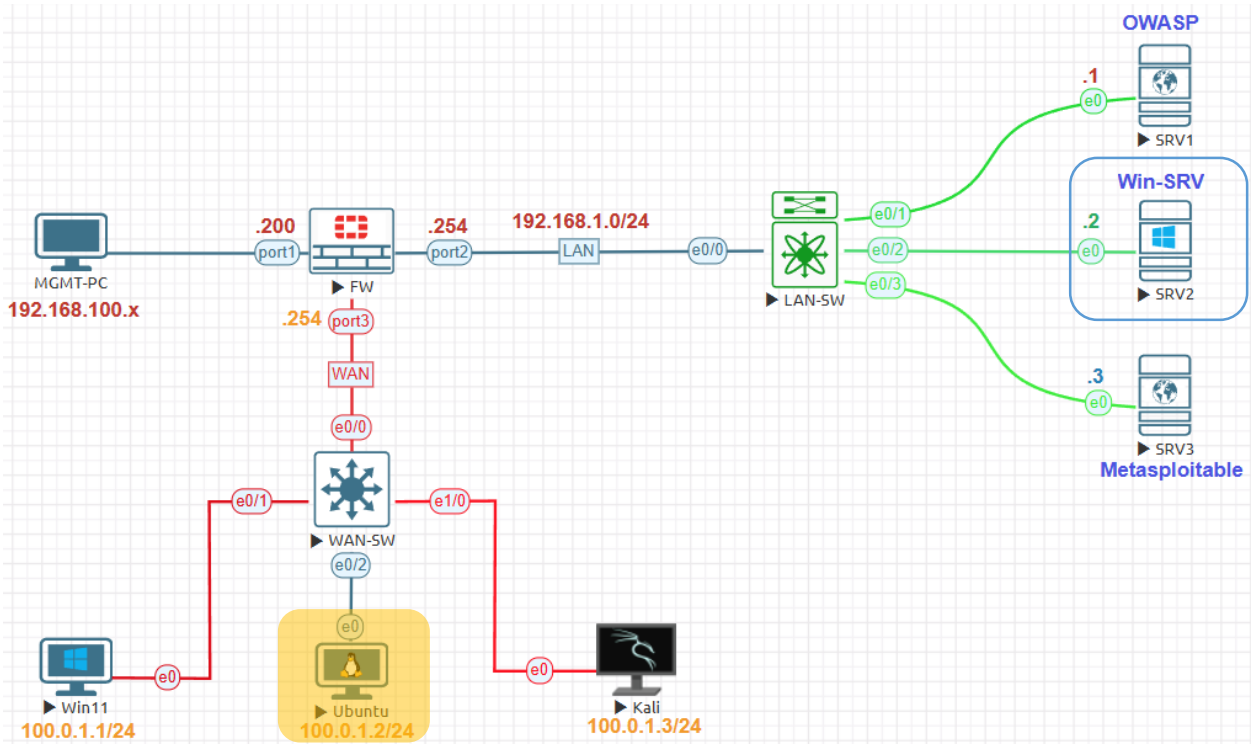
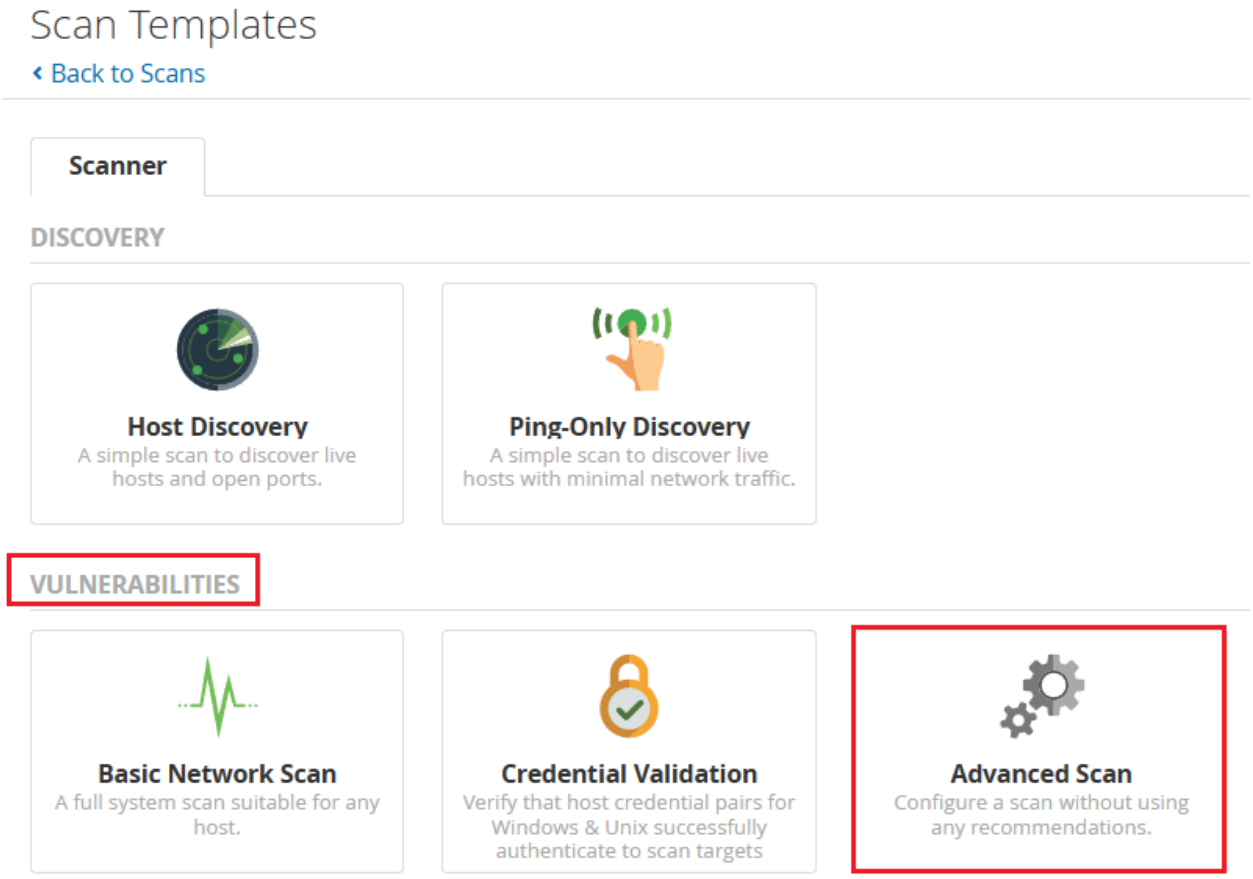
AD Advanced Scan Lab:



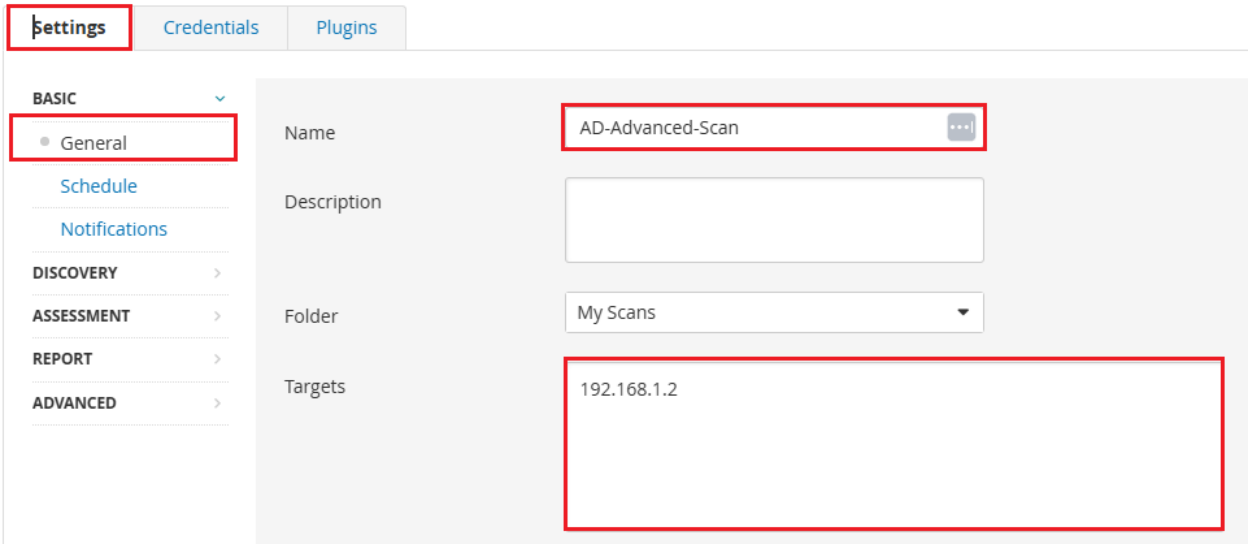
Management Subnet	192.168.100.0/24
FortiGate Management IP	192.168.100.200
Internal Servers Subnet	192.168.1.0/24
FortiGate Firewall External	100.0.1.0/24
FortiGate Firewall Internal IP	192.168.1.254
FortiGate Firewall External IP	100.0.1.254
SRV1 IP Address	192.168.1.1
SRV2 IP Address	192.168.1.2
SRV3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

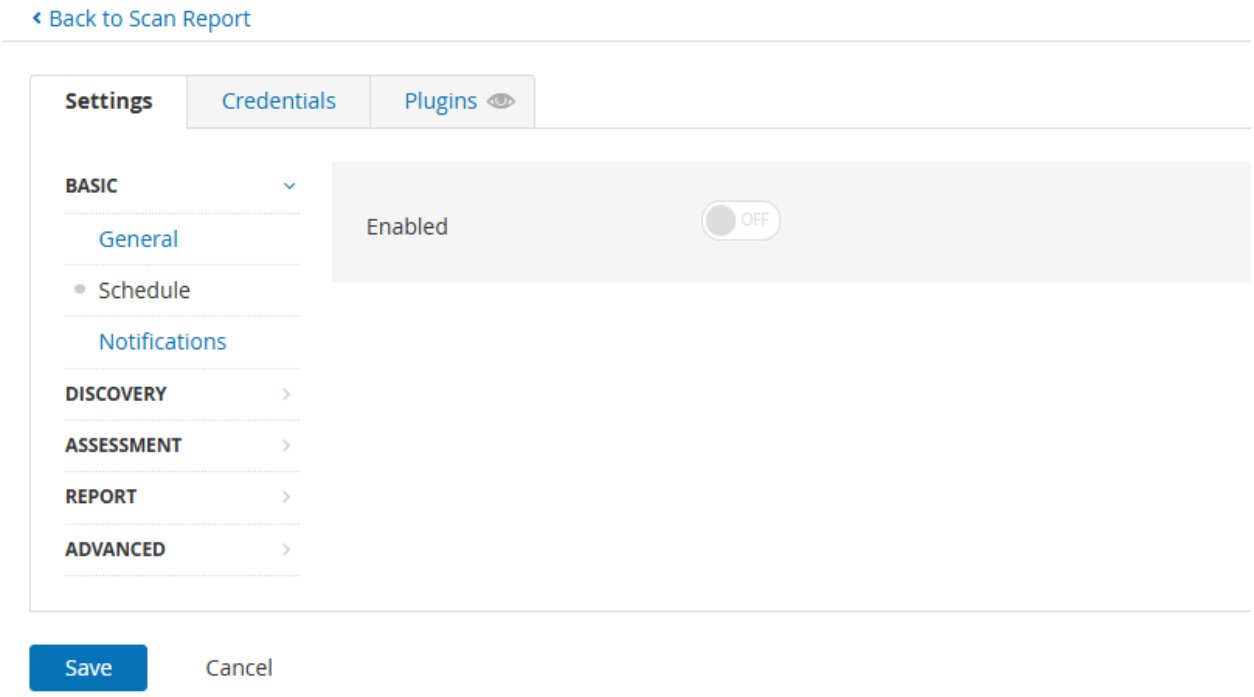
Go to Scans > New Scan. Choose Advanced Scan to open.



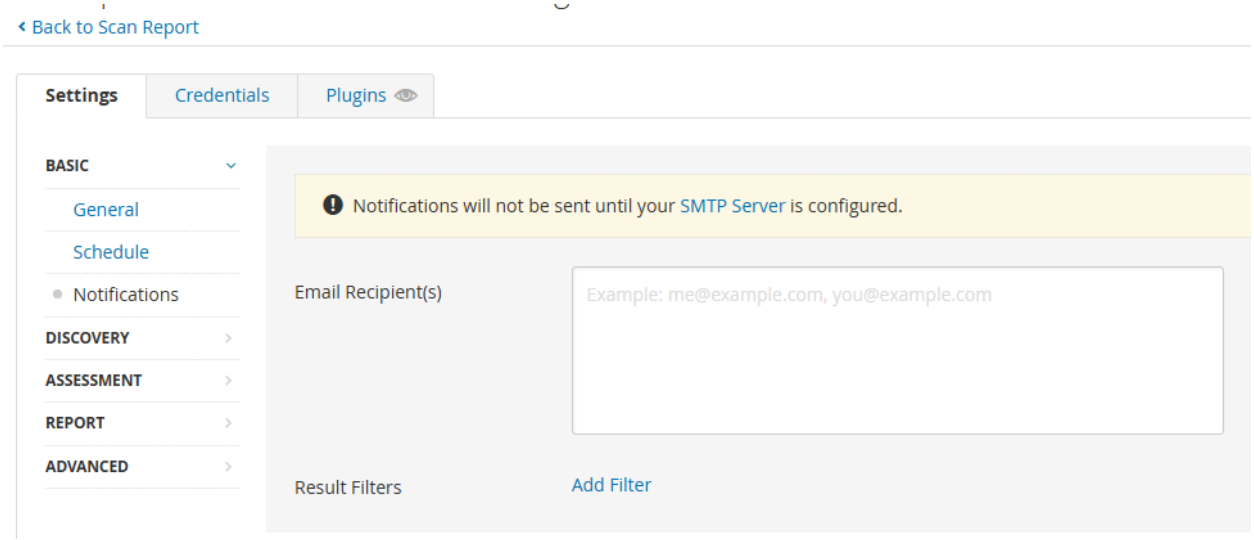
Name: AD-Advanced-Scan. Targets: IP address of target 192.168.1.2 the IP Address of Windows Server 2019 Active Directory.



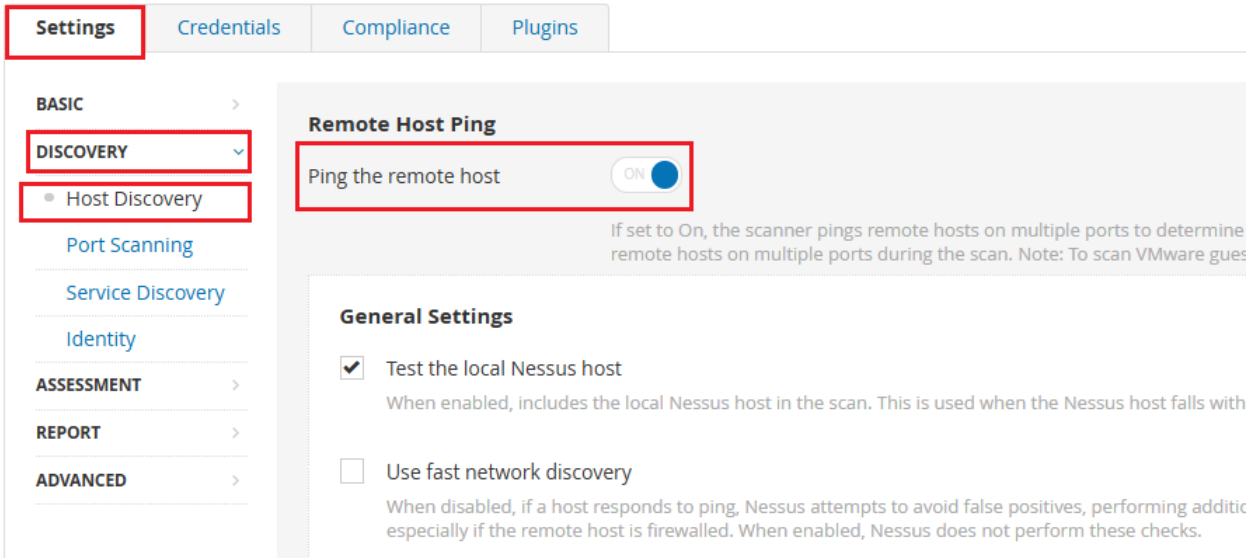
Setting>Basic>Schedule keep default disable.



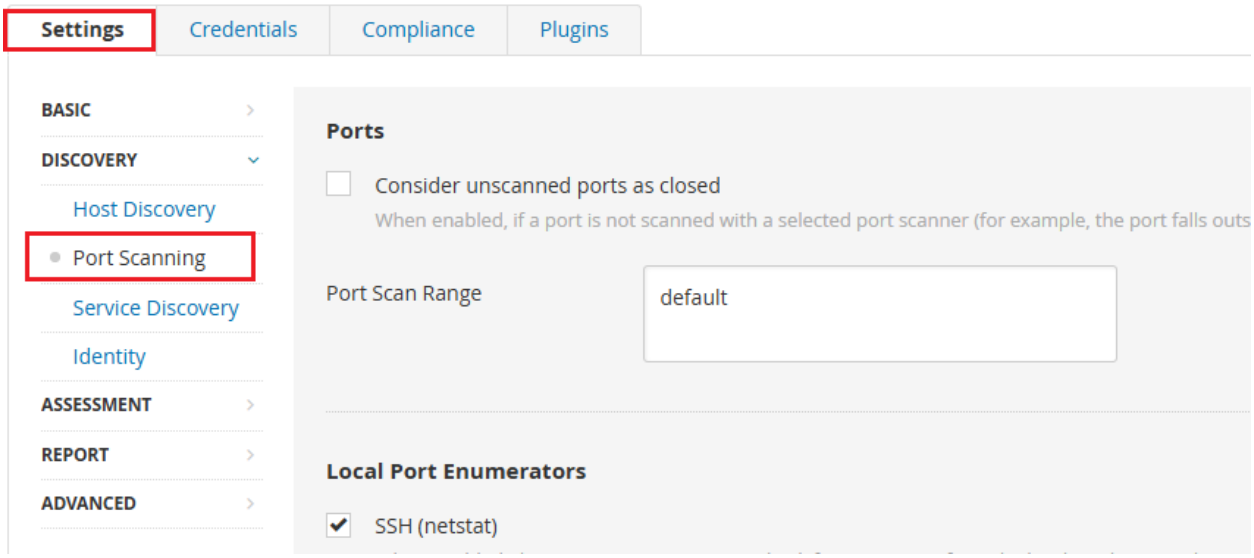
Settings>Basic>Notification keep default disable.



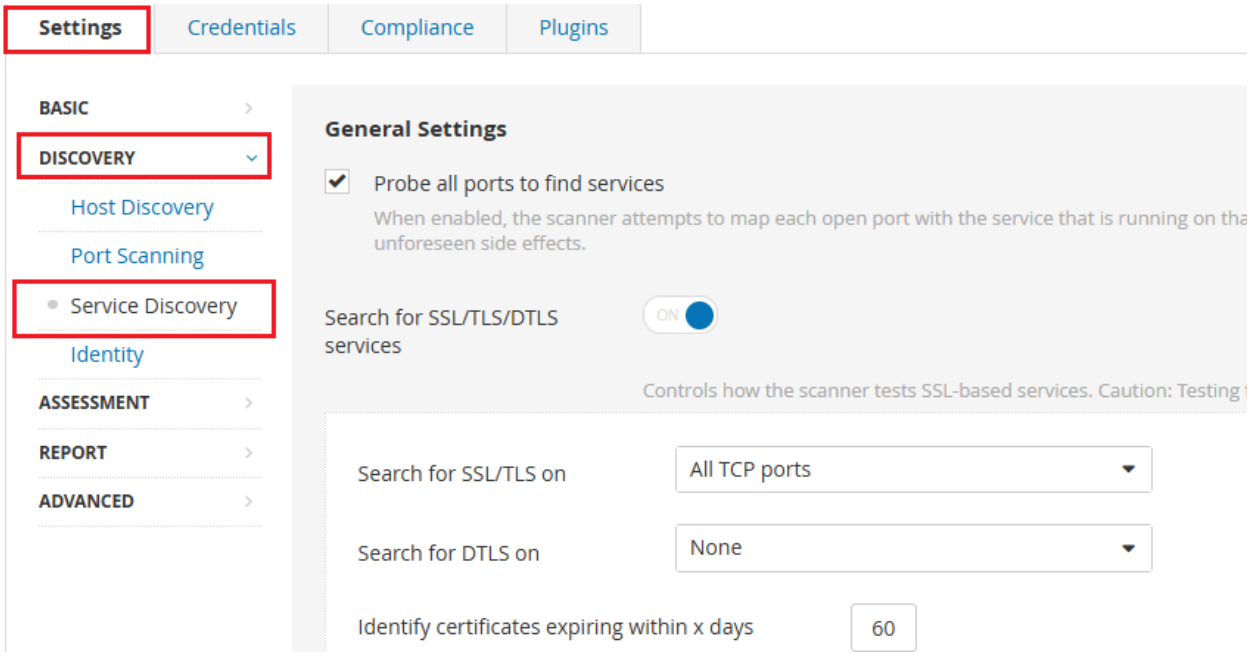
Settings>Basic>Discovery>Host Discovery keep default enable.



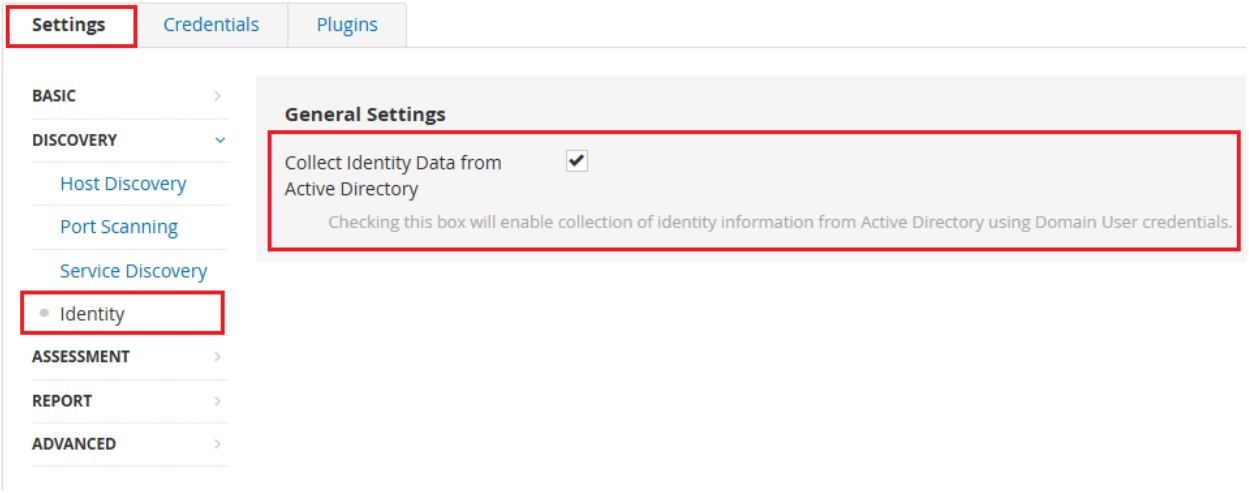
Setting>Discovery>Port Scanning keep default.



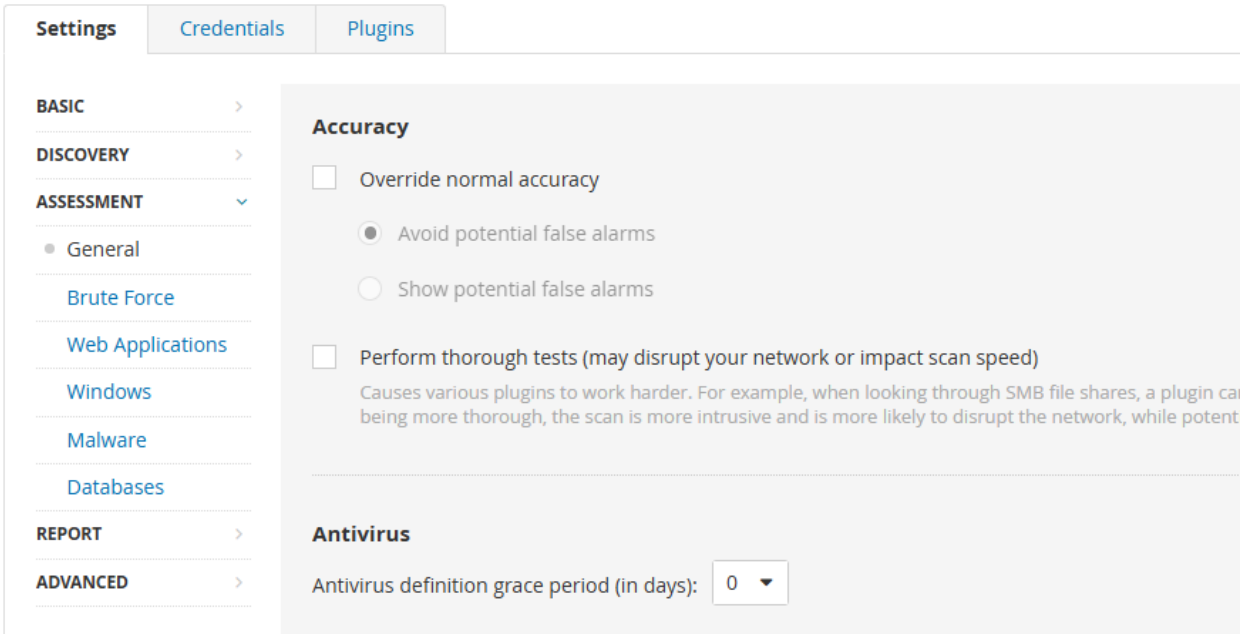
Setting>Discovery>Service Discovery keep default.



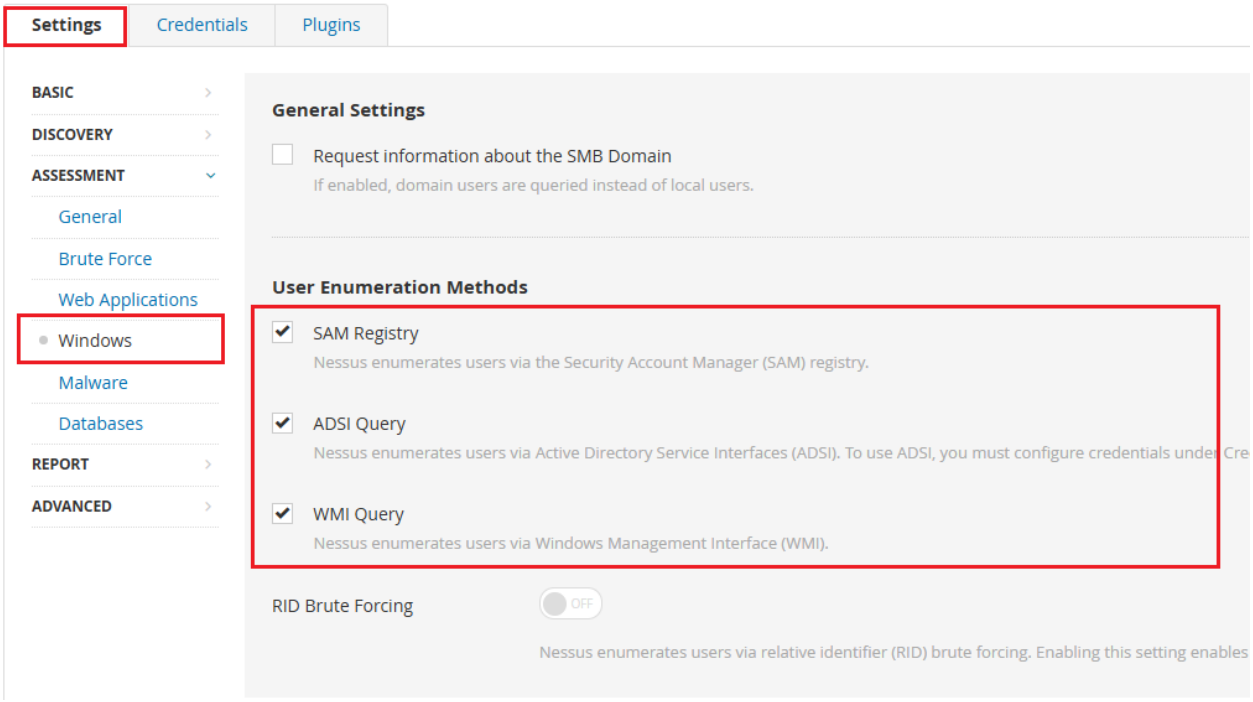
Setting> Discovery >Identity Enable Collect Identity Data from Active Directory.



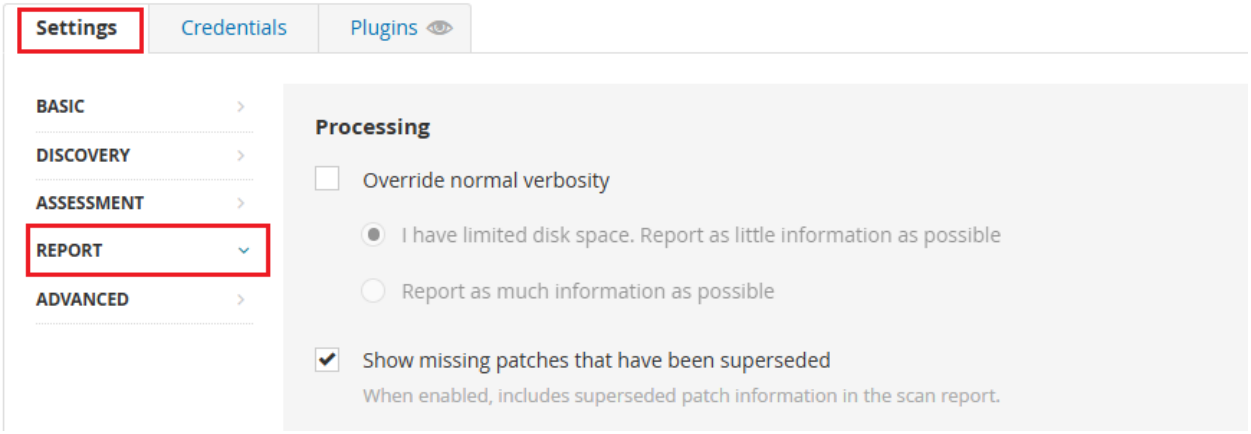
Setting>Assessment>General keep default.



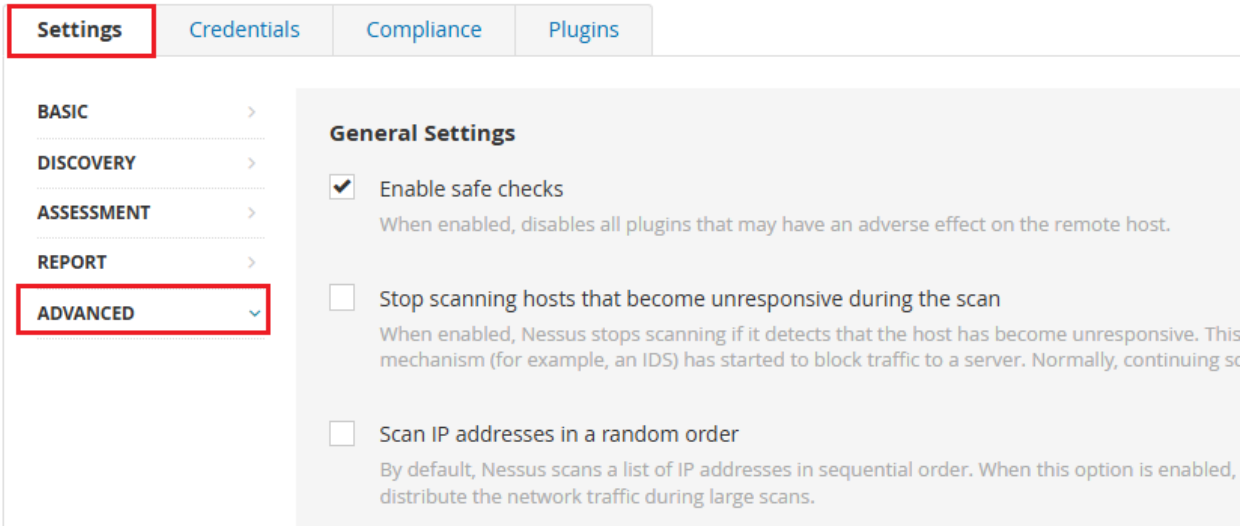
Settings>Assessment>Windows Enable SAM Registry, ADSI Query and WMI Quarry.



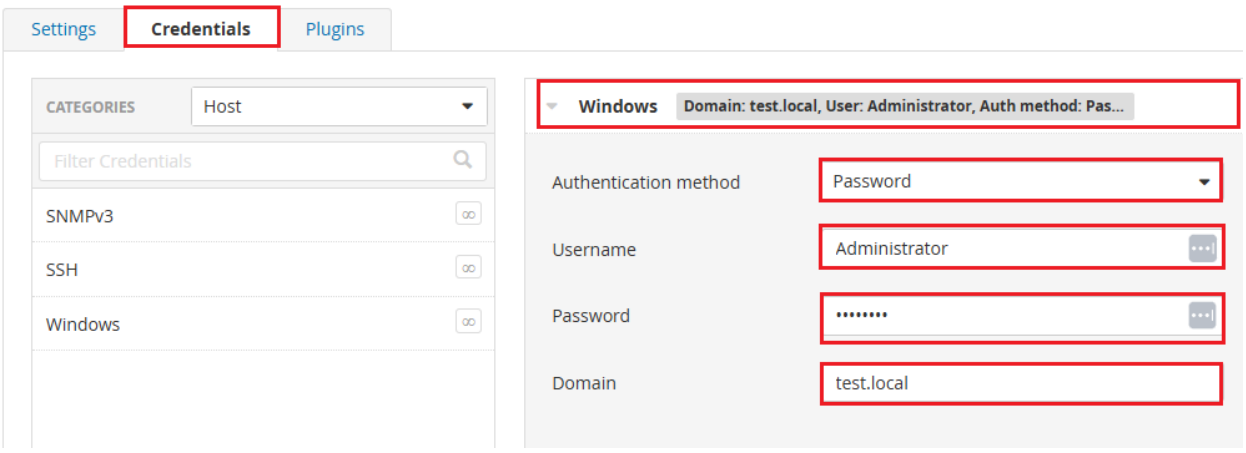
Settings>Report keep the default.



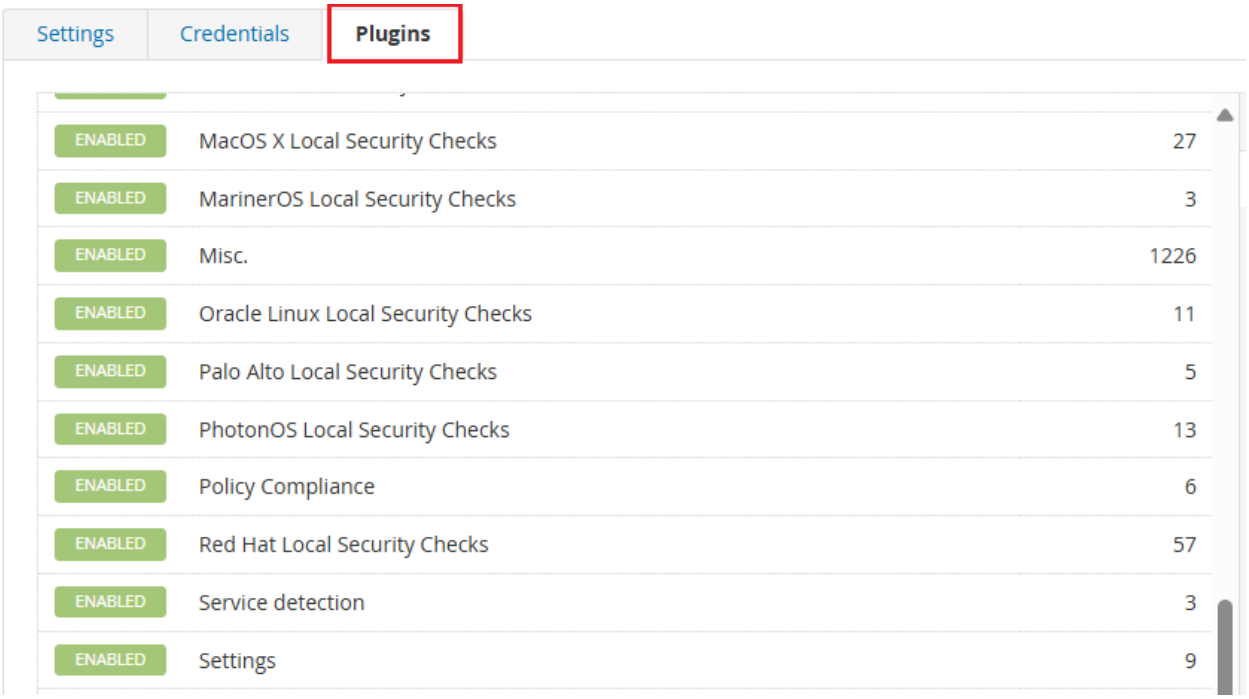
Settings>Advanced keep default no changes.



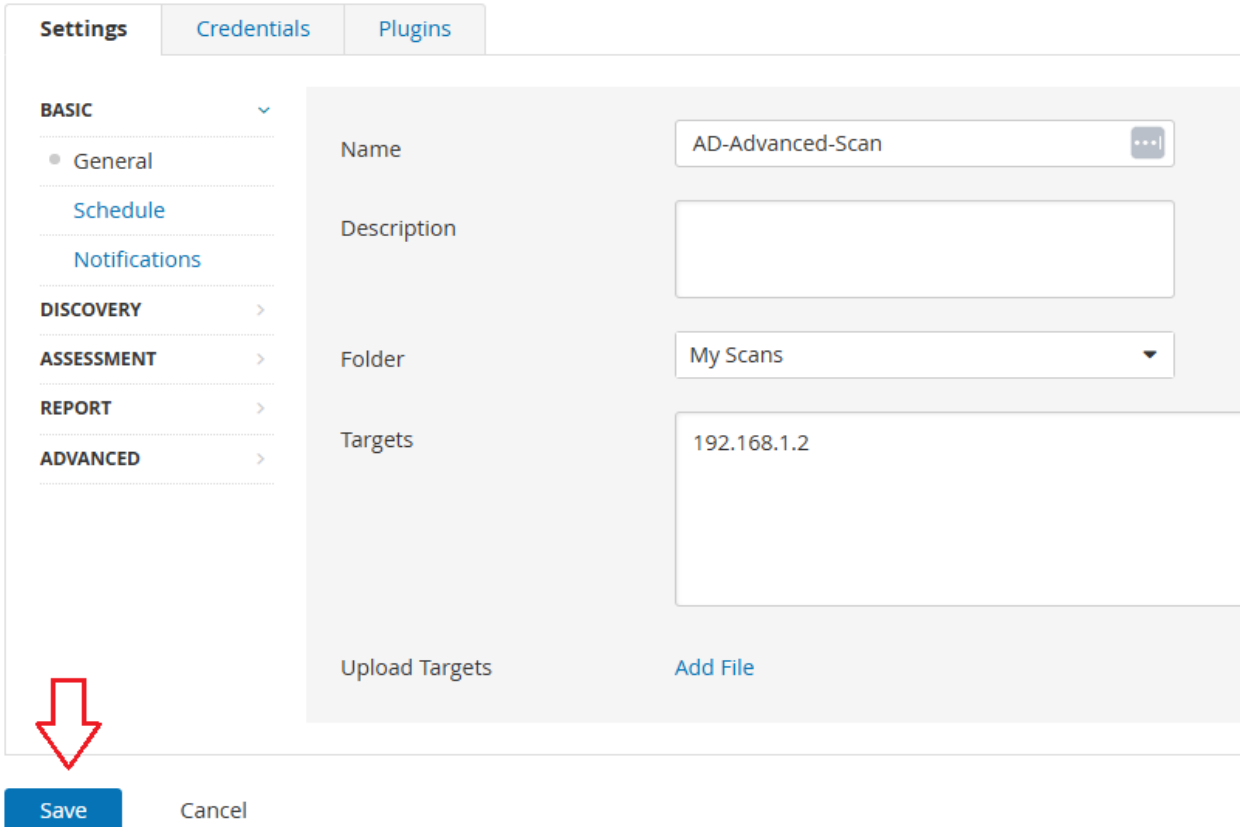
Under Credentials Tab. Choose Windows Authentication method: Password after that enter the username and password: Administrator/Test123 Domain:test.local



Plugins keep enabled All.

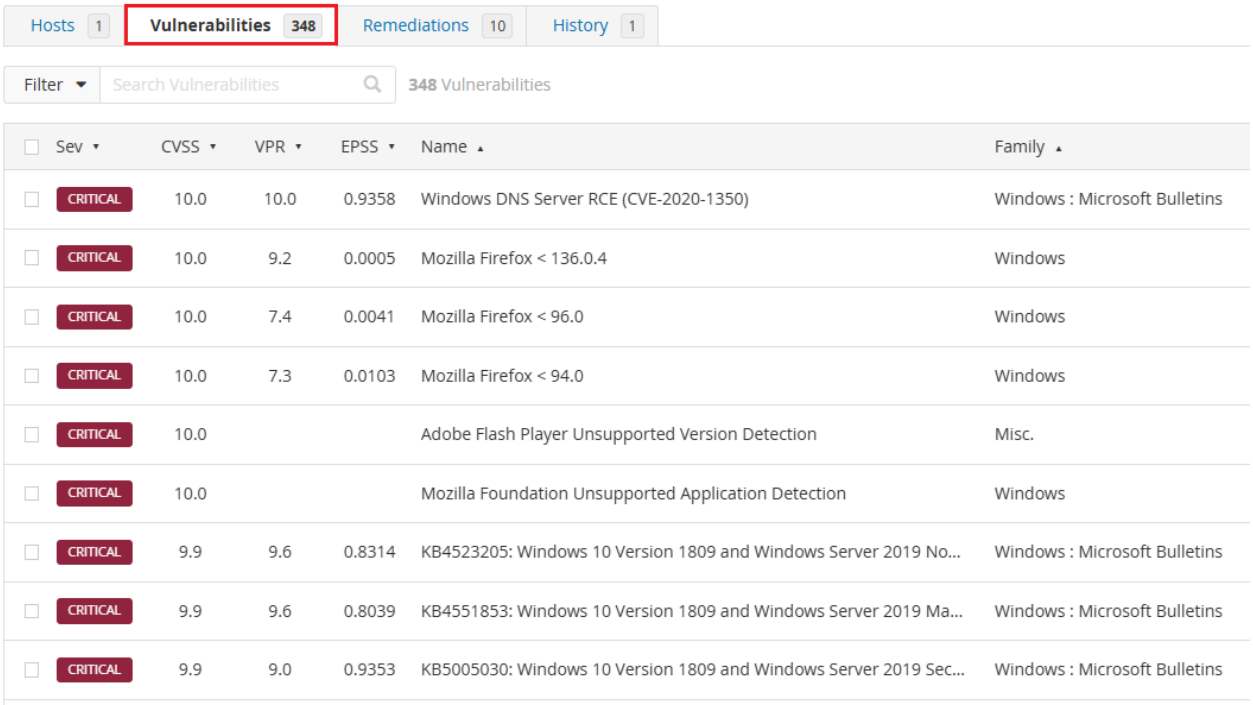


Click Save Then Launch. Wait for the scan to complete.

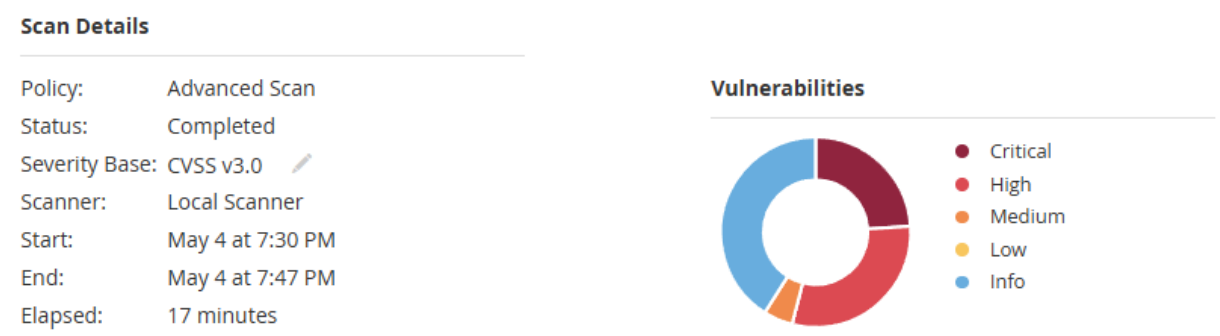


After complete the scan, in Hosts Tab.

Under Vulnerabilities Tab it shows almost 348



Sev	CVSS	VPR	EPSS	Name	Family
CRITICAL	10.0	10.0	0.9358	Windows DNS Server RCE (CVE-2020-1350)	Windows : Microsoft Bulletins
CRITICAL	10.0	9.2	0.0005	Mozilla Firefox < 136.0.4	Windows
CRITICAL	10.0	7.4	0.0041	Mozilla Firefox < 96.0	Windows
CRITICAL	10.0	7.3	0.0103	Mozilla Firefox < 94.0	Windows
CRITICAL	10.0			Adobe Flash Player Unsupported Version Detection	Misc.
CRITICAL	10.0			Mozilla Foundation Unsupported Application Detection	Windows
CRITICAL	9.9	9.6	0.8314	KB4523205: Windows 10 Version 1809 and Windows Server 2019 No...	Windows : Microsoft Bulletins
CRITICAL	9.9	9.6	0.8039	KB4551853: Windows 10 Version 1809 and Windows Server 2019 Ma...	Windows : Microsoft Bulletins
CRITICAL	9.9	9.0	0.9353	KB5005030: Windows 10 Version 1809 and Windows Server 2019 Sec...	Windows : Microsoft Bulletins



Under Remediation Tab.