



## task3

---

Report generated by Tenable Nessus™

Thu, 25 Sep 2025 22:23:03 India Standard Time

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 127.0.0.1.....	4
------------------	---

For Trial Use Only

---

## Vulnerabilities by Host

---

127.0.0.1



## Scan Information

Start time: Thu Sep 25 22:05:05 2025  
End time: Thu Sep 25 22:23:02 2025

## Host Information

Netbios Name: RAVISHANKAR  
IP: 127.0.0.1  
OS: Windows 11

## Vulnerabilities

### 55786 - Oracle Database Unsupported Version Detection

## Synopsis

The remote host is running an unsupported version of a database server.

## Description

According to its version, the installation of Oracle Database running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

## See Also

<http://www.nessus.org/u?ccd068d1>

## Solution

Upgrade to a version of Oracle Database that is currently supported.

## Risk Factor

Critical

## CVSS v2.0 Base Score

---

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

## References

---

XREF IAVA:0001-A-0574

## Plugin Information

---

Published: 2011/08/09, Modified: 2022/09/28

## Plugin Output

---

tcp/1521/oracle\_tnslnr

```
Version source      : TNSLSNR for : Version 11.2.0.2.0
Installed version   : 11.2.0.2.0
Supported versions  : 19c / 21c
```

## 69552 - Oracle TNS Listener Remote Poisoning

### Synopsis

It was possible to register with a remote Oracle TNS listener.

### Description

The remote Oracle TNS listener allows service registration from a remote host. An attacker can exploit this issue to divert data from a legitimate database server or client to an attacker-specified system.

Successful exploits will allow the attacker to manipulate database instances, potentially facilitating man-in-the-middle, session- hijacking, or denial of service attacks on a legitimate database server.

### See Also

<http://www.nessus.org/u?8c8334e6>

<http://www.nessus.org/u?06d298e5>

<https://seclists.org/fulldisclosure/2012/Apr/204>

### Solution

Apply the workaround in Oracle's advisory.

### Risk Factor

High

### CVSS v3.0 Base Score

7.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)

### CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:F/RL:O/RC:C)

### VPR Score

4.9

### EPSS Score

0.9216

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

6.8 (CVSS2#E:F/RL:W/RC:C)

References

BID	53308
CVE	CVE-2012-1675
XREF	CERT:359816

Exploitable With

Core Impact (true)

Plugin Information

Published: 2013/08/26, Modified: 2025/07/21

Plugin Output

tcp/1521/oracle\_tnslnr

The remote Oracle TNS listener returned the following response to a registration request :

```
0x0000: 00 00 02 5C 24 08 FF 03 01 00 12 34 34 78 78 34    ...\.$.44xx4
0x0010: 78 10 10 32 10 32 10 32 54 76 10 32 10 32 54 76    x..2.2.2Tv.2.2Tv
0x0020: 00 78 10 32 54 76 00 00 30 02 00 80 07 00 00 00    .x.2Tv..0.
0x0030: 00 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00    .....
0x0040: 10 00 00 00 02 00 00 00 00 00 00 00 50 B6 A5 05    .....P..
0x0050: 00 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00    .....
0x0060: 00 00 00 00 00 00 00 00 00 00 00 00 D0 D8 BB 05    .....
0x0070: 00 00 00 00 BC 91 FB 9F E8 86 4B CB B6 3D C5 18    .....K..=.
0x0080: C5 E3 42 40 05 00 00 00 0A 00 00 00 01 00 00 00    ..B@.....
0x0090: 00 00 00 00 D0 B6 A5 05 00 00 00 00 06 00 00 00    .....
0x00A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    .....
0x00B0: 00 00 00 00 90 D9 BB 05 00 00 00 00 6E 65 73 73    .....ness
0x00C0: 75 73 58 44 42 00 05 00 00 00 07 00 00 00 01 00    usXDB.....
0x00D0: 00 00 00 00 00 00 B0 C4 A5 05 00 00 00 00 06 00    .....
0x00E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    .....
0x00F0: 00 00 00 00 00 00 50 CF BB 05 00 00 00 00 6E 65    .....P.....ne
0x0100: 73 73 75 73 00 05 00 00 00 34 00 00 00 01 00 00    ssus.....4.....
0x0110: 00 00 00 00 00 50 CA BB 05 00 00 00 00 07 00 00    ....P.....
0x0120: 00 00 00 00 00 10 B3 A5 05 00 00 00 00 00 00 00    .....
0x0130: 00 00 00 00 00 D0 CA BB 05 00 00 00 00 28 41 44    ..... (AD
0x0140: 44 52 45 53 53 3D 28 50 52 4F 54 4F 43 4F 4C 3D    DRESS=(PROTOCOL=
0x0150: 54 43 50 29 28 48 4F 53 54 3D 31 32 37 2E 30 2E    TCP) (HOST=127.0.
0x0160: 30 2E 31 29 28 50 4F 52 54 3D 31 35 32 31 29 29    0.1) (PORT=1521))
0x0170: 00 42 00 00 00 00 00 00 70 7F 6F 05 00 00 00 00    .B.....p.o....
0x0180: 00 00 00 00 00 00 00 00 28 44 45 53 43 52 49    ..... (DESCRI
0x0190: 50 54 49 4F 4E 3D 28 4 [...]
```

## 64712 - Oracle Application Express (Apex) CVE-2011-3525

### Synopsis

The remote host is running a vulnerable version of Oracle Apex.

### Description

An unspecified vulnerability in versions 3.2 and 4.0 of the Application Express (Apex) component of the Oracle Database Server allows remote, authenticated users to affect confidentiality, integrity, and availability, relating to the Apex developer user.

### See Also

<http://www.oracle.com/technetwork/developer-tools/apex/index.html>

<https://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html>

<https://www.recx.co.uk/downloads/Recx-Apex-CVE-2011-3525.pdf>

### Solution

Upgrade Application Express to at least version 4.1.

### Risk Factor

Medium

### VPR Score

5.5

### EPSS Score

0.0057

### CVSS v2.0 Base Score

6.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

4.8 (CVSS2#E:U/RL:OF/RC:C)

### References

BID 50197

CVE CVE-2011-3525



## Plugin Information

---

Published: 2013/02/20, Modified: 2020/06/12

## Plugin Output

---

tcp/8080/www

```
URL           : http://127.0.0.1:8080/apex/  
Installed version : 4.0.2  
Fixed version   : 4.1
```

## 64713 - Oracle Application Express (Apex) CVE-2012-1708

### Synopsis

The remote host is running a vulnerable version of Oracle Apex.

### Description

An unspecified vulnerability in versions 4.0 and 4.1 of the Application Express (Apex) component of the Oracle Database Server allows remote attackers to affect integrity via unpublished vectors.

### See Also

<http://www.oracle.com/technetwork/developer-tools/apex/index.html>

<https://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html>

<https://www.recx.co.uk/downloads/Recx-Apex-CVE-2012-1708.pdf>

### Solution

Upgrade Application Express to at least version 4.1.1.

### Risk Factor

Medium

### VPR Score

2.7

### EPSS Score

0.0039

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

### References

BID 53104

CVE CVE-2012-1708

### Plugin Information

Published: 2013/02/20, Modified: 2020/06/12

## Plugin Output

---

tcp/8080/www

```
URL          : http://127.0.0.1:8080/apex/  
Installed version : 4.0.2  
Fixed version  : 4.1.1
```

## 57608 - SMB Signing not required

### Synopsis

---

Signing is not required on the remote SMB server.

### Description

---

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

### See Also

---

<http://www.nessus.org/u?df39b8b3>

<http://technet.microsoft.com/en-us/library/cc731957.aspx>

<http://www.nessus.org/u?74b80723>

<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>

<http://www.nessus.org/u?a3cac4ea>

### Solution

---

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

### Risk Factor

---

Medium

### CVSS v3.0 Base Score

---

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v3.0 Temporal Score

---

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

---

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### CVSS v2.0 Temporal Score

---

3.7 (CVSS2#E:U/RL:OF/RC:C)

### Plugin Information

---

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

---

tcp/445/cifs

## 51192 - SSL Certificate Cannot Be Trusted

### Synopsis

---

The SSL certificate for this service cannot be trusted.

### Description

---

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

### See Also

---

<https://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

### Solution

---

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

---

Medium

### CVSS v3.0 Base Score

---

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

---

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

## Plugin Information

---

Published: 2010/12/15, Modified: 2025/06/16

## Plugin Output

---

tcp/8834/www

The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :

```
| -Subject : O=Nessus Users United/OU=Nessus Server/L=New York/C=US/ST=NY/CN=RaviShankar  
| -Issuer  : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus  
            Certification Authority
```

## 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: 2025/07/14

### Plugin Output

tcp/0

```
The remote operating system matched the following CPE :
```

```
cpe:/o:microsoft:windows -> Microsoft Windows
```

```
Following application CPE's matched on the remote system :
```

```
cpe:/a:mysql:mysql:9.4.0 -> MySQL MySQL
```

```
cpe:/a:oracle:database_server:11.2.0.2.0 -> Oracle Database Server
```

```
cpe:/a:tenable:nessus -> Tenable Nessus
```



## 10736 - DCE Services Enumeration

### Synopsis

A DCE/RPC service is running on the remote host.

### Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

### Plugin Output

tcp/135/epmap

The following DCERPC services are available locally :

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0  
Description : Unknown RPC service  
Annotation : Ngc Pop Key Service  
Type : Local RPC service  
Named pipe : samss lpc

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0  
Description : Unknown RPC service  
Annotation : Ngc Pop Key Service  
Type : Local RPC service  
Named pipe : SidKey Local End Point

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0  
Description : Unknown RPC service  
Annotation : Ngc Pop Key Service  
Type : Local RPC service  
Named pipe : protected\_storage

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0  
Description : Unknown RPC service  
Annotation : Ngc Pop Key Service  
Type : Local RPC service

```
Named pipe : lsasspirpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : lsapolicylookup

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : lsacap

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc [...]
```

## 10736 - DCE Services Enumeration

### Synopsis

A DCE/RPC service is running on the remote host.

### Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

### Plugin Output

tcp/445/cifs

The following DCERPC services are available remotely :

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 650a7e26-eab8-5533-ce43-9cldfcel1511, version 1.0  
Description : Unknown RPC service  
Annotation : Vpn APIs  
Type : Remote RPC service  
Named pipe : \PIPE\ROUTER  
Netbios name : \RAVISHANKAR

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0  
Description : Unknown RPC service  
Annotation : DfsDs service  
Type : Remote RPC service  
Named pipe : \PIPE\wkssvc  
Netbios name : \RAVISHANKAR

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0  
Description : Unknown RPC service  
Annotation : Windows Event Log  
Type : Remote RPC service  
Named pipe : \pipe\eventlog  
Netbios name : \RAVISHANKAR

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0

Description : Scheduler Service  
Windows process : svchost.exe  
Type : Remote RPC service  
Named pipe : \PIPE\atsvc  
Netbios name : \\RAVISHANKAR

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0  
Description : Scheduler Service  
Windows process : svchost.exe  
Type : Remote RPC service  
Named pipe : \PIPE\atsvc  
Netbios name : \\RAVISHANKAR

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 33d84484-3626-47ee-8c6f-e7e98b113bel, version 2.0  
Description : Unknown RPC service  
Type : Remote RPC service  
Named pipe : \PIPE\atsvc  
Netbios name : \\RAVISHANKAR

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0  
Description : Unknown RPC service  
Type : Remote RPC service  
Named pipe : \PIPE\atsvc  
Netbios name : \\RAVISHANKAR

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0  
Description : Unknown RPC service  
Type : Remote RPC service  
Named pipe : \PIPE\atsvc  
Netbios name : \\RAVISHANKAR

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000  
UUID : 76f226c3- [...]

## 10736 - DCE Services Enumeration

### Synopsis

A DCE/RPC service is running on the remote host.

### Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

### Plugin Output

tcp/49664/dce-rpc

The following DCERPC services are available on TCP port 49664 :

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0  
Description : Unknown RPC service  
Annotation : Ngc Pop Key Service  
Type : Remote RPC service  
TCP Port : 49664  
IP : 127.0.0.1

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0  
Description : Security Account Manager  
Windows process : lsass.exe  
Type : Remote RPC service  
TCP Port : 49664  
IP : 127.0.0.1

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0  
Description : Unknown RPC service  
Annotation : KeyIso  
Type : Remote RPC service  
TCP Port : 49664  
IP : 127.0.0.1

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191felb, version 1.0

Description : Unknown RPC service  
Annotation : Ngc Pop Key Service  
Type : Remote RPC service  
TCP Port : 49664  
IP : 127.0.0.1

## 10736 - DCE Services Enumeration

### Synopsis

A DCE/RPC service is running on the remote host.

### Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

### Plugin Output

tcp/49665/dce-rpc

```
The following DCERPC services are available on TCP port 49665 :
```

```
Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49665
IP : 127.0.0.1
```

## 10736 - DCE Services Enumeration

### Synopsis

A DCE/RPC service is running on the remote host.

### Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

### Plugin Output

tcp/49666/dce-rpc

The following DCERPC services are available on TCP port 49666 :

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0  
Description : Unknown RPC service  
Type : Remote RPC service  
TCP Port : 49666  
IP : 127.0.0.1

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0  
Description : Unknown RPC service  
Type : Remote RPC service  
TCP Port : 49666  
IP : 127.0.0.1



## 10736 - DCE Services Enumeration

### Synopsis

A DCE/RPC service is running on the remote host.

### Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

### Plugin Output

tcp/49667/dce-rpc

The following DCERPC services are available on TCP port 49667 :

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Windows Event Log
Type : Remote RPC service
TCP Port : 49667
IP : 127.0.0.1
```

## 10736 - DCE Services Enumeration

### Synopsis

A DCE/RPC service is running on the remote host.

### Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

### Plugin Output

tcp/49668/dce-rpc

The following DCERPC services are available on TCP port 49668 :

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0  
Description : IPsec Services (Windows XP & 2003)  
Windows process : lsass.exe  
Type : Remote RPC service  
TCP Port : 49668  
IP : 127.0.0.1

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 0b6edbfa-4a24-4fc6-8a23-942bleca65d1, version 1.0  
Description : Unknown RPC service  
Type : Remote RPC service  
TCP Port : 49668  
IP : 127.0.0.1

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0  
Description : Unknown RPC service  
Type : Remote RPC service  
TCP Port : 49668  
IP : 127.0.0.1

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0  
Description : Unknown RPC service  
Type : Remote RPC service

TCP Port : 49668  
IP : 127.0.0.1

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0  
Description : Unknown RPC service  
Type : Remote RPC service  
TCP Port : 49668  
IP : 127.0.0.1

## 10736 - DCE Services Enumeration

### Synopsis

A DCE/RPC service is running on the remote host.

### Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

### Plugin Output

tcp/49676/dce-rpc

The following DCERPC services are available on TCP port 49676 :

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49676
IP : 127.0.0.1
```

## 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: 2025/03/12

### Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 70
```

## 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

### References

XREF IAVT:0001-T-0931

### Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

### Plugin Output

tcp/8080/www

```
The remote web server type is :  
Oracle XML DB/Oracle Database
```

## 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

### References

XREF IAVT:0001-T-0931

### Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

### Plugin Output

tcp/8834/www

```
The remote web server type is :  
NessusWWW
```

## 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: 2025/03/13

### Plugin Output

tcp/0

```
127.0.0.1 resolves as localhost.
```



## 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 is enabled, etc...

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

### Plugin Output

tcp/8080/www

```
Response Code : HTTP/1.1 401 Unauthorized

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

MS-Author-Via: DAV
DAV: 1,2,<http://www.oracle.com/xdb/webdav/props>
Server: Oracle XML DB/Oracle Database
WWW-Authenticate: Basic realm="XDB"
Date: Thu, 25 Sep 2025 16:37:54 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 147

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>401 Unauthorized</TITLE>
</HEAD><BODY><H1>Unauthorized</H1>
</BODY></HTML>
```

## 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 is enabled, etc...

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

### Plugin Output

tcp/8834/www

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : yes

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Cache-Control: must-revalidate

X-Frame-Options: DENY

Content-Type: text/html

ETag: b117142630298915d2aca85cc1c91c17

Connection: close

X-XSS-Protection: 1; mode=block

Server: NessusWWW

Date: Thu, 25 Sep 2025 16:38:00 GMT

X-Content-Type-Options: nosniff

Content-Length: 1629

Content-Security-Policy: upgrade-insecure-requests; block-all-mixed-content; form-action

'self'; frame-ancestors 'none'; frame-src https://store.tenable.com www.youtube.com; default-src

'self'; connect-src 'self' data.nessus-telemetry.tenable.com content.nessus-telemetry.tenable.com

api.tenable.com www.tenable.com; script-src 'self' content.nessus-telemetry.tenable.com

www.tenable.com; img-src 'self' data: content.nessus-telemetry.tenable.com data.nessus-

telemetry.tenable.com pendo-static-5689996938182656.storage.googleapis.com s.ytimg.com i.ytimg.com;

```
style-src 'self' content.nessus-telemetry.tenable.com data.nessus-telemetry.tenable.com pendo-
static-5689996938182656.storage.googleapis.com www.tenable.com; object-src 'none'; base-uri 'self';
Strict-Transport-Security: max-age=31536000; includeSubDomains
Expect-CT: max-age=0
```

Response Body :

```
<!doctype html>
<html lang="en">
  <head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
    <meta http-equiv="Content-Security-Policy" content="upgrade-insecure-requests; block-all-
mixed-content; form-action 'self'; frame-src https://store.tenable.com www.youtube.com; default-src
'self'; connect-src 'self' data.nessus-telemetry.tenable.com content.nessus-telemetry.tenable.com
api.tenable.com www.tenable.com; script-src 'self' content.nessus-telemetry.tenable.com
www.tenable.com; img-src 'self' data: data.nessus-telemetry.tenable.com content.nessus-
telemetry.tenable.com pendo-static-5689996938182656.storage.googleapis.com s.ytimg.com i.ytimg.com;
style-src 'self' c [...]
```

### Synopsis

It is possible to obtain the network name of the remote host.

### Description

The remote host listens on tcp port 445 and replies to SMB requests.

By sending an NTLMSSP authentication request it is possible to obtain the name of the remote system and the name of its domain.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/11/06, Modified: 2019/11/22

### Plugin Output

tcp/445/cifs

```
The following 2 NetBIOS names have been gathered :
```

```
RAVISHANKAR      = Computer name
RAVISHANKAR      = Workgroup / Domain name
```

### Synopsis

It was possible to obtain information about the remote operating system.

### Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

### Plugin Output

tcp/445/cifs

```
Nessus was able to obtain the following information about the host, by  
parsing the SMB2 Protocol's NTLM SSP message:
```

```
Target Name: RAVISHANKAR  
NetBIOS Domain Name: RAVISHANKAR  
NetBIOS Computer Name: RAVISHANKAR  
DNS Domain Name: RaviShankar  
DNS Computer Name: RaviShankar  
DNS Tree Name: unknown  
Product Version: 10.0.26100
```

## 11011 - Microsoft Windows SMB Service Detection

### Synopsis

A file / print sharing service is listening on the remote host.

### Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

### Plugin Output

tcp/445/cifs

```
A CIFS server is running on this port.
```

## 100871 - Microsoft Windows SMB Versions Supported (remote check)

### Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

### Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

### Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :  
SMBv2
```

## 106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

### Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

### Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

### Plugin Output

tcp/445/cifs

```
The remote host supports the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
3.0        Windows 8
3.0.2      Windows 8.1
3.1.1      Windows 10

The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.1        Windows 10
```



## 10719 - MySQL Server Detection

### Synopsis

A database server is listening on the remote port.

### Description

The remote host is running MySQL, an open source database server.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0802

### Plugin Information

Published: 2001/08/13, Modified: 2025/09/24

### Plugin Output

tcp/3306/mysql

```
Service : mysql
Version : 9.4.0
```

tcp/3306/mysql

```
Version : 9.4.0
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_PASSWORD (new more secure passwords)
  CLIENT_FOUND_ROWS (Found instead of affected rows)
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_NO_SCHEMA (Don't allow database.table.column)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_ODBC (ODBC client)
  CLIENT_LOCAL_FILES (Can use LOAD DATA LOCAL)
  CLIENT_IGNORE_SPACE (Ignore spaces before "(")
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_INTERACTIVE (This is an interactive client)
  CLIENT_SSL (Switch to SSL after handshake)
```

```
CLIENT_SIGPIPE (IGNORE sigpipes)
CLIENT_TRANSACTIONS (Client knows about transactions)
CLIENT_RESERVED (Old flag for 4.1 protocol)
CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

## 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: 2025/06/25

### Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.9.4
Nessus build : 20037
Plugin feed version : 202509250001
Scanner edition used : Nessus
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : task3
```

```
Scan policy used : Basic Network Scan
Scanner IP : 127.0.0.1
Ping RTT : Unavailable
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 : yes
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 : 2025/9/25 22:05 India Standard Time (UTC +05:30)
Scan duration : 1074 sec
Scan for malware : no
```

## 10147 - Nessus Server Detection

### Synopsis

A Nessus daemon is listening on the remote port.

### Description

A Nessus daemon is listening on the remote port.

### See Also

<https://www.tenable.com/products/nessus/nessus-professional>

### Solution

Ensure that the remote Nessus installation has been authorized.

### Risk Factor

None

### References

XREF IAVT:0001-T-0673

### Plugin Information

Published: 1999/10/12, Modified: 2023/02/08

### Plugin Output

tcp/8834/www

```
URL      : https://127.0.0.1:8834/  
Version  : unknown
```

## 64582 - Netstat Connection Information

### Synopsis

---

Nessus was able to parse the results of the 'netstat' command on the remote host.

### Description

---

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

### Solution

---

n/a

### Risk Factor

---

None

### Plugin Information

---

Published: 2013/02/13, Modified: 2023/05/23

### Plugin Output

---

tcp/0

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/135/epmap

```
Port 135/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/137

```
Port 137/udp was found to be open
```



## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/138

```
Port 138/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/139

```
Port 139/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/1521/oracle\_tnslnr

```
Port 1521/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/1900

```
Port 1900/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/3306/mysql

```
Port 3306/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/5040

```
Port 5040/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/5050

```
Port 5050/udp was found to be open
```



## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/5353

```
Port 5353/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/5355

```
Port 5355/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/7680

```
Port 7680/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/8080/www

```
Port 8080/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/8834/www

```
Port 8834/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/33060

```
Port 33060/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/49664/dce-rpc

```
Port 49664/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/49665/dce-rpc

```
Port 49665/tcp was found to be open
```



## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/49666/dce-rpc

```
Port 49666/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/49667/dce-rpc

```
Port 49667/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/49668/dce-rpc

```
Port 49668/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/49675

```
Port 49675/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/49676/dce-rpc

```
Port 49676/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/50594

```
Port 50594/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/59724

```
Port 59724/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/62333

```
Port 62333/udp was found to be open
```



## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/63399

```
Port 63399/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/63400

```
Port 63400/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/63402

```
Port 63402/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/63403

```
Port 63403/udp was found to be open
```

## 209654 - OS Fingerprints Detected

### Synopsis

Multiple OS fingerprints were detected.

### Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

### Plugin Output

tcp/0

Following OS Fingerprints were found

Remote operating system : Windows 11  
Confidence level : 70  
Method : Misc  
Type : general-purpose  
Fingerprint : unknown

Following fingerprints could not be used to determine OS :

HTTP:!:Server: NessusWWW

SSLcert:!:i/CN:Nessus Certification Authorityi/O:Nessus Users Unitedi/OU:Nessus Certification  
Authoritys/CN:RaviShankars/O:Nessus Users Uniteds/OU:Nessus Server  
1141dc3fcfc6ecfa1d9bb2c84eeb8e19612eff38

## 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: 2025/06/03

### Plugin Output

tcp/0

```
Remote operating system : Windows 11
Confidence level : 70
Method : Misc
```

```
The remote host is running Windows 11
```

## 97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

### Synopsis

Information about the remote host can be disclosed via an authenticated session.

### Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2017/05/30, Modified: 2025/02/11

### Plugin Output

tcp/0

```
Nessus can run commands on localhost to check if patches are applied.  
  
Credentialed checks of Windows are not supported using SSH.  
  
The remote host is not currently supported by this plugin.  
  
Runtime : 1.43145 seconds
```

## 117886 - OS Security Patch Assessment Not Available

### Synopsis

OS Security Patch Assessment is not available.

### Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVB:0001-B-0515

### Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

### Plugin Output

tcp/0

The following issues were reported :

```
- Plugin      : ssh_get_info2.nasl
  Plugin ID   : 97993
  Plugin Name : OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH
  Library)
  Protocol    : LOCALHOST
  Message     :
  Credentialed checks of Windows are not supported using SSH.

- Plugin      : no_local_checks_credentials.nasl
  Plugin ID   : 110723
  Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
```



Message :  
Credentials were not provided for detected SMB service.

## 64706 - Oracle Application Express (Apex) Administration Interface is Accessible

### Synopsis

The Oracle Application Express environment on the remote host has the Administration Builder interface enabled.

### Description

In production environments, the Apex Administration and Builder applications should be disabled to prevent administrator or developer access to the instance via a web browser.

### See Also

<http://www.oracle.com/technetwork/developer-tools/apex/index.html>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/02/20, Modified: 2020/06/12

### Plugin Output

tcp/8080/www

Oracle Apex Administration Interface :

URL : <http://127.0.0.1:8080/apex/>

## 64704 - Oracle Application Express (Apex) Detection

### Synopsis

The remote host is running Oracle Apex.

### Description

The remote host is running Oracle Application Express (Apex).

### See Also

<http://www.oracle.com/technetwork/developer-tools/apex/index.html>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/02/20, Modified: 2020/06/12

### Plugin Output

tcp/8080/www

```
An Oracle Application Express (Apex) instance was detected :  
URL : http://127.0.0.1:8080/apex/
```

## 64705 - Oracle Application Express (Apex) Version Detection

### Synopsis

The remote host is running a version Oracle Apex.

### Description

The remote host is running Oracle Application Express (Apex).

### See Also

<http://www.oracle.com/technetwork/developer-tools/apex/index.html>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/02/20, Modified: 2020/06/12

### Plugin Output

tcp/8080/www

```
URL      : http://127.0.0.1:8080/apex/  
Version  : 4.0.2  
Release Date : 19 November, 2010
```

## 22073 - Oracle Database Detection

### Synopsis

A database service is listening on the remote host.

### Description

The remote host is running an Oracle database server.

It may be possible to extract the version number of the remote TNS (Transparent Network Substrate) listener by sending a 'VERSION'

request to the TNS listener service operating on this port.

Note that the version of the TNS listener does not necessarily reflect the version of the Oracle database it provides access to.

### Solution

Restrict access to the database to allowed IPs only.

### Risk Factor

None

### Plugin Information

Published: 2006/07/19, Modified: 2025/07/21

### Plugin Output

tcp/1521/oracle\_tnslnr

```
The banner of the remote Oracle TNS listener on port 1521
contains the following version :
```

```
TNSLSNR for : Version 11.2.0.2.0
```

```
Note: This banner can be read without authentication.
```

## 10658 - Oracle Database tnslnr Service Remote Version Disclosure

### Synopsis

---

An Oracle tnslnr service is listening on the remote port.

### Description

---

The remote host is running the Oracle tnslnr service, a network interface to Oracle databases. This product allows a remote user to determine the presence and version number of a given Oracle installation.

### Solution

---

Filter incoming traffic to this port so that only authorized hosts can connect to it.

### Risk Factor

---

None

### Plugin Information

---

Published: 2001/05/01, Modified: 2022/10/12

### Plugin Output

---

tcp/1521/oracle\_tnslnr

```
A TNS service is running on this port but it
refused to honor an attempt to connect to it.
(The TNS reply code was 4)
```

### Synopsis

The remote host is missing several patches.

### Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

### Solution

Install the patches listed below.

### Risk Factor

None

### Plugin Information

Published: 2013/07/08, Modified: 2025/09/09

### Plugin Output

tcp/0

```
. You need to take the following 2 actions :

[ Oracle Application Express (Apex) CVE-2012-1708 (64713) ]
+ Action to take : Upgrade Application Express to at least version 4.1.1.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Oracle TNS Listener Remote Poisoning (69552) ]
+ Action to take : Apply the workaround in Oracle's advisory.
```

## 56984 - SSL / TLS Versions Supported

### Synopsis

The remote service encrypts communications.

### Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

### Plugin Output

tcp/8834/www

```
This port supports TLSv1.3/TLSv1.2.
```



## 10863 - SSL Certificate Information

### Synopsis

This plugin displays the SSL certificate.

### Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

### Plugin Output

tcp/8834/www

```
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: RaviShankar

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 C1 AE

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Sep 25 15:30:06 2025 GMT
Not Valid After: Sep 24 15:30:06 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 89 F4 19 E7 FD 08 A3 80 1C FE 56 BD 0D 32 24 4A 30 74 82
```

```
71 44 7D D3 2F E9 DB 3E C0 05 DD C8 F1 40 0B F9 AD 78 98 A0
99 70 BF D2 85 C1 59 36 57 30 21 00 ED 10 0F 18 D1 41 8F 5A
55 B4 D0 77 31 48 8E 8C 33 31 50 6F 92 90 28 3A AC FF 75 E4
F9 18 2D E1 1B 20 4A 92 D2 C4 B6 37 10 55 21 41 25 6E D8 66
40 27 03 1A E2 EB 56 F3 76 F7 16 A5 99 45 31 79 91 B1 DC 66
45 37 5C 15 28 E6 B0 F2 D5 54 33 FD FF 3E CF EC B0 8D B4 6B
02 D7 02 97 2D D5 A4 1A CD AC ED B2 38 81 D0 97 49 DE 0F 10
E9 9C 99 C2 03 FF 12 11 35 D8 45 5C 83 CB 96 80 39 8C 90 C4
2D B2 62 85 20 93 1A 12 C4 9E FC 50 EB AB 9B F7 67 5C 96 DE
74 F8 FB 6E 35 CC 2E 8F C6 EB 08 99 BE F2 E4 87 DB 81 C8 8C
F6 9B BE CC F2 DE BA 56 4D 9A 97 1C EA AB E7 3E A9 13 97 77
28 D2 BF 0C 50 54 E1 4D 0D BC 41 EA 05 22 4A 62 05
```

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits

Signature: 00 70 A9 F8 42 89 C5 1B 29 06 39 92 65 6A 04 1F 3E 1E 39 5C  
80 D7 17 F9 2D 1F 6C 3C CD 79 3A 46 6D 38 A3 78 E3 22 7C 38  
76 FE 30 C9 84 B9 E4 36 62 21 AE D1 C4 3D 3F DD 64 89 06 D1  
4B 25 75 58 0C 8E BB F3 73 44 D2 05 BD 9F AA 82 BB C7 09 CE  
99 B8 11 72 DF 9A 2D 73 C3 4D C0 9A 28 CD 05 D5 0E FD 6A AB  
A2 88 7C F1 B7 86 27 56 CE DB 85 76 3F EF 06 90 20 57 F6 EB  
7B A2 A5 C6 [...]

## 21643 - SSL Cipher Suites Supported

### Synopsis

The remote service encrypts communications using SSL.

### Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

### See Also

<https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>

<http://www.nessus.org/u?e17ffcd>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

### Plugin Output

tcp/8834/www

Here is the list of SSL ciphers supported by the remote server :  
Each group is reported per SSL Version.

SSL Version : TLSv13

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
TLS_AES_128_GCM_SHA256	0x13, 0x01	-	-	AES-GCM(128)	
AEAD					
TLS_AES_256_GCM_SHA384	0x13, 0x02	-	-	AES-GCM(256)	
AEAD					
TLS_CHACHA20_POLY1305_SHA256	0x13, 0x03	-	-	ChaCha20-Poly1305(256)	
AEAD					

SSL Version : TLSv12

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
ECDHE-RSA-AES128-SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)	
SHA256					

ECDHE-RSA-AES256-SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM(256)
SHA384				

The fields above are :

```
{Tenable ciphertype}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

## 57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

### Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

### Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

### See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>

[https://en.wikipedia.org/wiki/Diffie-Hellman\\_key\\_exchange](https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange)

[https://en.wikipedia.org/wiki/Perfect\\_forward\\_secrecy](https://en.wikipedia.org/wiki/Perfect_forward_secrecy)

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

### Plugin Output

tcp/8834/www

Here is the list of SSL PFS ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
ECDHE-RSA-AES128-SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)	
SHA256					
ECDHE-RSA-AES256-SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM(256)	
SHA384					

The fields above are :

```
{Tenable ciphertype}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
```

```
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

## 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

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/8080/www

```
A web server is running on this port.
```

## 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

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/8834/www

```
A TLSv1.2 server answered on this port.
```

tcp/8834/www

```
A web server is running on this port through TLSv1.2.
```



## 11153 - Service Detection (HELP Request)

### Synopsis

The remote service could be identified.

### Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/11/18, Modified: 2024/11/19

### Plugin Output

tcp/3306/mysql

```
A MySQL server is running on this port.
```

## 42822 - Strict Transport Security (STS) Detection

### Synopsis

The remote web server implements Strict Transport Security.

### Description

The remote web server implements Strict Transport Security (STS).

The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

### See Also

<http://www.nessus.org/u?2fb3aca6>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/11/16, Modified: 2019/11/22

### Plugin Output

tcp/8834/www

The STS header line is :

Strict-Transport-Security: max-age=31536000; includeSubDomains

## 136318 - TLS Version 1.2 Protocol Detection

### Synopsis

The remote service encrypts traffic using a version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.2.

### See Also

<https://tools.ietf.org/html/rfc5246>

### Solution

N/A

### Risk Factor

None

### Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

### Plugin Output

tcp/8834/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

## 138330 - TLS Version 1.3 Protocol Detection

### Synopsis

The remote service encrypts traffic using a version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.3.

### See Also

<https://tools.ietf.org/html/rfc8446>

### Solution

N/A

### Risk Factor

None

### Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

### Plugin Output

tcp/8834/www

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

## 110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

### Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

### Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.
- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVB:0001-B-0504

### Plugin Information

Published: 2018/06/27, Modified: 2024/04/19

### Plugin Output

tcp/0

```
SMB was detected on port 445 but no credentials were provided.  
SMB local checks were not enabled.
```



## 11154 - Unknown Service Detection: Banner Retrieval

### Synopsis

There is an unknown service running on the remote host.

### Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

### Plugin Output

tcp/33060

If you know what this service is and think the banner could be used to identify it, please send a description of the service along with the following output to [svc-signatures@nessus.org](mailto:svc-signatures@nessus.org) :

```
Port    : 33060
Type    : spontaneous
Banner  :
0x00:  05 00 00 00 0B 08 05 1A 00      .....
```

## 135860 - WMI Not Available

### Synopsis

WMI queries could not be made against the remote host.

### Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vulnerabilities that exist on the remote host.

### See Also

<https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2020/04/21, Modified: 2025/07/21

### Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```



## 11424 - WebDAV Detection

### Synopsis

---

The remote server is running with WebDAV enabled.

### Description

---

WebDAV is an industry standard extension to the HTTP specification.

It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

### Solution

---

<http://support.microsoft.com/default.aspx?kbid=241520>

### Risk Factor

---

None

### Plugin Information

---

Published: 2003/03/20, Modified: 2011/03/14

### Plugin Output

---

tcp/8080/www

### Synopsis

It was possible to obtain the network name of the remote host.

### Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

### Plugin Output

tcp/445/cifs

```
The following 2 NetBIOS names have been gathered :
```

```
RAVISHANKAR      = Computer name
RAVISHANKAR      = Workgroup / Domain name
```