



## scanallport

---

Report generated by Nessus™

Sun, 31 Dec 2023 09:55:05 EST

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.188.54.....	4
• 192.168.188.254.....	58

Nessus Essentials

---

## **Vulnerabilities by Host**

---

192.168.188.54



#### Scan Information

Start time: Sun Dec 31 09:34:06 2023  
End time: Sun Dec 31 09:55:04 2023

#### Host Information

Netbios Name: VICTIM  
IP: 192.168.188.54  
OS: Microsoft Windows 10 Enterprise

#### Vulnerabilities

##### 10297 - Web Server Directory Traversal Arbitrary File Access

#### Synopsis

The remote web server is affected by a directory traversal vulnerability.

#### Description

It appears possible to read arbitrary files on the remote host outside the web server's document directory using a specially crafted URL. An unauthenticated attacker may be able to exploit this issue to access sensitive information to aid in subsequent attacks.

Note that this plugin is not limited to testing for known vulnerabilities in a specific set of web servers. Instead, it attempts a variety of generic directory traversal attacks and considers a product to be vulnerable simply if it finds evidence of the contents of '/etc/passwd' or a Windows 'win.ini' file in the response. It may, in fact, uncover 'new' issues, that have yet to be reported to the product's vendor.

#### Solution

Contact the vendor for an update, use a different product, or disable the service altogether.

#### Risk Factor

High

#### CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.2 (CVSS2#E:H/RL:OF/RC:C)

References

XREF           CWE:22

Plugin Information

Published: 1999/11/05, Modified: 2023/04/07

Plugin Output

tcp/27498/www

```
Nessus was able to retrieve the remote host's 'win.ini' file using the
following URL :
```

```
- http://192.168.188.54:27498/../../../../../../../../../../../../windows/win.ini
```

```
Here are the contents :
```

```
----- snip -----
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
; OS{07d20642a9b928cdb6afe832f0f4ebe6}{}
----- snip -----
```

```
Note that Nessus stopped searching after one exploit was found. To
report all known exploits, enable the 'Perform thorough tests'
setting and re-scan.
```

## 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

## 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: 2023/12/27

### Plugin Output

tcp/0

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

```
cpe:/o:microsoft:windows_10::enterprise -> 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-ce43-9c1dfc11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Remote RPC service
Named pipe : \PIPE\ROUTER
Netbios name : \\VICTIM

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 : \\VICTIM

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 : \\VICTIM

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 : \\VICTIM

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0  
Description : Unknown RPC service  
Type : Remote RPC service  
Named pipe : \PIPE\atsvc  
Netbios name : \\VICTIM

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 : \\VICTIM

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 : \\VICTIM

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 : \\VICTIM

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000  
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0  
D [...]

## 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 : 192.168.188.54

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 : 192.168.188.54

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 : 192.168.188.54

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 : 192.168.188.54

## 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-2c84da1ddb0d, version 1.0  
Description : Unknown RPC service  
Type : Remote RPC service  
TCP Port : 49665  
IP : 192.168.188.54

## 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 : 192.168.188.54
```



## 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 : 192.168.188.54

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 : 192.168.188.54

## 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 : 192.168.188.54

Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0  
Description : Unknown RPC service  
Type : Remote RPC service  
TCP Port : 49668  
IP : 192.168.188.54

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 : 192.168.188.54

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 : 192.168.188.54

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 : 192.168.188.54

## 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/49669/dce-rpc

The following DCERPC services are available on TCP port 49669 :

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 : 49669  
IP : 192.168.188.54

## 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 : 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1.0
Description : Unknown RPC service
Annotation : Remote Fw APIs
Type : Remote RPC service
TCP Port : 49670
IP : 192.168.188.54
```

## 54615 - Device Type

### Synopsis

It is possible to guess the remote device type.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/0

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

## 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/27498/www

```
The remote web server type is :  
Easy Chat Server/1.0
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

### Plugin Output

tcp/27498/www

Response Code : HTTP/1.0 200 OK

Protocol version : HTTP/1.0

SSL : no

Keep-Alive : yes

Options allowed : (Not implemented)

Headers :

Date: Sun, 31 Dec 2023 14:41:43 GMT

Server: Easy Chat Server/1.0

Accept-Ranges: bytes

Content-Length: 6822

Connection: Keep-Alive

Content-Type: text/html

Response Body :

<HTML>

<HEAD>

<meta http-equiv=refresh content=150>

<TITLE>Easy Chat Server</TITLE>

<SCRIPT LANGUAGE=javascript>

<!--

```
var rooms = new Array("first chat room","0",false,"admin","/01/",0,1,"let's talk about  
love","0",false,"admin,Lisa","/01/",0,2,"football","0",false,"Jackson,fire","/01/",0,3,"vip  
room","0",false,"admin,David,Lisa","/01/",0,4)
```

```
var OnlineUsers = 0 ;
```



```

var MaxOnline = 100 ;
var RegUsers = 200 ;
var num=7, count=rooms.length/num ;
function GetRoomTitle(n){n=n*num;if (n<rooms.length)return rooms[n+0];else return null;}
function GetUserCount(n){n=n*num;if (n<rooms.length)return rooms[n+1];else return 0;}
function IsRoomFull(n) {n=n*num;if (n<rooms.length)return rooms[n+2];else return false;}
function GetRoomAdmin(n){n=n*num;if (n<rooms.length)return rooms[n+3];else return null;}
function GetRoomURL(n){n=n*num;if (n<rooms.length)return rooms[n+4];else return null;}
function GetRoomType(n){n=n*num;if (n<rooms.length)return rooms[n+5];else return null;}
function GetRoomID(n){n=n*num;if (n<rooms.length)return rooms[n+6];else return null;}
var iOpenWindowName=1;
function OnLogin(n)
{if(IsRoomFull(n)){alert("this chat room is full!") ;return;}
if(!validstr(document.login.user))return ;
var strSex = "&sex=" + document.login.sex.value ;
iOpenWindowName+=1;//new
var userAgent = navigator.userAgent; //2012/04/30
if(userAgent.indexOf("Chrome") > -1)
{
    chat=window.open("chat.ghp?"+document.login.user.value
+"&password="+document.login.pass.value
+"&room="+GetRoomID(n)+strSex,iOpenWindowName,"toolbar=no,location=no,directories=no,menubar=no,resizable=yes"+",w
+",height="+screen.height);
}
else
{
    chat=window.o [...]

```

## 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: 2023/04/27

### Plugin Output

icmp/0

```
This host returns non-standard timestamps (high bit is set)
The ICMP timestamps might be in little endian format (not in network format)
The difference between the local and remote clocks is -1 seconds.
```

## 42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

### 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 :
```

```
VICTIM          = Computer name
VICTIM          = Workgroup / Domain name
```

## 10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

### 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: VICTIM  
NetBIOS Domain Name: VICTIM  
NetBIOS Computer Name: VICTIM  
DNS Domain Name: VICTIM  
DNS Computer Name: VICTIM  
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: 2023/09/25

### 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: 2023/09/25

### 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: 2023/09/25

### Plugin Output

---

tcp/445/cifs

```
Port 445/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: 2023/09/25

### Plugin Output

---

tcp/5040

```
Port 5040/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: 2023/09/25

### Plugin Output

---

tcp/7680

```
Port 7680/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: 2023/09/25

### Plugin Output

---

tcp/27498/www

```
Port 27498/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: 2023/09/25

### Plugin Output

---

tcp/49664/dce-rpc

```
Port 49664/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: 2023/09/25

### Plugin Output

---

tcp/49665/dce-rpc

```
Port 49665/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: 2023/09/25

### Plugin Output

---

tcp/49666/dce-rpc

```
Port 49666/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: 2023/09/25

### Plugin Output

---

tcp/49667/dce-rpc

```
Port 49667/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: 2023/09/25

### Plugin Output

---

tcp/49668/dce-rpc

```
Port 49668/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: 2023/09/25

### Plugin Output

---

tcp/49669/dce-rpc

```
Port 49669/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: 2023/09/25

### Plugin Output

---

tcp/49670/dce-rpc

```
Port 49670/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: 2023/07/31

### Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.6.4
Nessus build : 20005
Plugin feed version : 202312310648
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1404-x86-64
Scan type : Normal
Scan name : scanallport
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.45.198
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 68.325 ms
Thorough tests : no
Experimental tests : 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 launched)
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 : 2023/12/31 9:34 EST
Scan duration : 1253 sec
Scan for malware : no
```

## 11936 - OS Identification

### Synopsis

It is possible to guess the remote operating system.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2003/12/09, Modified: 2023/11/08

### Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows 10 Enterprise
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.

```
HTTP:::Server: Easy Chat Server/1.0
```

```
SinFP:::
P1:B11113:F0x12:W65392:00204ffff:M1361:
P2:B11113:F0x12:W65535:00204ffff0103030801010402:M1361:
P3:B00000:F0x00:W0:00:M0
P4:190704_7_p=49669R
```

The remote host is running Microsoft Windows 10 Enterprise



## 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      : 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.
```

## 10919 - Open Port Re-check

### Synopsis

Previously open ports are now closed.

### Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.
- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.
- This scanner may have been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.
- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

### Solution

Steps to resolve this issue include :

- Increase checks\_read\_timeout and/or reduce max\_checks.
- Disable any IPS during the Nessus scan

### Risk Factor

None

### References

XREF IAVB:0001-B-0509

### Plugin Information

Published: 2002/03/19, Modified: 2023/06/20

### Plugin Output

tcp/0

Port 7680 was detected as being open but is now closed

## 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: 2023/07/10

### Plugin Output

tcp/27498/www

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

## 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: 2023/02/13

### Plugin Output

tcp/0

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



## 10287 - Traceroute Information

### Synopsis

It was possible to obtain traceroute information.

### Description

Makes a traceroute to the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.45.198 to 192.168.188.54 :
192.168.45.198
192.168.45.1
192.168.45.254
192.168.251.1
192.168.188.54

Hop Count: 4
```

## 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: 2023/11/14

### 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

tcp/445/cifs

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

```
VICTIM          = Computer name
VICTIM          = Workgroup / Domain name
```

192.168.188.254



#### Scan Information

Start time: Sun Dec 31 09:35:18 2023

End time: Sun Dec 31 09:40:18 2023

#### Host Information

IP: 192.168.188.254

OS: FreeBSD 12.3-STABLE (amd64)

#### Vulnerabilities

##### 97861 - Network Time Protocol (NTP) Mode 6 Scanner

#### Synopsis

The remote NTP server responds to mode 6 queries.

#### Description

The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.

#### See Also

<https://ntpscan.shadowserver.org>

#### Solution

Restrict NTP mode 6 queries.

#### Risk Factor

Medium

#### CVSS v3.0 Base Score

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

## CVSS v2.0 Base Score

---

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

## Plugin Information

---

Published: 2017/03/21, Modified: 2018/05/07

## Plugin Output

---

udp/123/ntp

```
Nessus elicited the following response from the remote  
host by sending an NTP mode 6 query :
```

```
'version="ntpd 4.2.8p15@1.3728-o Wed Jan 12 15:39:52 UTC 2022 (1)",  
processor="amd64", system="FreeBSD/12.3-STABLE", leap=0, stratum=3,  
precision=-20, rootdelay=21.340, rootdisp=41.733, refid=5.196.8.113,  
reftime=0xe93bfb31.313b7b3d, clock=0xe93bfb97.dcdc12b3, peer=9322, tc=8,  
mintc=3, offset=1.882146, frequency=5.532, sys_jitter=1.006572,  
clk_jitter=0.268, clk_wander=0.081'
```

## 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: 2023/12/27

### Plugin Output

tcp/0

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

```
cpe:/o:freebsd:freebsd:12.3 -> FreeBSD
```

## 11002 - DNS Server Detection

### Synopsis

A DNS server is listening on the remote host.

### Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

### See Also

[https://en.wikipedia.org/wiki/Domain\\_Name\\_System](https://en.wikipedia.org/wiki/Domain_Name_System)

### Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

### Risk Factor

None

### Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

### Plugin Output

tcp/53/dns

## 11002 - DNS Server Detection

### Synopsis

---

A DNS server is listening on the remote host.

### Description

---

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

### See Also

---

[https://en.wikipedia.org/wiki/Domain\\_Name\\_System](https://en.wikipedia.org/wiki/Domain_Name_System)

### Solution

---

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

### Risk Factor

---

None

### Plugin Information

---

Published: 2003/02/13, Modified: 2017/05/16

### Plugin Output

---

udp/53/dns

## 54615 - Device Type

### Synopsis

It is possible to guess the remote device type.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 98
```

## 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: 2023/04/27

### Plugin Output

icmp/0

```
The remote clock is synchronized with the local clock.
```



### 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: 2023/09/25

### Plugin Output

---

tcp/53/dns

```
Port 53/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: 2023/07/31

### Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.6.4
Nessus build : 20005
Plugin feed version : 202312310648
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1404-x86-64
Scan type : Normal
Scan name : scanallport
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.45.198
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 81.857 ms
Thorough tests : no
Experimental tests : 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 launched)
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 : 2023/12/31 9:35 EST
Scan duration : 291 sec
Scan for malware : no
```

## 10884 - Network Time Protocol (NTP) Server Detection

### Synopsis

An NTP server is listening on the remote host.

### Description

An NTP server is listening on port 123. If not securely configured, it may provide information about its version, current date, current time, and possibly system information.

### See Also

<http://www.ntp.org>

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0934

### Plugin Information

Published: 2015/03/20, Modified: 2021/02/24

### Plugin Output

udp/123/ntp

```
An NTP service has been discovered, listening on port 123.
```

```
Version : 4.2.8p15
```

## 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: 2023/11/08

### Plugin Output

tcp/0

```
Remote operating system : FreeBSD 12.3-STABLE (amd64)
Confidence level : 98
Method : NTP
```

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.

```
NTP:FreeBSD/12.3-STABLE
SinFP:::
P1:B10113:F0x12:W65228:00204ffff:M1361:
P2:B10113:F0x12:W65228:00204ffff010303070402080affffff44454144:M1361:
P3:B00000:F0x00:W0:00:M0
P4:190704_7_p=53R
```

```
The remote host is running FreeBSD 12.3-STABLE (amd64)
```

## 25220 - TCP/IP Timestamps Supported

### Synopsis

---

The remote service implements TCP timestamps.

### Description

---

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

### See Also

---

<http://www.ietf.org/rfc/rfc1323.txt>

### Solution

---

n/a

### Risk Factor

---

None

### Plugin Information

---

Published: 2007/05/16, Modified: 2023/10/17

### Plugin Output

---

tcp/0

## 10287 - Traceroute Information

### Synopsis

It was possible to obtain traceroute information.

### Description

Makes a traceroute to the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.45.198 to 192.168.188.254 :  
192.168.45.198  
192.168.45.1  
192.168.45.254  
192.168.188.254
```

```
Hop Count: 3
```