

# Nessus Report

Nessus Scan Report

Mon, 22 Aug 2016 20:49:46 IST

# Table Of Contents

Vulnerabilities By Host..... 3

    •test-proof.weboapps.com.....4

## Vulnerabilities By Host

| test-proof.weboapps.com  |      |   |     |      |       |  |
|--|------|---|-----|------|-------|--|
| Scan Information   |      |   |     |      |       |  |
| Start time:  |      | Mon Aug 22 20:35:13 2016                  |     |      |       |  |
| End time:  |      | Mon Aug 22 20:49:46 2016                  |     |      |       |  |
| Host Information   |      |   |     |      |       |  |
| DNS Name:  |      | ec2-52-23-179-239.compute-1.amazonaws.com |     |      |       |  |
| IP:  |      | 52.23.179.239                             |     |      |       |  |
| Results Summary  |      |   |     |      |       |  |
| Critical   | High | Medium                                    | Low | Info | Total |  |
| 0  | 0    | 2   | 2   | 22   | 26    |  |
| Results Details  |      |   |     |      |       |  |
| 0/tcp  |      |   |     |      |       |  |
| 25220 - TCP/IP Timestamps Supported  |      |   |     |      |       |  |
| Synopsis   |      |   |     |      |       |  |
| The remote service implements TCP timestamps.  |      |   |     |      |       |  |
| Description  |      |   |     |      |       |  |
| The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed. |      |   |     |      |       |  |
| See Also   |      |   |     |      |       |  |
| <a href="http://www.ietf.org/rfc/rfc1323.txt">http://www.ietf.org/rfc/rfc1323.txt</a>  |      |   |     |      |       |  |
| Solution   |      |   |     |      |       |  |
| n/a  |      |   |     |      |       |  |
| Risk Factor  |      |   |     |      |       |  |
| None   |      |   |     |      |       |  |
| Plugin Information:  |      |   |     |      |       |  |
| Publication date: 2007/05/16, Modification date: 2011/03/20  |      |   |     |      |       |  |
| Ports  |      |   |     |      |       |  |
| tcp/0  |      |   |     |      |       |  |
| 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 FQDN of the remote host.  |      |   |     |      |       |  |
| Solution   |      |   |     |      |       |  |
| n/a  |      |   |     |      |       |  |
| Risk Factor  |      |   |     |      |       |  |
| None   |      |   |     |      |       |  |
| Plugin Information:  |      |   |     |      |       |  |
| Publication date: 2004/02/11, Modification date: 2012/09/28  |      |   |     |      |       |  |
| Ports  |      |   |     |      |       |  |
| tcp/0  |      |   |     |      |       |  |
| 52.23.179.239 resolves as ec2-52-23-179-239.compute-1.amazonaws.com.   |      |   |     |      |       |  |
| 45590 - Common Platform Enumeration (CPE)  |      |   |     |      |       |  |
| Synopsis   |      |   |     |      |       |  |

It is 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/cpe.cfm>

## Solution

n/a

## Risk Factor

None

## Plugin Information:

Publication date: 2010/04/21, Modification date: 2014/11/20

## Ports

**tcp/0**

Following application CPE's matched on the remote system :

```
cpe:/a:openbsd:openssh:6.6 -> OpenBSD OpenSSH 6.6
cpe:/a:igor_sysoev:nginx:1.9.14
```

## 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.
- Whether credentialed or third-party patch management checks are possible.
- 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:

Publication date: 2005/08/26, Modification date: 2016/04/08

### Ports

**tcp/0**

Information about this scan :

```
Nessus version : 6.8.1
Plugin feed version : 201608191930
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Basic Network Scan
Scanner IP : 10.0.3.89
Port scanner(s) : nessus_syn_scanner
```

Port range : default  
Thorough tests : no  
Experimental tests : no  
Paranoia level : 1  
Report verbosity : 1  
Safe checks : yes  
Optimize the test : yes  
Credentialled checks : no  
Patch management checks : None  
CGI scanning : disabled  
Web application tests : disabled  
Max hosts : 30  
Max checks : 4  
Recv timeout : 5  
Backports : Detected  
Allow post-scan editing: Yes  
Scan Start Date : 2016/8/22 20:35 IST  
Scan duration : 873 sec

## 0/udp

### 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:

Publication date: 1999/11/27, Modification date: 2013/04/11

#### Ports

##### udp/0

For your information, here is the traceroute from 10.0.3.89 to 52.23.179.239 :

10.0.3.89  
10.0.0.1  
114.143.191.201  
182.156.79.10  
10.117.225.94  
14.141.63.189  
?  
180.87.38.5  
80.231.217.29  
80.231.217.6  
80.231.130.85  
80.231.130.34  
66.198.70.82  
63.243.128.141  
213.248.87.25  
80.239.132.214  
52.93.4.99  
52.93.4.28  
54.239.41.220  
54.239.42.182  
?  
54.239.110.137  
54.239.108.199  
205.251.245.55  
72.21.222.155  
?

## 22/tcp

### 90317 - SSH Weak Algorithms Supported

#### Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

#### Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

### See Also

<https://tools.ietf.org/html/rfc4253#section-6.3>

### Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

### Risk Factor

Medium

### CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

### Plugin Information:

Publication date: 2016/04/04, Modification date: 2016/04/26

### Ports

**tcp/22**

The following weak server-to-client encryption algorithms are supported :

```
arcfour
arcfour128
arcfour256
```

The following weak client-to-server encryption algorithms are supported :

```
arcfour
arcfour128
arcfour256
```

## 70658 - SSH Server CBC Mode Ciphers Enabled

### Synopsis

The SSH server is configured to use Cipher Block Chaining.

### Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

### Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

### Risk Factor

Low

### CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### CVSS Temporal Score

2.6 (CVSS2#E:ND/RL:ND/RC:ND)

### References

|             |               |
|-------------|---------------|
| <b>BID</b>  | 32319         |
| <b>CVE</b>  | CVE-2008-5161 |
| <b>XREF</b> | OSVDB:50035   |
| <b>XREF</b> | OSVDB:50036   |
| <b>XREF</b> | CERT:958563   |

**Plugin Information:**

Publication date: 2013/10/28, Modification date: 2016/05/12

**Ports****tcp/22**

The following client-to-server Cipher Block Chaining (CBC) algorithms are supported :

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

The following server-to-client Cipher Block Chaining (CBC) algorithms are supported :

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

**71049 - SSH Weak MAC Algorithms Enabled****Synopsis**

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

**Description**

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.  
Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

**Solution**

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

**Risk Factor**

Low

**CVSS Base Score**

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

**Plugin Information:**

Publication date: 2013/11/22, Modification date: 2016/04/04

**Ports****tcp/22**

The following client-to-server Message Authentication Code (MAC) algorithms are supported :

```
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
```

The following server-to-client Message Authentication Code (MAC) algorithms are supported :

```
hmac-md5
hmac-md5-96
```



hmac-md5-96-etm@openssh.com  
hmac-md5-etm@openssh.com  
hmac-sha1-96  
hmac-sha1-96-etm@openssh.com

## 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:

Publication date: 2009/02/04, Modification date: 2016/07/11

### Ports

#### tcp/22

Port 22/tcp was found to be open

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/03/17

### Ports

#### tcp/22

An SSH server is running on this port.

## 10267 - SSH Server Type and Version Information

### Synopsis

An SSH server is listening on this port.

### Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 1999/10/12, Modification date: 2016/07/11

### Ports

#### tcp/22

SSH version : SSH-2.0-OpenSSH\_6.6.1p1 Ubuntu-2ubuntu2.4  
SSH supported authentication : publickey

## 70657 - SSH Algorithms and Languages Supported

### Synopsis

An SSH server is listening on this port.

### Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2013/10/28, Modification date: 2014/04/04

### Ports

**tcp/22**

Nessus negotiated the following encryption algorithm with the server : aes128-cbc

The server supports the following options for kex\_algorithms :

```
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
```

The server supports the following options for server\_host\_key\_algorithms :

```
ecdsa-sha2-nistp256
ssh-dss
ssh-rsa
```

The server supports the following options for encryption\_algorithms\_client\_to\_server :

```
3des-cbc
aes128-cbc
aes128-ctr
aes128-gcm@openssh.com
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
aes256-gcm@openssh.com
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
chacha20-poly1305@openssh.com
rijndael-cbc@lysator.liu.se
```

The server supports the following options for encryption\_algorithms\_server\_to\_client :

```
3des-cbc
aes128-cbc
aes128-ctr
aes128-gcm@openssh.com
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
```

```
aes256-gcm@openssh.com
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
chacha20-poly1305@openssh.com
rijndael-cbc@lysator.liu.se
```

The server supports the following options for `mac_algorithms_client_to_server` :

```
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-ripemd160
hmac-ripemd160-etm@openssh.com
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
```

The server supports the following options for `mac_algorithms_server_to_client` :

```
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-ripemd160
hmac-ripemd160-etm@openssh.com
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
hmac-sha1-e [...]
```

## 10881 - SSH Protocol Versions Supported

### Synopsis

A SSH server is running on the remote host.

### Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2002/03/06, Modification date: 2013/10/21

### Ports

#### tcp/22

The remote SSH daemon supports the following versions of the SSH protocol :

- 1.99
- 2.0

SSHv2 host key fingerprint : d2:db:9e:14:7c:4d:62:69:dd:82:af:31:ab:87:b3:97

## 39520 - Backported Security Patch Detection (SSH)

## Synopsis

Security patches are backported.

## Description

Security patches may have been 'backported' to the remote SSH server without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem.

## See Also

[https://access.redhat.com/security/updates/backporting/?sc\\_cid=3093](https://access.redhat.com/security/updates/backporting/?sc_cid=3093)

## Solution

n/a

## Risk Factor

None

## Plugin Information:

Publication date: 2009/06/25, Modification date: 2015/07/07

## Ports

**tcp/22**

Give Nessus credentials to perform local checks.

## 80/tcp

## 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:

Publication date: 2009/02/04, Modification date: 2016/07/11

## Ports

**tcp/80**

Port 80/tcp was found to be open

## 22964 - Service Detection

## Synopsis

The remote service could be identified.

## Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

## Solution

n/a

## Risk Factor

None

## Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/03/17

## Ports

## tcp/80

A web server is running on this port.

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

This plugin attempts to determine the type and the version of the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2000/01/04, Modification date: 2016/02/19

### Ports

#### tcp/80

The remote web server type is :

nginx/1.9.14

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

### Ports

#### tcp/80

Protocol version : HTTP/1.1

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Server: nginx/1.9.14

Date: Mon, 22 Aug 2016 15:14:00 GMT

Content-Type: text/html

Content-Length: 875

Last-Modified: Mon, 22 Aug 2016 14:34:58 GMT

Connection: keep-alive

Vary: Accept-Encoding

ETag: "57bb0d92-36b"

Accept-Ranges: bytes

## 443/tcp

## 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:

Publication date: 2009/02/04, Modification date: 2016/07/11

## Ports

**tcp/443**

Port 443/tcp was found to be open

**8080/tcp**

**12085 - Apache Tomcat Servlet / JSP Container Default Files**

## Synopsis

The remote web server contains example files.

## Description

Example JSPs and Servlets are installed in the remote Apache Tomcat servlet / JSP container. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself. The example files may also contain vulnerabilities such as cross-site scripting vulnerabilities.

## Solution

Review the files and delete those that are not needed.

## Risk Factor

Medium

## CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

## References

|      |         |
|------|---------|
| XREF | CWE:20  |
| XREF | CWE:74  |
| XREF | CWE:79  |
| XREF | CWE:442 |
| XREF | CWE:629 |
| XREF | CWE:711 |
| XREF | CWE:712 |
| XREF | CWE:722 |
| XREF | CWE:725 |
| XREF | CWE:750 |
| XREF | CWE:751 |
| XREF | CWE:800 |
| XREF | CWE:801 |

|             |         |
|-------------|---------|
| <b>XREF</b> | CWE:809 |
| <b>XREF</b> | CWE:811 |
| <b>XREF</b> | CWE:864 |
| <b>XREF</b> | CWE:900 |
| <b>XREF</b> | CWE:928 |
| <b>XREF</b> | CWE:931 |
| <b>XREF</b> | CWE:990 |

#### Plugin Information:

Publication date: 2004/03/02, Modification date: 2016/05/09

#### Ports

**tcp/8080**

The following default files were found :

```
/examples/servlets/index.html
/examples/jsp/snp/snoop.jsp
/examples/jsp/index.html
```

### 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:

Publication date: 2009/02/04, Modification date: 2016/07/11

#### Ports

**tcp/8080**

Port 8080/tcp was found to be open

### 22964 - Service Detection

#### Synopsis

The remote service could be identified.

#### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

#### Solution

n/a

#### Risk Factor

None

#### Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/03/17

#### Ports

## tcp/8080

A web server is running on this port.

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

This plugin attempts to determine the type and the version of the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2000/01/04, Modification date: 2016/02/19

### Ports

#### tcp/8080

The remote web server type is :

Restlet-Framework/3.0m1

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

### Ports

#### tcp/8080

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : GET, HEAD, POST, PUT, DELETE, OPTIONS
Headers :
```

```
Date: Mon, 22 Aug 2016 15:14:02 GMT
Accept-Ranges: bytes
Server: Restlet-Framework/3.0m1
Content-Type: application/json
Transfer-Encoding: chunked
Connection: close
```

## 9090/tcp

## 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:

Publication date: 2009/02/04, Modification date: 2016/07/11

#### Ports

**tcp/9090**

Port 9090/tcp was found to be open

### 22964 - Service Detection

#### Synopsis

The remote service could be identified.

#### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

#### Solution

n/a

#### Risk Factor

None

#### Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/03/17

#### Ports

**tcp/9090**

A web server is running on this port.