



NUCES

Report generated by Tenable Nessus™

Tue, 11 Feb 2025 02:50:08 EST

TABLE OF CONTENTS

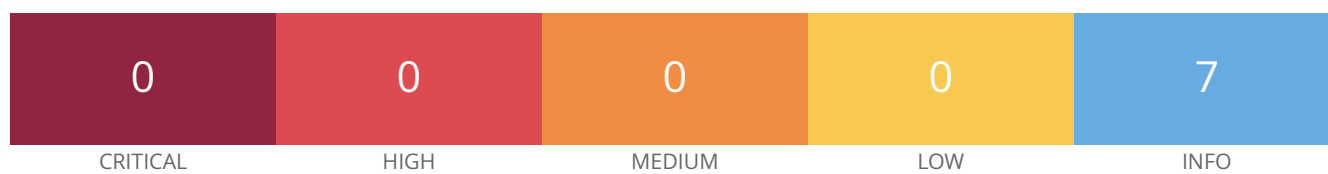
Vulnerabilities by Host

• nu.edu.pk.....	4
------------------	---

Nessus Essentials

Vulnerabilities by Host

nu.edu.pk



Scan Information

Start time: Tue Feb 11 02:41:38 2025

End time: Tue Feb 11 02:50:08 2025

Host Information

DNS Name: nu.edu.pk

IP: 203.124.44.78

OS: CISCO PIX 7.0

Vulnerabilities

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

<http://cpe.mitre.org/>

<https://nvd.nist.gov/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/02/10

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:cisco:pix_firewall:7.0 -> Cisco PIX Firewall Software

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : firewall  
Confidence level : 70
```

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

```
203.124.44.78 resolves as host2021228.comsatshosting.com.
```

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/5060

```
Port 5060/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 : NUCES
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.65.133
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 122.242 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 2:41 EST (UTC -05:00)
Scan duration : 500 sec
Scan for malware : no
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : CISCO PIX 7.0  
Confidence level : 70  
Method : SinFP
```

```
The remote host is running CISCO PIX 7.0
```

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 203.124.44.78 :  
192.168.65.133  
192.168.65.2  
203.124.44.78
```

```
Hop Count: 2
```