



# FIA

---

Report generated by Tenable Nessus™

Tue, 11 Feb 2025 03:03:43 EST

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

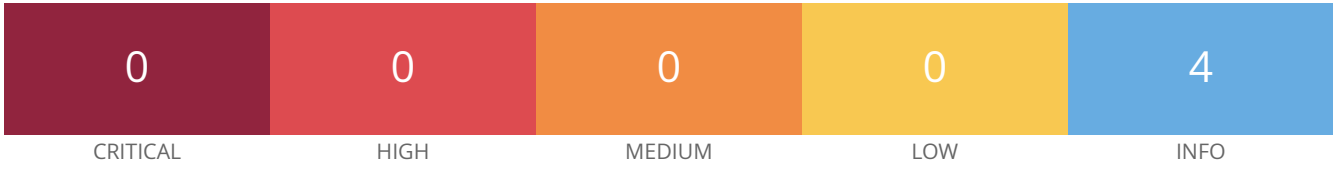
- fia.gov.pk.....4

Nessus Essentials

---

## **Vulnerabilities by Host**

---



Scan Information

Start time: Tue Feb 11 02:54:11 2025  
End time: Tue Feb 11 03:03:43 2025

Host Information

DNS Name: fia.gov.pk  
IP: 43.250.84.226

Vulnerabilities

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

43.250.84.226 resolves as 43-250-84-226.reverse.ntc.net.pk.

### 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: 2025/02/10

### Plugin Output

---

tcp/443

```
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- Whether the display of superseded patches is enabled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 : 202502102343
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : FIA
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.65.133
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 557.636 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 : disabled
Web application tests : disabled
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 : 2025/2/11 2:54 EST (UTC -05:00)
Scan duration : 560 sec
Scan for malware : no
```



## 10287 - Traceroute Information

### Synopsis

It was possible to obtain traceroute information.

### Description

Makes a traceroute to the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

### Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.65.133 to 43.250.84.226 :
192.168.65.133
192.168.65.2
43.250.84.226
?
43.250.84.226

Hop Count: 5
```