



## windows 10 single host

---

Report generated by Nessus™

Thu, 19 May 2022 14:32:47 India Standard Time

---

---

TABLE OF CONTENTS

---

**Vulnerabilities by Host**

- 192.168.1.101.....4

---

## **Vulnerabilities by Host**

---

---

**192.168.1.101**



---

#### Scan Information

Start time: Thu May 19 14:25:20 2022  
End time: Thu May 19 14:32:47 2022

---

#### Host Information

Netbios Name: DESKTOP-0N46D3D  
IP: 192.168.1.101  
MAC Address: 80:2B:F9:8C:E6:2F 00:0C:29:07:AC:A3  
OS: Microsoft Windows 10 Pro

---

#### Vulnerabilities

**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: 2021/03/15

#### Plugin Output

---

tcp/445/cifs

## 11197 - Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)

### Synopsis

The remote host appears to leak memory in network packets.

### Description

The remote host uses a network device driver that pads ethernet frames with data which vary from one packet to another, likely taken from kernel memory, system memory allocated to the device driver, or a hardware buffer on its network interface card.

Known as 'Etherleak', this information disclosure vulnerability may allow an attacker to collect sensitive information from the affected host provided he is on the same physical subnet as that host.

### See Also

<http://www.nessus.org/u?719c90b4>

### Solution

Contact the network device driver's vendor for a fix.

### Risk Factor

Low

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

2.6 (CVSS2#E:POC/RL:OF/RC:C)

### References

BID	6535
CVE	CVE-2003-0001

### Plugin Information

Published: 2003/01/14, Modified: 2019/03/06

### Plugin Output

icmp/0

Padding observed in one frame :

```
0x00: 47 D7 B0 F2 37 C5 87 36 DA D8 F8 02 75 2E B8 24   G...7..6....u..$
0x10: D8                                                .
```

Padding observed in another frame :

```
0x00: 95 41 3C 5F 04 DD AB B9 D2 61 48 32 62 B2 90 9D   .A<_.....aH2b...
0x10: 76                                                v
```

## 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: 2022/05/02

### Plugin Output

tcp/0

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

```
cpe:/o:microsoft:windows_10 -> Microsoft Windows 10 64-bit
```



## 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-ce43-9cldfcell1511, version 1.0  
Description : Unknown RPC service  
Annotation : Vpn APIs  
Type : Remote RPC service  
Named pipe : \PIPE\ROUTER  
Netbios name : \\DESKTOP-0N46D3D

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 338cd001-2244-31f1-aaaa-900038001003, version 1.0  
Description : Remote Registry  
Windows process : svchost.exe  
Annotation : RemoteRegistry Interface  
Type : Remote RPC service  
Named pipe : \PIPE\winreg  
Netbios name : \\DESKTOP-0N46D3D

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : da5a86c5-12c2-4943-ab30-7f74a813d853, version 1.0  
Description : Unknown RPC service  
Annotation : RemoteRegistry Perflib Interface  
Type : Remote RPC service  
Named pipe : \PIPE\winreg  
Netbios name : \\DESKTOP-0N46D3D

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 : \\DESKTOP-0N46D3D

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0  
Description : Unknown RPC service  
Annotation : Event log TCPIP  
Type : Remote RPC service  
Named pipe : \pipe\eventlog  
Netbios name : \\DESKTOP-0N46D3D

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 : \\DESKTOP-0N46D3D

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 : \\DESKTOP-0N46D3D

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0  
Description : Unknown RPC service  
Type : Rem [...]

## 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 : 192.168.1.101

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 : 192.168.1.101

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 : 192.168.1.101

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 : 192.168.1.101

## 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 : 192.168.1.101
```

## 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 : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.101
```



## 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 : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0  
Description : Unknown RPC service  
Type : Remote RPC service  
TCP Port : 49667  
IP : 192.168.1.101

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 : 49667  
IP : 192.168.1.101

## 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 : 192.168.1.101

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 : 192.168.1.101

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 : 192.168.1.101

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 : 192.168.1.101

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 : 192.168.1.101

## 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/49670/dce-rpc

The following DCERPC services are available on TCP port 49670 :

```
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 : 49670
IP : 192.168.1.101
```

## 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/49671/dce-rpc

The following DCERPC services are available on TCP port 49671 :

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6b5biddle-528c-422c-af8c-a4079be4fe48, version 1.0
Description : Unknown RPC service
Annotation : Remote Fw APIs
Type : Remote RPC service
TCP Port : 49671
IP : 192.168.1.101
```

## 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: 2011/05/23

### Plugin Output

tcp/0

```
Remote device type : unknown  
Confidence level : 56
```

## 35716 - Ethernet Card Manufacturer Detection

### Synopsis

The manufacturer can be identified from the Ethernet OUI.

### Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

### See Also

<https://standards.ieee.org/faqs/regauth.html>

<http://www.nessus.org/u?794673b4>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

### Plugin Output

tcp/0

The following card manufacturers were identified :

80:2B:F9:8C:E6:2F : Hon Hai Precision Ind. Co.,Ltd.  
00:0C:29:07:AC:A3 : VMware, Inc.

## 86420 - Ethernet MAC Addresses

### Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

### Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

### Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:  
- 80:2B:F9:8C:E6:2F  
- 00:0C:29:07:AC:A3
```



## 12053 - Host Fully Qualified Domain Name (FQDN) Resolution

### Synopsis

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

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/0

```
192.168.1.101 resolves as DESKTOP-0N46D3D.
```

## 10114 - ICMP Timestamp Request Remote Date Disclosure

### Synopsis

It is possible to determine the exact time set on the remote host.

### Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

### Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

### Risk Factor

None

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

### References

CVE CVE-1999-0524

XREF CWE:200

### Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

### Plugin Output

icmp/0

```
The ICMP timestamps seem to be in little endian format (not in network format)
The difference between the local and remote clocks is -44998 seconds.
```

### 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: DESKTOP-0N46D3D
NetBIOS Domain Name: DESKTOP-0N46D3D
NetBIOS Computer Name: DESKTOP-0N46D3D
DNS Domain Name: DESKTOP-0N46D3D
DNS Computer Name: DESKTOP-0N46D3D
DNS Tree Name: unknown
Product Version: 10.0.19041
```

## 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/139/smb

```
An SMB server is running on this port.
```

## 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
```

### Synopsis

---

It is possible to determine which TCP ports are open.

### Description

---

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

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

### Solution

---

Protect your target with an IP filter.

### Risk Factor

---

None

### Plugin Information

---

Published: 2009/02/04, Modified: 2022/02/14

### Plugin Output

---

tcp/135/epmap

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



### Synopsis

---

It is possible to determine which TCP ports are open.

### Description

---

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

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

### Solution

---

Protect your target with an IP filter.

### Risk Factor

---

None

### Plugin Information

---

Published: 2009/02/04, Modified: 2022/02/14

### Plugin Output

---

tcp/139/smb

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

### Synopsis

---

It is possible to determine which TCP ports are open.

### Description

---

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

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

### Solution

---

Protect your target with an IP filter.

### Risk Factor

---

None

### Plugin Information

---

Published: 2009/02/04, Modified: 2022/02/14

### Plugin Output

---

tcp/445/cifs

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

## 19506 - Nessus Scan Information

### Synopsis

This plugin displays information about the Nessus scan.

### Description

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/08/26, Modified: 2022/04/12

### Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 10.1.2  
Nessus build : 20068  
Plugin feed version : 202205190351  
Scanner edition used : Nessus Home  
Scanner OS : WINDOWS  
Scanner distribution : win-x86-64  
Scan type : Normal  
Scan name : windows 10 single host
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.1.110
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 108.301 ms
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
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2022/5/19 14:25 India Standard Time
Scan duration : 439 sec
```

## 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: 2022/03/09

### Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows 10 Pro
Confidence level : 56
Method : MLSinFP
```

Not all fingerprints could give a match. If you think some or all of the following could be used to identify the host's operating system, please email them to [os-signatures@nessus.org](mailto:os-signatures@nessus.org). Be sure to include a brief description of the host itself, such as the actual operating system or product / model names.

```
SinFP::
P1:B11113:F0x12:W8192:00204ffff:M1460:
P2:B11113:F0x12:W8192:00204ffff0103030801010402:M1460:
P3:B00000:F0x00:W0:00:M0
P4:190101_7_p=139
```

The remote host is running Microsoft Windows 10 Pro

## 21745 - OS Security Patch Assessment Failed

### Synopsis

Errors prevented OS Security Patch Assessment.

### Description

OS Security Patch Assessment is not available for this host because either the credentials supplied in the scan policy did not allow Nessus to log into it or some other problem occurred.

### Solution

Fix the problem(s) so that OS Security Patch Assessment is possible.

### Risk Factor

None

### References

XREF IAVB:0001-B-0501

### Plugin Information

Published: 2006/06/23, Modified: 2021/07/12

### Plugin Output

tcp/0

The following service errors were logged :

```
- Plugin      : smb_login.nasl
  Plugin ID   : 10394
  Plugin Name : Microsoft Windows SMB Log In Possible
  Protocol    : SMB
  Message     :
```

It was not possible to log into the remote host via smb (invalid credentials).

## 104410 - Target Credential Status by Authentication Protocol - Failure for Provided Credentials

### Synopsis

Nessus was unable to log into the detected authentication protocol, using the provided credentials, in order to perform credentialed checks.

### Description

Nessus failed 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 failure in protocol negotiation or communication that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may have been invalid. A protocol failure may indicate a compatibility issue with the protocol configuration. A protocol failure due to an environmental issue such as resource or congestion issues may also prevent valid credentials from being identified. 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

Address the reported problem(s) so that credentialed checks can be executed.

### Risk Factor

None

### References

XREF IAVB:0001-B-0503

### Plugin Information

Published: 2017/11/06, Modified: 2020/10/19

### Plugin Output

tcp/445/cifs

Nessus was unable to log into the following host for which credentials have been provided :

Protocol : SMB  
Port : 445  
Failure details :

- User : Mohammad

- Plugin : smb\_login.nasl  
Plugin ID : 10394  
Plugin Name : Microsoft Windows SMB Log In Possible  
Message : SMB2 authentication : smb2\_session\_setup() failed.

- Plugin : smb\_login.nasl  
Plugin ID : 10394  
Plugin Name : Microsoft Windows SMB Log In Possible  
Message :

Initial SMB negotiation : smb\_negotiate\_protocol() failed.

- Plugin : smb\_login.nasl  
Plugin ID : 10394  
Plugin Name : Microsoft Windows SMB Log In Possible  
Message :

Failed to authenticate using the supplied credentials.



## 10287 - Traceroute Information

### Synopsis

It was possible to obtain traceroute information.

### Description

Makes a traceroute to the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

### Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.110 to 192.168.1.101 :
192.168.1.110
192.168.1.101

Hop Count: 1
```

## 20094 - VMware Virtual Machine Detection

### Synopsis

The remote host is a VMware virtual machine.

### Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

### Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

### Risk Factor

None

### Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

### Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

## 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: 2022/05/03

### Plugin Output

tcp/445/cifs

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

### 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

udp/137/netbios-ns

```
The following 6 NetBIOS names have been gathered :
```

```
DESKTOP-0N46D3D  = Computer name
WORKGROUP        = Workgroup / Domain name
DESKTOP-0N46D3D  = File Server Service
WORKGROUP        = Browser Service Elections
WORKGROUP        = Master Browser
__MSBROWSE__     = Master Browser
```

```
The remote host has the following MAC address on its adapter :
```

```
00:0c:29:07:ac:a3
```