

Network_Security_Audit_Report_ Banupriya.pdf

Network Security Audit Report

INTRODUCTION

Network security audit is a process of evaluating the security of a network infrastructure to identify vulnerabilities, risks, and misconfigurations. This audit helps organizations understand their security posture and improve protection against cyber threats.

OBJECTIVE

The objectives of this audit are:

- To identify open ports and running services
- To analyze network exposure
- To evaluate SSL/TLS security
- To provide security recommendations

SCOPE OF AUDIT

- Target: scanme.nmap.org
- Audit Type: External Network Security Audit
- Platform Used: Android Mobile
- Tools: Online scanning tools

TOOLS USED

- Pentest-Tools (Online Port Scanner)
- Qualys SSL Labs (SSL/TLS Security Test)
- Web Browser (Google Chrome)
- Android Mobile Device

METHODOLOGY

The audit was conducted using passive and active scanning techniques. Online Nmap scanner was used to identify open ports and services. SSL Labs tool was used to analyze encryption strength and HTTPS configuration.

SCAN RESULTS

◆ Port Scan Results:

Port - 22

Service - SSH

Description - Remote login service

Port - 80

Service - HTTP

Description - Web service (unencrypted)

Port - 443

Service - HTTPS

Description - Secure web service

FINDINGS

- The target system has limited open ports
- SSH service can be targeted for brute force attacks if not secured
- HTTP service may expose data without encryption
- HTTPS is enabled which improves security

RECOMMENDATIONS

- Disable unused ports and services
- Use strong authentication for SSH
- Redirect HTTP traffic to HTTPS
- Regularly conduct network audits
- Implement firewall and IDS/IPS systems



Free Port Scanne...

pentest-tools.com



Pentest
Tools

Free sign up



> [Port Scanner](#) > [Scans](#) >



Free Port Scanner Report (Light)

Port Scanner (Light)

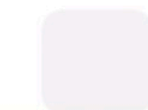
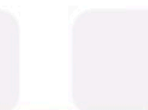
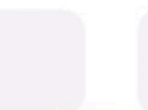
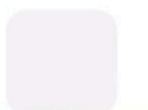
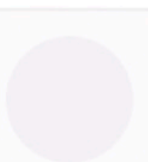
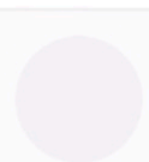
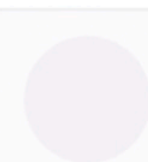
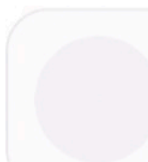
... Waiting

Target

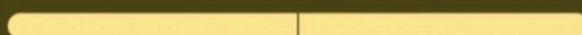
scanme.nmap.org

Waiting...

0%



2/2 daily free scans available



AI Scanner



Pentest
Tools

Free sign up



Port Scanner with Nmap

Light

Deep

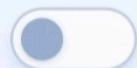
Target

IP or Hostname

Scan options



Detect service version



Detect operating system

Protocol



TCP



UDP

Port selection



Common ports



List of ports



Scan finished



Your scan for scanme.nmap.org has
finished successfully.



AI Scanner

Port selection

☒ Common ports ☐ List of ports



Scan finished



Your scan for scanme.nmap.org has finished successfully.

The port scanning process was carried out on the target system scanme.nmap.org using the Pentest-Tools online port scanner. The scan was completed successfully and provided a summary of open ports detected on the system.

Port Scanner Report (Light)



Unlock the full capabilities of this scanner



See what the DEEP scanner can do

Perform full port scanning with additional options.

Options	Light scan	Deep scan
Top 100 ports	✓	✓
All 65535 ports	✗	✓
Single IP or hostname	✓	✓
Detect service version	✓	✓
Detect operating system	✗	✓
Traceroute	✗	✓

✓ scanme.nmap.org



The Light Port Scanner ran on a limited set of ports. [Upgrade to run Deep scans](#) and check for all 65535 ports.

Found 2 open ports (1 host)



45.33.32.156

> scanme.nmap.org

Port Number	Protocol	State	Service Name	Service Product	Service Version	Service Extra Info
22	TCP	open	ssh	OpenSSH	6.6.1p1 Ubuntu 2ubuntu2.13	Ubuntu Linux; protocol 2.0
80	TCP	open	http	Apache httpd	2.4.7	(Ubuntu)

Scan parameters

Host: scanme.nmap.org
Protocol: TCP
Scan type: Custom
Ports: Top 100 ports
Check alive: False
Detect service version: True
Detect OS: False
Traceroute: False
Scan Technique: TCP SYN

Scan information

1 / 2

Start time: Feb 03, 2026 / 08:35:31 UTC+02
Finish time: Feb 03, 2026 / 08:35:49 UTC+02
Scan duration: 18 sec
Scan status: Finished

The results of the port scan revealed that port 22 (SSH) and port 80 (HTTP) are open and running on the target system. These open ports indicate that the corresponding services are active and accessible over the network.



AI Scanner



SSL Server Test (... ssllabs.com



Qualys. SSL Labs

[Home](#)

[Projects](#)

[Qualys Free Trial](#)

[Contact](#)

You are here: [Home](#) > [Projects](#) > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.

Hostname:

Submit

☐ Do not show the results on the boards

Recently Seen

[certif.micromedexcloud](#)
[hewlett.de](#)
[s9-r-u-in-cert-2.micromedexcloud](#)
[certif.cloud.hewlett.de](#)
[certif.hewlett.de](#)
[www.sironia.com.br](#)
[www.sironia.com.br](#)
[www.sironia.com.br](#)
[www.sironia.com.br](#)
[www.sironia.com.br](#)

Recent Best

[www.certif.micromedexcloud](#) A+
[www.micromedexcloud.com](#) A+
[www.hewlett.de](#) A+
[www.sironia.com](#) A+
[www.ad.fr](#) A+
[www.hewlett.de](#) A
[www.hewlett.de](#) A-
[www.ad.fr](#) A-
[www.ad.fr](#) B
[www.ad.fr](#) B

Recent Worst

[www.ad.fr](#) T
[www.ad.fr](#) T
[www.ad.fr](#) T
[www.ad.fr](#) T
[www.ad.fr](#) T
[www.ad.fr](#) F
[www.ad.fr](#) T
[www.ad.fr](#) T
[www.ad.fr](#) F
[www.ad.fr](#) T
[www.ad.fr](#) T

SSL Report v2.4.1

Copyright © 2009-2020 Qualys, Inc. All Rights Reserved. [Privacy Policy](#)

[Terms and Conditions](#)

[Try Qualys Free Trial](#) Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.



AI Scanner

SSL Server Test

SSL Server Test: ...

ssllabs.com

Qualys. SSL Labs

[Home](#)
[Projects](#)
[Qualys Free Trial](#)
[Contact](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [scanme.nmap.org](#)

SSL Report: scanme.nmap.org

Assessed on: Tue, 09 Feb 2026 06:42:09 UTC | [Hide](#) | [Clear cache](#)

[Scan Another >>](#)

	Server	Test time	Grade
1	2600:3c01:0:0:f03c:91ff:fe18:1b2f scanme.nmap.org Unable to connect to the server	Tue, 09 Feb 2026 06:42:01 UTC Duration: 0.129 sec	
2	45.99.92.156 scanme.nmap.org Unable to connect to the server	Tue, 09 Feb 2026 06:42:09 UTC Duration: 0.116 sec	

SSL Report v3.4.1

Copyright © 2009-2026 Qualys, Inc. All Rights Reserved. [Privacy Policy](#)

[Try Qualys Free Trial](#) Experience the award-winning [Qualys Cloud Platform](#) and the entire collection of [Qualys Cloud Apps](#), including [certificate security](#) solutions.

[Terms and Conditions](#)

An SSL/TLS security assessment was performed using Qualys SSL Labs. The analysis showed that the target system does not primarily expose secure HTTPS services. This is acceptable since the target system is intended for testing and demonstration purposes.

- The target system has open TCP ports.
- SSH and HTTP services are actively running.
- Open ports can become potential security risks if misconfigured.

Conclusion

This project successfully demonstrated a basic port scanning and security analysis process using online penetration testing tools. The results highlight the importance of identifying open ports and understanding their security implications to improve overall system security.

Submitted by
Banupriya B

