



**gym**

---

Report generated by Tenable Nessus™

Wed, 05 Feb 2025 13:10:59 India Standard Time

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

- 192.124.249.4.....4

Nessus Essentials

---

## Vulnerabilities by Host

---

192.124.249.4



Scan Information

Start time: Wed Feb 5 13:02:22 2025  
End time: Wed Feb 5 13:10:59 2025

Host Information

DNS Name: cloudproxy10004.sucuri.net  
IP: 192.124.249.4

Vulnerabilities

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.  
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/80/www

Port 80/tcp was found to be open

## 11219 - Nessus SYN scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

### Plugin Output

tcp/443/www

Port 443/tcp was found to be open

## 19506 - Nessus Scan Information

### Synopsis

This plugin displays information about the Nessus scan.

### Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).

- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

## Solution

---

n/a

## Risk Factor

---

None

## Plugin Information

---

Published: 2005/08/26, Modified: 2024/12/31

## Plugin Output

---

tcp/0

Information about this scan :

```

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202502050117
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : gym
Scan policy used : Web Application Tests
Scanner IP : 192.168.49.232
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 277.686 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled

```

```
Web app tests - Test mode : single
Web app tests - Try all HTTP methods : no
Web app tests - Maximum run time : 5 minutes.
Web app tests - Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/2/5 13:02 India Standard Time (UTC +05:30)
Scan duration : 507 sec
Scan for malware : no
```