KPMC

Report generated by Nessus™ Wed, 06 Jun 2018 17:39:54 GMT+0100

TABLE OF CONTENTS

Vulnerabilities by Host

Remediations

Vulnerabilities by Host

192.168.1.64

0	0	1	0	36
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Wed Jun 06 17:41:23 2018
End time:	Wed Jun 06 17:51:35 2018

Host Information

DNS Name:	DESKTOP-8TD7MQ3.lan
Netbios Name:	DESKTOP-8TD7MQ3
IP:	192.168.1.64
MAC Address:	90:e6:ba:b7:33:77
OS:	Microsoft Windows Server 2003, Microsoft Windows Vista, Microsoft Windows Server 2008, Microsoft Windows 7, Microsoft Windows Server 2008 R2

Vulnerabilities

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

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Published: 1999/08/01, Modified: 2012/06/18

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 -3 seconds.
```

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 has 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

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

Plugin Information:

Published: 2002/03/19, Modified: 2014/06/04

Plugin Output

tcp/0

```
Port 2869 was detected as being open but is now unresponsive
Port 2968 was detected as being open but is now unresponsive
Port 135 was detected as being open but is now unresponsive
Port 80 was detected as being open but is now unresponsive
Port 8000 was detected as being open but is now unresponsive
```

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: 2018/04/19

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows Server 2003
Microsoft Windows Vista
Microsoft Windows Server 2008
Microsoft Windows 7
Microsoft Windows Server 2008 R2
Confidence level : 70
Method : HTTP


The remote host is running one of these operating systems :
Microsoft Windows Server 2003
Microsoft Windows Vista
Microsoft Windows Server 2008
Microsoft Windows 7
Microsoft Windows Server 2008 R2
```

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

```
192.168.1.64 resolves as DESKTOP-8TD7MQ3.lan.
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.1.0
Plugin feed version : 201806052020
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.77
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 5
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2018/6/6 17:41
Scan duration : 605 sec
```

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

http://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: 2017/11/17

Plugin Output

tcp/0

```

The following card manufacturers were identified :

90:e6:ba:b7:33:77 : ASUSTek COMPUTER INC.
```

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: 2017/06/06

Plugin Output

tcp/0

```

The remote operating system matched the following CPE's :

  cpe:/o:microsoft:windows_2003_server
  cpe:/o:microsoft:windows_vista
  cpe:/o:microsoft:windows_server_2008
  cpe:/o:microsoft:windows_7
  cpe:/o:microsoft:windows_server_2008:r2 -> Microsoft Windows Server 2008 R2

Following application CPE matched on the remote system :

  cpe:/a:microsoft:iis:10.0
```

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

https://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information:

Published: 2010/04/29, Modified: 2017/04/27

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - desktop-8td7mq3
```

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 : general-purpose
Confidence level : 70
```

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: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.77 to 192.168.1.64 :
192.168.1.77
192.168.1.64

Hop Count: 1
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/80

```
The remote web server type is :

Microsoft-IIS/10.0
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/80

```
Port 80/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/80

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

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: 2017/11/13

Plugin Output

tcp/80

```

Response Code : HTTP/1.1 200 OK

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

  Content-Type: text/html
  Last-Modified: Sat, 19 May 2018 09:45:19 GMT
  Accept-Ranges: bytes
  ETag: "81629b1956efd31:0"
  Server: Microsoft-IIS/10.0
  X-Powered-By: ASP.NET
  Date: Wed, 06 Jun 2018 16:43:54 GMT
  Content-Length: 696

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows</title>
<style type="text/css">
<!--
```

```
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img src="iisstart.png"
 alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/12/10, Modified: 2018/05/23

Plugin Output

tcp/80

```
Based on the response to an OPTIONS request :

  - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP methods   -
 HTTP methods    - HTTP methods   - HTTP methods  GET    - HTTP methods   - HTTP methods    - HTTP
 methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods
  GET  HEAD   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP
 methods   - HTTP methods    - HTTP methods   - HTTP methods  GET    - HTTP methods   - HTTP methods
    - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   -
 HTTP methods  GET  HEAD    - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET
  - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET    - HTTP methods   - HTTP
 methods    - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods
   - HTTP methods  GET  HEAD   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods
 GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET    - HTTP methods
 - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP
 methods   - HTTP methods  GET  HEAD  POST   - HTTP methods   - HTTP methods    - HTTP methods
 - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET
 - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP
 methods    - HTTP methods   - HTTP methods  GET  HEAD   - HTTP methods   - HTTP methods    - HTTP
 methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods
  GET    - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP methods
  - HTTP methods    - HTTP methods   - HTTP methods  GET  HEAD    - HTTP methods   - HTTP methods
```

```
   - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP
  methods  GET    - HTTP methods   - HTTP m [...]
```

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: 2014/05/12

Plugin Output

tcp/135

```
The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc07D9C0

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc07D9C0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
```

```
Description : Unknown RPC service
Type : Local RPC service
Named pipe : dabrpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : csebpub

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-77e3fa4e324e7c7a6e

Object UUID : 18a27bed-fb3c-0007-4b50-525250524944
UUID : 18a27bed-d801-7233-4b50-525250524f50, version 46.99
Description : Unknown RPC service
Annotation : PR_REMOTE_MANAGER_PROP
Type : Local RPC service
Named pipe : PRRNameService:3340

Object UUID : 18a27bed-e72a-000f-4b50-525250524944
UUID : 18a27bed-e474-f035-4b50-525250524f50, version 46.99
Description : Unknown RPC service
Annotation : cpnPRAGUE_REMOTE_API
Type : Local RPC service
Named pipe : PRRNameService:3340

Object UUID : 00763004-0000-0000-4b50-5252484e444c
UUID : 18a27bed-c75c-28ad-4b50-52524f424a53, version 46.99
Description : Unknown RPC service
Annot [...]
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/135

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

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

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: 2017/09/27

Plugin Output

udp/137

```
The following 4 NetBIOS names have been gathered :

 DESKTOP-8TD7MQ3  = File Server Service
 DESKTOP-8TD7MQ3  = Computer name
 WORKGROUP        = Workgroup / Domain name
 WORKGROUP        = Browser Service Elections

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

   90:e6:ba:b7:33:77
```

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: 2015/06/02

Plugin Output

tcp/139

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/139

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

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

https://support.microsoft.com/en-us/kb/887429

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

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

http://www.samba.org/samba/docs/man/manpages-3/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 Base Score

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

CVSS Temporal Score

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

Plugin Information:

Published: 2012/01/19, Modified: 2018/05/02

Plugin Output

tcp/445

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: 2014/05/12

Plugin Output

tcp/445

```

The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\DESKTOP-8TD7MQ3

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\DESKTOP-8TD7MQ3

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
Named pipe : \pipe\lsass
Netbios name : \\DESKTOP-8TD7MQ3

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
Named pipe : \pipe\lsass
Netbios name : \\DESKTOP-8TD7MQ3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\DESKTOP-8TD7MQ3

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
Named pipe : \pipe\lsass
Netbios name : \\DESKTOP-8TD7MQ3

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-8TD7MQ3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0767a036-0d22-48aa-ba69-b619480f38cb, version 1.0
Description : Unknown RPC service
Annotation : PcaSvc
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\DESKTOP-8TD [...]
```

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: 2015/06/02

Plugin Output

tcp/445

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/445

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

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: 2017/06/19

Plugin Output

tcp/445

```

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

106716 - Microsoft Windows SMB2 Dialects Supported (remote check)

Synopsis

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

Description

Nessus was able to obtain the set of SMB2 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: 2018/02/09

Plugin Output

tcp/445

```

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
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/2869

```
Port 2869/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/2869

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/2968

```
Port 2968/tcp was found to be open
```

53513 - Link-Local Multicast Name Resolution (LLMNR) Detection

Synopsis

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

See Also

http://www.nessus.org/u?85beb421

http://technet.microsoft.com/en-us/library/bb878128.aspx

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Published: 2011/04/21, Modified: 2012/03/05

Plugin Output

udp/5355

```
According to LLMNR, the name of the remote host is 'DESKTOP-8TD7MQ3'.
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/8000

```
Port 8000/tcp was found to be open
```

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: 2014/05/12

Plugin Output

tcp/49664

```
The following DCERPC services are available on TCP port 49664 :

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 : 49664
IP : 192.168.1.64
```

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: 2014/05/12

Plugin Output

tcp/49665

```

The following DCERPC services are available on TCP port 49665 :

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 : 49665
IP : 192.168.1.64

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.1.64

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.1.64

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.1.64

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.1.64

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.1.64
```

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: 2014/05/12

Plugin Output

tcp/49666

```
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 : 192.168.1.64

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 : 192.168.1.64

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b18fbab6-56f8-4702-84e0-41053293a869, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.64

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
```

```
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.64

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.64

Object UUID : ccb8aa07-7225-4ea0-8501-4b3c1b1acd43
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.64

Object UUID : 582a47b2-bcd8-4d3c-8acb-fe09d5bd6eec
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.64

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.64

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.64

Object UUI [...]
```

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: 2014/05/12

Plugin Output

tcp/49667

```

The following DCERPC services are available on TCP port 49667 :

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 : 49667
IP : 192.168.1.64

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 : 49667
IP : 192.168.1.64

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 : 49667
IP : 192.168.1.64

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 : 49667
IP : 192.168.1.64

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 : 49667
IP : 192.168.1.64
```

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: 2014/05/12

Plugin Output

tcp/49670

```

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 : 192.168.1.64

```

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: 2014/05/12

Plugin Output

tcp/49682

```
The following DCERPC services are available on TCP port 49682 :

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 : 49682
IP : 192.168.1.64
```

192.168.1.77

0	0	11	1	100
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Wed Jun 06 17:41:47 2018
End time:	Wed Jun 06 17:54:13 2018

Host Information

DNS Name:	SERVIDOR.lan
Netbios Name:	SERVIDOR
IP:	192.168.1.77
OS:	Microsoft Windows 10

Vulnerabilities

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: 2018/04/19

Plugin Output

tcp/0

```

Remote operating system : Microsoft Windows 10
Confidence level : 75
Method : HTTP


The remote host is running Microsoft Windows 10
```

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

```
192.168.1.77 resolves as SERVIDOR.lan.
```

12634 - Authenticated Check : OS Name and Installed Package Enumeration

Synopsis

This plugin gathers information about the remote host via an authenticated session.

Description

This plugin logs into the remote host using SSH, RSH, RLOGIN, Telnet, or local commands and extracts the list of installed packages.

If using SSH, the scan should be configured with a valid SSH public key and possibly an SSH passphrase (if the SSH public key is protected by a passphrase).

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/07/06, Modified: 2018/05/11

Plugin Output

tcp/0

```
Nessus can run commands on localhost to check if patches are applied.

However, the execution of the command "uname -a" failed, so local security
checks have not been enabled.

SSH Version Banner :
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.1.0
Plugin feed version : 201806052020
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.77
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
```

```
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 5
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2018/6/6 17:41
Scan duration : 746 sec
```

21745 - Authentication Failure - Local Checks Not Run

Synopsis

The local security checks are disabled.

Description

Local security checks have been disabled 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

Address the problem(s) so that local security checks are enabled.

Risk Factor

None

Plugin Information:

Published: 2006/06/23, Modified: 2017/11/29

Plugin Output

tcp/0

```

Additional failure information from ssh_get_info2.nasl :
The remote host is not currently supported by this plugin.
```

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: 2017/06/06

Plugin Output

tcp/0

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

  cpe:/o:microsoft:windows_10

Following application CPE matched on the remote system :

  cpe:/a:microsoft:iis:10.0
```

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

https://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information:

Published: 2010/04/29, Modified: 2017/04/27

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - servidor
```

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 : general-purpose
Confidence level : 75
```

58651 - Netstat Active Connections

Synopsis

Active connections are enumerated via the 'netstat' command.

Description

This plugin runs 'netstat' on the remote machine to enumerate all active 'ESTABLISHED' or 'LISTENING' tcp/udp connections.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2012/04/10, Modified: 2018/05/16

Plugin Output

tcp/0

```

Netstat output :

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1801           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2103           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2105           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2107           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2968           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5452           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8000           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8834           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49673          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49681          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:50658          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1241         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:50191        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:50191        127.0.0.1:60557        ESTABLISHED
  TCP    127.0.0.1:50191        127.0.0.1:60837        ESTABLISHED
  TCP    127.0.0.1:50192        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:50192        127.0.0.1:60011        ESTABLISHED
  TCP    127.0.0.1:50192        127.0.0.1:60228        ESTABLISHED
  TCP    127.0.0.1:50192        127.0.0.1:60637        ESTABLISHED
  TCP    127.0.0.1:50192        127.0.0.1:60848        ESTABLISHED
  TCP    127.0.0.1:50192        127.0.0.1:60855      [...]
```

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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/02/13, Modified: 2018/05/16

Plugin Output

tcp/0

```
tcp4 (listen)
  src: [host=0.0.0.0, port=80]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=135]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=445]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=1801]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=2103]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=2105]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=2107]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=2968]
```

```
    dst: [host=0.0.0.0, port=0]

  tcp4 (listen)
    src: [host=0.0.0.0, port=5040]
    dst: [host=0.0.0.0, port=0]

  tcp4 (listen)
    src: [host=0.0.0.0, port=5452]
    dst: [host=0.0.0.0, port=0]

  tcp4 (listen)
    src: [host=0.0.0.0, port=8000]
    dst: [host=0.0.0.0, port=0]

  tcp4 (listen)
    src: [host=0.0.0.0, port=8834]
    dst: [host=0.0.0.0, port=0]

  tcp4 (listen)
    src: [host=0.0.0.0, port=49664]
    dst: [host=0.0.0.0, port=0]

  tcp4 (listen)
    src: [host=0.0.0.0, port=49665]
    dst: [host=0.0.0.0, port=0]

  tcp4 (listen)
    src: [host=0.0.0.0, port=49666]
    dst: [host=0.0.0.0, port=0]

  tcp4 (listen)
    src: [host=0.0.0.0, port=49667]
    dst: [host=0.0.0.0, port=0]

  tcp4 (listen)
    src: [host=0.0.0.0, port=49668]
    dst: [host=0.0.0.0, port=0]

  tcp4 (listen)
    src: [host=0.0.0.0, port=49673]
    dst: [host=0.0.0.0, port=0]

  tcp4 (listen)
    src: [host=0.0.0.0, port=49681]
    dst: [host=0.0.0.0, port=0]

  tcp4 (listen)
    src: [host=0.0.0.0, port=50658]
    dst: [host=0.0.0.0, port=0]

  tcp4 (listen)
    src: [host=127.0.0.1, port=1241]
    dst: [host=0.0.0.0, port=0]

  tcp4 (listen)
    src: [host=127.0.0.1, port=50191]
    dst: [host=0.0.0.0, port=0]

  tcp4 (established)
    src: [host=127.0.0.1, port=50191]
    dst: [host=127.0.0.1, port=60557]

  tcp4 (established)
    src: [host=127.0.0.1, port=50191]
    dst: [host=127.0.0.1, port=60837]

  tcp4 (listen)
    src: [host=127.0.0.1, port=50192]
    dst: [host=0.0.0.0, port=0]
```

```
tcp4 (established)
  src: [host=127.0.0.1, port=50192]
  ds [...]
```

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: 2018/05/25

Plugin Output

tcp/0

```

Credentialed checks of Windows are not supported using SSH.

The remote host is not currently supported by this plugin.

Runtime : 1.56880 seconds
```

11714 - Nonexistent Page (404) Physical Path Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server reveals the physical path of the webroot when a nonexistent page is requested.

While printing errors to the output is useful for debugging applications, this feature should be disabled on production servers.

See Also

http://www.nessus.org/u?a3e58d0b

http://www.nessus.org/u?9c4d1560

http://www.nessus.org/u?67b9e782

Solution

Upgrade the web server to the latest version. Alternatively, reconfigure the web server to disable debug reporting.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:C)

References

BID	3341
BID	4035
BID	4261
BID	5054
BID	8075
CVE	CVE-2001-1372
CVE	CVE-2002-0266
CVE	CVE-2002-2008
CVE	CVE-2003-0456

XREF	OSVDB:4313
XREF	OSVDB:5406
XREF	OSVDB:6547
XREF	OSVDB:34884
XREF	CERT:278971
XREF	EDB-ID:21276
XREF	CWE:200

Plugin Information:

Published: 2003/06/11, Modified: 2016/05/13

Plugin Output

tcp/80

```
  URL                 : http://SERVIDOR.lan/niet984037992
  Path disclosed      : C:\inetpub\wwwroot\
  Response snippet    :
------------------------------ snip ------------------------------
   <table border="0" cellpadding="0" cellspacing="0">

    <tr class="alt"><th>URL Pedido</th><td>&nbsp;&nbsp;&nbsp;http://SERVIDOR.lan:80/niet984037992</
td></tr>

    <tr><th>Caminho F..sico</th><td>&nbsp;&nbsp;&nbsp;C:\inetpub\wwwroot\niet984037992</td></tr>

    <tr class="alt"><th>M..todo de In..cio de Sess..o</th><td>&nbsp;&nbsp;&nbsp;An..nimo</td></tr>

    <tr><th>Utilizador de In..cio de Sess..o</th><td>&nbsp;&nbsp;&nbsp;An..nimo</td></tr>


------------------------------ snip ------------------------------
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/80

```
The remote web server type is :

Microsoft-IIS/10.0
```

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.

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: 2018/05/30

Plugin Output

tcp/80

```
Port 80/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/80

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

24242 - Microsoft .NET Handlers Enumeration

Synopsis

It is possible to enumerate the remote .NET handlers used by the remote web server.

Description

It is possible to obtain the list of handlers the remote ASP.NET web server supports.

See Also

http://support.microsoft.com/kb/815145

Solution

None

Risk Factor

None

Plugin Information:

Published: 2007/01/26, Modified: 2011/03/14

Plugin Output

tcp/80

```
The remote extensions are handled by the remote ASP.NET server :

 - .rem
 - .soap
```

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: 2017/11/13

Plugin Output

tcp/80

```

Response Code : HTTP/1.1 200 OK

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

  Content-Type: text/html
  Last-Modified: Tue, 15 May 2018 14:03:04 GMT
  Accept-Ranges: bytes
  ETag: "bd638d7155ecd31:0"
  Server: Microsoft-IIS/10.0
  X-Powered-By: ASP.NET
  Date: Wed, 06 Jun 2018 16:43:12 GMT
  Content-Length: 696

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows</title>
<style type="text/css">
<!--
```

```
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img src="iisstart.png"
 alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/12/10, Modified: 2018/05/23

Plugin Output

tcp/80

```
Based on the response to an OPTIONS request :

  - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP methods   -
 HTTP methods    - HTTP methods   - HTTP methods  GET    - HTTP methods   - HTTP methods    - HTTP
 methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods
  GET  HEAD   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP
 methods   - HTTP methods    - HTTP methods   - HTTP methods  GET    - HTTP methods   - HTTP methods
   - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   -
 HTTP methods  GET  HEAD    - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET
  - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET    - HTTP methods   - HTTP
 methods    - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods
   - HTTP methods  GET  HEAD   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods
 GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET    - HTTP methods
 - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP
 methods   - HTTP methods  GET  HEAD  POST   - HTTP methods   - HTTP methods    - HTTP methods
 - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET
 - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP
 methods    - HTTP methods   - HTTP methods  GET  HEAD   - HTTP methods   - HTTP methods    - HTTP
 methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods
  GET    - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP methods
  - HTTP methods    - HTTP methods   - HTTP methods  GET  HEAD    - HTTP methods   - HTTP methods
  - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP
 methods  GET    - HTTP methods   - HTTP m [...]
```

85805 - HTTP/2 Cleartext Detection

Synopsis

An HTTP/2 server is listening on the remote host.

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information:

Published: 2015/09/04, Modified: 2016/01/07

Plugin Output

tcp/80

```

The server supports direct HTTP/2 connections
without encryption.
```

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: 2014/05/12

Plugin Output

tcp/135

```
The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc085280

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc085280

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
```

```
Description : Unknown RPC service
Type : Local RPC service
Named pipe : dabrpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : csebpub

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-83b511c34e5179403d

Object UUID : 18a27bed-fb3c-0007-4b50-525250524944
UUID : 18a27bed-d801-7233-4b50-525250524f50, version 92.122
Description : Unknown RPC service
Annotation : PR_REMOTE_MANAGER_PROP
Type : Local RPC service
Named pipe : PRRNameService:2604

Object UUID : 18a27bed-e72a-000f-4b50-525250524944
UUID : 18a27bed-e474-f035-4b50-525250524f50, version 92.122
Description : Unknown RPC service
Annotation : cpnPRAGUE_REMOTE_API
Type : Local RPC service
Named pipe : PRRNameService:2604

Object UUID : 07df8668-0000-0000-4b50-5252484e444c
UUID : 18a27bed-c75c-28ad-4b50-52524f424a53, version 92.122
Description : Unknown RPC service
An [...]
```

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.

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: 2018/05/30

Plugin Output

tcp/135

```
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.

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: 2018/05/30

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.

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: 2018/05/30

Plugin Output

udp/138

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

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: 2015/06/02

Plugin Output

tcp/139

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

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.

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: 2018/05/30

Plugin Output

tcp/139

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

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

https://support.microsoft.com/en-us/kb/887429

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

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

http://www.samba.org/samba/docs/man/manpages-3/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 Base Score

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

CVSS Temporal Score

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

Plugin Information:

Published: 2012/01/19, Modified: 2018/05/02

Plugin Output

tcp/445

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

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: 2017/09/27

Plugin Output

tcp/445

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

 SERVIDOR          = Computer name
 SERVIDOR          = Workgroup / Domain name
```

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: 2014/05/12

Plugin Output

tcp/445

```

The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\SERVIDOR

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\SERVIDOR

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
Named pipe : \pipe\lsass
Netbios name : \\SERVIDOR

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
```

```
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\SERVIDOR

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
Named pipe : \pipe\lsass
Netbios name : \\SERVIDOR

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
Named pipe : \pipe\lsass
Netbios name : \\SERVIDOR

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Remote RPC service
Named pipe : \PIPE\ROUTER
Netbios name : \\SERVIDOR

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 : \\SERVIDOR

Object UUID : 00000000-0000-0000-0000-0000000000 [...]
```

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: 2015/06/02

Plugin Output

tcp/445

```

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

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.

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: 2018/05/30

Plugin Output

tcp/445

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

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: 2011/03/27

Plugin Output

tcp/445

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

 SERVIDOR          = Computer name
 SERVIDOR          = Workgroup / Domain name
```

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: 2017/06/19

Plugin Output

tcp/445

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

106716 - Microsoft Windows SMB2 Dialects Supported (remote check)

Synopsis

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

Description

Nessus was able to obtain the set of SMB2 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: 2018/02/09

Plugin Output

tcp/445

```

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
```

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.

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: 2018/05/30

Plugin Output

udp/500

```
Port 500/udp was found to be open
```

10674 - Microsoft SQL Server UDP Query Remote Version Disclosure

Synopsis

It is possible to determine the remote SQL server version.

Description

Microsoft SQL server has a function wherein remote users can query the database server for the version that is being run. The query takes place over the same UDP port that handles the mapping of multiple SQL server instances on the same machine.

It is important to note that, after Version 8.00.194, Microsoft decided not to update this function. This means that the data returned by the SQL ping is inaccurate for newer releases of SQL Server.

Solution

If there is only a single SQL instance installed on the remote host, consider filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Published: 2001/05/25, Modified: 2018/03/13

Plugin Output

udp/1434

```
A 'ping' request returned the following information about the remote
SQL instance :

  ServerName   : SERVIDOR
  InstanceName : PRIMAVERA
  IsClustered  : No
  Version      : 12.0.2000.8
  tcp          : 50658
  np           : \\SERVIDOR\pipe\MSSQL$PRIMAVERA\sql\query
```

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.

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: 2018/05/30

Plugin Output

udp/1434

```
Port 1434/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.

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: 2018/05/30

Plugin Output

tcp/1801

```
Port 1801/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.

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: 2018/05/30

Plugin Output

udp/1900

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

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: 2014/05/12

Plugin Output

tcp/2103

```
The following DCERPC services are available on TCP port 2103 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.1.77

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.1.77

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.1.77
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.1.77
```

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.

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: 2018/05/30

Plugin Output

tcp/2103

```
Port 2103/tcp was found to be open
```

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: 2014/05/12

Plugin Output

tcp/2105

```

The following DCERPC services are available on TCP port 2105 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.1.77

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.1.77

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.1.77
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.1.77
```

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.

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: 2018/05/30

Plugin Output

tcp/2105

```
Port 2105/tcp was found to be open
```

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: 2014/05/12

Plugin Output

tcp/2107

```

The following DCERPC services are available on TCP port 2107 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.1.77

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.1.77

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.1.77
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.1.77
```

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.

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: 2018/05/30

Plugin Output

tcp/2107

```
Port 2107/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.

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: 2018/05/30

Plugin Output

udp/2968

```
Port 2968/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.

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: 2018/05/30

Plugin Output

udp/3702

```
Port 3702/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.

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: 2018/05/30

Plugin Output

udp/4500

```
Port 4500/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.

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: 2018/05/30

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.

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: 2018/05/30

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.

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: 2018/05/30

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.

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: 2018/05/30

Plugin Output

udp/5355

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

11714 - Nonexistent Page (404) Physical Path Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server reveals the physical path of the webroot when a nonexistent page is requested.

While printing errors to the output is useful for debugging applications, this feature should be disabled on production servers.

See Also

http://www.nessus.org/u?a3e58d0b

http://www.nessus.org/u?9c4d1560

http://www.nessus.org/u?67b9e782

Solution

Upgrade the web server to the latest version. Alternatively, reconfigure the web server to disable debug reporting.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:C)

References

BID	3341
BID	4035
BID	4261
BID	5054
BID	8075
CVE	CVE-2001-1372
CVE	CVE-2002-0266
CVE	CVE-2002-2008
CVE	CVE-2003-0456

XREF	OSVDB:4313
XREF	OSVDB:5406
XREF	OSVDB:6547
XREF	OSVDB:34884
XREF	CERT:278971
XREF	EDB-ID:21276
XREF	CWE:200

Plugin Information:

Published: 2003/06/11, Modified: 2016/05/13

Plugin Output

tcp/5452

```

  URL                  : http://SERVIDOR.lan:5452/niet345934085
  Path disclosed       : C:\Program Files (x86)\PRIMAVERA\CloudServices900\CloudConnector\Host\
  Response snippet     :
------------------------------ snip ------------------------------
   <table border="0" cellpadding="0" cellspacing="0">

    <tr class="alt"><th>URL Pedido</th><td>&nbsp;&nbsp;&nbsp;http://SERVIDOR.lan:5452/
niet345934085</td></tr>

    <tr><th>Caminho F..sico</th><td>&nbsp;&nbsp;&nbsp;C:\Program Files (x86)\PRIMAVERA
\CloudServices900\CloudConnector\Host\niet345934085</td></tr>

    <tr class="alt"><th>M..todo de In..cio de Sess..o</th><td>&nbsp;&nbsp;&nbsp;An..nimo</td></tr>

    <tr><th>Utilizador de In..cio de Sess..o</th><td>&nbsp;&nbsp;&nbsp;An..nimo</td></tr>


------------------------------ snip ------------------------------
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/5452

```
The remote web server type is :

Microsoft-IIS/10.0
```

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.

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: 2018/05/30

Plugin Output

tcp/5452

```
Port 5452/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/5452

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

24242 - Microsoft .NET Handlers Enumeration

Synopsis

It is possible to enumerate the remote .NET handlers used by the remote web server.

Description

It is possible to obtain the list of handlers the remote ASP.NET web server supports.

See Also

http://support.microsoft.com/kb/815145

Solution

None

Risk Factor

None

Plugin Information:

Published: 2007/01/26, Modified: 2011/03/14

Plugin Output

tcp/5452

```
The remote extensions are handled by the remote ASP.NET server :

 - .rem
 - .soap
```

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: 2017/11/13

Plugin Output

tcp/5452

```
Response Code : HTTP/1.1 403 Forbidden

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

  Cache-Control: private
  Content-Type: text/html; charset=utf-8
  Server: Microsoft-IIS/10.0
  X-Powered-By: ASP.NET
  Date: Wed, 06 Jun 2018 16:43:12 GMT
  Content-Length: 5352

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Erro Detalhado do IIS 10.0 - 403.14 - Forbidden</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana,Arial,Helvetica,sans-serif;}
code{margin:0;color:#006600;font-size:1.1em;font-weight:bold;}
.config_source code{font-size:.8em;color:#000000;}
```

```
pre{margin:0;font-size:1.4em;word-wrap:break-word;}
ul,ol{margin:10px 0 10px 5px;}
ul.first,ol.first{margin-top:5px;}
fieldset{padding:0 15px 10px 15px;word-break:break-all;}
.summary-container fieldset{padding-bottom:5px;margin-top:4px;}
legend.no-expand-all{padding:2px 15px 4px 10px;margin:0 0 0 -12px;}
legend{color:#333333;;margin:4px 0 8px -12px;_margin-top:0px;
font-weight:bold;font-size:1em;}
a:link,a:visited{color:#007EFF;font-weight:bold;}
a:hover{text-decoration:none;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.4em;margin:10px 0 0 0;color:#CC0000;}
h4{font-size:1.2em;margin:10px 0 5px 0;
}#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS",Verdana,sans-
serif;
 color:#FFF;background-color:#5C87B2;
}#content{margin:0 0 0 2%;position:relative;}
.summary-container,.content-container{background:#FFF;width:96%;margin-
top:8px;padding:10px;position:relative;}
.content-container p{margin:0 0 10px 0;
}#details-left{width:35%;float:left;margin-right:2%;
}#details-right{width:63%;float:left;overflow:hidden;
}#server_version{width:96%;_height:1px;min-height:1px;margin:0 0 5px 0;padding:11px 2% 8px
 2%;color:#FFFFFF;
  [...]
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/12/10, Modified: 2018/05/23

Plugin Output

tcp/5452

```
Based on the response to an OPTIONS request :

  - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP methods   -
 HTTP methods    - HTTP methods   - HTTP methods  GET    - HTTP methods   - HTTP methods    - HTTP
 methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods
  GET  HEAD   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP
 methods   - HTTP methods    - HTTP methods   - HTTP methods  GET    - HTTP methods   - HTTP methods
    - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   -
 HTTP methods  GET  HEAD    - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET
  - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET    - HTTP methods   - HTTP
 methods    - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods
   - HTTP methods  GET  HEAD   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods
 GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET    - HTTP methods
 - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP
 methods   - HTTP methods  GET  HEAD  POST   - HTTP methods   - HTTP methods    - HTTP methods
 - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET
 - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP
 methods    - HTTP methods   - HTTP methods  GET  HEAD   - HTTP methods   - HTTP methods    - HTTP
 methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods
  GET    - HTTP methods   - HTTP methods    - HTTP methods   - HTTP methods  GET   - HTTP methods
  - HTTP methods    - HTTP methods   - HTTP methods  GET  HEAD    - HTTP methods   - HTTP methods
  - HTTP methods   - HTTP methods  GET   - HTTP methods   - HTTP methods    - HTTP methods   - HTTP
 methods  GET    - HTTP methods   - HTTP m [...]
```

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.

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: 2018/05/30

Plugin Output

tcp/8000

```
Port 8000/tcp was found to be open
```

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

http://www.itu.int/rec/T-REC-X.509/en

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

Solution

Purchase or generate a proper 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 Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/8834

```

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

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/8834

```
The remote web server type is :

NessusWWW
```

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

http://www.tenable.com/products/nessus-vulnerability-scanner

Solution

Ensure that the remote Nessus installation has been authorized.

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2016/02/25

Plugin Output

tcp/8834

```
URL               : https://SERVIDOR.lan:8834/
Version           : 7.1.0
Nessus UI Version : 7.1.0
```

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: 2015/12/30

Plugin Output

tcp/8834

```
Subject Name:

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

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: 21 E9

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jun 06 16:14:13 2018 GMT
Not Valid After: Jun 05 16:14:13 2022 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 9A 01 0C 1D 97 6C B7 6A 89 16 24 1E 3B 2A 11 F2 01 7E 02
```

```
            4B EF 35 F7 FE A2 DA 57 66 E4 E9 D7 B8 F8 6C 69 A2 95 11 62
            E5 17 3C 0D E0 30 16 76 9A DA EC D0 78 AB 40 C2 86 CD B3 BB
            C2 EE 34 4D 9B 0B 7B 1A D1 3A 2C 0A DB 83 F8 E2 AE C9 24 A4
            3D FB CE 94 30 B5 C3 F9 94 2D 17 97 66 1F 8F 67 AC 36 CF 50
            67 87 23 6D 9D F3 4F AB 75 24 69 92 9B BF 44 42 06 2B EB D9
            37 3B 3E 6A 38 A2 39 79 82 1B 53 45 52 58 9E AB 5B 5B 81 6D
            1E A3 BB 72 12 D8 2E BF CF 4B B0 40 9F B3 6C 95 89 4B A2 0C
            28 BB 3C 22 C4 02 75 93 67 72 EB A5 9C 3C 06 A6 3B 9F 17 38
            EB CE ED AA 59 89 50 D8 0A 69 EE DA FC 09 C9 C0 7C B1 B6 7A
            54 F0 1F 11 CE 63 E5 32 13 40 36 A4 DD FE E9 2E CC C8 54 2C
            B7 64 F8 D1 E0 7D 45 15 27 52 5D DB D3 25 24 58 D0 C7 F5 9B
            C0 6A F6 07 3A 7C 58 5A 38 48 7F F7 BD FE 91 CA 7F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 60 18 9A C1 52 56 D6 E8 7B 28 7D BC CE 44 BF 4B 66 B0 65
           B7 DC 1B 15 2C 84 91 D9 39 06 C7 4B 62 FB 13 DA AA C2 A9 6F
           AF 4C BF BE 52 4C F3 BB F0 63 6E 5D D0 D4 D7 CF 0C 4B 9F BC
           32 61 F8 24 3B 41 AE 38 CC B1 2A 43 48 82 18 9A CF 21 F3 6D
           85 A1 1C 67 72 21 06 11 D6 89 B9 D7 6B 84 A7 69 87 99 E9 4C
           40 C3 4F 91 04 95 A9 4C E3 8E FB C8 85 7C DF 5F 32 BC C7 A0
           60 77 63 20 AA 3C [...]
```

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.

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: 2018/05/30

Plugin Output

tcp/8834

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

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/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/03/29

Plugin Output

tcp/8834

```

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

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={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: 2018/05/03

Plugin Output

tcp/8834

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

tcp/8834

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

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: 2017/11/13

Plugin Output

tcp/8834

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Cache-Control:
  X-Frame-Options: DENY
  Etag: 55218a6fb08e3e76a84e7ddcf1d1e973
  Content-Type: text/html
  Date: : Wed, 06 Jun 2018 16:43:12 GMT
  Connection: close
  Server: NessusWWW
  Content-Length: 715
  Expires: 0
  Pragma:

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="default-src 'self'; img-src 'self'
 data:; style-src 'self' 'unsafe-inline';" />
```

```
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <meta charset="utf-8" />
        <title>Nessus</title>
        <link rel="stylesheet" href="nessus6.css?v=1525909252661" />
        <!--[if lt IE 11]>
            <script>
                window.location = '/unsupported6.html';
            </script>
        <![endif]-->
        <script src="nessus6.js?v=1525909252661"></script>
    </head>
    <body>
    </body>
</html>
```

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: 2018/02/15

Plugin Output

tcp/8834

```
This port supports TLSv1.2.
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/8834

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

  High Strength Ciphers (>= 112-bit key)

    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information:

Published: 2015/07/02, Modified: 2015/07/02

Plugin Output

tcp/8834

```

  The remote HTTPS server does not send the HTTP
  "Strict-Transport-Security" header.
```

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: 2014/05/12

Plugin Output

tcp/49664

```
The following DCERPC services are available on TCP port 49664 :

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 : 49664
IP : 192.168.1.77
```

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.

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: 2018/05/30

Plugin Output

tcp/49664

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

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: 2014/05/12

Plugin Output

tcp/49665

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

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 : 49665
IP : 192.168.1.77

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 : 49665
IP : 192.168.1.77
```

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.

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: 2018/05/30

Plugin Output

tcp/49665

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

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: 2014/05/12

Plugin Output

tcp/49666

```
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 : 192.168.1.77
```

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.

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: 2018/05/30

Plugin Output

tcp/49666

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

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: 2014/05/12

Plugin Output

tcp/49667

```

The following DCERPC services are available on TCP port 49667 :

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 : 49667
IP : 192.168.1.77

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 : 49667
IP : 192.168.1.77

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 : 49667
IP : 192.168.1.77

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 : 49667
IP : 192.168.1.77

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 : 49667
IP : 192.168.1.77
```

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.

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: 2018/05/30

Plugin Output

tcp/49667

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

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: 2014/05/12

Plugin Output

tcp/49668

```

The following DCERPC services are available on TCP port 49668 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.1.77

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.1.77

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.1.77
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.1.77
```

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.

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: 2018/05/30

Plugin Output

tcp/49668

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

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: 2014/05/12

Plugin Output

tcp/49673

```

The following DCERPC services are available on TCP port 49673 :

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 : 49673
IP : 192.168.1.77

```

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.

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: 2018/05/30

Plugin Output

tcp/49673

```
Port 49673/tcp was found to be open
```

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: 2014/05/12

Plugin Output

tcp/49681

```
The following DCERPC services are available on TCP port 49681 :

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 : 49681
IP : 192.168.1.77
```

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.

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: 2018/05/30

Plugin Output

tcp/49681

```
Port 49681/tcp was found to be open
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?0bb7b67d

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.1 (with approved cipher suites) or higher instead.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2005/10/12, Modified: 2017/07/11

Plugin Output

tcp/50658

```

- SSLv3 is enabled and the server supports at least one cipher.
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?e120eea1

http://technet.microsoft.com/en-us/security/advisory/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	OSVDB:45106
XREF	OSVDB:45108

XREF	OSVDB:45127
XREF	CERT:836068
XREF	CWE:310

Plugin Information:

Published: 2009/01/05, Modified: 2018/05/21

Plugin Output

tcp/50658

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject             : CN=SSL_Self_Signed_Fallback
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : May 22 10:45:08 2018 GMT
|-Valid To            : May 22 10:45:08 2048 GMT
```

42873 - SSL Medium Strength Cipher Suites Supported

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/50658

```

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

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :
```

```
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

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 Base Score

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

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/50658

```

The identities known by Nessus are :

  servidor
  SERVIDOR.lan

The Common Name in the certificate is :

  SSL_Self_Signed_Fallback
```

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

http://www.itu.int/rec/T-REC-X.509/en

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

Solution

Purchase or generate a proper 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 Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/50658

```
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 : CN=SSL_Self_Signed_Fallback
|-Issuer  : CN=SSL_Self_Signed_Fallback
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/50658

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=SSL_Self_Signed_Fallback
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	70574
CVE	CVE-2014-3566
XREF	OSVDB:113251
XREF	CERT:577193

Plugin Information:

Published: 2014/10/15, Modified: 2016/11/30

Plugin Output

tcp/50658

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Description

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

https://www.cabforum.org/Baseline_Requirements_V1.pdf

Solution

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Risk Factor

Low

Plugin Information:

Published: 2013/09/03, Modified: 2014/04/10

Plugin Output

tcp/50658

```
The following certificates were part of the certificate chain
sent by the remote host, but contain RSA keys that are considered
to be weak :

|-Subject        : CN=SSL_Self_Signed_Fallback
|-RSA Key Length : 1024 bits
```

10144 - Microsoft SQL Server TCP/IP Listener Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MSSQL, a database server from Microsoft. It is possible to extract the version number of the remote installation from the server pre-login response.

Solution

Restrict access to the database to allowed IPs only.

Risk Factor

None

References

XREF	OSVDB:112

Plugin Information:

Published: 1999/10/12, Modified: 2018/03/30

Plugin Output

tcp/50658

```
The remote MSSQL server accepts cleartext logins.
The remote SQL Server version is 12.0.2569.0.

The remote SQL Server instance name is PRIMAVERA.
```

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: 2015/12/30

Plugin Output

tcp/50658

```
Subject Name:

Common Name: SSL_Self_Signed_Fallback

Issuer Name:

Common Name: SSL_Self_Signed_Fallback

Serial Number: 52 F5 0A CD 53 2A FB B0 4F B7 FA 48 C9 16 DC 56

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 22 10:45:08 2018 GMT
Not Valid After: May 22 10:45:08 2048 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 B0 CC 0A DD 78 FB 45 78 95 FB CF CA A4 0A D3 AD 8E FC 8A
            4C AA 05 43 5C 48 27 43 F6 C3 42 A5 63 0C D5 E8 26 9A 2C 2D
            35 79 68 11 CB 70 1D DA 39 39 CC E9 58 02 93 79 15 FB CB 09
            56 B0 EA E5 85 2C E4 57 20 78 FA 14 F0 60 DC 1D C3 09 38 78
            32 89 AB 47 1C 58 34 5D 5B 23 6C 43 78 9D 53 89 CC 1E 01 B4
            29 B5 05 60 60 3A DF D5 C7 76 8E D6 EE 6D 9D BD 77 A1 26 FC
            18 7B 74 C6 72 70 75 2A 5D
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 98 7F 04 C9 8B 08 A7 36 20 7C 05 63 40 7D E0 66 D3 4C 85
```

```
           BC 8F 86 B4 0D D5 79 B6 84 B7 4F 63 7D 3C 0C 21 E8 2A 47 BE
           7C 5F 0A 6D 7A B4 0F 4F B8 E7 E6 D5 55 F2 F1 E3 FD FE 8C 3F
           C0 F4 D0 F5 76 86 25 D9 64 FB 4B 0F 27 B4 8E 9B B0 A0 10 6C
           E3 AC B4 53 49 41 C7 AA 01 87 EB 48 01 66 4D 93 C2 06 2B DD
           13 5F 61 ED B0 70 EC 3C 1D D8 9C 2C BE 17 13 DE 94 68 96 10
           0E C6 89 B7 45 4D 00 7F 37

Fingerprints :

SHA-256 Fingerprint: C9 3A 5C 10 C9 FF D7 A4 D0 42 68 31 60 D7 4D D7 05 59 F6 23
                     52 E8 F4 F9 E7 E6 BE F0 18 B2 F1 3D
SHA-1 Fingerprint: 34 17 1A 19 02 86 6F 4F 8C 9B 85 39 79 AD F1 7D 50 CD 93 E9
MD5 Fingerprint: 9F CC CD 84 73 D9 BE F5 84 84 7B 61 52 B5 C0 37
```

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.

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: 2018/05/30

Plugin Output

tcp/50658

```
Port 50658/tcp was found to be open
```

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/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/03/29

Plugin Output

tcp/50658

```

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

SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    RSA-AES256-SHA384            Kx=RSA         Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256


SSL Version : TLSv11
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SH [...]
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/50658

```

The host names known by Nessus are :

  servidor
  servidor.lan

The Common Name in the certificate is :

  ssl_self_signed_fallback
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/02/07, Modified: 2013/10/18

Plugin Output

tcp/50658

```
This port supports resuming TLSv1 / SSLv3 sessions.
```

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: 2018/02/15

Plugin Output

tcp/50658

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

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

http://www.openssl.org/docs/apps/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/12/07, Modified: 2017/06/12

Plugin Output

tcp/50658

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

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
```

```
    Au={authentication}
    Enc={symmetric encryption method}
    Mac={message authentication code}
    {export flag}
```

69482 - Microsoft SQL Server STARTTLS Support

Synopsis

The remote service supports encrypting traffic.

Description

The remote Microsoft SQL Server service supports the use of encryption initiated during pre-login to switch from a cleartext to an encrypted communications channel.

See Also

http://msdn.microsoft.com/en-us/library/dd304523.aspx

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/07/04, Modified: 2018/03/13

Plugin Output

tcp/50658

```

Here is the Microsoft SQL Server's SSL certificate that Nessus
was able to collect after sending a pre-login packet :

------------------------------ snip ------------------------------
Subject Name:

Common Name: SSL_Self_Signed_Fallback

Issuer Name:

Common Name: SSL_Self_Signed_Fallback

Serial Number: 52 F5 0A CD 53 2A FB B0 4F B7 FA 48 C9 16 DC 56

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 22 10:45:08 2018 GMT
Not Valid After: May 22 10:45:08 2048 GMT

Public Key Info:
```

```
Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 B0 CC 0A DD 78 FB 45 78 95 FB CF CA A4 0A D3 AD 8E FC 8A
            4C AA 05 43 5C 48 27 43 F6 C3 42 A5 63 0C D5 E8 26 9A 2C 2D
            35 79 68 11 CB 70 1D DA 39 39 CC E9 58 02 93 79 15 FB CB 09
            56 B0 EA E5 85 2C E4 57 20 78 FA 14 F0 60 DC 1D C3 09 38 78
            32 89 AB 47 1C 58 34 5D 5B 23 6C 43 78 9D 53 89 CC 1E 01 B4
            29 B5 05 60 60 3A DF D5 C7 76 8E D6 EE 6D 9D BD 77 A1 26 FC
            18 7B 74 C6 72 70 75 2A 5D
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 98 7F 04 C9 8B 08 A7 36 20 7C 05 63 40 7D E0 66 D3 4C 85
           BC 8F 86 B4 0D D5 79 B6 84 B7 4F 63 7D 3C 0C 21 E8 2A 47 BE
           7C 5F 0A 6D 7A B4 0F 4F B8 E7 E6 D5 55 F2 F1 E3 FD FE 8C 3F
           C0 F4 D0 F5 76 86 25 D9 64 FB 4B 0F 27 B4 8E 9B B0 A0 10 6C
           E3 AC B4 53 49 41 C7 AA 01 87 EB 48 01 66 4D 93 C2 06 2B DD
           13 5F 61 ED B0 70 EC 3C 1D D8 9C 2C BE 17 13 DE 94 68 96 10
           0E C6 89 B7 45 4D 00 7F 37


------------------------------ snip ------------------------------


  SQL Server Version   : 12.0.2569.0
  SQL Server Instance  : PRIMAVERA
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/50658

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

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256
```

```
 The fields above are :

   {OpenSSL ciphername}
   Kx={key exchange}
   Au={authentication}
   Enc={symmetric encryption method}
   Mac={message authentication code}
   {export flag}
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2018/04/24

Plugin Output

tcp/50658

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

108761 - MSSQL Host Information in NTLM SSP

Synopsis

Nessus can obtain information about the host by examining the NTLM SSP message.

Description

Nessus can obtain information about the host by examining the NTLM SSP challenge issued during NTLM authentication, over MSSQL.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/03/30, Modified: 2018/03/30

Plugin Output

tcp/50658

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

 Target Name:            SERVIDOR
 NetBIOS Domain Name:    SERVIDOR
 NetBIOS Computer Name: SERVIDOR
 DNS Domain Name:        SERVIDOR
 DNS Computer Name:      SERVIDOR
 DNS Tree Name:          unknown
 Product Version:        10.0.17134
```

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.

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: 2018/05/30

Plugin Output

udp/60833

```
Port 60833/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.

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: 2018/05/30

Plugin Output

udp/60834

```
Port 60834/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.

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: 2018/05/30

Plugin Output

udp/61575

```
Port 61575/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.

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: 2018/05/30

Plugin Output

udp/61581

```
Port 61581/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.

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: 2018/05/30

Plugin Output

udp/64241

```
Port 64241/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.

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: 2018/05/30

Plugin Output

udp/64243

```
Port 64243/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.

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: 2018/05/30

Plugin Output

udp/64311

```
Port 64311/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.

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: 2018/05/30

Plugin Output

udp/64312

```
Port 64312/udp was found to be open
```

192.168.1.253

2	1	7	2	39
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Wed Jun 06 17:48:47 2018
End time:	Wed Jun 06 18:04:40 2018

Host Information

Netbios Name:	MEO
IP:	192.168.1.253
MAC Address:	5a:98:35:5a:38:7e
OS:	Technicolor / Thomson Wireless Router

Vulnerabilities

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

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -3602 seconds.
```

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 has 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

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

Plugin Information:

Published: 2002/03/19, Modified: 2014/06/04

Plugin Output

tcp/0

```
Port 443 was detected as being open but is now unresponsive
Port 515 was detected as being open but is now unresponsive
Port 22 was detected as being open but is now unresponsive
Port 80 was detected as being open but is now unresponsive
```

11026 - Wireless Access Point Detection

Synopsis

The remote host is a wireless access point.

Description

Nessus has determined that the remote host is a wireless access point (AP).

Ensure that proper physical and logical controls are in place for its use. A misconfigured access point may allow an attacker to gain access to an internal network without being physically present on the premises. If the access point is using an 'off-the-shelf'

configuration (such as 40 or 104 bit WEP encryption), the data being passed through the access point may be vulnerable to hijacking or sniffing.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/06/09, Modified: 2014/08/19

Plugin Output

tcp/0

```
Nessus has classified this device as a wireless access point based on
its OS fingerprint.
```

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: 2018/04/19

Plugin Output

tcp/0

```

Remote operating system : Technicolor / Thomson Wireless Router
Confidence level : 90
Method : SSLcert


The remote host is running Technicolor / Thomson Wireless Router
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.1.0
Plugin feed version : 201806052020
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.77
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 5
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2018/6/6 17:48
Scan duration : 949 sec
```

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: 2011/03/20

Plugin Output

tcp/0

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: 2017/06/06

Plugin Output

tcp/0

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

  cpe:/a:samba:samba:2.2.12 -> Samba 2.2.12
```

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 : wireless-access-point
Confidence level : 90
```

66334 - Patch Report

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.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information:

Published: 2013/07/08, Modified: 2018/06/05

Plugin Output

tcp/0

```

. You need to take the following 2 actions :


[ Dropbear SSH Server < 2016.72 Multiple Vulnerabilities (93650) ]

+ Action to take : Upgrade to Dropbear SSH version 2016.74 or later.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).



[ Samba Badlock Vulnerability (90509) ]

+ Action to take : Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

```

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: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.77 to 192.168.1.253 :
192.168.1.77
192.168.1.253

Hop Count: 1
```

93650 - Dropbear SSH Server < 2016.72 Multiple Vulnerabilities

Synopsis

The SSH service running on the remote host is affected by multiple vulnerabilities.

Description

According to its self-reported version in its banner, Dropbear SSH running on the remote host is prior to 2016.74. It is, therefore, affected by the following vulnerabilities :

- A format string flaw exists due to improper handling of string format specifiers (e.g., %s and %x) in usernames and host arguments. An unauthenticated, remote attacker can exploit this to execute arbitrary code with root privileges. (CVE-2016-7406)

- A flaw exists in dropbearconvert due to improper handling of specially crafted OpenSSH key files. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-7407)

- A flaw exists in dbclient when handling the -m or -c arguments in scripts. An unauthenticated, remote attacker can exploit this, via a specially crafted script, to execute arbitrary code. (CVE-2016-7408)

- A flaw exists in dbclient or dropbear server if they are compiled with the DEBUG_TRACE option and then run using the -v switch. A local attacker can exploit this to disclose process memory. (CVE-2016-7409)

See Also

https://matt.ucc.asn.au/dropbear/CHANGES

Solution

Upgrade to Dropbear SSH version 2016.74 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	92970
BID	92972
BID	92973
BID	92974
CVE	CVE-2016-7406
CVE	CVE-2016-7407
CVE	CVE-2016-7408
CVE	CVE-2016-7409
XREF	OSVDB:142291
XREF	OSVDB:142292
XREF	OSVDB:142293
XREF	OSVDB:142294

Plugin Information:

Published: 2016/09/22, Modified: 2016/12/06

Plugin Output

tcp/22

```

  Version source    : SSH-2.0-dropbear_0.44
  Installed version : 0.44
  Fixed version     : 2016.74
```

34769 - Dropbear SSH Server svr_ses.childpidsize Remote Overflow

Synopsis

Authenticated users can gain elevated privileges.

Description

According to its banner, the remote host is runnning a version of Dropbear SSH before 0.47. Such versions contain a buffer allocation error that may allow an authenticated user to gain elevated privileges.

See Also

http://lists.ucc.gu.uwa.edu.au/pipermail/dropbear/2005q4/000312.html

http://matt.ucc.asn.au/dropbear/CHANGES

Solution

Upgrade to the Dropbear SSH 0.47 or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

7.8 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	15923
CVE	CVE-2005-4178
XREF	OSVDB:21847

Plugin Information:

Published: 2008/11/13, Modified: 2016/10/17

Plugin Output

tcp/22

21023 - Dropbear SSH Authorization-pending Connection Saturation DoS

Synopsis

The remote SSH server is susceptible to denial of service attacks.

Description

The remote host is running Dropbear, a small, open source SSH server.

The version of Dropbear installed on the remote host, by default, has a limit of 30 connections in the authorization-pending state; subsequent connections are closed immediately. This issue can be exploited trivially by an unauthenticated attacker to deny service to legitimate users.

See Also

http://www.securityfocus.com/archive/1/426999/30/0/threaded

http://seclists.org/fulldisclosure/2006/Mar/222

Solution

Upgrade to Dropbear 0.48 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	17024
CVE	CVE-2006-1206
XREF	OSVDB:23960

Plugin Information:

Published: 2006/03/08, Modified: 2017/06/01

Plugin Output

tcp/22

70545 - Dropbear SSH Server < 2013.59 Multiple Vulnerabilities

Synopsis

The remote SSH service is affected by multiple vulnerabilities.

Description

According to its self-reported banner, the version of Dropbear SSH running on this port is earlier than 2013.59. As such, it is potentially affected by multiple vulnerabilities :

- A denial of service vulnerability caused by the way the 'buf_decompress()' function handles compressed files. (CVE-2013-4421)

- User-enumeration is possible due to a timing error when authenticating users. (CVE-2013-4434)

See Also

https://matt.ucc.asn.au/dropbear/CHANGES

https://secure.ucc.asn.au/hg/dropbear/rev/0bf76f54de6f

https://secure.ucc.asn.au/hg/dropbear/rev/a625f9e135a4

Solution

Upgrade to the Dropbear SSH 2013.59 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	62958
BID	62993
CVE	CVE-2013-4421
CVE	CVE-2013-4434
XREF	OSVDB:98303
XREF	OSVDB:98365

Plugin Information:

Published: 2013/10/22, Modified: 2014/05/29

Plugin Output

tcp/22

```
  Version source    : SSH-2.0-dropbear_0.44
  Installed version : 0.44
  Fixed version     : 2013.59
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

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

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

Solution

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

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	32319
CVE	CVE-2008-5161
XREF	OSVDB:50035
XREF	OSVDB:50036
XREF	CERT:958563
XREF	CWE:200

Plugin Information:

Published: 2013/10/28, Modified: 2016/05/12

Plugin Output

tcp/22

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

  3des-cbc
  aes128-cbc
  blowfish-cbc
  twofish-cbc

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

  3des-cbc
  aes128-cbc
  blowfish-cbc
  twofish-cbc
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

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

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

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

Solution

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

Risk Factor

Low

CVSS Base Score

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

Plugin Information:

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22

```

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

  hmac-md5

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

  hmac-md5
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/22

```
SSH version : SSH-2.0-dropbear_0.44
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/22

```
Port 22/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/22

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

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22

```

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  diffie-hellman-group1-sha1

The server supports the following options for server_host_key_algorithms :

  ssh-dss
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  blowfish-cbc
  twofish-cbc

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  blowfish-cbc
  twofish-cbc

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-sha1
```

```
The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-sha1

The server supports the following options for compression_algorithms_client_to_server :

  none

The server supports the following options for compression_algorithms_server_to_client :

  none
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/80

```
The remote web server type is :

The Knopflerfish HTTP Server
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/80

```
Port 80/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/80

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

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: 2017/11/13

Plugin Output

tcp/80

```

Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html
  MIME-Version: 1.0
  Server: The Knopflerfish HTTP Server
  Date: Wed, 06 Jun 2018 17:54:02 GMT
  Connection: Close
  Content-Length: 105

Response Body :
```

85805 - HTTP/2 Cleartext Detection

Synopsis

An HTTP/2 server is listening on the remote host.

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information:

Published: 2015/09/04, Modified: 2016/01/07

Plugin Output

tcp/80

```

The server supports direct HTTP/2 connections
without encryption.
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

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: 2017/09/27

Plugin Output

udp/137

```
The following 7 NetBIOS names have been gathered :

 MEO                = Computer name
 MEO                = Messenger Service
 MEO                = File Server Service
 __MSBROWSE__       = Master Browser
 WORKGROUP          = Workgroup / Domain name
 WORKGROUP          = Master Browser
 WORKGROUP          = Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.
```

15985 - Samba smbd Security Descriptor Parsing Remote Overflow

Synopsis

Remote code may be run on the remote server.

Description

The remote Samba server, according to its version number, is vulnerable to a remote buffer overrun resulting from an integer overflow vulnerability.

To exploit this flaw, an attacker would need to send to the remote host a malformed packet containing hundreds of thousands of ACLs, which would in turn cause an integer overflow resulting in a small pointer being allocated.

An attacker needs a valid account or enough credentials to exploit this flaw.

Solution

Upgrade to Samba 3.0.10 or later.

Risk Factor

Critical

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	11973
CVE	CVE-2004-1154
XREF	OSVDB:12422

Plugin Information:

Published: 2004/12/16, Modified: 2011/04/13

Plugin Output

tcp/139

90509 - Samba Badlock Vulnerability

Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

See Also

http://badlock.org

https://www.samba.org/samba/security/CVE-2016-2118.html

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

5.6 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	86002
CVE	CVE-2016-2118
XREF	OSVDB:136339
XREF	CERT:813296

Plugin Information:

Published: 2016/04/13, Modified: 2016/07/25

Plugin Output

tcp/139

```
Nessus detected that the Samba Badlock patch has not been applied.
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- NULL session

- Guest account

- Supplied credentials

See Also

https://support.microsoft.com/kb/143474

https://support.microsoft.com/kb/246261

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/05/09, Modified: 2017/11/06

Plugin Output

tcp/139

```
- NULL sessions are enabled on the remote host.
```

10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

Synopsis

It is possible to obtain network information.

Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Solution

n/a

Risk Factor

None

References

XREF	OSVDB:300

Plugin Information:

Published: 2000/05/09, Modified: 2015/01/12

Plugin Output

tcp/139

```

Here is the browse list of the remote host :

DESKTOP-8TD7MQ3 ( os : 0.0 )
MEO ( os : 0.0 )
```

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 SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/10/17, Modified: 2017/11/30

Plugin Output

tcp/139

```
The remote Operating System is : Unix
The remote native LAN manager is : Samba 2.2.12
The remote SMB Domain Name is : WORKGROUP
```

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: 2015/06/02

Plugin Output

tcp/139

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/139

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

25240 - Samba Server Detection

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

http://www.samba.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/05/16, Modified: 2013/01/07

Plugin Output

tcp/139

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/kb/2696547

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?36fd3072

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF	OSVDB:151058

Plugin Information:

Published: 2017/02/03, Modified: 2017/02/16

Plugin Output

tcp/139

```
The remote host supports SMBv1.
```

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: 2017/06/19

Plugin Output

tcp/139

```
The remote host supports the following versions of SMB :
  SMBv1
```

104887 - Samba Version

Synopsis

It was possible to obtain the samba version from the remote operating system.

Description

Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2017/11/30, Modified: 2017/11/30

Plugin Output

tcp/139

```

The remote Samba Version is : Samba 2.2.12
```

106716 - Microsoft Windows SMB2 Dialects Supported (remote check)

Synopsis

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

Description

Nessus was able to obtain the set of SMB2 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: 2018/02/09

Plugin Output

tcp/139

```

The remote host does NOT support the following SMB dialects :
 _version_  _introduced in windows version_
 2.0.2      Windows 2008
 2.1        Windows 7
 2.2.2      Windows 8 Beta
 2.2.4      Windows 8 Beta
 3.0        Windows 8
 3.0.2      Windows 8.1
 3.1        Windows 10
 3.1.1      Windows 10
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?e120eea1

http://technet.microsoft.com/en-us/security/advisory/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	OSVDB:45106
XREF	OSVDB:45108

XREF	OSVDB:45127
XREF	CERT:836068
XREF	CWE:310

Plugin Information:

Published: 2009/01/05, Modified: 2018/05/21

Plugin Output

tcp/443

```

The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject             : CN=Thomson TG784n/O=THOMSON/OU=1148NT8UT
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Jan 01 00:00:00 2005 GMT
|-Valid To            : Dec 31 00:00:00 2024 GMT
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

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 Base Score

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

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/443

```
The identities known by Nessus are :

  192.168.1.253
  192.168.1.253

The Common Name in the certificate is :

  Thomson TG784n
```

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

http://www.itu.int/rec/T-REC-X.509/en

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

Solution

Purchase or generate a proper 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 Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/443

```
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 : CN=Thomson TG784n/O=THOMSON/OU=1148NT8UT
|-Issuer  : CN=Thomson TG784n/O=THOMSON/OU=1148NT8UT
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/443

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=Thomson TG784n/O=THOMSON/OU=1148NT8UT
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/443

```
The remote web server type is :

The Knopflerfish HTTP Server
```

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: 2015/12/30

Plugin Output

tcp/443

```
Subject Name:

Common Name: Thomson TG784n
Organization: THOMSON
Organization Unit: 1148NT8UT

Issuer Name:

Common Name: Thomson TG784n
Organization: THOMSON
Organization Unit: 1148NT8UT

Serial Number: 85 D3 4B 52

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jan 01 00:00:00 2005 GMT
Not Valid After: Dec 31 00:00:00 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D3 6A D3 0A 78 15 49 09 9D B0 EA 12 D8 99 74 A8 44 5C 8B
            96 B3 7D A7 42 A2 00 0D F6 66 9D 92 FB E5 06 8B 0B 84 B5 9F
            7C 3B 5C 48 0B 5E 26 60 DB DE 73 73 31 1F 40 17 7F 45 F1 5E
            27 35 AF 82 1C 03 32 36 9A E4 D2 2C 0D 8F 1B 8E F7 F8 D4 6B
            72 31 3D 8A E2 FD 50 AD 21 4D F7 FD 92 86 39 7C 50 7F 4E 7A
            89 CB EA E8 39 90 83 A8 CD 8C 24 5E 1B 5A 7B C6 AD BF EC 4C
            DB 0C 67 15 08 43 D1 26 B1
```

```
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 49 5A 05 3C E0 DA 61 31 6D F8 30 F0 76 70 7F D2 50 F2 6D
           77 E1 D1 45 6A 00 57 A7 1A 0F D1 0C 4A E7 5F 28 99 BD 80 90
           6B 52 E5 8D 79 3B 9E E8 AA 94 12 4F C7 3D BB 65 0A 44 DB 70
           E3 2B 11 D2 C2 48 B5 DD 31 1B 79 09 A6 F6 2F 7C D4 6A 00 87
           AA 61 F4 CA 6F B3 ED 9E E5 88 5F AE C2 00 D3 7F F6 AA 5A 6D
           14 8A D2 5A 45 AF A7 17 03 AB AF 95 26 F4 26 24 14 5A E9 7D
           07 9E 5F 5C 8F B6 89 75 56

Fingerprints :

SHA-256 Fingerprint: 58 AC 9C E8 ED 91 D9 B3 8F EE 40 15 F5 39 F9 C6 94 5E C1 38
                     6A 66 B1 E5 C7 65 0F 83 76 9B 65 A8
SHA-1 Fingerprint: 52 7A 1F AE C0 B8 80 A9 B1 63 2B A5 68 4D 69 28 72 F1 1A F5
MD5 Fingerprint: B1 30 A7 E9 96 89 F7 B4 9C BF 93 97 EB CF B8 F6
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/443

```
Port 443/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/443

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

tcp/443

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

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/443

```

The host name known by Nessus is :

  meo

The Common Name in the certificate is :

  thomson tg784n
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/11/30, Modified: 2013/10/18

Plugin Output

tcp/443

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: 2018/02/15

Plugin Output

tcp/443

```
This port supports SSLv3/TLSv1.0.
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/515

```
Port 515/tcp was found to be open
```

30207 - LPD Detection

Synopsis

A printer service is listening on the remote host.

Description

The remote service supports the line printer daemon (lpd) protocol, which is widely-used by print servers.

See Also

https://tools.ietf.org/html/rfc1179

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information:

Published: 2008/02/08, Modified: 2017/05/16

Plugin Output

tcp/515

192.168.1.254

0	0	1	0	20
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Wed Jun 06 17:48:48 2018
End time:	Wed Jun 06 18:05:10 2018

Host Information

DNS Name:	dsldevice.lan
IP:	192.168.1.254
MAC Address:	58:98:35:5a:38:7e
OS:	SCO UnixWare 7.1.1

Vulnerabilities

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 has 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

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

Plugin Information:

Published: 2002/03/19, Modified: 2014/06/04

Plugin Output

tcp/0

```
Port 443 was detected as being open but is now closed
Port 80 was detected as being open but is now closed
```

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: 2018/04/19

Plugin Output

tcp/0

```

Remote operating system : SCO UnixWare 7.1.1
Confidence level : 65
Method : SinFP


The remote host is running SCO UnixWare 7.1.1
```

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

```
192.168.1.254 resolves as dsldevice.lan.
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.1.0
Plugin feed version : 201806052020
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.77
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 5
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2018/6/6 17:48
Scan duration : 972 sec
```

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: 2011/03/20

Plugin Output

tcp/0

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

http://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: 2017/11/17

Plugin Output

tcp/0

```
The following card manufacturers were identified :

58:98:35:5a:38:7e : Technicolor
```

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 : general-purpose
Confidence level : 65
```

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: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.77 to 192.168.1.254 :
192.168.1.77
192.168.1.254

Hop Count: 1
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/21

```
Port 21/tcp was found to be open
```

42263 - Unencrypted Telnet Server

Synopsis

The remote Telnet server transmits traffic in cleartext.

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2009/10/27, Modified: 2015/10/21

Plugin Output

tcp/23

```
Nessus collected the following banner from the remote Telnet server :

------------------------------ snip ------------------------------
Username :
------------------------------ snip ------------------------------
```

10281 - Telnet Server Detection

Synopsis

A Telnet server is listening on the remote port.

Description

The remote host is running a Telnet server, a remote terminal server.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2018/02/12

Plugin Output

tcp/23

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------
Username :
------------------------------ snip ------------------------------
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/23

```
Port 23/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/53

```
Port 53/tcp was found to be open
```

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

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/80

```
Port 80/tcp was found to be open
```

85805 - HTTP/2 Cleartext Detection

Synopsis

An HTTP/2 server is listening on the remote host.

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information:

Published: 2015/09/04, Modified: 2016/01/07

Plugin Output

tcp/80

```
The server supports direct HTTP/2 connections
without encryption.
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/443

```
Port 443/tcp was found to be open
```

85805 - HTTP/2 Cleartext Detection

Synopsis

An HTTP/2 server is listening on the remote host.

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information:

Published: 2015/09/04, Modified: 2016/01/07

Plugin Output

tcp/443

```
The server supports direct HTTP/2 connections
without encryption.
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/1723

```
Port 1723/tcp was found to be open
```

35711 - Universal Plug and Play (UPnP) Protocol Detection

Synopsis

The remote device supports UPnP.

Description

The remote device answered an SSDP M-SEARCH request. Therefore, it supports 'Universal Plug and Play' (UPnP). This protocol provides automatic configuration and device discovery. It is primarily intended for home networks. An attacker could potentially leverage this to discover your network architecture.

See Also

https://en.wikipedia.org/wiki/Universal_Plug_and_Play

https://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol

http://quimby.gnus.org/internet-drafts/draft-cai-ssdp-v1-03.txt

Solution

Filter access to this port if desired.

Risk Factor

None

Plugin Information:

Published: 2009/02/19, Modified: 2017/06/12

Plugin Output

udp/1900

```
The device responded to an SSDP M-SEARCH request with the following locations :

    http://192.168.1.254:8000/xv8zhtd5q6e/IGD/upnp/IGD.xml
    http://192.168.1.254:8000/zrg1leli3jc/WFA/WFA.xml

And advertises these unique service names :

    uuid:UPnP_Thomson TG784n-1_58-98-35-5A-38-7E::upnp:rootdevice
    uuid:UPnP_Thomson TG784n-1_58-98-35-5A-38-7E::urn:schemas-upnp-
org:device:InternetGatewayDevice:1
    uuid:UPnP_Thomson TG784n-1_58-98-35-5A-38-7E_LD_1::urn:schemas-upnp-org:device:LANDevice:1
    uuid:UPnP_Thomson TG784n-1_58-98-35-5A-38-7E_WD_1::urn:schemas-upnp-org:device:WANDevice:1
    uuid:UPnP_Thomson TG784n-1_58-98-35-5A-38-7E_WCD_1_1::urn:schemas-upnp-
org:device:WANConnectionDevice:1
    uuid:UPnP_Thomson TG784n-1_58-98-35-5A-38-7E::urn:schemas-upnp-org:service:Layer3Forwarding:1
    uuid:UPnP_Thomson TG784n-1_58-98-35-5A-38-7E_LD_1::urn:schemas-upnp-
org:service:LANHostConfigManagement:1
    uuid:UPnP_Thomson TG784n-1_58-98-35-5A-38-7E_WD_1::urn:schemas-upnp-
org:service:WANCommonInterfaceConfig:1
```

```
    uuid:UPnP_Thomson TG784n-1_58-98-35-5A-38-7E_WCD_1_1::urn:schemas-upnp-
org:service:WANDSLLinkConfig:1
    uuid:UPnP_Thomson TG784n-1_58-98-35-5A-38-7E_WCD_1_1::urn:schemas-upnp-
org:service:WANIPConnection:1
    uuid:2a33ee61-3a66-58e0-90e8-20a5e9f406e8::upnp:rootdevice
    uuid:2a33ee61-3a66-58e0-90e8-20a5e9f406e8::urn:schemas-wifialliance-org:device:WFADevice:1
    uuid:2a33ee61-3a66-58e0-90e8-20a5e9f406e8::urn:schemas-wifialliance-org:service:WFAWLANConfig:1
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/8000

```
Port 8000/tcp was found to be open
```

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 29% of the vulnerabilities on the network.

ACTION TO TAKE	VULNS	HOSTS
Dropbear SSH Server < 2016.72 Multiple Vulnerabilities: Upgrade to Dropbear SSH version 2016.74 or later.	6	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	1	1