

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.

The screenshot displays the Pentest Tools web interface. The top navigation bar includes a 'New scan' button and links for 'Export Results', 'New scan', 'Rescan', 'Schedule', and 'Report incorrect'. The left sidebar contains a 'My Workspace' dropdown and a list of tools: Dashboard, Assets, Scans, Findings, Attack Surface, Handlers, Reports, Automation, Team, Integrations, and Settings. The main content area is divided into three sections: Summary, Results, and Scan Parameters. The Summary section shows '2 open ports', 'Start time: Feb 26, 2025 - 22:09', 'Finish time: Feb 26, 2025 - 22:10', and 'Scan duration: 32 seconds'. The Results section shows a table of open ports for the host 45.33.32.156 (scanme-nmap.org). The Scan Parameters section shows the scan configuration: 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: 172.236.0.253.

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

Host	Protocol	Scan type	Ports
scanme-nmap.org	TCP	Light	Top 100 ports

Check alive	Detect svc version	Detect OS	Traceroute
True	True	False	False

Scan Technique	Source IP
TCP SYN	172.236.0.253

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

