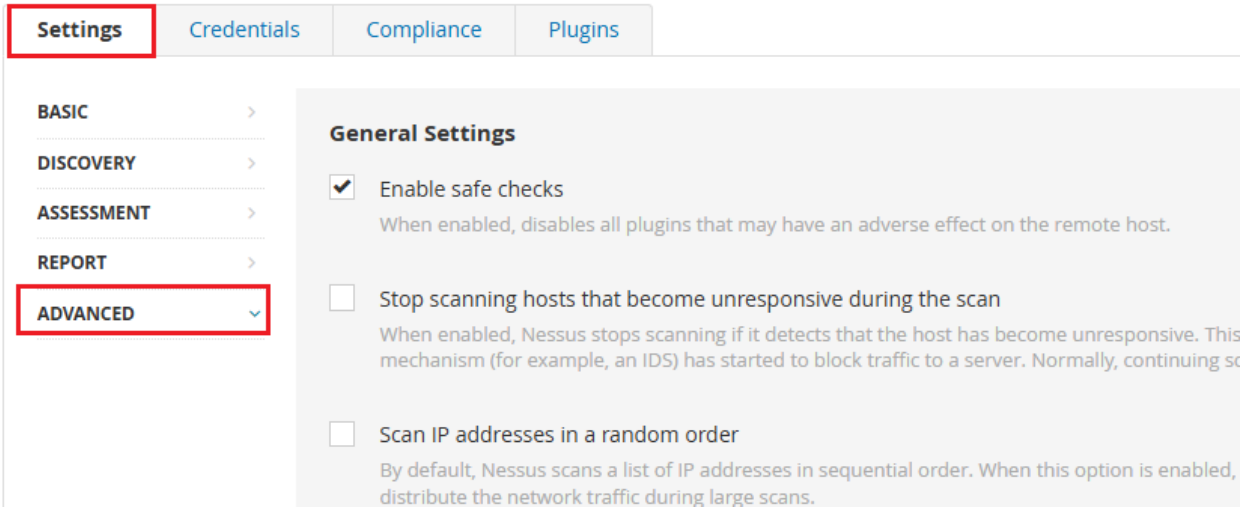
Settings>Assessment Keep default.



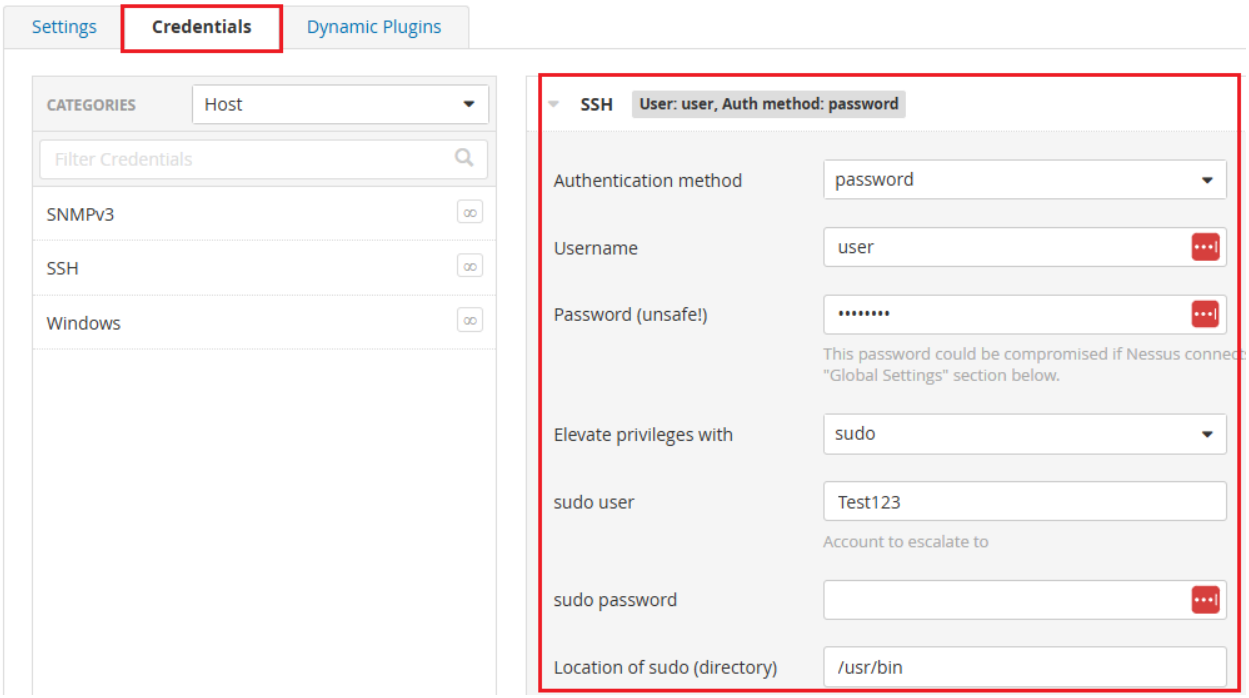
Settings>Report keep the default.



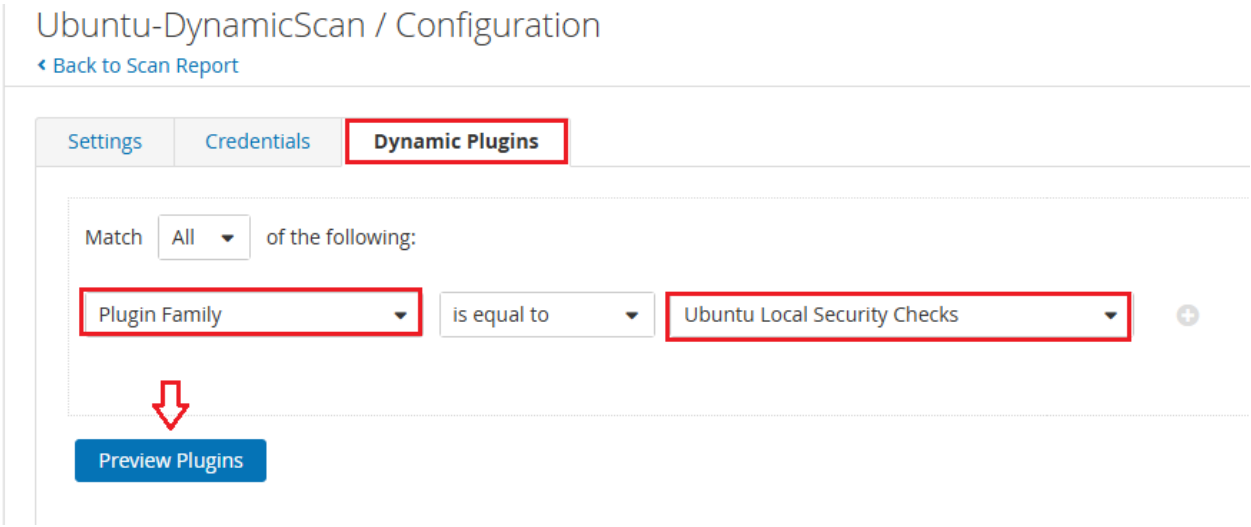
Settings>Advanced keep default no changes.

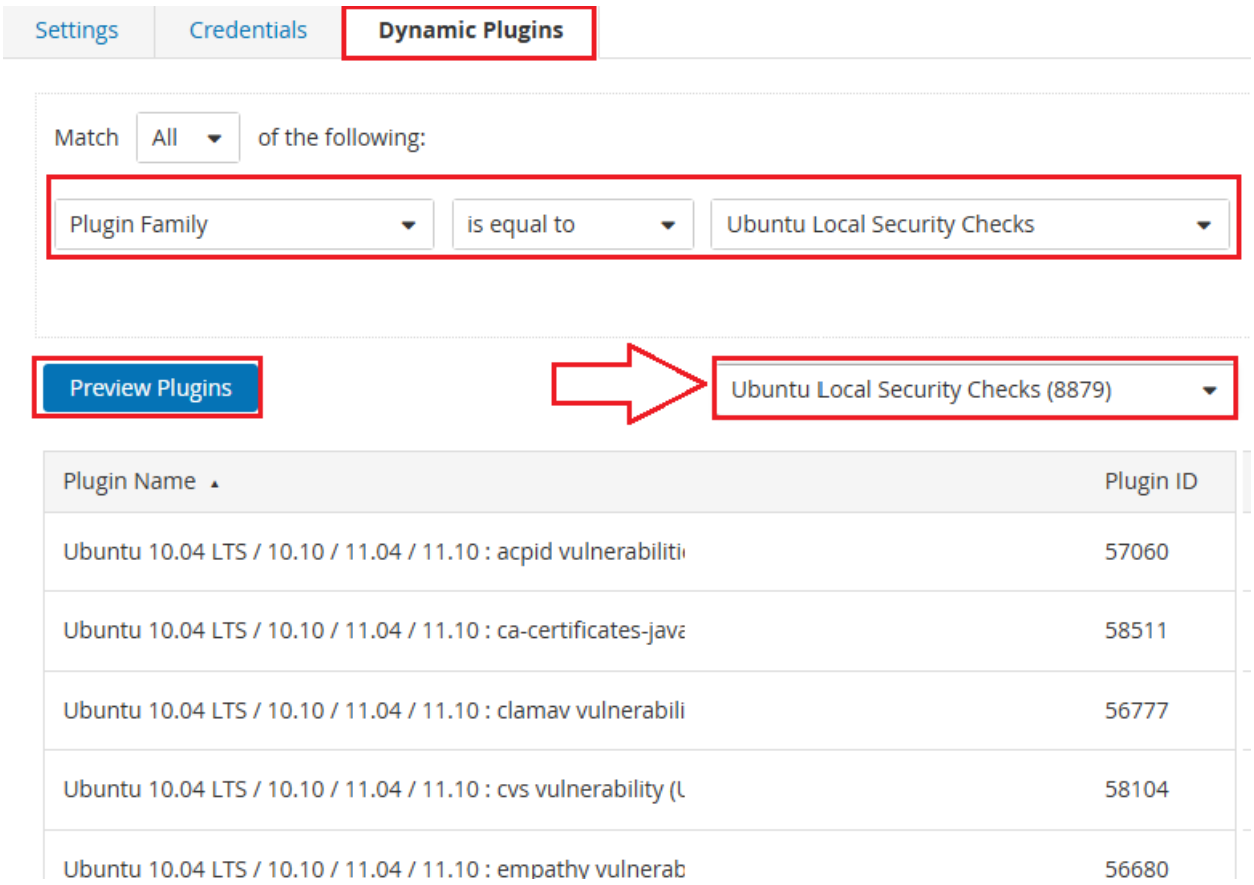


Under Credentials Tab. Choose SSH Authentication method: Password

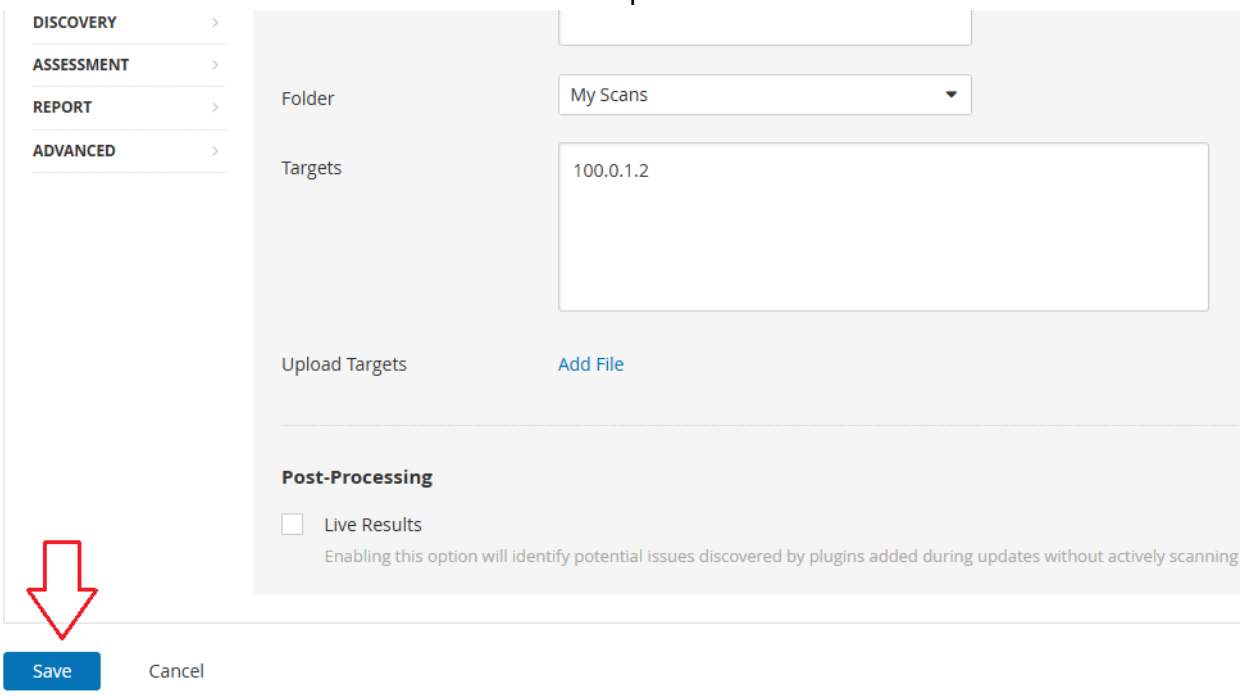


Dynamic Plugins choose Plugin Family is equal to Ubuntu Local Security Checks after that click on Preview Plugins

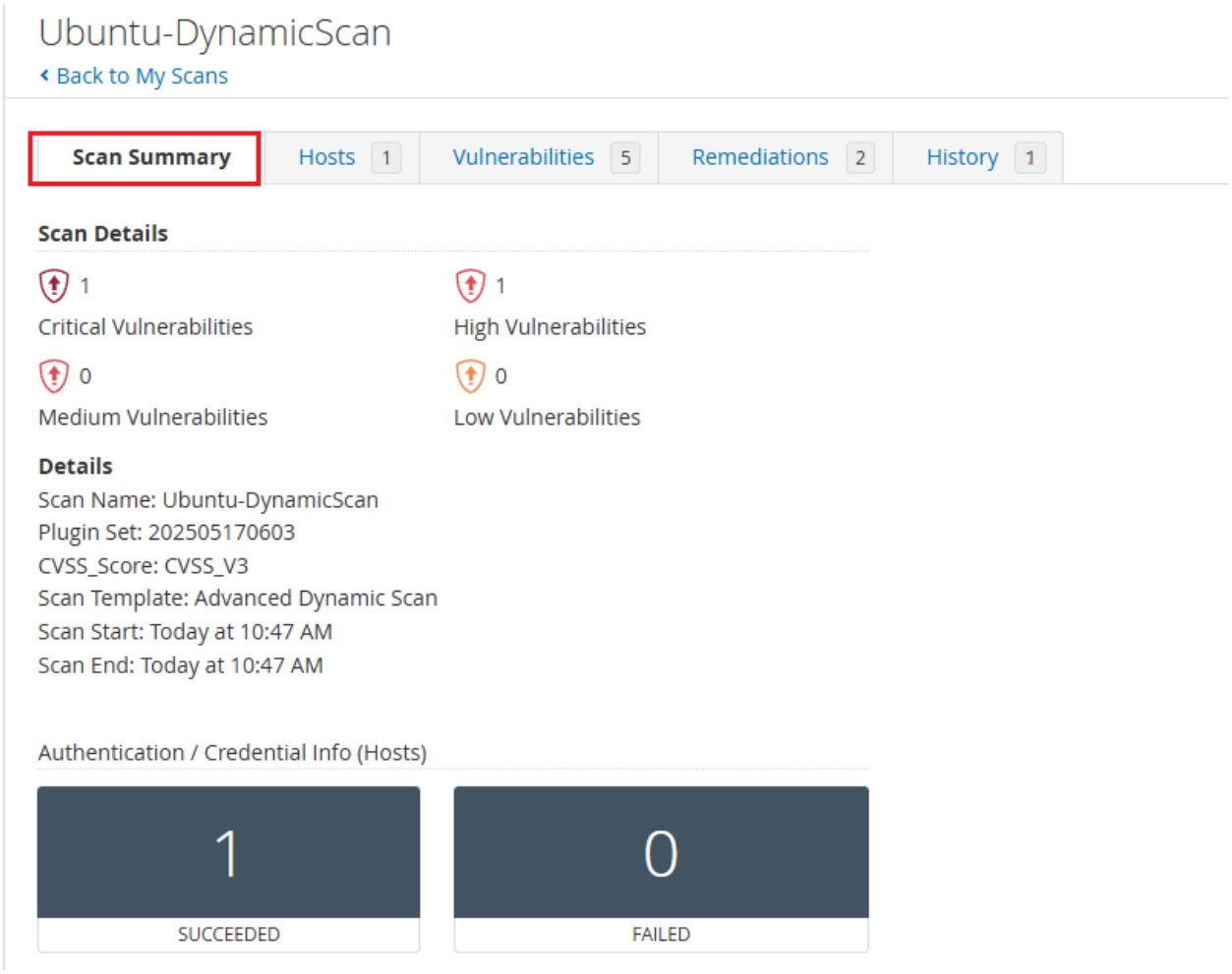




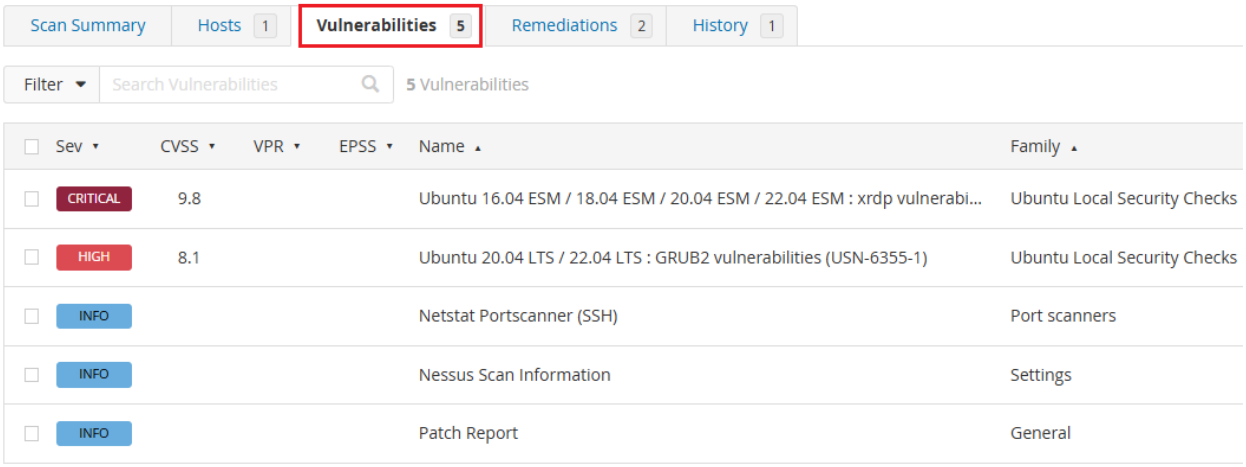
Click Save Then Launch. Wait for the scan to complete.



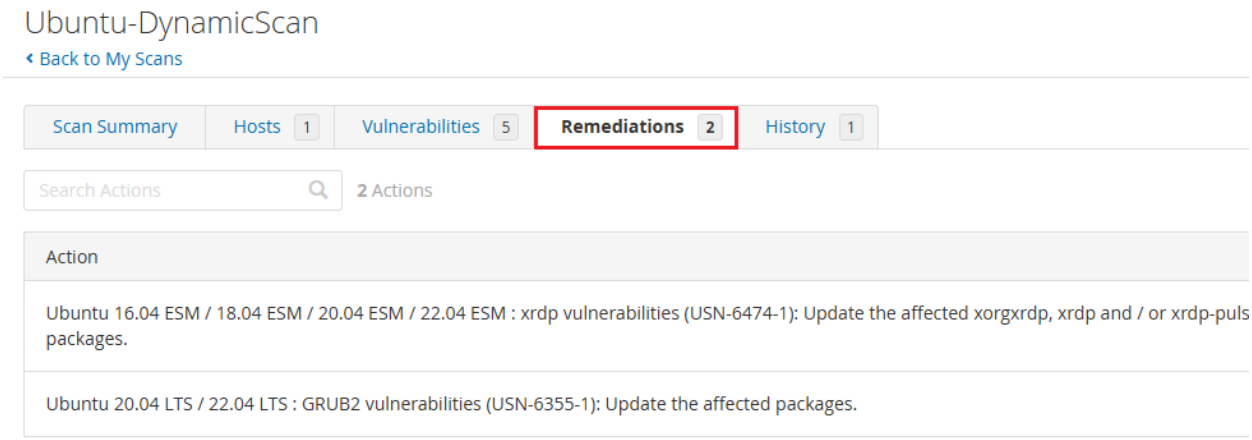
After complete the scan, in Scan Summary Tab.



Under Vulnerabilities Tab it shows almost 5



Under Remediation Tab.



Under Hosts Tab.