Phase 3. Identify Vulnerabilities

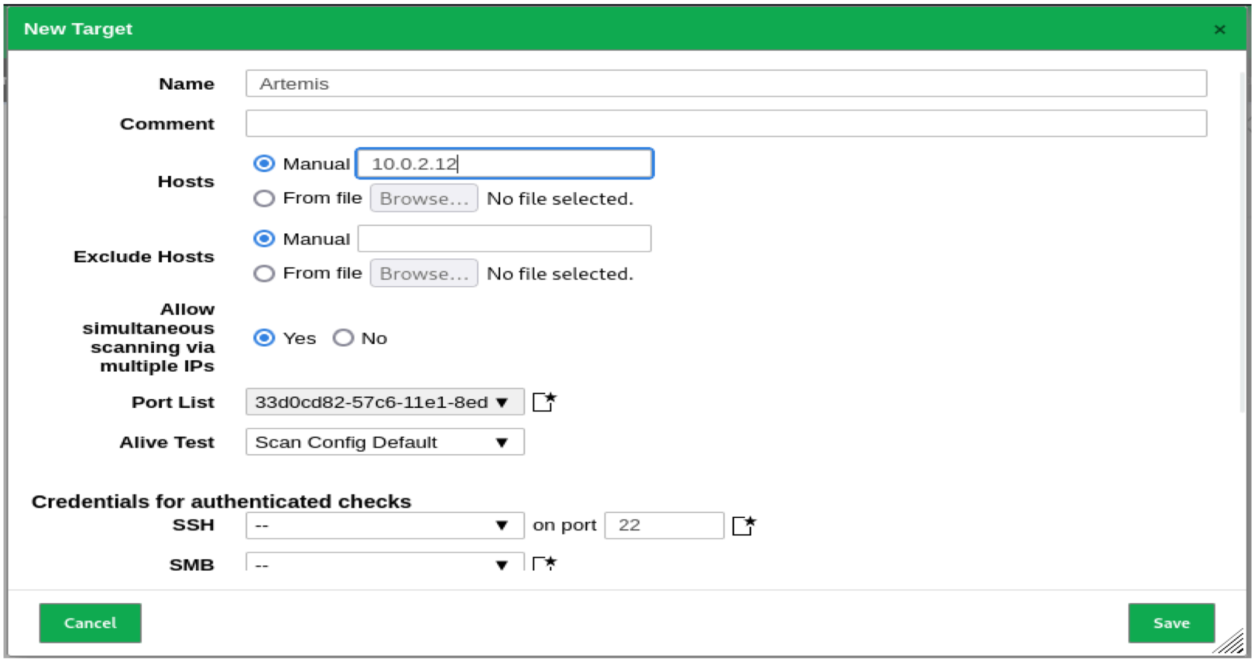
Objective

The primary goal is to identify vulnerabilities within the network using a variety of specialized tools. This phase involves scanning for vulnerabilities in different technologies, platforms, and services.

Procedure

1. OpenVAS: OpenVAS is a free, open-source tool for scanning networks, systems, and software for vulnerabilities. It features a comprehensive database of vulnerability signatures and provides detailed reports with risk ratings, CVSS values, and CVE numbers. While it's powerful, it can be challenging for non-technical users to configure and use, and its database may not always have the latest vulnerabilities.

Configuring target:



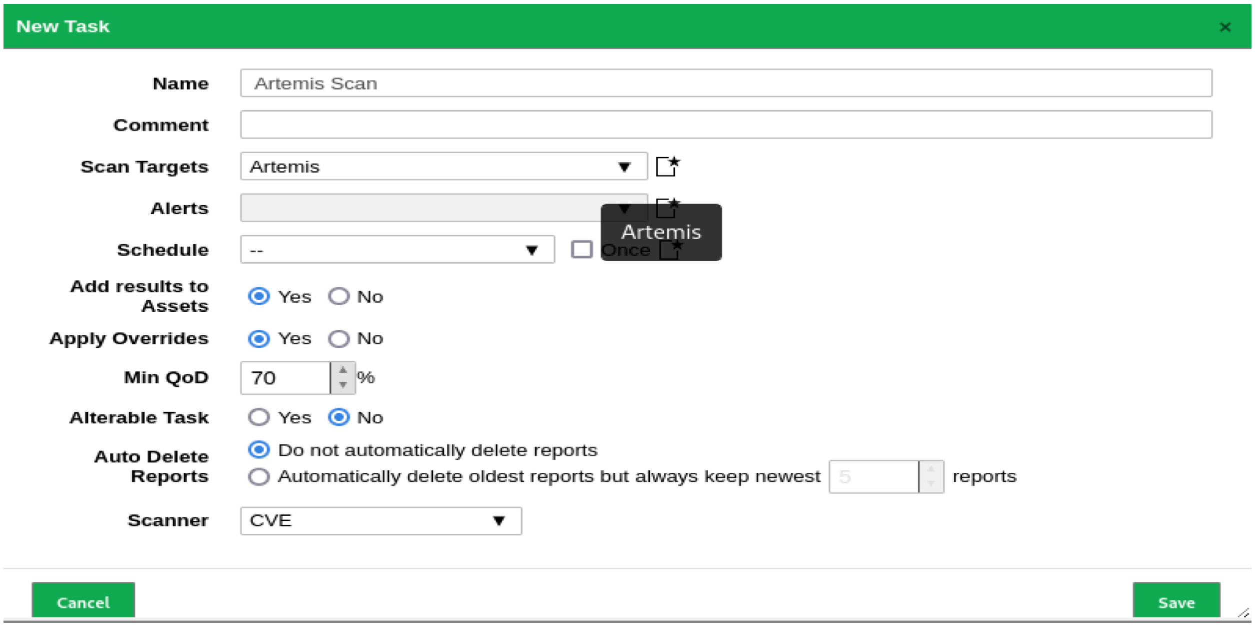
New Target ×

Name	Artemis
Comment	
Hosts	● Manual 10.0.2.12 ○ From file Browse… No file selected.
Exclude Hosts	● Manual ○ From file Browse… No file selected.
Allow simultaneous scanning via multiple IPs	● Yes ○ No
Port List	33d0cd82-57c6-11e1-8ed ▼
Alive Test	Scan Config Default ▼

Credentials for authenticated checks

SSH	-- ▼ on port 22
SMB	-- ▼

Configuring scan:

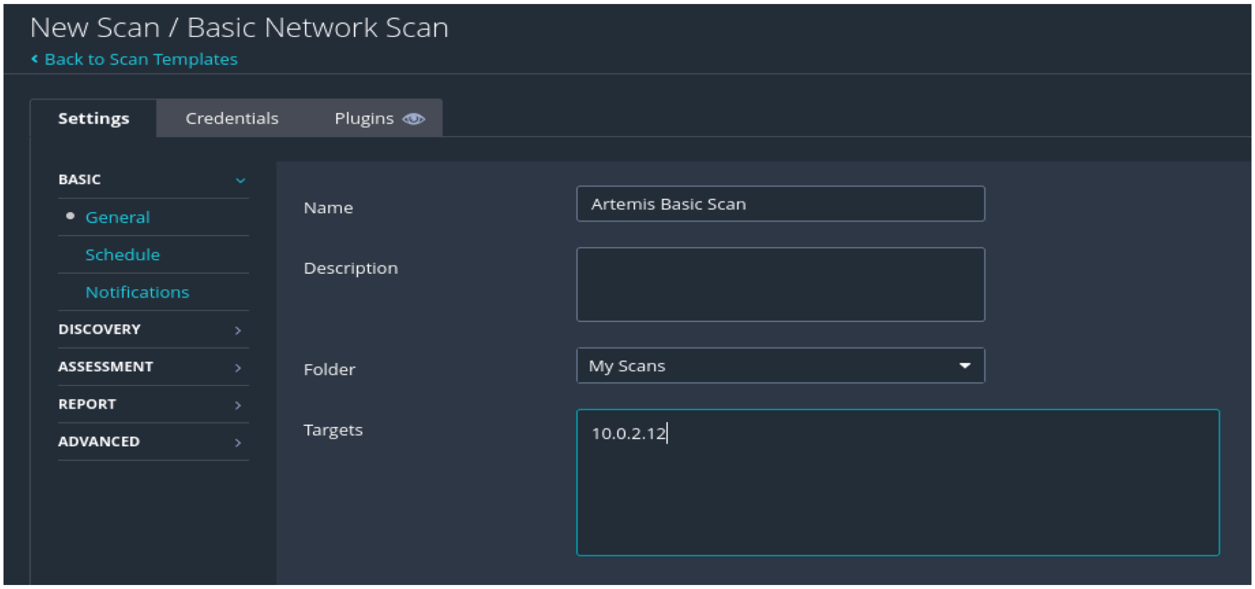


New Task ×

Name	Artemis Scan
Comment	
Scan Targets	Artemis ▼
Alerts	▼
Schedule	-- ▼ □ Once
Add results to Assets	● Yes ○ No
Apply Overrides	● Yes ○ No
Min QoD	70 %
Alterable Task	○ Yes ● No
Auto Delete Reports	● Do not automatically delete reports ○ Automatically delete oldest reports but always keep newest 5 reports
Scanner	CVE ▼

2. Nessus: Tenable Nessus is a powerful vulnerability scanning tool. Nessus can be used to to complete a basic or advanced network scan, web application scans and other scans to measure security controls' effectiveness. Nessus comes with an extensive vulnerability database and various scanning options and plugins which makes it a robust tool for scanning. However, it's enterprise edition can be costly for large networks.

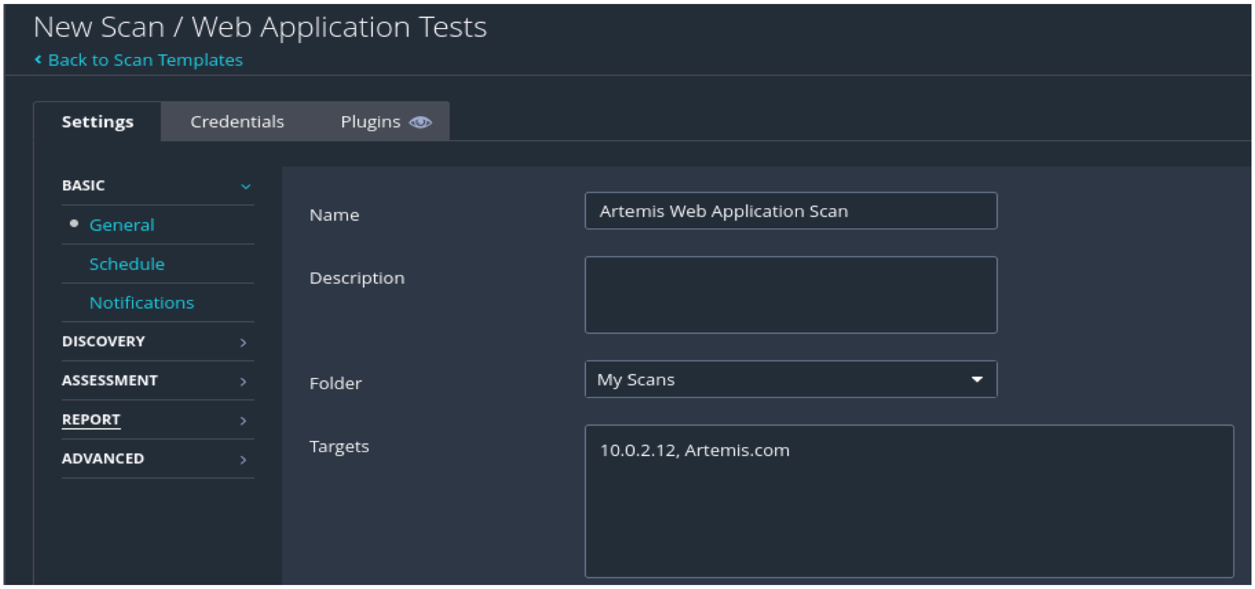
Basic scan configuration:



New Scan / Basic Network Scan

Name	Artemis Basic Scan
Description	
Folder	My Scans
Targets	10.0.2.12

Web application scan configuration:



New Scan / Web Application Tests

Name: Artemis Web Application Scan

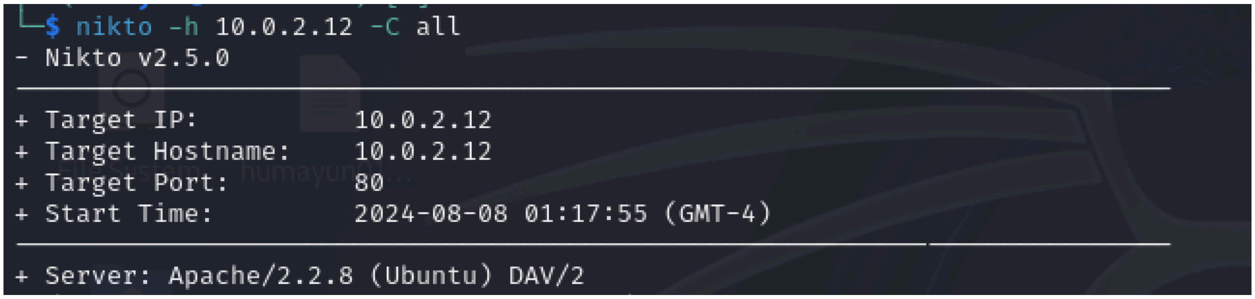
Description:

Folder: My Scans

Targets: 10.0.2.12, Artemis.com

3. Nikto: Nikto is a web server scanner that identifies vulnerabilities and misconfigurations in web servers and web applications. Although it is a very simple and easy to use, it is not accurate all the time.

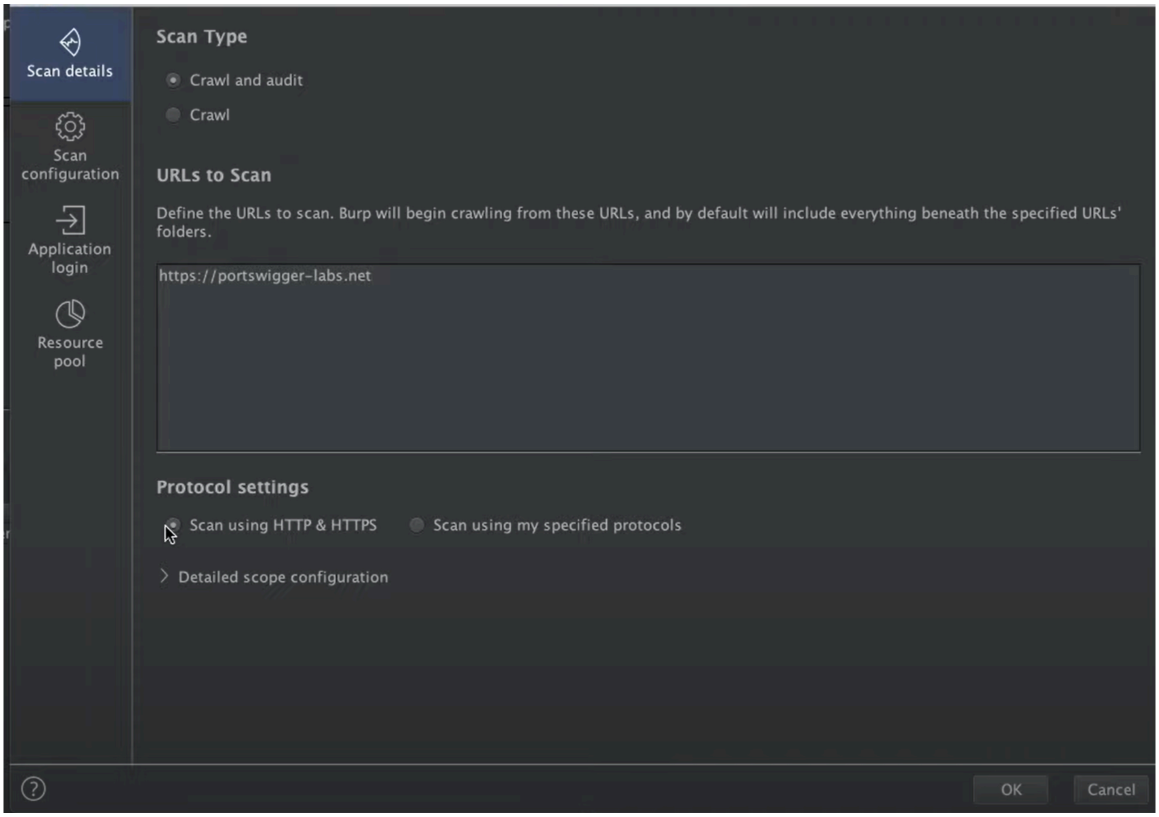
Nikto Scan:



```
└─$ nikto -h 10.0.2.12 -C all
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.12
+ Target Hostname:    10.0.2.12
+ Target Port:        80
+ Start Time:         2024-08-08 01:17:55 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
```

4. Burp Suite: Burp Suite is as web vulnerability scanner for identifying security flaws in web applications. It can intercept and capture HTTP request and response for analysis and can list vulnerabilities when discovered. Burp Suite has powerful scanning capabilities and extensive plugin support. However, learning how to use burp Suite as a beginner can be difficult and a lot of important features are only available in paid version.

Configuring Burp Suite:



Scan Type

● Crawl and audit

○ Crawl

URLs to Scan

Define the URLs to scan. Burp will begin crawling from these URLs, and by default will include everything beneath the specified URLs' folders.

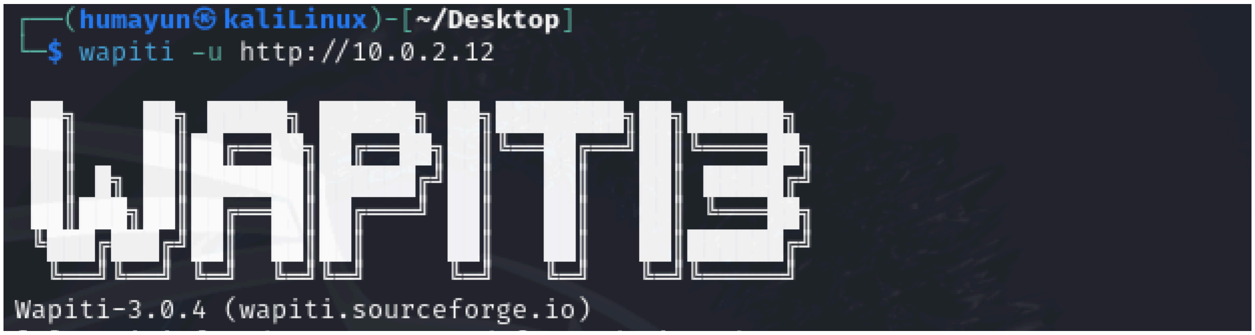
https://portswigger-labs.net

Protocol settings

● Scan using HTTP & HTTPS ○ Scan using my specified protocols

> Detailed scope configuration

5. Wapiti: Wapiti is a web application vulnerability scanner that tests web application for security issues such as SQL injection, XSS, file inclusion and more. It is free and simple but less comprehensive than Burp Suite.



```
┌──(humayun㉿kaliLinux)-[~/Desktop]
└─$ wapiti -u http://10.0.2.12

Wapiti-3.0.4 (wapiti.sourceforge.io)
```

Conclusion

These tools provide a robust framework for identifying vulnerabilities within the network. Each tool offers unique features and strengths, allowing for comprehensive scanning and vulnerability assessment. By using a combination of these tools, we can thoroughly identify and address security weaknesses across different platforms and technologies.