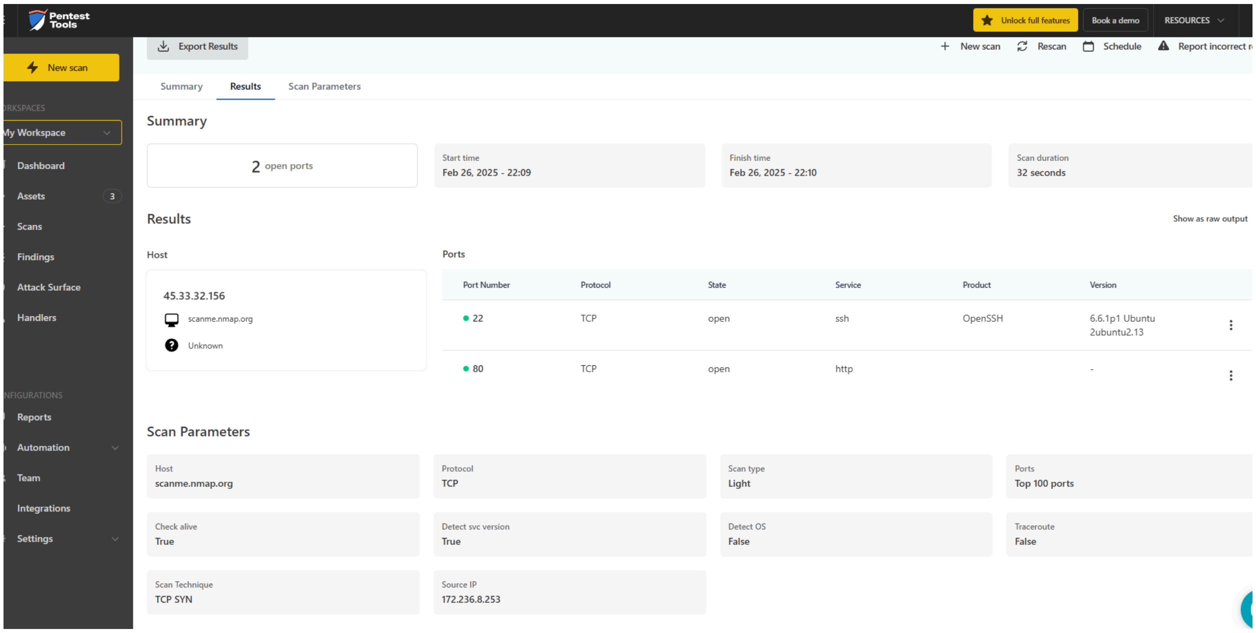
In this short lab I will be performing a port scan and a website scan using online penetration tools. The website I will be using is pentest-tools.com.
After creating a free account, I select new-scan and Port-scanner entering the address scanme-nmap.org. After completing a default scan I receive information such as the service name and port status.



Summary

2 open ports

Start time
Feb 26, 2025 - 22:09

Finish time
Feb 26, 2025 - 22:10

Scan duration
32 seconds

Results

Host

45.33.32.156
scanme.nmap.org
Unknown

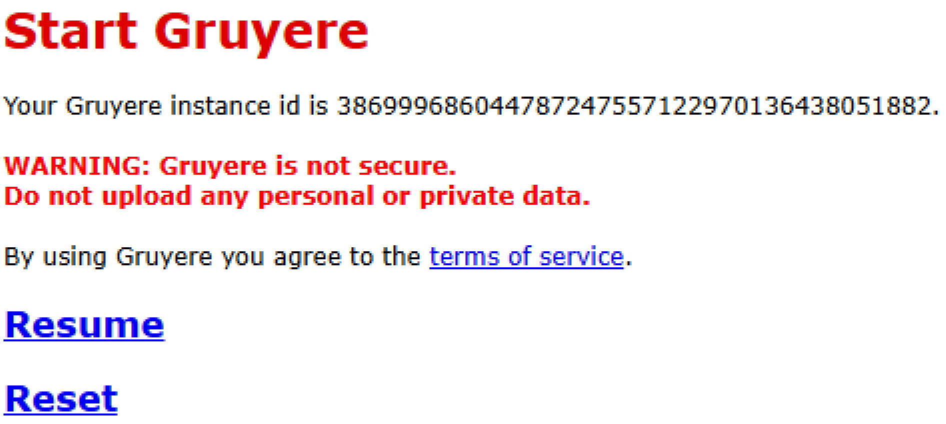
Ports

Port Number	Protocol	State	Service	Product	Version
22	TCP	open	ssh	OpenSSH	6.6.1p1 Ubuntu 2ubuntu2.13
80	TCP	open	http		-

Scan Parameters

Host: scanme.nmap.org
Protocol: TCP
Scan type: Light
Ports: Top 100 ports
Check alive: True
Detect svc version: True
Detect OS: False
Traceroute: False
Scan Technique: TCP SYN
Source IP: 172.236.8.253

Next I will scan the website https://google-gruyere.appspot.com/ using the website vulnerability scanner.



Start Gruyere

Your Gruyere instance id is 386999686044787247557122970136438051882.

WARNING: Gruyere is not secure.
Do not upload any personal or private data.

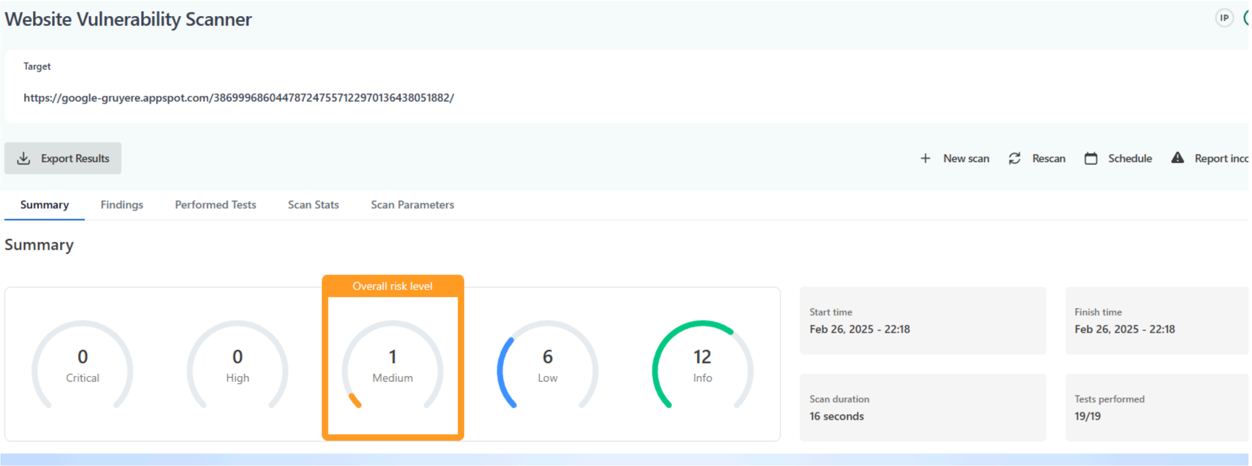
By using Gruyere you agree to the terms of service.

Resume

Reset

Completing a website vulnerability scan on my instance shows several different vulnerabilities including:

- Insecure cookie setting: missing Secure flag
- Missing security header: X-Content-Type-Options
- Missing security header: Referrer-Policy
- Missing security header: Strict-Transport-Security
- Robots.txt file found
- Server software and technology found



Website Vulnerability Scanner

Target

https://google-gruyere.appspot.com/386999686044787247557122970136438051882/

Summary

0 Critical

0 High

1 Medium

6 Low

12 Info

Start time
Feb 26, 2025 - 22:18

Finish time
Feb 26, 2025 - 22:18

Scan duration
16 seconds

Tests performed
19/19