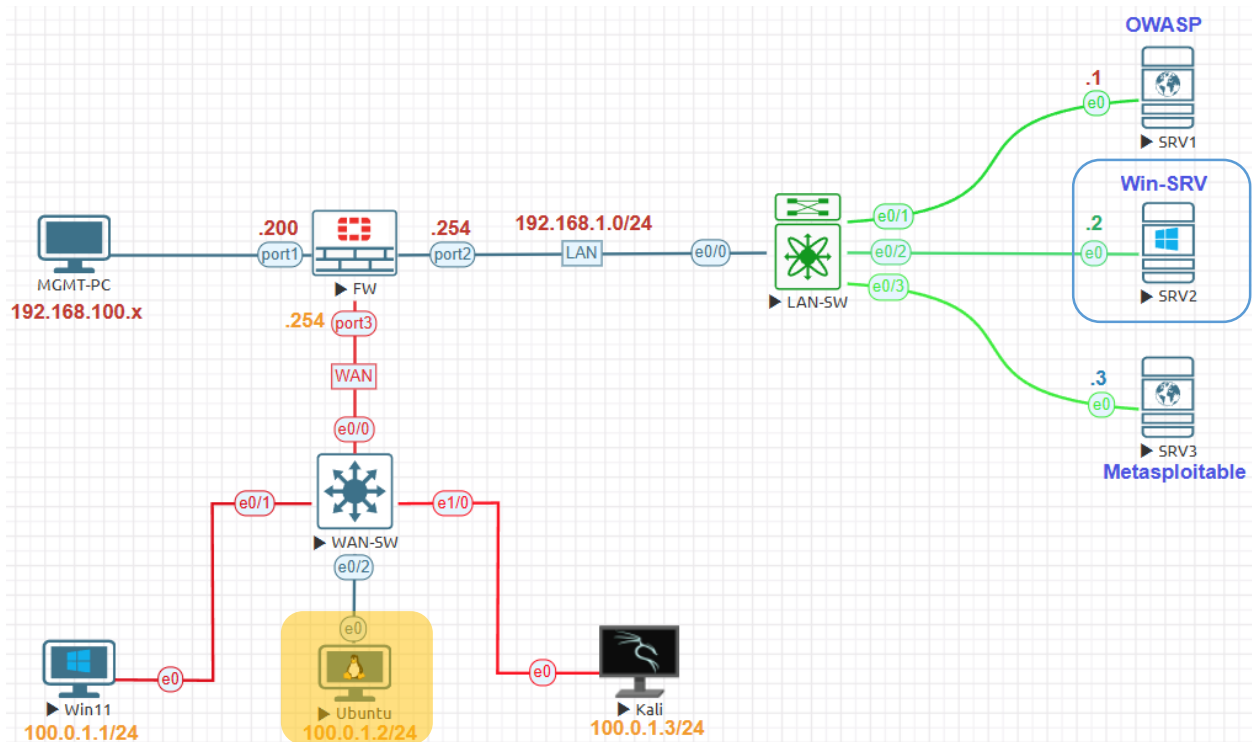


AD Advanced Scan Lab:



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.

Scan Templates

[← Back to Scans](#)

Scanner

DISCOVERY



Host Discovery

A simple scan to discover live hosts and open ports.



Ping-Only Discovery

A simple scan to discover live hosts with minimal network traffic.

VULNERABILITIES



Basic Network Scan

A full system scan suitable for any host.



Credential Validation

Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets



Advanced Scan

Configure a scan without using any recommendations.

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

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

AD-Advanced-Scan

Description

Folder

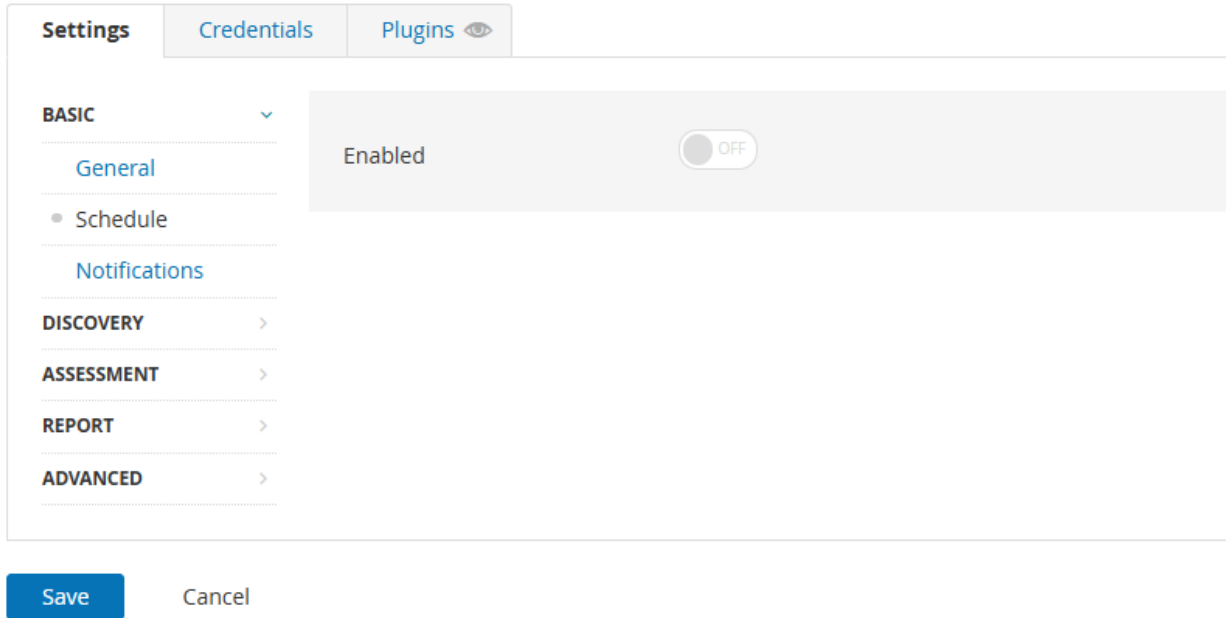
My Scans

Targets

192.168.1.2

Setting>Basic>Schedule keep default disable.

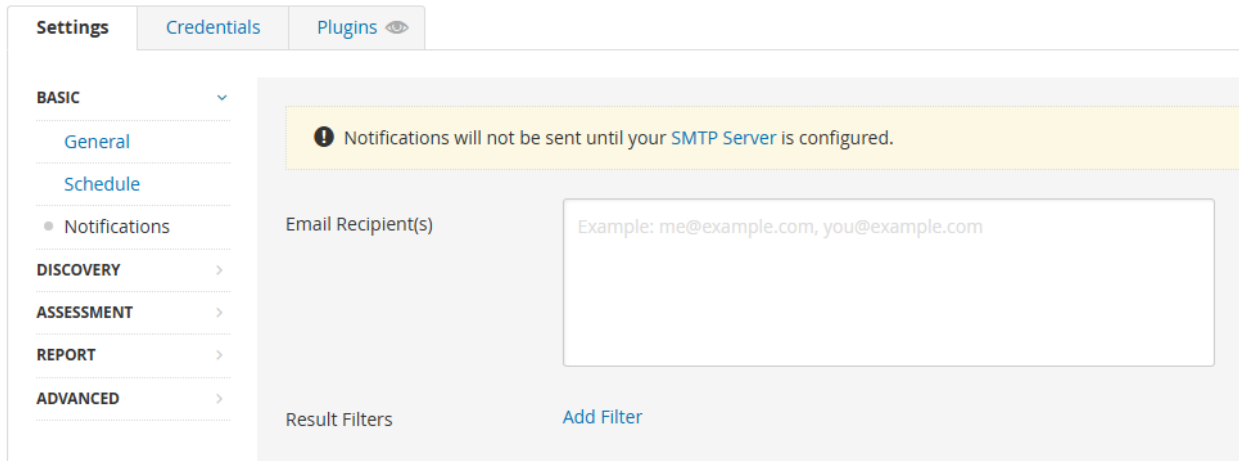
[← Back to Scan Report](#)



The screenshot shows the 'Settings' page with tabs for 'Settings', 'Credentials', and 'Plugins'. The 'BASIC' section is expanded, showing 'General', 'Schedule', and 'Notifications'. The 'Schedule' option is selected, and a toggle switch is shown in the 'OFF' position. Below the settings are 'Save' and 'Cancel' buttons.

Settings>Basic>Notification keep default disable.

[← Back to Scan Report](#)



The screenshot shows the 'Settings' page with tabs for 'Settings', 'Credentials', and 'Plugins'. The 'BASIC' section is expanded, showing 'General', 'Schedule', and 'Notifications'. The 'Notifications' option is selected. A yellow warning banner at the top states: 'Notifications will not be sent until your SMTP Server is configured.' Below this, there is a text input field for 'Email Recipient(s)' with the placeholder text 'Example: me@example.com, you@example.com'. At the bottom, there is a 'Result Filters' section with an 'Add Filter' button.

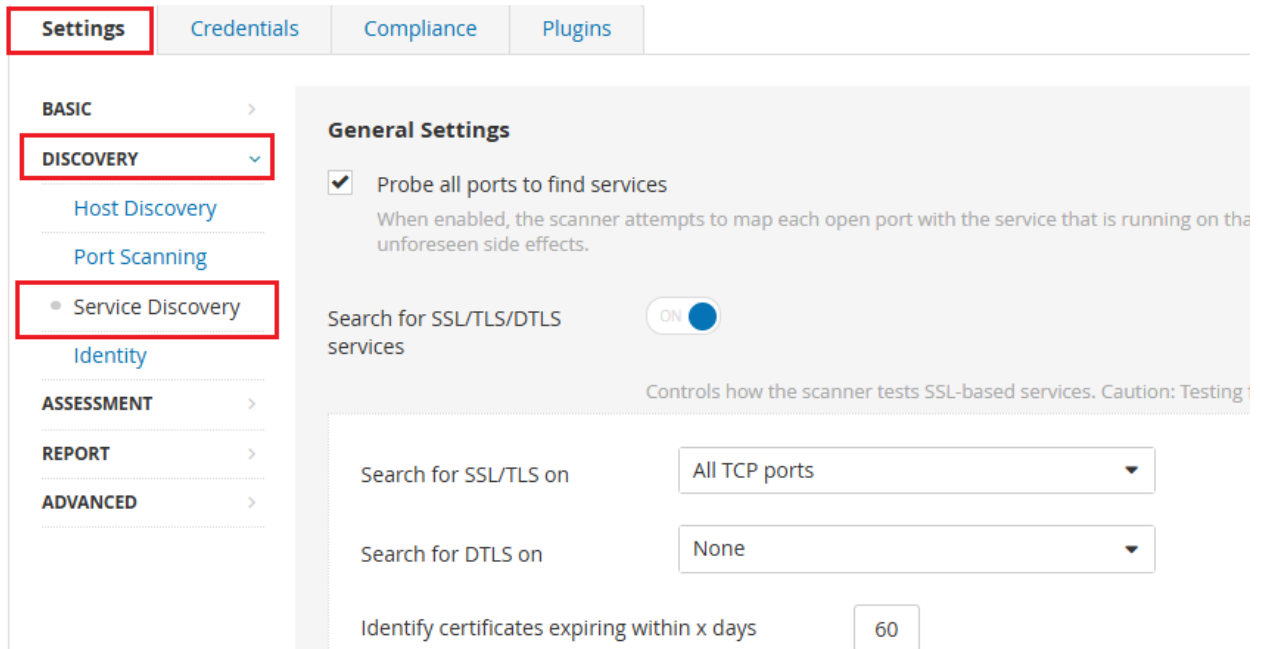
Settings>Basic>Discovery>Host Discovery keep default enable.

The screenshot shows the Nessus configuration interface. At the top, there are tabs for 'Settings', 'Credentials', 'Compliance', and 'Plugins'. The left sidebar has a tree view with 'BASIC' expanded, 'DISCOVERY' selected, and 'Host Discovery' highlighted. The main content area is titled 'Remote Host Ping' and features a toggle switch labeled 'Ping the remote host' which is currently turned ON. Below this, there is a note: 'If set to On, the scanner pings remote hosts on multiple ports to determine remote hosts on multiple ports during the scan. Note: To scan VMware guests'. Underneath, the 'General Settings' section includes two options: 'Test the local Nessus host' (checked) and 'Use fast network discovery' (unchecked).

Setting>Discovery>Port Scanning keep default.

The screenshot shows the Nessus configuration interface. At the top, there are tabs for 'Settings', 'Credentials', 'Compliance', and 'Plugins'. The left sidebar has a tree view with 'BASIC' expanded, 'DISCOVERY' selected, and 'Port Scanning' highlighted. The main content area is titled 'Ports' and includes a checkbox for 'Consider unscanned ports as closed' (unchecked) with a note: 'When enabled, if a port is not scanned with a selected port scanner (for example, the port falls out)'. Below this is a text input field for 'Port Scan Range' containing the value 'default'. Underneath, the 'Local Port Enumerators' section includes a checked checkbox for 'SSH (netstat)'.

Setting>Discovery>Service Discovery keep default.



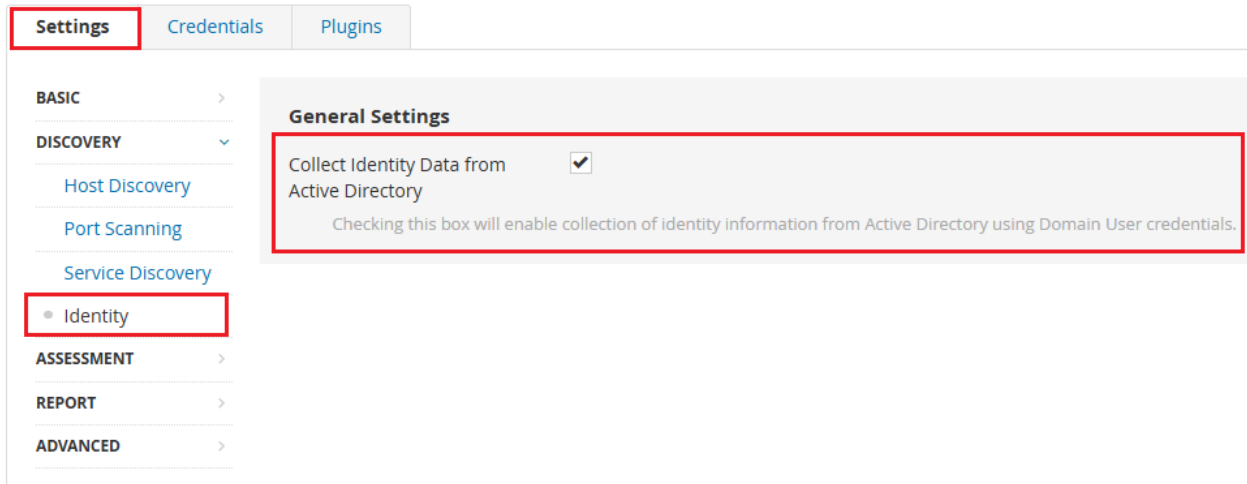
Settings | Credentials | Compliance | Plugins

BASIC >
DISCOVERY ▾
Host Discovery
Port Scanning
• Service Discovery
Identity
ASSESSMENT >
REPORT >
ADVANCED >

General Settings

- Probe all ports to find services
When enabled, the scanner attempts to map each open port with the service that is running on the unforeseen side effects.
- Search for SSL/TLS/DTLS services ON
- Search for SSL/TLS on
- Search for DTLS on
- Identify certificates expiring within x days

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



Settings | Credentials | Plugins

BASIC >
DISCOVERY ▾
Host Discovery
Port Scanning
Service Discovery
• Identity
ASSESSMENT >
REPORT >
ADVANCED >

General Settings

- Collect Identity Data from Active Directory
Checking this box will enable collection of identity information from Active Directory using Domain User credentials.

Setting>Assessment>General keep default.

Settings | Credentials | Plugins

BASIC >
DISCOVERY >
ASSESSMENT ▾
• General
Brute Force
Web Applications
Windows
Malware
Databases
REPORT >
ADVANCED >

Accuracy

- Override normal accuracy
- Avoid potential false alarms
- Show potential false alarms

Perform thorough tests (may disrupt your network or impact scan speed)
Causes various plugins to work harder. For example, when looking through SMB file shares, a plugin can be more thorough, the scan is more intrusive and is more likely to disrupt the network, while potential

Antivirus

Antivirus definition grace period (in days): 0 ▾

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

Settings | Credentials | Plugins

BASIC >
DISCOVERY >
ASSESSMENT ▾
General
Brute Force
Web Applications
• Windows
Malware
Databases
REPORT >
ADVANCED >

General Settings

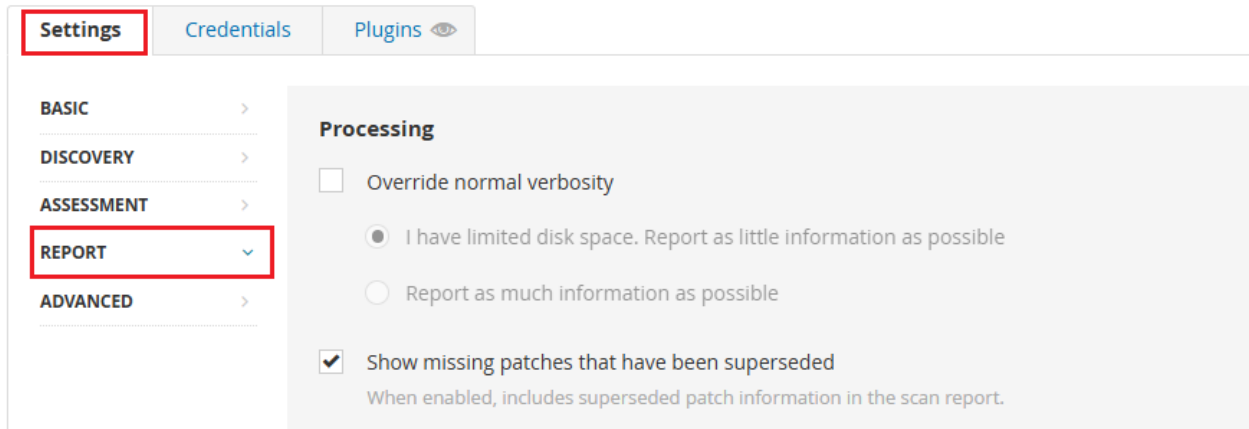
- Request information about the SMB Domain
If enabled, domain users are queried instead of local users.

User Enumeration Methods

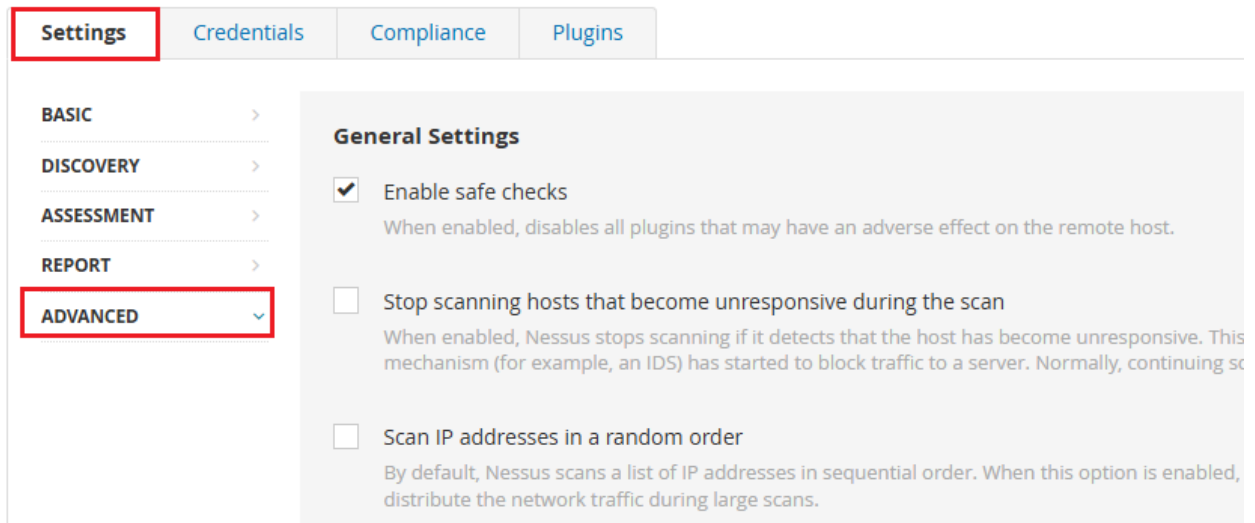
- SAM Registry
Nessus enumerates users via the Security Account Manager (SAM) registry.
- ADSI Query
Nessus enumerates users via Active Directory Service Interfaces (ADSI). To use ADSI, you must configure credentials under Credentials.
- WMI Query
Nessus enumerates users via Windows Management Interface (WMI).

RID Brute Forcing OFF
Nessus enumerates users via relative identifier (RID) brute forcing. Enabling this setting enables

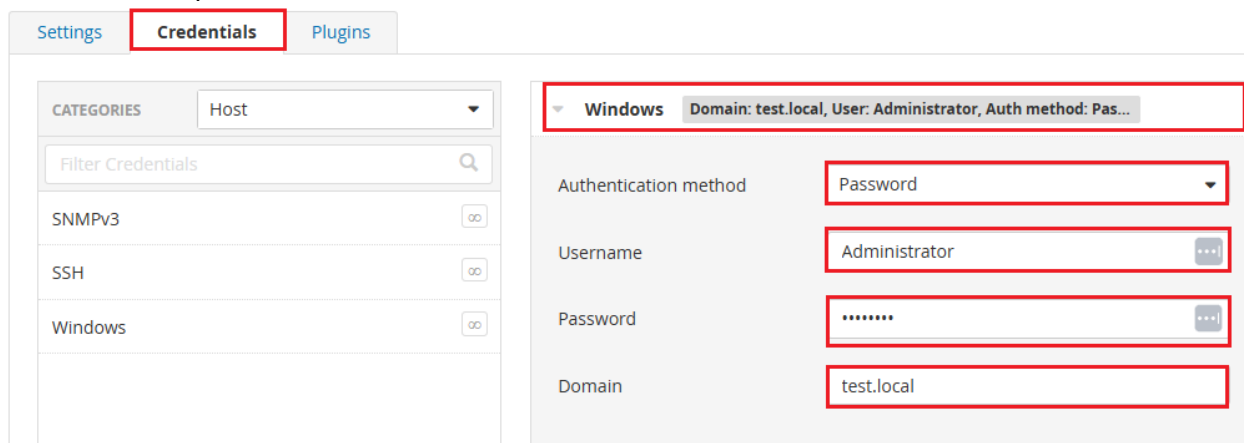
Settings>Report keep the default.



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.

Settings	Credentials	Plugins
ENABLED	MacOS X Local Security Checks	27
ENABLED	MarinerOS Local Security Checks	3
ENABLED	Misc.	1226
ENABLED	Oracle Linux Local Security Checks	11
ENABLED	Palo Alto Local Security Checks	5
ENABLED	PhotonOS Local Security Checks	13
ENABLED	Policy Compliance	6
ENABLED	Red Hat Local Security Checks	57
ENABLED	Service detection	3
ENABLED	Settings	9

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

Settings | Credentials | Plugins

BASIC ▾

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >


Name: AD-Advanced-Scan

Description:

Folder: My Scans

Targets: 192.168.1.2

Upload Targets [Add File](#)

 **Save** Cancel

After complete the scan, in **Hosts** Tab.

AD-Advanced-Scan

[← Back to All Scans](#)

Hosts **1** Vulnerabilities 348 Remediations 10 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.1.2	85 High, 103 Critical, 17 Medium, 241 Info

Under **Vulnerabilities** Tab it shows almost 348

Hosts 1 **Vulnerabilities 348** Remediations 10 History 1

Filter Search Vulnerabilities 348 Vulnerabilities

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

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: May 4 at 7:30 PM
End: May 4 at 7:47 PM
Elapsed: 17 minutes

Vulnerabilities



Under Remediation Tab.

AD-Advanced-Scan

[← Back to All Scans](#)

Hosts 1 Vulnerabilities 348 **Remediations 10** History 1

Search Actions 10 Actions

Action
KB4570333: Windows 10 Version 1809 and Windows Server 2019 September 2020 Security Update: Apply Cumulative Update KB4570333.
Mozilla Firefox < 138.0: Upgrade to Mozilla Firefox version 138.0 or later.
Install KB5055519
Security Updates for Microsoft .NET Framework (January 2025): Microsoft has released security updates for Microsoft .NET Framework.
Adobe Flash Player <= 32.0.0.433 (APSB20-58): Upgrade to Adobe Flash Player version 32.0.0.445 or later.
7-Zip < 24.09 (ZDI-25-045): Upgrade to 7-Zip version 24.09 or later.
PuTTY < 0.81 Key Recovery Attack Vulnerability: Upgrade to PuTTY version 0.81 or later.
WinSCP < 6.3.3 Key Recovery Attack Vulnerability: Upgrade to WinSCP version 6.3.3 or later.
Curl Use-After-Free < 7.87 (CVE-2022-43552): Upgrade Curl to version 7.87.0 or later
KB4580325: Security update for Adobe Flash Player (October 2020): Microsoft has released KB4580325 to address this issue.