Nessus Report

Nessus Scan Report

Fri, 08 Dec 2017 18:00:36 EET

Table Of Contents

Vulnerabilities By Host

10.0.100.1

Scan Information

Start time:	Fri Dec 8 16:41:24 2017
End time:	Fri Dec 8 16:50:58 2017

Host Information

IP:	10.0.100.1
MAC Address:	00:50:56:84:23:ff

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	5	6

Results Details

0/icmp

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:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

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

0/tcp

50686 - IP Forwarding Enabled

Synopsis

The remote host has IP forwarding enabled.

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.
Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :
echo 0 > /proc/sys/net/ipv4/ip_forward

On Windows, set the key 'IPEnableRouter' to 0 under
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
On Mac OS X, you can disable IP forwarding by executing the command :
sysctl -w net.inet.ip.forwarding=0
For other systems, check with your vendor.

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-1999-0511
XREF	OSVDB:8114

Plugin Information:

Publication date: 2010/11/23, Modification date: 2015/07/16

Ports

tcp/0

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 10.0.100.234
Port scanner(s) : nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2017/12/8 16:41 EET
Scan duration : 548 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

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

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:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:84:23:ff : VMware, Inc.
```

0/udp

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/0

```
The UDP port scan could not complete: The remote host has remained silent for too long
This might be due to a firewall filtering UDP and/or ICMP packets
```

10.0.100.10

Scan Information

Start time:	Fri Dec 8 16:41:24 2017
End time:	Fri Dec 8 16:51:49 2017

Host Information

DNS Name:	dc.ldil.de
Netbios Name:	DC
IP:	10.0.100.10
MAC Address:	00:50:56:01:29:90
OS:	Microsoft Windows Server 2008 R2 Standard Service Pack 1

Results Summary

Critical	High	Medium	Low	Info	Total
4	0	21	0	83	108

Results Details

0/tcp

50686 - IP Forwarding Enabled

Synopsis

The remote host has IP forwarding enabled.

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.
Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :
echo 0 > /proc/sys/net/ipv4/ip_forward
On Windows, set the key 'IPEnableRouter' to 0 under
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
On Mac OS X, you can disable IP forwarding by executing the command :
sysctl -w net.inet.ip.forwarding=0
For other systems, check with your vendor.

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-1999-0511
XREF	OSVDB:8114

Plugin Information:

Publication date: 2010/11/23, Modification date: 2015/07/16

Ports

tcp/0

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:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```

Remote operating system : Microsoft Windows Server 2008 R2 Standard Service Pack 1
Confidence level : 99
Method : MSRPC

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

NTP:!:unknown
SSLcert:!:i/CN:DC.ldil.des/CN:DC.ldil.de
706da7581df2e85451a6143817130be0e9f365b5
i/CN:DC.ldil.des/CN:DC.ldil.de
706da7581df2e85451a6143817130be0e9f365b5
i/CN:dc.ldil.des/CN:dc.ldil.de
65ffd7a40cd4a4146d50e19e6bfe0e0e3a594798



The remote host is running Microsoft Windows Server 2008 R2 Standard Service Pack 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:

Publication date: 2004/02/11, Modification date: 2017/04/14

Ports

tcp/0

```

10.0.100.10 resolves as dc.ldil.de.
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 10.0.100.234
Port scanner(s) : nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2017/12/8 16:41 EET
Scan duration : 615 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

```

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

24786 - Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.
Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.
If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

Plugin Information:

Publication date: 2007/03/12, Modification date: 2013/01/07

Ports

tcp/0

```
It was not possible to connect to '\\DC\ADMIN$' with the supplied credentials.
```

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:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

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:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:01:29:90 : VMware, 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:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

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

  cpe:/o:microsoft:windows_server_2008:r2:sp1 -> Microsoft Windows Server 2008 R2 Service Pack 1
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 99
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2017/08/22

Ports

udp/0

```
For your information, here is the traceroute from 10.0.100.234 to 10.0.100.10 :
10.0.100.234
10.0.100.10

Hop Count: 1
```

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/0

```
The UDP port scan could not complete: The remote host has remained silent for too long
This might be due to a firewall filtering UDP and/or ICMP packets
```

53/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

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:

Publication date: 2003/02/13, Modification date: 2017/05/16

Ports

tcp/53

72779 - DNS Server Version Detection

Synopsis

Nessus was able to obtain version information on the remote DNS server.

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.
Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2014/03/03, Modification date: 2014/11/05

Ports

tcp/53

```

DNS server answer for "version" (over TCP) :

  Microsoft DNS 6.1.7601 (1DB1446A)
```

53/udp

72836 - MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)

Synopsis

The DNS server running on the remote host has multiple vulnerabilities.

Description

According to its self-reported version number, the Microsoft DNS Server running on the remote host has the following vulnerabilities :
- A memory corruption vulnerability exists that can be triggered by an attacker sending a specially crafted NAPTR query. This could result in arbitrary code execution. (CVE-2011-1966)
- A denial of service vulnerability exists related to the improper handling of uninitialized memory. This may result in the DNS service becoming unresponsive.
(CVE-2011-1970)

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms11-058

Solution

Microsoft has released a set of patches for Windows 2003, 2008, and 2008 R2.

Risk Factor

Critical

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	49012
BID	49019
CVE	CVE-2011-1966
CVE	CVE-2011-1970
MSKB	2562485
XREF	OSVDB:74399
XREF	OSVDB:74400
XREF	MSFT:MS11-058

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2014/03/05, Modification date: 2017/08/30

Ports

udp/53

```
  Installed version : 6.1.7601.17514
  Fixed version     : 6.1.7601.17639
```

72837 - MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)

Synopsis

The DNS server running on the remote host is susceptible to a denial of service attack.

Description

According to its self-reported version number, the Microsoft DNS server running on the remote host does not properly handle objects in memory when looking up the resource record of a domain. By sending a specially crafted DNS query an attacker may be able to exploit this flaw and cause the DNS server on the remote host to stop responding and eventually restart.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms12-017

Solution

Microsoft has released a set of patches for Windows 2003, 2008, and 2008 R2.

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:C)

References

BID	52374
CVE	CVE-2012-0006
MSKB	2647170
XREF	OSVDB:80005
XREF	MSFT:MS12-017

Plugin Information:

Publication date: 2014/03/05, Modification date: 2017/08/30

Ports

udp/53

```
  Installed version : 6.1.7601.17514
  Fixed version     : 6.1.7601.17750
```

72780 - Microsoft DNS Server Version Detection

Synopsis

Nessus was able to obtain version information on the remote Microsoft DNS server.

Description

Nessus was able to obtain version information from the remote Microsoft DNS server by sending a special TXT record query to the remote host.

See Also

http://technet.microsoft.com/en-us/library/cc772069.aspx

Solution

The command 'dnscmd /config /EnableVersionQuery 0' can be used to disable version queries if desired.

Risk Factor

None

Plugin Information:

Publication date: 2014/03/03, Modification date: 2014/03/03

Ports

udp/53

```
  Reported version : Microsoft DNS 6.1.7601 (1DB1446A)
  Extended version : 6.1.7601.17514
```

88/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/88

```
Port 88/tcp was found to be open
```

43829 - Kerberos Information Disclosure

Synopsis

The remote Kerberos server is leaking information.

Description

Nessus was able to retrieve the realm name and/or server time of the remote Kerberos server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/01/08, Modification date: 2015/09/24

Ports

tcp/88

```
Nessus gathered the following information :

  Server time  : 2017-12-08 14:45:57 UTC
  Realm        : LDIL.DE
```

123/udp

10884 - Network Time Protocol (NTP) Server Detection

Synopsis

An NTP server is listening on the remote host.

Description

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

See Also

http://www.ntp.org

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2015/03/20, Modification date: 2017/05/31

Ports

udp/123

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

  No sensitive information has been disclosed.

  Version : unknown
```

135/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/135

```
Port 135/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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/135

```
The following DCERPC services are available locally :

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-c5da40415a3c2eb246

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 : WMsgKRpc07C880

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 : WMsgKRpc07C880

Object UUID : 52ef130c-08fd-4388-86b3-6edf00000001
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc07CD41

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc07CD41

Object UUID : 48e94d9f-8674-45c0-84a8-4819f0c18b07
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : OLE82BCAD99DE824A5BB69C31D447E0

Object UUID : 48e94d9f-8674-45c0-84a8-4819f0c18b07
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-14b1dc18c3e3923c7c

Object UUID : 00000000-0000-0 [...]
```

137/udp

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:

Publication date: 1999/10/12, Modification date: 2017/09/27

Ports

udp/137

```
The following 5 NetBIOS names have been gathered :

 DC                = Computer name
 LDIL              = Workgroup / Domain name
 LDIL              = Domain Controllers
 DC                = File Server Service
 LDIL              = Domain Master Browser

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

   00:50:56:01:29:90
```

139/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/139

```
Port 139/tcp 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:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/139

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

389/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/389

```
Port 389/tcp was found to be open
```

20870 - LDAP Server Detection

Synopsis

An LDAP server was detected on the remote host.

Description

The remote host is running a Lightweight Directory Access Protocol (LDAP) server. LDAP is a protocol for providing access to directory services over TCP/IP.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/02/10, Modification date: 2017/05/16

Ports

tcp/389

25701 - LDAP Crafted Search Request Server Information Disclosure

Synopsis

It is possible to discover information about the remote LDAP server.

Description

By sending a search request with a filter set to 'objectClass=*', it is possible to extract information about the remote LDAP server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/07/12, Modification date: 2012/02/20

Ports

tcp/389

```
[+]-namingContexts:
   |  DC=ldil,DC=de
   |  CN=Configuration,DC=ldil,DC=de
   |  CN=Schema,CN=Configuration,DC=ldil,DC=de
   |  DC=DomainDnsZones,DC=ldil,DC=de
   |  DC=ForestDnsZones,DC=ldil,DC=de
[+]-currentTime:
   |  20171208144918.0Z
[+]-subschemaSubentry:
   |  CN=Aggregate,CN=Schema,CN=Configuration,DC=ldil,DC=de
[+]-dsServiceName:
   |  CN=NTDS Settings,CN=DC,CN=Servers,CN=Internal,CN=Sites,CN=Configuration,DC=ldil,DC=de
[+]-namingContexts:
   |  DC=ldil,DC=de
   |  CN=Configuration,DC=ldil,DC=de
   |  CN=Schema,CN=Configuration,DC=ldil,DC=de
   |  DC=DomainDnsZones,DC=ldil,DC=de
   |  DC=ForestDnsZones,DC=ldil,DC=de
[+]-defaultNamingContext:
   |  DC=ldil,DC=de
[+]-schemaNamingContext:
   |  CN=Schema,CN=Configuration,DC=ldil,DC=de
[+]-configurationNamingContext:
   |  CN=Configuration,DC=ldil,DC=de
[+]-rootDomainNamingContext:
   |  DC=ldil,DC=de
[+]-supportedControl:
   |  1.2.840.113556.1.4.319
   |  1.2.840.113556.1.4.801
   |  1.2.840.113556.1.4.473
   |  1.2.840.113556.1.4.528
   |  1.2.840.113556.1.4.417
   |  1.2.840.113556.1.4.619
   |  1.2.840.113556.1.4.841
   |  1.2.840.113556.1.4.529
   |  1.2.840.113556.1.4.805
   |  1.2.840.113556.1.4.521
   |  1.2.840.113556.1.4.970
   |  1.2.840.113556.1.4.1338
   |  1.2.840.113556.1.4.474
   |  1.2.840.113556.1.4.1339
   |  1.2.840.113556.1.4.1340
   |  1.2.840.113556.1.4.1413
   |  2.16.840.1.113730.3.4.9
   |  2.16.840.1.113730.3.4.10
   |  1.2.840.113556.1.4.1504
   |  1.2.840.113556.1.4.1852
   |  1.2.840.113556.1.4.802
   |  1.2.840.113556.1.4.1907
   |  1.2.840.113556.1.4.1948
   |  1.2.840.113556.1.4.1974
   |  1.2.840.113556.1.4.1341
   |  1.2.840.113556.1.4.2026
   |  1.2.840.113556.1.4.2064
   |  1.2.840.113556.1.4.2065
   |  1.2.840.113556.1.4.2066
[+]-supportedLDAPVersion:
   |  3
   |  2
[+]-supportedLDAPPolicies:
   |  MaxPoolThreads
   |  MaxDatagramRecv
   |  MaxReceiveBuffer
   |  InitRecvTimeout
   |  MaxConnections
   |  MaxConnIdleTime
   |  MaxPageSize
   |  MaxQueryDuration
   |  MaxTempTableSize
   |  MaxResultSetSize
   |  MinRe [...]
```

445/tcp

97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :
- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)
ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

https://technet.microsoft.com/library/security/MS17-010

http://www.nessus.org/u?321523eb

http://www.nessus.org/u?7bec1941

http://www.nessus.org/u?d9f569cf

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

https://github.com/stamparm/EternalRocks/

http://www.nessus.org/u?59db5b5b

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.
For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users 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

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.5 (CVSS:3.0/E:F/RL:U/RC:X)

CVSS Base Score

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

CVSS Temporal Score

9.5 (CVSS2#E:F/RL:U/RC:ND)

STIG Severity

I

References

BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146

CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212
MSKB	4012213
MSKB	4012214
MSKB	4012215
MSKB	4012216
MSKB	4012217
MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XREF	OSVDB:153673
XREF	OSVDB:153674
XREF	OSVDB:153675
XREF	OSVDB:153676
XREF	OSVDB:153677
XREF	OSVDB:153678
XREF	OSVDB:155620
XREF	OSVDB:155634
XREF	OSVDB:155635
XREF	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065

Exploitable with

Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2017/03/20, Modification date: 2017/09/07

Ports

tcp/445

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/445

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

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:

Publication date: 2000/05/09, Modification date: 2017/11/06

Ports

tcp/445

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

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/445

```
The following DCERPC services are available remotely :

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 : \\DC

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 : \\DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Description : Telephony service
Windows process : svchost.exe
Annotation : Unimodem LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\tapsrv
Netbios name : \\DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0
Description : Active Directory Replication Interface
Windows process : unknown
Annotation : MS NT Directory DRS Interface
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0
Description : Active Directory Replication Interface
Windows process : unknown
Annotation : MS NT Directory DRS Interface
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0
Description : Local Security Authority
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0
Description : Local Security Authority
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Wi [...]
```

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:

Publication date: 2001/10/17, Modification date: 2017/02/21

Ports

tcp/445

```
The remote Operating System is : Windows Server 2008 R2 Standard 7601 Service Pack 1
The remote native LAN manager is : Windows Server 2008 R2 Standard 6.1
The remote SMB Domain Name is : LDIL
```

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:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/445

```

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

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.
If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'
service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/10/04, Modification date: 2011/03/27

Ports

tcp/445

```
Could not connect to the registry because:
Could not connect to \winreg
```

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:

Publication date: 2017/02/03, Modification date: 2017/02/16

Ports

tcp/445

```
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:

Publication date: 2017/06/19, Modification date: 2017/06/19

Ports

tcp/445

```
The remote host supports the following versions of SMB :
  SMBv1
  SMBv2
```

464/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/464

```
Port 464/tcp was found to be open
```

500/udp

62695 - IPSEC Internet Key Exchange (IKE) Version 2 Detection

Synopsis

A VPN server is listening on the remote port.

Description

The remote host seems to be enabled to do Internet Key Exchange (IKE).
This is typically indicative of a VPN server. VPN servers are used to connect remote hosts into internal resources.
Make sure that the use of this VPN endpoint is done in accordance with your corporate security policy.
Note that if the remote host is not configured to allow the Nessus host to perform IKE/IPSEC negotiations, Nessus won't be able to detect the IKE service.
Also note that this plugin does not run over IPv6.

Solution

If this service is not needed, disable it or filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Publication date: 2012/10/24, Modification date: 2016/02/15

Ports

udp/500

593/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/593

```
Port 593/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/593

```
An http-rpc-epmap is running on this port.
```

636/tcp

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

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

CVSS Temporal Score

3.5 (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:

Publication date: 2009/01/05, Modification date: 2017/06/12

Ports

tcp/636

```
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=DC.ldil.de
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Feb 21 13:50:27 2017 GMT
|-Valid To            : Feb 21 14:10:27 2018 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:

Publication date: 2009/11/23, Modification date: 2017/09/01

Ports

tcp/636

```
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}
```

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:

Publication date: 2010/12/15, Modification date: 2017/05/18

Ports

tcp/636

```
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=DC.ldil.de
|-Issuer  : CN=DC.ldil.de
```

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:

Publication date: 2012/01/17, Modification date: 2016/12/14

Ports

tcp/636

```
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=DC.ldil.de
```

80035 - TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)

Synopsis

It was possible to obtain sensitive information from the remote host with 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 TLS server not verifying block cipher padding when using a cipher suite that employs a block cipher such as AES and DES. The lack of padding checking can allow encrypted TLS traffic to be decrypted. This vulnerability could allow for the decryption of HTTPS traffic by an unauthorized third party.

See Also

https://www.imperialviolet.org/2014/12/08/poodleagain.html

https://support.f5.com/csp/#/article/K15882

http://www.nessus.org/u?3bcd20bf

Solution

Contact the vendor for an update.

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

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

CVSS Temporal Score

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

References

BID	71549
CVE	CVE-2014-8730
XREF	OSVDB:115590
XREF	OSVDB:115591

Plugin Information:

Publication date: 2014/12/15

Ports

tcp/636

94437 - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of 64-bit block ciphers.

Description

The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.
Proof-of-concepts have shown that attackers can recover authentication cookies from an HTTPS session in as little as 30 hours.
Note that the ability to send a large number of requests over the same TLS connection between the client and server is an important requirement for carrying out this attack. If the number of requests allowed for a single connection were limited, this would mitigate the vulnerability. However, Nessus has not checked for such a mitigation.

See Also

https://sweet32.info

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

Solution

Reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers. Alternatively, place limitations on the number of requests that are allowed to be processed over the same TLS connection to mitigate this vulnerability.

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 v3.0 Temporal Score

5.1 (CVSS:3.0/E:F/RL:X/RC:X)

CVSS Base Score

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

CVSS Temporal Score

4.8 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	92630
BID	92631
CVE	CVE-2016-2183
CVE	CVE-2016-6329
XREF	OSVDB:143387
XREF	OSVDB:143388

Plugin Information:

Publication date: 2016/11/01, Modification date: 2017/01/24

Ports

tcp/636

```
List of 64-bit block cipher suites 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}
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/636

```
Port 636/tcp was found to be open
```

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:

Publication date: 2008/05/19, Modification date: 2015/12/30

Ports

tcp/636

```
Subject Name:

Common Name: DC.ldil.de

Issuer Name:

Common Name: DC.ldil.de

Serial Number: 4C 8E 9F 4D 48 D4 1C A8 41 01 3F 0F 9A DA 8F 16

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Feb 21 13:50:27 2017 GMT
Not Valid After: Feb 21 14:10:27 2018 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B7 0F AA 3A 06 F3 28 F9 28 0B 1D 5F EF 74 30 C2 89 4D BF
            33 02 36 0B 93 C8 72 3E 71 C4 F2 AF 2B 52 6A 88 A6 6C 3F C0
            E2 6A 92 B9 C9 D5 79 66 28 B6 01 91 0F 2B 30 BC F7 C5 71 D8
            F3 24 CB 62 06 B8 74 78 B0 14 96 24 3C 63 98 D7 00 D9 AF 9F
            8B A1 02 99 8C EC BC A6 42 74 0F 7C B7 B2 87 23 4B 65 15 91
```

```
              0D 93 B6 DE 58 F1 A0 26 E3 E3 C8 E7 0A 7E 8C D5 96 87 F4 E4
              2D BA F0 EA FF 30 03 88 02 01 54 9F 1B B7 69 B9 A5 C7 CF 84
              A6 79 92 30 67 C6 B1 97 79 55 6F 6A D4 A6 17 B1 AD AC EA 97
              6D 54 E8 67 59 87 8E E4 27 F8 91 B0 6A CD BF C2 64 C2 92 93
              7C C7 F6 85 0D 12 FF 12 0A 22 2E B3 D7 49 8D 94 D0 0C 4A A4
              20 FC F5 45 90 FB D0 A7 17 B0 DE B7 51 96 C9 2D 2E 3C A0 3F
              B9 AF F5 4E 05 16 22 6F 87 07 5B 09 D1 39 89 1D FE 2E 2D 31
              A6 11 77 A7 E5 02 C9 34 F7 91 A9 A2 70 1D 8F 33 61
  Exponent: 01 00 01

  Signature Length: 256 bytes / 2048 bits
  Signature: 00 66 CA 43 94 FA 84 05 03 9F B1 E2 61 76 5D 3F A6 CE 16 A4
             4C 8F 4D CE E1 16 E8 BF 1E BF DA B6 A0 38 E8 0B 6F 9D C5 CB
             DB 6F 2B E0 5A 0B 07 76 A6 38 F3 CE BB 8B B3 58 05 75 BD 8B
             D1 91 9A F7 B3 B7 5C 89 F3 3E 8F E6 3A D1 F2 00 FA 53 BF 18
             93 32 32 EF 84 8D F1 CD 02 34 0B 1D 41 FB F2 74 76 2D AA C5
             2C 61 B6 06 22 8C F3 B1 D7 23 6C F8 A5 E9 10 FD 3A 51 66 50
             DB A5 4A 29 1F 1E F0 5A CE 9E C2 A6 C6 63 35 FD F1 37 4D E7
             41 76 A0 FC 9D 17 11 66 09 CF 3C 51 50 8E DF 86 04 4D 60 42
             9C F6 25 44 10 BE E0 8C A5 39 0C 5A 76 8B 7F 70 79 C3 87 39
             6F 7F C4 59 92 CA 9D EA 20 AC  [...]
```

20870 - LDAP Server Detection

Synopsis

An LDAP server was detected on the remote host.

Description

The remote host is running a Lightweight Directory Access Protocol (LDAP) server. LDAP is a protocol for providing access to directory services over TCP/IP.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/02/10, Modification date: 2017/05/16

Ports

tcp/636

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:

Publication date: 2006/06/05, Modification date: 2017/11/13

Ports

tcp/636

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

SSL Version : TLSv1
  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

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:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/636

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

25701 - LDAP Crafted Search Request Server Information Disclosure

Synopsis

It is possible to discover information about the remote LDAP server.

Description

By sending a search request with a filter set to 'objectClass=*', it is possible to extract information about the remote LDAP server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/07/12, Modification date: 2012/02/20

Ports

tcp/636

```
[+]-namingContexts:
   |  DC=ldil,DC=de
   |  CN=Configuration,DC=ldil,DC=de
   |  CN=Schema,CN=Configuration,DC=ldil,DC=de
   |  DC=DomainDnsZones,DC=ldil,DC=de
```

```
    |  DC=ForestDnsZones,DC=ldil,DC=de
 [+]-currentTime:
    |  20171208144918.0Z
 [+]-subschemaSubentry:
    |  CN=Aggregate,CN=Schema,CN=Configuration,DC=ldil,DC=de
 [+]-dsServiceName:
    |  CN=NTDS Settings,CN=DC,CN=Servers,CN=Internal,CN=Sites,CN=Configuration,DC=ldil,DC=de
 [+]-namingContexts:
    |  DC=ldil,DC=de
    |  CN=Configuration,DC=ldil,DC=de
    |  CN=Schema,CN=Configuration,DC=ldil,DC=de
    |  DC=DomainDnsZones,DC=ldil,DC=de
    |  DC=ForestDnsZones,DC=ldil,DC=de
 [+]-defaultNamingContext:
    |  DC=ldil,DC=de
 [+]-schemaNamingContext:
    |  CN=Schema,CN=Configuration,DC=ldil,DC=de
 [+]-configurationNamingContext:
    |  CN=Configuration,DC=ldil,DC=de
 [+]-rootDomainNamingContext:
    |  DC=ldil,DC=de
 [+]-supportedControl:
    |  1.2.840.113556.1.4.319
    |  1.2.840.113556.1.4.801
    |  1.2.840.113556.1.4.473
    |  1.2.840.113556.1.4.528
    |  1.2.840.113556.1.4.417
    |  1.2.840.113556.1.4.619
    |  1.2.840.113556.1.4.841
    |  1.2.840.113556.1.4.529
    |  1.2.840.113556.1.4.805
    |  1.2.840.113556.1.4.521
    |  1.2.840.113556.1.4.970
    |  1.2.840.113556.1.4.1338
    |  1.2.840.113556.1.4.474
    |  1.2.840.113556.1.4.1339
    |  1.2.840.113556.1.4.1340
    |  1.2.840.113556.1.4.1413
    |  2.16.840.1.113730.3.4.9
    |  2.16.840.1.113730.3.4.10
    |  1.2.840.113556.1.4.1504
    |  1.2.840.113556.1.4.1852
    |  1.2.840.113556.1.4.802
    |  1.2.840.113556.1.4.1907
    |  1.2.840.113556.1.4.1948
    |  1.2.840.113556.1.4.1974
    |  1.2.840.113556.1.4.1341
    |  1.2.840.113556.1.4.2026
    |  1.2.840.113556.1.4.2064
    |  1.2.840.113556.1.4.2065
    |  1.2.840.113556.1.4.2066
 [+]-supportedLDAPVersion:
    |  3
    |  2
 [+]-supportedLDAPPolicies:
    |  MaxPoolThreads
    |  MaxDatagramRecv
    |  MaxReceiveBuffer
    |  InitRecvTimeout
    |  MaxConnections
    |  MaxConnIdleTime
    |  MaxPageSize
    |  MaxQueryDuration
    |  MaxTempTableSize
    |  MaxResultSetSize
    |  MinRe [...]
```

35297 - SSL Service Requests Client Certificate

Synopsis

The remote service requests an SSL client certificate.

Description

The remote service encrypts communications using SSL/TLS, requests a client certificate, and may require a valid certificate in order to establish a connection to the underlying service.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/01/06, Modification date: 2017/06/15

Ports

tcp/636

```
A TLSv1 server is listening on this port that requests a client certificate.
```

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:

Publication date: 2011/02/07, Modification date: 2013/10/18

Ports

tcp/636

```
This port supports resuming TLSv1 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:

Publication date: 2011/12/01, Modification date: 2017/11/06

Ports

tcp/636

```
This port supports TLSv1.0.
```

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:

Publication date: 2011/12/07, Modification date: 2017/06/12

Ports

tcp/636

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

  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

The fields above are :

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

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:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/636

```
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

The fields above are :

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

3268/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/3268

```
Port 3268/tcp was found to be open
```

20870 - LDAP Server Detection

Synopsis

An LDAP server was detected on the remote host.

Description

The remote host is running a Lightweight Directory Access Protocol (LDAP) server. LDAP is a protocol for providing access to directory services over TCP/IP.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/02/10, Modification date: 2017/05/16

Ports

tcp/3268

25701 - LDAP Crafted Search Request Server Information Disclosure

Synopsis

It is possible to discover information about the remote LDAP server.

Description

By sending a search request with a filter set to 'objectClass=*', it is possible to extract information about the remote LDAP server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/07/12, Modification date: 2012/02/20

Ports

tcp/3268

```
[+]-namingContexts:
   |  DC=ldil,DC=de
   |  CN=Configuration,DC=ldil,DC=de
   |  CN=Schema,CN=Configuration,DC=ldil,DC=de
   |  DC=DomainDnsZones,DC=ldil,DC=de
   |  DC=ForestDnsZones,DC=ldil,DC=de
[+]-currentTime:
   |  20171208144918.0Z
[+]-subschemaSubentry:
   |  CN=Aggregate,CN=Schema,CN=Configuration,DC=ldil,DC=de
[+]-dsServiceName:
   |  CN=NTDS Settings,CN=DC,CN=Servers,CN=Internal,CN=Sites,CN=Configuration,DC=ldil,DC=de
[+]-namingContexts:
   |  DC=ldil,DC=de
   |  CN=Configuration,DC=ldil,DC=de
   |  CN=Schema,CN=Configuration,DC=ldil,DC=de
   |  DC=DomainDnsZones,DC=ldil,DC=de
   |  DC=ForestDnsZones,DC=ldil,DC=de
[+]-defaultNamingContext:
   |  DC=ldil,DC=de
[+]-schemaNamingContext:
   |  CN=Schema,CN=Configuration,DC=ldil,DC=de
[+]-configurationNamingContext:
   |  CN=Configuration,DC=ldil,DC=de
[+]-rootDomainNamingContext:
   |  DC=ldil,DC=de
[+]-supportedControl:
   |  1.2.840.113556.1.4.319
   |  1.2.840.113556.1.4.801
   |  1.2.840.113556.1.4.473
   |  1.2.840.113556.1.4.528
   |  1.2.840.113556.1.4.417
   |  1.2.840.113556.1.4.619
   |  1.2.840.113556.1.4.841
   |  1.2.840.113556.1.4.529
   |  1.2.840.113556.1.4.805
   |  1.2.840.113556.1.4.521
   |  1.2.840.113556.1.4.970
   |  1.2.840.113556.1.4.1338
   |  1.2.840.113556.1.4.474
   |  1.2.840.113556.1.4.1339
   |  1.2.840.113556.1.4.1340
   |  1.2.840.113556.1.4.1413
   |  2.16.840.1.113730.3.4.9
   |  2.16.840.1.113730.3.4.10
   |  1.2.840.113556.1.4.1504
   |  1.2.840.113556.1.4.1852
   |  1.2.840.113556.1.4.802
   |  1.2.840.113556.1.4.1907
   |  1.2.840.113556.1.4.1948
   |  1.2.840.113556.1.4.1974
   |  1.2.840.113556.1.4.1341
   |  1.2.840.113556.1.4.2026
   |  1.2.840.113556.1.4.2064
   |  1.2.840.113556.1.4.2065
   |  1.2.840.113556.1.4.2066
[+]-supportedLDAPVersion:
   |  3
   |  2
[+]-supportedLDAPPolicies:
   |  MaxPoolThreads
   |  MaxDatagramRecv
   |  MaxReceiveBuffer
   |  InitRecvTimeout
   |  MaxConnections
   |  MaxConnIdleTime
   |  MaxPageSize
   |  MaxQueryDuration
   |  MaxTempTableSize
   |  MaxResultSetSize
   |  MinRe [...]
```

3269/tcp

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

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

CVSS Temporal Score

3.5 (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:

Publication date: 2009/01/05, Modification date: 2017/06/12

Ports

tcp/3269

```
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=DC.ldil.de
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Feb 21 13:50:27 2017 GMT
|-Valid To            : Feb 21 14:10:27 2018 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:

Publication date: 2009/11/23, Modification date: 2017/09/01

Ports

tcp/3269

```
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}
```

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:

Publication date: 2010/12/15, Modification date: 2017/05/18

Ports

tcp/3269

```
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=DC.ldil.de
|-Issuer  : CN=DC.ldil.de
```

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:

Publication date: 2012/01/17, Modification date: 2016/12/14

Ports

tcp/3269

```
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=DC.ldil.de
```

80035 - TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)

Synopsis

It was possible to obtain sensitive information from the remote host with 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 TLS server not verifying block cipher padding when using a cipher suite that employs a block cipher such as AES and DES. The lack of padding checking can allow encrypted TLS traffic to be decrypted. This vulnerability could allow for the decryption of HTTPS traffic by an unauthorized third party.

See Also

https://www.imperialviolet.org/2014/12/08/poodleagain.html

https://support.f5.com/csp/#/article/K15882

http://www.nessus.org/u?3bcd20bf

Solution

Contact the vendor for an update.

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

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

CVSS Temporal Score

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

References

BID	71549
CVE	CVE-2014-8730
XREF	OSVDB:115590
XREF	OSVDB:115591

Plugin Information:

Publication date: 2014/12/15

Ports

tcp/3269

94437 - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of 64-bit block ciphers.

Description

The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.

Proof-of-concepts have shown that attackers can recover authentication cookies from an HTTPS session in as little as 30 hours.
Note that the ability to send a large number of requests over the same TLS connection between the client and server is an important requirement for carrying out this attack. If the number of requests allowed for a single connection were limited, this would mitigate the vulnerability. However, Nessus has not checked for such a mitigation.

See Also

https://sweet32.info

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

Solution

Reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers. Alternatively, place limitations on the number of requests that are allowed to be processed over the same TLS connection to mitigate this vulnerability.

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 v3.0 Temporal Score

5.1 (CVSS:3.0/E:F/RL:X/RC:X)

CVSS Base Score

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

CVSS Temporal Score

4.8 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	92630
BID	92631
CVE	CVE-2016-2183
CVE	CVE-2016-6329
XREF	OSVDB:143387
XREF	OSVDB:143388

Plugin Information:

Publication date: 2016/11/01, Modification date: 2017/01/24

Ports

tcp/3269

```

List of 64-bit block cipher suites 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}
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/3269

```
Port 3269/tcp was found to be open
```

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:

Publication date: 2008/05/19, Modification date: 2015/12/30

Ports

tcp/3269

```
Subject Name:

Common Name: DC.ldil.de

Issuer Name:

Common Name: DC.ldil.de

Serial Number: 4C 8E 9F 4D 48 D4 1C A8 41 01 3F 0F 9A DA 8F 16

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Feb 21 13:50:27 2017 GMT
Not Valid After: Feb 21 14:10:27 2018 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B7 0F AA 3A 06 F3 28 F9 28 0B 1D 5F EF 74 30 C2 89 4D BF
            33 02 36 0B 93 C8 72 3E 71 C4 F2 AF 2B 52 6A 88 A6 6C 3F C0
            E2 6A 92 B9 C9 D5 79 66 28 B6 01 91 0F 2B 30 BC F7 C5 71 D8
            F3 24 CB 62 06 B8 74 78 B0 14 96 24 3C 63 98 D7 00 D9 AF 9F
            8B A1 02 99 8C EC BC A6 42 74 0F 7C B7 B2 87 23 4B 65 15 91
            0D 93 B6 DE 58 F1 A0 26 E3 E3 C8 E7 0A 7E 8C D5 96 87 F4 E4
            2D BA F0 EA FF 30 03 88 02 01 54 9F 1B B7 69 B9 A5 C7 CF 84
            A6 79 92 30 67 C6 B1 97 79 55 6F 6A D4 A6 17 B1 AD AC EA 97
            6D 54 E8 67 59 87 8E E4 27 F8 91 B0 6A CD BF C2 64 C2 92 93
            7C C7 F6 85 0D 12 FF 12 0A 22 2E B3 D7 49 8D 94 D0 0C 4A A4
            20 FC F5 45 90 FB D0 A7 17 B0 DE B7 51 96 C9 2D 2E 3C A0 3F
            B9 AF F5 4E 05 16 22 6F 87 07 5B 09 D1 39 89 1D FE 2E 2D 31
            A6 11 77 A7 E5 02 C9 34 F7 91 A9 A2 70 1D 8F 33 61
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 66 CA 43 94 FA 84 05 03 9F B1 E2 61 76 5D 3F A6 CE 16 A4
           4C 8F 4D CE E1 16 E8 BF 1E BF DA B6 A0 38 E8 0B 6F 9D C5 CB
           DB 6F 2B E0 5A 0B 07 76 A6 38 F3 CE BB 8B B3 58 05 75 BD 8B
           D1 91 9A F7 B3 B7 5C 89 F3 3E 8F E6 3A D1 F2 00 FA 53 BF 18
           93 32 32 EF 84 8D F1 CD 02 34 0B 1D 41 FB F2 74 76 2D AA C5
           2C 61 B6 06 22 8C F3 B1 D7 23 6C F8 A5 E9 10 FD 3A 51 66 50
           DB A5 4A 29 1F 1E F0 5A CE 9E C2 A6 C6 63 35 FD F1 37 4D E7
           41 76 A0 FC 9D 17 11 66 09 CF 3C 51 50 8E DF 86 04 4D 60 42
           9C F6 25 44 10 BE E0 8C A5 39 0C 5A 76 8B 7F 70 79 C3 87 39
           6F 7F C4 59 92 CA 9D EA 20 AC  [...]
```

20870 - LDAP Server Detection

Synopsis

An LDAP server was detected on the remote host.

Description

The remote host is running a Lightweight Directory Access Protocol (LDAP) server. LDAP is a protocol for providing access to directory services over TCP/IP.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/02/10, Modification date: 2017/05/16

Ports

tcp/3269

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:

Publication date: 2006/06/05, Modification date: 2017/11/13

Ports

tcp/3269

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

SSL Version : TLSv1
  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

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:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/3269

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

25701 - LDAP Crafted Search Request Server Information Disclosure

Synopsis

It is possible to discover information about the remote LDAP server.

Description

By sending a search request with a filter set to 'objectClass=*', it is possible to extract information about the remote LDAP server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/07/12, Modification date: 2012/02/20

Ports

tcp/3269

```
[+]-namingContexts:
   |  DC=ldil,DC=de
   |  CN=Configuration,DC=ldil,DC=de
   |  CN=Schema,CN=Configuration,DC=ldil,DC=de
   |  DC=DomainDnsZones,DC=ldil,DC=de
   |  DC=ForestDnsZones,DC=ldil,DC=de
[+]-currentTime:
   |  20171208144918.0Z
[+]-subschemaSubentry:
   |  CN=Aggregate,CN=Schema,CN=Configuration,DC=ldil,DC=de
```

```
  [+]-dsServiceName:
     |  CN=NTDS Settings,CN=DC,CN=Servers,CN=Internal,CN=Sites,CN=Configuration,DC=ldil,DC=de
  [+]-namingContexts:
     |  DC=ldil,DC=de
     |  CN=Configuration,DC=ldil,DC=de
     |  CN=Schema,CN=Configuration,DC=ldil,DC=de
     |  DC=DomainDnsZones,DC=ldil,DC=de
     |  DC=ForestDnsZones,DC=ldil,DC=de
  [+]-defaultNamingContext:
     |  DC=ldil,DC=de
  [+]-schemaNamingContext:
     |  CN=Schema,CN=Configuration,DC=ldil,DC=de
  [+]-configurationNamingContext:
     |  CN=Configuration,DC=ldil,DC=de
  [+]-rootDomainNamingContext:
     |  DC=ldil,DC=de
  [+]-supportedControl:
     |  1.2.840.113556.1.4.319
     |  1.2.840.113556.1.4.801
     |  1.2.840.113556.1.4.473
     |  1.2.840.113556.1.4.528
     |  1.2.840.113556.1.4.417
     |  1.2.840.113556.1.4.619
     |  1.2.840.113556.1.4.841
     |  1.2.840.113556.1.4.529
     |  1.2.840.113556.1.4.805
     |  1.2.840.113556.1.4.521
     |  1.2.840.113556.1.4.970
     |  1.2.840.113556.1.4.1338
     |  1.2.840.113556.1.4.474
     |  1.2.840.113556.1.4.1339
     |  1.2.840.113556.1.4.1340
     |  1.2.840.113556.1.4.1413
     |  2.16.840.1.113730.3.4.9
     |  2.16.840.1.113730.3.4.10
     |  1.2.840.113556.1.4.1504
     |  1.2.840.113556.1.4.1852
     |  1.2.840.113556.1.4.802
     |  1.2.840.113556.1.4.1907
     |  1.2.840.113556.1.4.1948
     |  1.2.840.113556.1.4.1974
     |  1.2.840.113556.1.4.1341
     |  1.2.840.113556.1.4.2026
     |  1.2.840.113556.1.4.2064
     |  1.2.840.113556.1.4.2065
     |  1.2.840.113556.1.4.2066
  [+]-supportedLDAPVersion:
     |  3
     |  2
  [+]-supportedLDAPPolicies:
     |  MaxPoolThreads
     |  MaxDatagramRecv
     |  MaxReceiveBuffer
     |  InitRecvTimeout
     |  MaxConnections
     |  MaxConnIdleTime
     |  MaxPageSize
     |  MaxQueryDuration
     |  MaxTempTableSize
     |  MaxResultSetSize
     |  MinRe [...]
```

35297 - SSL Service Requests Client Certificate

Synopsis

The remote service requests an SSL client certificate.

Description

The remote service encrypts communications using SSL/TLS, requests a client certificate, and may require a valid certificate in order to establish a connection to the underlying service.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/01/06, Modification date: 2017/06/15

Ports

tcp/3269

```
A TLSv1 server is listening on this port that requests a client certificate.
```

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:

Publication date: 2011/02/07, Modification date: 2013/10/18

Ports

tcp/3269

```
This port supports resuming TLSv1 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:

Publication date: 2011/12/01, Modification date: 2017/11/06

Ports

tcp/3269

```
This port supports TLSv1.0.
```

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:

Publication date: 2011/12/07, Modification date: 2017/06/12

Ports

tcp/3269

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

  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

The fields above are :

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

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:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/3269

```
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

The fields above are :

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

3389/tcp

79638 - MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)

Synopsis

The remote Windows host is affected by a remote code execution vulnerability.

Description

The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server.
Note that this plugin sends a client Certificate TLS handshake message followed by a CertificateVerify message. Some Windows hosts will close the connection upon receiving a client certificate for which it did not ask for with a CertificateRequest message. In this case, the plugin cannot proceed to detect the vulnerability as the CertificateVerify message cannot be sent.

See Also

https://technet.microsoft.com/library/security/ms14-066

Solution

Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.

Risk Factor

Critical

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	70954
CVE	CVE-2014-6321
MSKB	2992611
XREF	OSVDB:114506
XREF	CERT:505120
XREF	MSFT:MS14-066

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2014/12/01, Modification date: 2017/11/06

Ports

tcp/3389

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

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

CVSS Temporal Score

3.5 (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:

Publication date: 2009/01/05, Modification date: 2017/06/12

Ports

tcp/3389

```
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=dc.ldil.de
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Jul 21 21:28:13 2017 GMT
|-Valid To            : Jan 20 21:28:13 2018 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:

Publication date: 2009/11/23, Modification date: 2017/09/01

Ports

tcp/3389

```

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}
```

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:

Publication date: 2010/12/15, Modification date: 2017/05/18

Ports

tcp/3389

```
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=dc.ldil.de
|-Issuer  : CN=dc.ldil.de
```

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:

Publication date: 2012/01/17, Modification date: 2016/12/14

Ports

tcp/3389

```
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=dc.ldil.de
```

94437 - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of 64-bit block ciphers.

Description

The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.

Proof-of-concepts have shown that attackers can recover authentication cookies from an HTTPS session in as little as 30 hours.

Note that the ability to send a large number of requests over the same TLS connection between the client and server is an important requirement for carrying out this attack. If the number of requests allowed for a single connection were limited, this would mitigate the vulnerability. However, Nessus has not checked for such a mitigation.

See Also

https://sweet32.info

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

Solution

Reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers. Alternatively, place limitations on the number of requests that are allowed to be processed over the same TLS connection to mitigate this vulnerability.

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 v3.0 Temporal Score

5.1 (CVSS:3.0/E:F/RL:X/RC:X)

CVSS Base Score

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

CVSS Temporal Score

4.8 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	92630
BID	92631
CVE	CVE-2016-2183
CVE	CVE-2016-6329
XREF	OSVDB:143387
XREF	OSVDB:143388

Plugin Information:

Publication date: 2016/11/01, Modification date: 2017/01/24

Ports

tcp/3389

```

List of 64-bit block cipher suites 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}
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/3389

```
Port 3389/tcp was found to be open
```

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:

Publication date: 2008/05/19, Modification date: 2015/12/30

Ports

tcp/3389

```
Subject Name:

Common Name: dc.ldil.de

Issuer Name:

Common Name: dc.ldil.de

Serial Number: 51 40 5D 79 B7 E8 88 8D 47 DD DA E0 C8 94 A5 72

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jul 21 21:28:13 2017 GMT
Not Valid After: Jan 20 21:28:13 2018 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 8A 43 7B A0 1C 2E EF FF 07 C1 56 19 98 94 26 15 74 9C 93
            9F 83 B4 4B 1B CA 88 5C A6 AF ED 63 E1 25 04 A4 F9 C8 63 E9
            ED B7 23 BA FE 41 42 D4 D2 7C E8 F6 2B CD F2 82 B1 44 6D 11
            05 40 5F C3 94 78 7D 83 09 0B 1F D7 FA 1E C6 D5 B8 D0 4A D6
            50 17 98 8E F8 38 B5 B5 96 C3 A0 DB 6E 2B 41 BA D3 3C CD 42
            A1 84 A6 6F 05 77 A0 D7 09 66 56 E9 B6 1D 11 BF 29 2E A5 FA
            F2 E2 A2 36 C5 72 03 F4 88 9C AE A9 7D AF FA 7A F8 88 15 60
            0B 8E F9 7A 6D D6 FF D1 15 31 CC 78 E1 EC 38 DE 1A 80 EE 01
            4A B0 C1 DD 4A 50 AA DB 20 D4 70 16 8B 19 16 20 A0 02 AF B5
```

```
              0D E6 40 FE 74 2C 42 E6 7E 4E D8 24 FE 8D 88 9A DA B2 84 17
              B8 7C BA EA A0 68 AF 9F B9 D1 3D EC 1C B4 4B 74 8A F9 E9 1E
              EB 25 90 2D 0D 76 2C 86 FF 7F 92 35 00 0B 3D 50 27 E6 F7 73
              6A 5B 4B B4 2B 97 BB DB 5F 45 92 57 03 59 C0 6A B3
  Exponent: 01 00 01

  Signature Length: 256 bytes / 2048 bits
  Signature: 00 3D 1E DF 89 3C C8 A5 07 0C 4D 07 C0 BC E7 55 1B F5 60 C5
             6E 37 63 14 50 32 2E F3 04 09 67 EB 1E 46 BD 18 E2 17 0E CC
             86 20 79 53 D9 24 91 27 F6 E8 F0 5A 89 91 8B DA 2F 41 37 B7
             B8 48 5C ED A0 4B 4E EC B9 70 74 0F 96 EB 31 0F B6 35 7A CA
             CD BD C2 73 C3 22 F6 8E C0 3D 61 00 AC 3A 9C 2D 51 99 CB 04
             D2 BD BB A7 9D 5A D4 43 A7 F2 CF 14 E3 76 C3 7D 94 88 12 0A
             E5 20 E5 C9 66 7A 82 8D EF 5B 4D E1 D4 AA 44 2A 4A 38 BF 36
             8E EE 28 44 77 3C F6 0A CE 57 E7 4A 23 CD CB 3E 75 3A C3 86
             04 42 2A 1D EA 11 16 C6 6B 1A B4 76 3C C6 23 C0 4C BC 59 9D
             6E A0 0A 5F C2 44 31 26 02 44  [...]
```

10940 - Windows Terminal Services Enabled

Synopsis

The remote Windows host has Terminal Services enabled.

Description

Terminal Services allows a Windows user to remotely obtain a graphical login (and therefore act as a local user on the remote host).
If an attacker gains a valid login and password, this service could be used to gain further access on the remote host.
An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.
Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Solution

Disable Terminal Services if you do not use it, and do not allow this service to run across the Internet.

Risk Factor

None

Plugin Information:

Publication date: 2002/04/20, Modification date: 2017/08/07

Ports

tcp/3389

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:

Publication date: 2006/06/05, Modification date: 2017/11/13

Ports

tcp/3389

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

```
SSL Version : TLSv1
  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}
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Solution

Purchase or generate a new SSL certificate in the near future to replace the existing one.

Risk Factor

None

Plugin Information:

Publication date: 2009/12/02, Modification date: 2012/04/02

Ports

tcp/3389

```
The SSL certificate will expire within 60 days, at
Jan 20 21:28:13 2018 GMT :

  Subject          : CN=dc.ldil.de
  Issuer           : CN=dc.ldil.de
  Not valid before : Jul 21 21:28:13 2017 GMT
  Not valid after  : Jan 20 21:28:13 2018 GMT
```

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:

Publication date: 2011/02/07, Modification date: 2013/10/18

Ports

tcp/3389

```
This port supports resuming TLSv1 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:

Publication date: 2011/12/01, Modification date: 2017/11/06

Ports

tcp/3389

```
This port supports TLSv1.0.
```

64814 - Terminal Services Use SSL/TLS

Synopsis

The remote Terminal Services use SSL/TLS.

Description

The remote Terminal Services is configured to use SSL/TLS.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/02/22, Modification date: 2017/06/15

Ports

tcp/3389

```
Subject Name:

Common Name: dc.ldil.de

Issuer Name:

Common Name: dc.ldil.de

Serial Number: 51 40 5D 79 B7 E8 88 8D 47 DD DA E0 C8 94 A5 72

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jul 21 21:28:13 2017 GMT
Not Valid After: Jan 20 21:28:13 2018 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 8A 43 7B A0 1C 2E EF FF 07 C1 56 19 98 94 26 15 74 9C 93
            9F 83 B4 4B 1B CA 88 5C A6 AF ED 63 E1 25 04 A4 F9 C8 63 E9
            ED B7 23 BA FE 41 42 D4 D2 7C E8 F6 2B CD F2 82 B1 44 6D 11
            05 40 5F C3 94 78 7D 83 09 0B 1F D7 FA 1E C6 D5 B8 D0 4A D6
            50 17 98 8E F8 38 B5 B5 96 C3 A0 DB 6E 2B 41 BA D3 3C CD 42
            A1 84 A6 6F 05 77 A0 D7 09 66 56 E9 B6 1D 11 BF 29 2E A5 FA
            F2 E2 A2 36 C5 72 03 F4 88 9C AE A9 7D AF FA 7A F8 88 15 60
            0B 8E F9 7A 6D D6 FF D1 15 31 CC 78 E1 EC 38 DE 1A 80 EE 01
            4A B0 C1 DD 4A 50 AA DB 20 D4 70 16 8B 19 16 20 A0 02 AF B5
            0D E6 40 FE 74 2C 42 E6 7E 4E D8 24 FE 8D 88 9A DA B2 84 17
            B8 7C BA EA A0 68 AF 9F B9 D1 3D EC 1C B4 4B 74 8A F9 E9 1E
            EB 25 90 2D 0D 76 2C 86 FF 7F 92 35 00 0B 3D 50 27 E6 F7 73
            6A 5B 4B B4 2B 97 BB DB 5F 45 92 57 03 59 C0 6A B3
Exponent: 01 00 01
```

```
Signature Length: 256 bytes / 2048 bits
Signature: 00 3D 1E DF 89 3C C8 A5 07 0C 4D 07 C0 BC E7 55 1B F5 60 C5
           6E 37 63 14 50 32 2E F3 04 09 67 EB 1E 46 BD 18 E2 17 0E CC
           86 20 79 53 D9 24 91 27 F6 E8 F0 5A 89 91 8B DA 2F 41 37 B7
           B8 48 5C ED A0 4B 4E EC B9 70 74 0F 96 EB 31 0F B6 35 7A CA
           CD BD C2 73 C3 22 F6 8E C0 3D 61 00 AC 3A 9C 2D 51 99 CB 04
           D2 BD BB A7 9D 5A D4 43 A7 F2 CF 14 E3 76 C3 7D 94 88 12 0A
           E5 20 E5 C9 66 7A 82 8D EF 5B 4D E1 D4 AA 44 2A 4A 38 BF 36
           8E EE 28 44 77 3C F6 0A CE 57 E7 4A 23 CD CB 3E 75 3A C3 86
           04 42 2A 1D EA 11 16 C6 6B 1A B4 76 3C C6 23 C0 4C BC 59 9D
           6E A0 0A 5F C2 44 31 26 02 44  [...]
```

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:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/3389

```
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

The fields above are :

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

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information:

Publication date: 2015/05/08, Modification date: 2015/05/08

Ports

tcp/3389

```

The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=dc.ldil.de
|-Not After : Jan 20 21:28:13 2018 GMT
```

5355/udp

53514 - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

Synopsis

Arbitrary code can be executed on the remote host through the installed Windows DNS client.

Description

A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.
Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms11-030

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Risk Factor

Critical

CVSS Base Score

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

CVSS Temporal Score

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

STIG Severity

I

References

BID	47242
CVE	CVE-2011-0657
MSKB	2509553
XREF	OSVDB:71780
XREF	IAVA:2011-A-0039
XREF	MSFT:MS11-030

Exploitable with

Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2011/04/21, Modification date: 2017/08/30

Ports

udp/5355

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:

Publication date: 2011/04/21, Modification date: 2012/03/05

Ports

udp/5355

```
According to LLMNR, the name of the remote host is 'dc'.
```

5722/tcp

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/5722

```
The following DCERPC services are available on TCP port 5722 :

Object UUID : 5bc1ed07-f5f5-485f-9dfd-6fd0acf9a23c
UUID : 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1.0
Description : Unknown RPC service
Annotation : Frs2 Service
Type : Remote RPC service
TCP Port : 5722
IP : 10.0.100.10
```

49152/tcp

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49152

```
The following DCERPC services are available on TCP port 49152 :

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 : 49152
IP : 10.0.100.10
```

49153/tcp

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49153

```
The following DCERPC services are available on TCP port 49153 :

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 : 49153
IP : 10.0.100.10

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 : 49153
IP : 10.0.100.10

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 : 49153
IP : 10.0.100.10

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 : 49153
IP : 10.0.100.10
```

49154/tcp

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49154

```
The following DCERPC services are available on TCP port 49154 :

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 : 49154
IP : 10.0.100.10

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 : 49154
IP : 10.0.100.10

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 : 49154
IP : 10.0.100.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.100.10

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
```

```
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.100.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.100.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.100.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.100.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote R [...]
```

49155/tcp

90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Synopsis

The remote Windows host is affected by an elevation of privilege vulnerability.

Description

The remote Windows host is affected by an elevation of privilege vulnerability 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 able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

See Also

https://technet.microsoft.com/library/security/MS16-047

http://badlock.org/

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

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)

STIG Severity

I

References

BID	86002
CVE	CVE-2016-0128
MSKB	3148527
MSKB	3149090
MSKB	3147461
MSKB	3147458
XREF	OSVDB:136339
XREF	MSFT:MS16-047
XREF	CERT:813296
XREF	IAVA:2016-A-0093

Plugin Information:

Publication date: 2016/04/13, Modification date: 2017/08/30

Ports

tcp/49155

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49155

```
The following DCERPC services are available on TCP port 49155 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0
Description : Active Directory Replication Interface
Windows process : unknown
Annotation : MS NT Directory DRS Interface
Type : Remote RPC service
TCP Port : 49155
IP : 10.0.100.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0
Description : Local Security Authority
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49155
IP : 10.0.100.10

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 : 49155
IP : 10.0.100.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0
Description : Network Logon Service
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49155
IP : 10.0.100.10
```

49158/tcp

90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Synopsis

The remote Windows host is affected by an elevation of privilege vulnerability.

Description

The remote Windows host is affected by an elevation of privilege vulnerability 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 able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

See Also

https://technet.microsoft.com/library/security/MS16-047

http://badlock.org/

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

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)

STIG Severity

I

References

BID	86002
CVE	CVE-2016-0128
MSKB	3148527
MSKB	3149090
MSKB	3147461
MSKB	3147458
XREF	OSVDB:136339
XREF	MSFT:MS16-047
XREF	CERT:813296

XREF	IAVA:2016-A-0093

Plugin Information:

Publication date: 2016/04/13, Modification date: 2017/08/30

Ports

tcp/49158

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49158

```
The following DCERPC services are available on TCP port 49158 :

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 : 49158
IP : 10.0.100.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0
Description : Network Logon Service
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49158
IP : 10.0.100.10
```

49164/tcp

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49164

```
The following DCERPC services are available on TCP port 49164 :

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 : 49164
IP : 10.0.100.10
```

55034/tcp

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/55034

```
The following DCERPC services are available on TCP port 55034 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5.0
Description : DNS Server
Windows process : dns.exe
Type : Remote RPC service
TCP Port : 55034
IP : 10.0.100.10
```

63180/tcp

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/63180

```
The following DCERPC services are available on TCP port 63180 :
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6bffd098-a112-3610-9833-46c3f874532d, version 1.0
Description : DHCP Server Service
Windows process : unknown
Type : Remote RPC service
TCP Port : 63180
IP : 10.0.100.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5b821720-f63b-11d0-aad2-00c04fc324db, version 1.0
Description : DHCP Server Service
Windows process : unknown
Type : Remote RPC service
TCP Port : 63180
IP : 10.0.100.10
```

10.0.100.20

Scan Information

Start time:	Fri Dec 8 16:41:24 2017
End time:	Fri Dec 8 16:50:23 2017

Host Information

Netbios Name:	FILES
IP:	10.0.100.20
MAC Address:	00:50:56:01:29:8f
OS:	Microsoft Windows Server 2008 R2 Standard Service Pack 1

Results Summary

Critical	High	Medium	Low	Info	Total
2	0	0	0	30	32

Results Details

0/tcp

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:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```
Remote operating system : Microsoft Windows Server 2008 R2 Standard Service Pack 1
Confidence level : 99
Method : MSRPC


The remote host is running Microsoft Windows Server 2008 R2 Standard Service Pack 1
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.

- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 10.0.100.234
Port scanner(s) : nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2017/12/8 16:41 EET
Scan duration : 529 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

```

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

24786 - Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.
Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.
If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

Plugin Information:

Publication date: 2007/03/12, Modification date: 2013/01/07

Ports

tcp/0

```
It was not possible to connect to '\\FILES\ADMIN$' with the supplied credentials.
```

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:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

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:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:01:29:8f : VMware, 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:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

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

  cpe:/o:microsoft:windows_server_2008:r2:sp1 -> Microsoft Windows Server 2008 R2 Service Pack 1
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 99
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2017/08/22

Ports

udp/0

```
For your information, here is the traceroute from 10.0.100.234 to 10.0.100.20 :
10.0.100.234
10.0.100.20

Hop Count: 1
```

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/0

```
The UDP port scan could not complete: The remote host has remained silent for too long
This might be due to a firewall filtering UDP and/or ICMP packets
```

135/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/135

```
Port 135/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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/135

```
The following DCERPC services are available locally :

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-c29bd9b99eca2b37de

Object UUID : 52ef130c-08fd-4388-86b3-6edf00000001
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc07C391

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc07C391

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 : WMsgKRpc07C080

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 : WMsgKRpc07C080

Object UUID : b674f6fb-0310-4f86-a1e9-41181e24321e
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
```

```
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : OLEB08E9226415B4300967732F5F5EA

Object UUID : b674f6fb-0310-4f86-a1e9-41181e24321e
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-9268dfb1f1f8c1b232

Object UUID : 00000000-0000-0 [...]
```

137/udp

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:

Publication date: 1999/10/12, Modification date: 2017/09/27

Ports

udp/137

```
The following 3 NetBIOS names have been gathered :

 FILES            = Computer name
 LDIL             = Workgroup / Domain name
 FILES            = File Server Service

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

   00:50:56:01:29:8f
```

139/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/139

```
Port 139/tcp 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:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/139

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

445/tcp

97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

https://technet.microsoft.com/library/security/MS17-010

http://www.nessus.org/u?321523eb

http://www.nessus.org/u?7bec1941

http://www.nessus.org/u?d9f569cf

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

https://github.com/stamparm/EternalRocks/

http://www.nessus.org/u?59db5b5b

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.
For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users 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

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.5 (CVSS:3.0/E:F/RL:U/RC:X)

CVSS Base Score

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

CVSS Temporal Score

9.5 (CVSS2#E:F/RL:U/RC:ND)

STIG Severity

I

References

BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212
MSKB	4012213
MSKB	4012214
MSKB	4012215
MSKB	4012216
MSKB	4012217

MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XREF	OSVDB:153673
XREF	OSVDB:153674
XREF	OSVDB:153675
XREF	OSVDB:153676
XREF	OSVDB:153677
XREF	OSVDB:153678
XREF	OSVDB:155620
XREF	OSVDB:155634
XREF	OSVDB:155635
XREF	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065

Exploitable with

Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2017/03/20, Modification date: 2017/09/07

Ports

tcp/445

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/445

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

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:

Publication date: 2000/05/09, Modification date: 2017/11/06

Ports

tcp/445

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

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/445

```

The following DCERPC services are available remotely :

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 : \\FILES

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 : \\FILES

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 : \\FILES

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\protected_storage
Netbios name : \\FILES

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Remote RPC service
Named pipe : \pipe\spoolss
Netbios name : \\FILES

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Annotation : Spooler base remote object endpoint
Type : Remote RPC service
Named pipe : \pipe\spoolss
Netbios name : \\FILES

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Remote RPC service
Named pipe : \pipe\spoolss
Netbios name : \\FILES

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Remote RPC service
Named pipe : \pipe\spoolss
Netbios name : [...]
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

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

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/10/17, Modification date: 2017/02/21

Ports

tcp/445

```
The remote Operating System is : Windows Server 2008 R2 Standard 7601 Service Pack 1
The remote native LAN manager is : Windows Server 2008 R2 Standard 6.1
The remote SMB Domain Name is : LDIL
```

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:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/445

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

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.
If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'
service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/10/04, Modification date: 2011/03/27

Ports

tcp/445

```
Could not connect to the registry because:
Could not connect to \winreg
```

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:

Publication date: 2017/02/03, Modification date: 2017/02/16

Ports

tcp/445

```
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:

Publication date: 2017/06/19, Modification date: 2017/06/19

Ports

tcp/445

```
The remote host supports the following versions of SMB :
  SMBv1
  SMBv2
```

5355/udp

53514 - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

Synopsis

Arbitrary code can be executed on the remote host through the installed Windows DNS client.

Description

A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.

Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms11-030

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Risk Factor

Critical

CVSS Base Score

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

CVSS Temporal Score

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

STIG Severity

I

References

BID	47242
CVE	CVE-2011-0657
MSKB	2509553
XREF	OSVDB:71780
XREF	IAVA:2011-A-0039
XREF	MSFT:MS11-030

Exploitable with

Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2011/04/21, Modification date: 2017/08/30

Ports

udp/5355

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:

Publication date: 2011/04/21, Modification date: 2012/03/05

Ports

udp/5355

```
According to LLMNR, the name of the remote host is 'files'.
```

49152/tcp

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49152

```
The following DCERPC services are available on TCP port 49152 :

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 : 49152
IP : 10.0.100.20
```

49153/tcp

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49153

```
The following DCERPC services are available on TCP port 49153 :

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 : 49153
IP : 10.0.100.20

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 : 49153
IP : 10.0.100.20

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 : 49153
IP : 10.0.100.20

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 : 49153
IP : 10.0.100.20
```

49154/tcp

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49154

```
The following DCERPC services are available on TCP port 49154 :

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 : 49154
IP : 10.0.100.20

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.100.20

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 : 49154
IP : 10.0.100.20

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.100.20

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
```

```
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.100.20

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 : 49154
IP : 10.0.100.20

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.100.20

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.100.20

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote R [...]
```

49161/tcp

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49161

```
The following DCERPC services are available on TCP port 49161 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Remote RPC service
TCP Port : 49161
IP : 10.0.100.20

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Annotation : Spooler base remote object endpoint
Type : Remote RPC service
```

```
TCP Port : 49161
IP : 10.0.100.20

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Remote RPC service
TCP Port : 49161
IP : 10.0.100.20

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Remote RPC service
TCP Port : 49161
IP : 10.0.100.20
```

49177/tcp

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49177

```
The following DCERPC services are available on TCP port 49177 :

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 : 49177
IP : 10.0.100.20
```

62091/tcp

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:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/62091

```
The following DCERPC services are available on TCP port 62091 :

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 : 62091
IP : 10.0.100.20
```

10.0.100.30

Scan Information

Start time:	Fri Dec 8 16:41:24 2017
End time:	Fri Dec 8 16:45:38 2017

Host Information

IP:	10.0.100.30
MAC Address:	00:50:56:01:29:91
OS:	Linux Kernel 2.6 on CentOS Linux release 6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	12	4	40	56

Results Details

0/icmp

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:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is 3 seconds.
```

0/tcp

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:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```
Remote operating system : Linux Kernel 2.6 on CentOS Linux release 6
Confidence level : 95
Method : HTTP


The remote host is running Linux Kernel 2.6 on CentOS Linux release 6
```

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.
n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/05/15, Modification date: 2017/03/13

Ports

tcp/0

```
The Linux distribution detected was :
 - CentOS 6
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 10.0.100.234
Port scanner(s) : nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2017/12/8 16:41 EET
Scan duration : 251 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

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

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:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

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:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:01:29:91 : VMware, 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:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

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

  cpe:/o:centos:centos:6 -> CentOS-6

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

```
cpe:/a:openbsd:openssh:5.3 -> OpenBSD  OpenSSH 5.3
cpe:/a:apache:http_server:2.2.15 -> Apache Software Foundation Apache HTTP Server 2.2.15
cpe:/a:php:php:5.3.3 -> PHP 5.3.3
```

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:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 95
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2017/08/22

Ports

udp/0

```
For your information, here is the traceroute from 10.0.100.234 to 10.0.100.30 :
10.0.100.234
10.0.100.30

Hop Count: 1
```

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/0

```
The UDP port scan could not complete: The remote host has remained silent for too long
This might be due to a firewall filtering UDP and/or ICMP packets
```

22/tcp

90317 - SSH Weak Algorithms Supported

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Publication date: 2016/04/04, Modification date: 2016/12/14

Ports

tcp/22

```

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

  arcfour
  arcfour128
  arcfour256

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

  arcfour
  arcfour128
  arcfour256
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.
Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

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

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

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

References

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

Plugin Information:

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

Ports

tcp/22

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

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

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

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

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

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

Description

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

Solution

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

Risk Factor

Low

CVSS Base Score

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

Plugin Information:

Publication date: 2013/11/22, Modification date: 2016/12/14

Ports

tcp/22

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

  hmac-md5
  hmac-md5-96
  hmac-sha1-96

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

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2017/11/17

Ports

tcp/22

```
SSH version : SSH-2.0-OpenSSH_5.3
SSH supported authentication : publickey,gssapi-keyex,gssapi-with-mic,password
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/22

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

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/03/06, Modification date: 2017/05/30

Ports

tcp/22

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

  - 1.99
  - 2.0
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/22

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

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

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

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

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

Ports

tcp/22

```

Give Nessus credentials to perform local checks.
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/28, Modification date: 2017/08/28

Ports

tcp/22

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-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
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

80/tcp

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

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

Ports

tcp/80

```
The remote web server type is :

Apache/2.2.15 (CentOS)

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/80

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

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.
Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/04/28, Modification date: 2015/10/13

Ports

tcp/80

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :

    http://10.0.100.30/j8TQeI9GqjB1.html
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

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:

Publication date: 2007/01/30, Modification date: 2017/11/13

Ports

tcp/80

```
Response Code : HTTP/1.1 301 Moved Permanently

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

  Date: Fri, 08 Dec 2017 14:44:32 GMT
  Server: Apache/2.2.15 (CentOS)
  Location: https://10.0.100.30/
  Content-Length: 305
  Connection: close
  Content-Type: text/html; charset=iso-8859-1

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://10.0.100.30/">here</a>.</p>
<hr>
<address>Apache/2.2.15 (CentOS) Server at 10.0.100.30 Port 80</address>
</body></html>
```

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

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

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

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

Ports

tcp/80

```
Give Nessus credentials to perform local checks.
```

443/tcp

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

http://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648
XREF	OSVDB:11408
XREF	OSVDB:50485
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information:

Publication date: 2003/01/23, Modification date: 2016/11/23

Ports

tcp/443

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]
```

```
Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus835817163.html HTTP/1.1
Connection: Close
Host: 10.0.100.30
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

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

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.0 200 OK
Date: Fri, 08 Dec 2017 14:44:13 GMT
Server: Apache/2.2.15 (CentOS)
Connection: close
Content-Type: message/http


TRACE /Nessus835817163.html HTTP/1.1
Connection: Close
Host: 10.0.100.30
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

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

15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Publication date: 2004/12/03, Modification date: 2016/01/08

Ports

tcp/443

```
The SSL certificate has already expired :

  Subject          : C=--, ST=SomeState, L=SomeCity, O=SomeOrganization,
 OU=SomeOrganizationalUnit, CN=wordpress, emailAddress=root@wordpress
  Issuer           : C=--, ST=SomeState, L=SomeCity, O=SomeOrganization,
 OU=SomeOrganizationalUnit, CN=wordpress, emailAddress=root@wordpress
  Not valid before : Mar  1 06:20:27 2016 GMT
  Not valid after  : Mar  1 06:20:27 2017 GMT
```

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:

Publication date: 2005/10/12, Modification date: 2017/07/11

Ports

tcp/443

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

26928 - SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

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

Solution

Reconfigure the affected application, if possible to avoid the use of weak 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

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

References

XREF	CWE:326
XREF	CWE:327
XREF	CWE:720
XREF	CWE:753
XREF	CWE:803
XREF	CWE:928
XREF	CWE:934

Plugin Information:

Publication date: 2007/10/08, Modification date: 2017/09/01

Ports

tcp/443

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

  Low Strength Ciphers (<= 64-bit key)

    EDH-RSA-DES-CBC-SHA           Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
    DES-CBC-SHA                   Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

The fields above are :

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

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

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

CVSS Temporal Score

3.5 (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:

Publication date: 2009/01/05, Modification date: 2017/06/12

Ports

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             : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=wordpress/E=root@wordpress
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Mar 01 06:20:27 2016 GMT
|-Valid To            : Mar 01 06:20:27 2017 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:

Publication date: 2009/11/23, Modification date: 2017/09/01

Ports

tcp/443

```
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)

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

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:

Publication date: 2010/12/15, Modification date: 2017/05/18

Ports

tcp/443

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=wordpress/E=root@wordpress
|-Not After : Mar 01 06:20:27 2017 GMT

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 : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=wordpress/E=root@wordpress
|-Issuer  : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=wordpress/E=root@wordpress
```

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:

Publication date: 2012/01/17, Modification date: 2016/12/14

Ports

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 : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=wordpress/E=root@wordpress
```

62565 - Transport Layer Security (TLS) Protocol CRIME Vulnerability

Synopsis

The remote service has a configuration that may make it vulnerable to the CRIME attack.

Description

The remote service has one of two configurations that are known to be required for the CRIME attack :

- SSL / TLS compression is enabled.
- TLS advertises the SPDY protocol earlier than version 4.

Note that Nessus did not attempt to launch the CRIME attack against the remote service.

See Also

http://www.iacr.org/cryptodb/data/paper.php?pubkey=3091 https://discussions.nessus.org/thread/5546

http://www.nessus.org/u?8ec18eb5

https://issues.apache.org/bugzilla/show_bug.cgi?id=53219

Solution

Disable compression and / or the SPDY service.

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	55704
BID	55707
CVE	CVE-2012-4929
CVE	CVE-2012-4930
XREF	OSVDB:85926
XREF	OSVDB:85927

Plugin Information:

Publication date: 2012/10/16, Modification date: 2014/09/26

Ports

tcp/443

```
The following configuration indicates that the remote service
may be vulnerable to the CRIME attack :

  - SSL / TLS compression is enabled.
```

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:

Publication date: 2014/10/15, Modification date: 2016/11/30

Ports

tcp/443

```
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.
```

94437 - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of 64-bit block ciphers.

Description

The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.
Proof-of-concepts have shown that attackers can recover authentication cookies from an HTTPS session in as little as 30 hours.
Note that the ability to send a large number of requests over the same TLS connection between the client and server is an important requirement for carrying out this attack. If the number of requests allowed for a single connection were limited, this would mitigate the vulnerability. However, Nessus has not checked for such a mitigation.

See Also

https://sweet32.info

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

Solution

Reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers. Alternatively, place limitations on the number of requests that are allowed to be processed over the same TLS connection to mitigate this vulnerability.

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 v3.0 Temporal Score

5.1 (CVSS:3.0/E:F/RL:X/RC:X)

CVSS Base Score

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

CVSS Temporal Score

4.8 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	92630
BID	92631
CVE	CVE-2016-2183
CVE	CVE-2016-6329
XREF	OSVDB:143387
XREF	OSVDB:143388

Plugin Information:

Publication date: 2016/11/01, Modification date: 2017/01/24

Ports

tcp/443

```
List of 64-bit block cipher suites supported by the remote server :

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

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

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.2 (CVSS2#E:F/RL:TF/RC:ND)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808
XREF	OSVDB:91162
XREF	OSVDB:117855

Plugin Information:

Publication date: 2013/04/05, Modification date: 2016/12/14

Ports

tcp/443

```

List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                      Kx=RSA        Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                      Kx=RSA        Au=RSA      Enc=RC4(128)             Mac=SHA1

The fields above are :

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

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:

Publication date: 2013/09/03, Modification date: 2014/04/10

Ports

tcp/443

```
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        : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=wordpress/E=root@wordpress
|-RSA Key Length : 1024 bits
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

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

Ports

tcp/443

```
The remote web server type is :

Apache/2.2.15 (CentOS)

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/443

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

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:

Publication date: 2008/05/19, Modification date: 2015/12/30

Ports

tcp/443

```
Subject Name:

Country: --
State/Province: SomeState
Locality: SomeCity
Organization: SomeOrganization
Organization Unit: SomeOrganizationalUnit
Common Name: wordpress
Email Address: root@wordpress

Issuer Name:

Country: --
State/Province: SomeState
Locality: SomeCity
Organization: SomeOrganization
Organization Unit: SomeOrganizationalUnit
Common Name: wordpress
Email Address: root@wordpress

Serial Number: 68 81

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 01 06:20:27 2016 GMT
Not Valid After: Mar 01 06:20:27 2017 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 E5 50 18 4E 64 A2 D1 37 D6 B3 93 F1 70 EF DE 72 2D E6 7C
            4C FF BE DD 25 6C 49 88 89 89 CE DF 66 14 D9 22 7D 33 FF A4
            87 AB 54 52 1E 65 10 03 A1 17 49 34 E0 EC 3E 6E 6F BD 6E 0C
            25 AF D1 DE CA 4A 28 E7 99 EC 49 D2 6D E7 53 85 D7 90 B9 4E
            77 CD 1A C2 00 57 39 FB 14 56 52 C5 C6 F1 11 31 72 10 A0 27
            63 DB B9 D6 D0 A6 9C 7F C3 6A 65 4A 7D 4F B7 49 3C 62 C3 9A
            EF 42 31 04 EF 9D 4F EE BD
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 CB 62 BB 5F 4E 83 C9 8F 82 10 CD 85 1E AC 00 FA E3 A3 97
           CE 23 A8 12 27 A7 0B EE A9 38 2C 2C 7D 9F C6 24 19 72 82 6F
           06 45 8E C6 17 64 28 8E 42 92 46 ED 34 DE D4 23 2A C3 B2 43
           83 C9 9D 58 3B ED B1 11 24 68 E6 E8 B9 B1 84 2B CE A3 F5 7F
           5A 92 6A 71 CF 41 2C C9 4B C6 75 E5 C5 E7 12 4A 9E 3F 69 0C
           30 00 11 C3 F6 A8 9B 14 A7 B3 A7 F7 F6 6A C7 A0 CF A7 5E 71
           1B F9 42 89 BB 19 54 F3 70

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: B5 CE 38 F7 56 A9 F0 2F BC 28 6E 76 CC EC 64 00 B6 20 59 59
```

```
Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: B5 CE 38 F7 56 A9 F0 2F BC 28 6E 76 CC EC 64 00 B6 20 59 59


Extension: Basic Constraints (2.5.29.19)
Critical: 0
CA: TRUE


Fingerprints :

SHA-256 Fingerprint: 36 84 DF 87 3B 2D [...]
```

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:

Publication date: 2006/06/05, Modification date: 2017/11/13

Ports

tcp/443

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

SSL Version : TLSv1
  Low Strength Ciphers (<= 64-bit key)

    EDH-RSA-DES-CBC-SHA          Kx=DH        Au=RSA      Enc=DES-CBC(56)           Mac=SHA1
    DES-CBC-SHA                  Kx=RSA       Au=RSA      Enc=DES-CBC(56)           Mac=SHA1

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

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

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA           Kx=DH        Au=RSA      Enc=AES-CBC(128)          Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH        Au=RSA      Enc=AES-CBC(256)          Mac=SHA1
    DHE-RSA-CAMELLIA128-SHA      Kx=DH        Au=RSA      Enc=Camellia-CBC(128)     Mac=SHA1
    DHE-RSA-CAMELLIA256-SHA      Kx=DH        Au=RSA      Enc=Camellia-CBC(256)     Mac=SHA1
    DHE-RSA-SEED-SHA             Kx=DH        Au=RSA      Enc=SEED-CBC(128)         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
    CAMELLIA128-SHA              Kx=RSA       Au=RSA      Enc=Camellia-CBC(128)     Mac=SHA1
    CAMELLIA256-SHA              Kx=RSA       Au=RSA      Enc=Camellia-CBC(256)     Mac=SHA1
    RC4-MD5                      Kx=RSA       Au=RSA      Enc=RC4(128)              Mac=MD5
    RC4-SHA                      Kx=RSA       Au=RSA      Enc=RC4(128)              Mac=SHA1
    SEED-SHA                     Kx=RSA       Au=RSA      Enc=SEED-CBC(128)         Mac=SHA1


SSL Version : SSLv3
  Low Strength Ciphers (<= 64-bit key)
```

```
        EDH-RSA-DES-CBC-SHA            Kx=DH          Au=RSA      Enc=DES-CBC(56)           Mac=SHA1
        DES-CBC-SHA                    Kx=RSA         Au=RSA      En [...]
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/443

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

tcp/443

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

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2017/11/13

Ports

tcp/443

```

Response Code : HTTP/1.0 200 OK

Protocol version : HTTP/1.0
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Date: Fri, 08 Dec 2017 14:44:34 GMT
  Server: Apache/2.2.15 (CentOS)
  X-Powered-By: PHP/5.3.3
  Link: <https://131.207.103.191/wp-json/>; rel="https://api.w.org/"
  Connection: close
  Content-Type: text/html; charset=UTF-8

Response Body :

<!DOCTYPE html>
<html lang="en-US" class="no-js">
<head>
```

```
 <meta charset="UTF-8">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <link rel="profile" href="http://gmpg.org/xfn/11">
  <script>(function(html){html.className = html.className.replace(/\bno-js\b/,'js')})
(document.documentElement);</script>
<title>wordpress &#8211; Just another WordPress site</title>
<link rel="alternate" type="application/rss+xml" title="wordpress &raquo; Feed"
 href="https://131.207.103.191/index.php/feed/" />
<link rel="alternate" type="application/rss+xml" title="wordpress &raquo; Comments Feed"
 href="https://131.207.103.191/index.php/comments/feed/" />
  <script type="text/javascript">
   window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji
\/72x72\/","ext":".png","source":{"concatemoji":"https:\/\/intra.ldil.de\/wp-includes\/js\/wp-
emoji-release.min.js?ver=4.4.1"}};
   !function(a,b,c){function d(a){var
 c,d=b.createElement("canvas"),e=d.getContext&&d.getContext("2d");return
 e&&e.fillText?(e.textBaseline="top",e.font="600 32px Arial","flag"===a?
(e.fillText(String.fromCharCode(55356,56806,55356,56826),0,0),d.toDataURL().length>3e3):"diversity"===a?
(e.fillText(String.fromCharCode(55356,57221),0,0),c=e.getImageData(16,16,1,1).data.toString(),e.fillText(Strin
==e.getImageData(16,16,1,1).data.toString()):("simple"===a?
e.fillText(String.fromCharCode(55357,56835),0,0):e.fillText(String.fromCharCode(55356,57135),0,0),0!
==e.getImageData(16,16,1,1).data[0])):!1}function e(a){var
 c=b.createElement("script");c.src=a,c.type="text/javascript",b.getElementsByTagName("head")
[0].appen [...]
```

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

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

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

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

Ports

tcp/443

```
Give Nessus credentials to perform local checks.
```

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/04, Modification date: 2017/07/07

Ports

tcp/443

```
Nessus was able to identify the following PHP version information :

  Version : 5.3.3
  Source  : X-Powered-By: PHP/5.3.3
```

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:

Publication date: 2010/11/30, Modification date: 2013/10/18

Ports

tcp/443

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:

Publication date: 2011/02/07, Modification date: 2013/10/18

Ports

tcp/443

```
This port supports resuming 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:

Publication date: 2011/12/01, Modification date: 2017/11/06

Ports

tcp/443

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

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:

Publication date: 2011/12/07, Modification date: 2017/06/12

Ports

tcp/443

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

  Low Strength Ciphers (<= 64-bit key)

    EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

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

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

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    DHE-RSA-CAMELLIA128-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
    DHE-RSA-CAMELLIA256-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
    DHE-RSA-SEED-SHA             Kx=DH          Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1

The fields above are :

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

62563 - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

https://tools.ietf.org/html/rfc3749

https://tools.ietf.org/html/rfc3943

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2017/11/13

Ports

tcp/443

```
Nessus was able to confirm that the following compression method is
supported by the target :

  DEFLATE (0x01)
```

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:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/443

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

  Low Strength Ciphers (<= 64-bit key)

    EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
    DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

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

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

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

    High Strength Ciphers (>= 112-bit key)

      DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      DHE-RSA-SEED-SHA             Kx=DH          Au=RSA      Enc=SEED-CBC(128)        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
      CAMELLIA128-SHA              Kx=RSA         Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      CAMELLIA256-SHA              Kx=RSA         Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      SEED-SHA                     Kx=RSA         Au=RSA      Enc=SEED-CBC(128)        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:

Publication date: 2015/07/02, Modification date: 2015/07/02

Ports

tcp/443

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

84574 - Backported Security Patch Detection (PHP)

Synopsis

Security patches have been backported.

Description

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

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2015/07/07, Modification date: 2015/07/07

Ports

tcp/443

```
Give Nessus credentials to perform local checks.
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://technet.microsoft.com/en-us/library/cc778623

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2016/11/14, Modification date: 2016/11/14

Ports

tcp/443

```
The following root Certification Authority certificate was found :

|-Subject             : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=wordpress/E=root@wordpress
|-Issuer              : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=wordpress/E=root@wordpress
|-Valid From          : Mar 01 06:20:27 2016 GMT
|-Valid To            : Mar 01 06:20:27 2017 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

10.0.100.50

Scan Information

Start time:	Fri Dec 8 16:41:24 2017
End time:	Fri Dec 8 16:44:41 2017

Host Information

IP:	10.0.100.50
MAC Address:	00:50:56:01:29:8e
OS:	Linux Kernel 2.6 on CentOS Linux release 6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	2	2	26	30

Results Details

0/icmp

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:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is 2 seconds.
```

0/tcp

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:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```
Remote operating system : Linux Kernel 2.6 on CentOS Linux release 6
Confidence level : 95
Method : HTTP


The remote host is running Linux Kernel 2.6 on CentOS Linux release 6
```

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.
n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/05/15, Modification date: 2017/03/13

Ports

tcp/0

```
The Linux distribution detected was :
 - CentOS 6
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 10.0.100.234
Port scanner(s) : nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2017/12/8 16:41 EET
Scan duration : 193 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

```

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

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:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

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:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:01:29:8e : VMware, 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:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

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

  cpe:/o:centos:centos:6 -> CentOS-6

Following application CPE's matched on the remote system :
  cpe:/a:mysql:mysql:5.1.67
  cpe:/a:openbsd:openssh:5.3 -> OpenBSD  OpenSSH 5.3
  cpe:/a:apache:http_server:2.2.15 -> Apache Software Foundation Apache HTTP Server 2.2.15
```

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:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 95
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2017/08/22

Ports

udp/0

```
For your information, here is the traceroute from 10.0.100.234 to 10.0.100.50 :
10.0.100.234
10.0.100.50

Hop Count: 1
```

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/0

```
The UDP port scan could not complete: The remote host has remained silent for too long
This might be due to a firewall filtering UDP and/or ICMP packets
```

22/tcp

90317 - SSH Weak Algorithms Supported

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Publication date: 2016/04/04, Modification date: 2016/12/14

Ports

tcp/22

```

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

  arcfour
  arcfour128
  arcfour256

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

  arcfour
  arcfour128
  arcfour256
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.
Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

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

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

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

References

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

Plugin Information:

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

Ports

tcp/22

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

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

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

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

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

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

Description

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

Solution

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

Risk Factor

Low

CVSS Base Score

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

Plugin Information:

Publication date: 2013/11/22, Modification date: 2016/12/14

Ports

tcp/22

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

  hmac-md5
  hmac-md5-96
  hmac-sha1-96

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

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2017/11/17

Ports

tcp/22

```
SSH version : SSH-2.0-OpenSSH_5.3
SSH supported authentication : publickey,gssapi-keyex,gssapi-with-mic,password
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/22

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

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/03/06, Modification date: 2017/05/30

Ports

tcp/22

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

  - 1.99
  - 2.0
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/22

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

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

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

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

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

Ports

tcp/22

```

Give Nessus credentials to perform local checks.
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/28, Modification date: 2017/08/28

Ports

tcp/22

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-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
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

80/tcp

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

http://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386

XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648
XREF	OSVDB:11408
XREF	OSVDB:50485
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information:

Publication date: 2003/01/23, Modification date: 2016/11/23

Ports

tcp/80

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus561435367.html HTTP/1.1
Connection: Close
Host: 10.0.100.50
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

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

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Fri, 08 Dec 2017 14:43:45 GMT
Server: Apache/2.2.15 (CentOS)
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus561435367.html HTTP/1.1
Connection: Close
Host: 10.0.100.50
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ 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:

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

Ports

tcp/80

```
The remote web server type is :

Apache/2.2.15 (CentOS)

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/80

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

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:

Publication date: 2007/01/30, Modification date: 2017/11/13

Ports

tcp/80

```
Response Code : HTTP/1.1 403 Forbidden

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

  Date: Fri, 08 Dec 2017 14:43:48 GMT
  Server: Apache/2.2.15 (CentOS)
  Accept-Ranges: bytes
  Content-Length: 5039
  Connection: close
  Content-Type: text/html; charset=UTF-8

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
 <head>
  <title>Apache HTTP Server Test Page powered by CentOS</title>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <style type="text/css">
   body {
    background-color: #fff;
    color: #000;
    font-size: 0.9em;
    font-family: sans-serif,helvetica;
    margin: 0;
    padding: 0;
   }
   :link {
    color: #0000FF;
   }
   :visited {
    color: #0000FF;
   }
   a:hover {
    color: #3399FF;
   }
   h1 {
    text-align: center;
    margin: 0;
    padding: 0.6em 2em 0.4em;
    background-color: #3399FF;
    color: #ffffff;
    font-weight: normal;
    font-size: 1.75em;
    border-bottom: 2px solid #000;
   }
   h1 strong {
    font-weight: bold;
   }
   h2 {
    font-size: 1.1em;
    font-weight: bold;
   }
   .content {
    padding: 1em 5em;
   }
   .content-columns {
    /* Setting relative positioning allows for
    absolute positioning for sub-classes */
    position: relative;
    padding-top: 1em;
   }
   .content-column-left {
    /* Value for IE/Win; will be overwritten for other browsers */
    width: 47%;
    padding-right: 3%;
    float: left;
    padding-bottom: 2em;
   }
   .content-column-right {
    /* Values for IE/Win; will be overwritten for other browsers */
    width: 47%;
    padding-left: 3%;
    float: left;
    padding-bottom: 2em;
   }
   .content-columns>.content-column-left, .content-columns>.content-column-right {
    /* Non-IE/Win */
   }
   img {
    border: 2px solid #fff;
    padding: 2px;
    margin: 2px;
   }
   a:hover img {
    border: 2px solid #3399FF;
   }
  </style>
 </head>

 <body>
 <h1>Apache 2 Test Page<br [...]
```

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

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

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

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

Ports

tcp/80

```
Give Nessus credentials to perform local checks.
```

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:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports

tcp/80

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

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /
```

3306/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/3306

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

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/13, Modification date: 2013/01/07

Ports

tcp/3306

```
Version  : 5.1.67
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_PASSWORD (new more secure passwords)
  CLIENT_FOUND_ROWS (Found instead of affected rows)
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_NO_SCHEMA (Don't allow database.table.column)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_ODBC (ODBC client)
  CLIENT_LOCAL_FILES (Can use LOAD DATA LOCAL)
  CLIENT_IGNORE_SPACE (Ignore spaces before "("
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_INTERACTIVE (This is an interactive client)
  CLIENT_SIGPIPE (IGNORE sigpipes)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_RESERVED (Old flag for 4.1 protocol)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/11/18, Modification date: 2017/06/08

Ports

tcp/3306

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

10.0.100.91

Scan Information

Start time:	Fri Dec 8 16:41:24 2017
End time:	Fri Dec 8 18:00:36 2017

Host Information

IP:	10.0.100.91
MAC Address:	00:50:56:01:18:84
OS:	Linux Kernel 3.1, Linux Kernel 3.3

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	18	19

Results Details

0/icmp

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:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is 2 seconds.
```

0/tcp

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:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```
Remote operating system : Linux Kernel 3.1
Linux Kernel 3.3
Confidence level : 59
Method : SinFP


The remote host is running one of these operating systems :
Linux Kernel 3.1
Linux Kernel 3.3
```

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.
n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/05/15, Modification date: 2017/03/13

Ports

tcp/0

```
The Linux distribution detected was :
 - Debian 7.0 (wheezy)
 - Debian unstable (sid)
 - Debian testing (wheezy)
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 10.0.100.234
Port scanner(s) : nessus_udp_scanner nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2017/12/8 16:41 EET
Scan duration : 4748 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

```

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

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:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

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:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```

The following card manufacturers were identified :

00:50:56:01:18:84 : VMware, 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:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

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

  cpe:/o:linux:linux_kernel:3.1
  cpe:/o:linux:linux_kernel:3.3

Following application CPE matched on the remote system :

  cpe:/a:apache:http_server:2.2.22 -> Apache Software Foundation Apache HTTP Server 2.2.22
```

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:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 59
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2017/08/22

Ports

udp/0

```
For your information, here is the traceroute from 10.0.100.234 to 10.0.100.91 :
10.0.100.234
10.0.100.91

Hop Count: 1
```

23/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/23

```
Port 23/tcp was found to be open
```

80/tcp

88098 - Apache Server ETag Header Information Disclosure

Synopsis

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

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.8 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	6939
CVE	CVE-2003-1418
XREF	OSVDB:60395
XREF	CWE:200

Plugin Information:

Publication date: 2016/01/22, Modification date: 2016/08/01

Ports

tcp/80

```
Nessus was able to determine that the Apache Server listening on
port 80 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                 : ETag: "22c9b-fc-5050e9c759908"
  Inode number           : 142491
  File size              : 252 bytes
  File modification time : Oct. 10, 2014 at 09:59:56 GMT
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

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

Ports

tcp/80

```
The remote web server type is :

Apache/2.2.22 (Debian)

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/80

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

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:

Publication date: 2007/01/30, Modification date: 2017/11/13

Ports

tcp/80

```
Response Code : HTTP/1.1 200 OK

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

  Date: Fri, 08 Dec 2017 15:59:34 GMT
  Server: Apache/2.2.22 (Debian)
  Last-Modified: Fri, 10 Oct 2014 09:59:56 GMT
  ETag: "22c9b-fc-5050e9c759908"
  Accept-Ranges: bytes
  Content-Length: 252
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<html>
<body>

<h2>I-Spy IP Camera 0.9</h2>

<img src="/cgi-bin/video.cgi">

<p><a href="/cgi-bin/video.cgi">Plain image</a></p>
<p><a href="cgi-bin/video_full.cgi">Plain image (High resolution)</a></p>

<p>I-SPY FW Version 7.87B-55-R2.6B</p>

</body>
```

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

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

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

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

Ports

tcp/80

```
Give Nessus credentials to perform local checks.
```

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:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports

tcp/80

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

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
```

1072/udp

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/1072

```
Port 1072/udp was found to be open
```

10.0.100.234

Scan Information

Start time:	Fri Dec 8 16:41:31 2017
End time:	Fri Dec 8 16:45:35 2017

Host Information

DNS Name:	kali
IP:	10.0.100.234
MAC Address:	00:50:56:01:32:f5 00:50:56:01:32:fa 00:50:56:01:32:f4 00:50:56:01:32:f9 00:50:56:01:32:f6 00:50:56:01:32:f7 00:50:56:01:32:f8
OS:	Linux Kernel 4.12.0-kali1-amd64

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	40	41

Results Details

0/tcp

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:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```
Remote operating system : Linux Kernel 4.12.0-kali1-amd64
Confidence level : 99
Method : uname


The remote host is running Linux Kernel 4.12.0-kali1-amd64
```

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:

Publication date: 2004/02/11, Modification date: 2017/04/14

Ports

tcp/0

```
10.0.100.234 resolves as kali.
```

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:

Publication date: 2004/07/06, Modification date: 2017/11/17

Ports

tcp/0

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

The output of "uname -a" is :
Linux kali 4.12.0-kali1-amd64 #1 SMP Debian 4.12.6-1kali6 (2017-08-30) x86_64 GNU/Linux

Local security checks have NOT been enabled because the remote Linux
distribution is not supported.
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
```

```
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 10.0.100.234
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 : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2017/12/8 16:41 EET
Scan duration : 244 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

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

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:

Publication date: 2006/06/23, Modification date: 2017/05/30

Ports

tcp/0

```
Additional failure information from ssh_get_info2.nasl :
Debian version does not match known patterns
```

25202 - Enumerate IPv6 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv6 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Plugin Information:

Publication date: 2007/05/11, Modification date: 2017/01/26

Ports

tcp/0

```

The following IPv6 interfaces are set on the remote host :

 - fe80::250:56ff:fe01:32f4 (on interface eth0)
 - fe80::90f4:2d78:8dc6:1282 (on interface eth1)
 - fe80::6561:631c:86eb:a5e6 (on interface eth2)
 - fe80::ff46:ee3e:87a2:9753 (on interface eth3)
 - fe80::35d6:ae07:7359:e655 (on interface eth4)
 - fe80::6e4c:90ef:a2f2:a8ec (on interface eth5)
 - fe80::fcda:cc39:e730:eea4 (on interface eth6)
 - ::1 (on interface lo)
```

25203 - Enumerate IPv4 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information:

Publication date: 2007/05/11, Modification date: 2017/01/26

Ports

tcp/0

```

The following IPv4 addresses are set on the remote host :

 - 10.99.0.234 (on interface eth0)
 - 10.10.10.234 (on interface eth1)
 - 10.0.100.234 (on interface eth2)
 - 10.10.0.10 (on interface eth3)
 - 172.20.0.234 (on interface eth4)
 - 192.168.10.234 (on interface eth5)
 - 192.168.20.234 (on interface eth6)
 - 127.0.0.1 (on interface lo)
```

33276 - Enumerate MAC Addresses via SSH

Synopsis

Nessus was able to enumerate MAC addresses on the remote host.

Description

Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information:

Publication date: 2008/06/30, Modification date: 2017/01/26

Ports

tcp/0

```
The following MAC addresses exist on the remote host :

  - 00:50:56:01:32:f5 (interface eth1)
  - 00:50:56:01:32:fa (interface eth6)
  - 00:50:56:01:32:f4 (interface eth0)
  - 00:50:56:01:32:f9 (interface eth5)
  - 00:50:56:01:32:f6 (interface eth2)
  - 00:50:56:01:32:f7 (interface eth3)
  - 00:50:56:01:32:f8 (interface eth4)
```

34098 - BIOS version (SSH)

Synopsis

The BIOS version could be read.

Description

Using the SMBIOS (aka DMI) interface, it was possible to get the BIOS vendor and version.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2008/09/08, Modification date: 2017/08/28

Ports

tcp/0

```
Version      : 6.00
Vendor       : Phoenix Technologies LTD
Release Date : 09/17/2015
UUID         : 4204D3C5-5DF6-9C4C-5D0B-7A6E24E5AD02
```

35351 - System Information Enumeration (via DMI)

Synopsis

Information about the remote system's hardware can be read.

Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's hardware, such as its product name and serial number.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/01/12, Modification date: 2016/08/17

Ports

tcp/0

```
Chassis Information
  Serial Number : None
  Version       : N/A
```

```
    Manufacturer  : No Enclosure
    Lock          : Not Present
    Type          : Other

  System Information
    Serial Number : VMware-42 04 d3 c5 5d f6 9c 4c-5d 0b 7a 6e 24 e5 ad 02
    Version       : None
    Manufacturer  : VMware, Inc.
    Product Name  : VMware Virtual Platform
    Family        : Not Specified
```

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:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```
  The following card manufacturers were identified :

  00:50:56:01:32:f8 : VMware, Inc.
  00:50:56:01:32:f7 : VMware, Inc.
  00:50:56:01:32:f6 : VMware, Inc.
  00:50:56:01:32:f9 : VMware, Inc.
  00:50:56:01:32:f4 : VMware, Inc.
  00:50:56:01:32:fa : VMware, Inc.
  00:50:56:01:32:f5 : VMware, Inc.
```

45432 - Processor Information (via DMI)

Synopsis

Nessus was able to read information about the remote system's processor.

Description

Nessus was able to retrieve information about the remote system's hardware, such as its processor type, by using the SMBIOS (aka DMI) interface.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/06, Modification date: 2016/02/25

Ports

tcp/0

```
  Nessus detected 2 processors :
```

```
Current Speed   : 3000 MHz
Version         : Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz
Manufacturer    : GenuineIntel
External Clock  : Unknown
Status          : Populated, Enabled
Family          : Unknown
Type            : Central Processor

Current Speed   : 3000 MHz
Version         : Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz
Manufacturer    : GenuineIntel
External Clock  : Unknown
Status          : Populated, Enabled
Family          : Unknown
Type            : Central Processor
```

45433 - Memory Information (via DMI)

Synopsis

Information about the remote system's memory devices can be read.

Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's memory devices, such as the total amount of installed memory.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/06, Modification date: 2011/03/21

Ports

tcp/0

```
Total memory : 8192 MB
```

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:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

```
The remote operating system matched the following CPE :
  cpe:/o:linux:linux_kernel:4.12

Following application CPE matched on the remote system :

  cpe:/a:openbsd:openssh:7.5
```

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:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 99
```

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/06/30, Modification date: 2017/11/06

Ports

tcp/0

```

  Hostname : kali
    kali (hostname command)
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/10/12, Modification date: 2015/08/21

Ports

tcp/0

```
reboot   system boot  4.12.0-kali1-amd Wed Nov 22 21:45   still running
reboot   system boot  4.12.0-kali1-amd Mon Nov 20 14:15   still running
reboot   system boot  4.12.0-kali1-amd Mon Nov 20 13:27 - 14:15  (00:48)
reboot   system boot  4.12.0-kali1-amd Mon Nov 20 13:18 - 14:15  (00:57)

wtmp begins Mon Nov 20 13:18:34 2017
```

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:

Publication date: 2012/04/10, Modification date: 2015/06/02

Ports

tcp/0

```
Netstat output :
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8834            0.0.0.0:*               LISTEN
tcp        0      0 10.99.0.234:8834        77.74.137.114:32658     TIME_WAIT
tcp        0      0 10.99.0.234:8834        77.74.137.114:50512     TIME_WAIT
tcp        0      0 10.99.0.234:8834        77.74.137.114:8887      TIME_WAIT
tcp        0      0 10.0.100.234:45976      10.0.100.91:80          ESTABLISHED
tcp        0      0 10.0.100.234:39486      10.0.100.91:23          ESTABLISHED
tcp        0      0 10.99.0.234:8834        77.74.137.114:55829     TIME_WAIT
tcp        0      0 10.99.0.234:8834        77.74.137.114:51269     TIME_WAIT
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::8834                 :::*                    LISTEN
udp        0      0 10.0.100.234:36209      10.0.100.10:53          ESTABLISHED
udp        0      0 10.0.100.234:60803      10.0.100.50:137         ESTABLISHED
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 10.0.100.234:45424      10.0.100.20:161         ESTABLISHED
udp        0      0 10.0.100.234:41432      10.0.100.10:161         ESTABLISHED
udp        0      0 10.0.100.234:58311      10.0.100.1:161          ESTABLISHED
udp        0      0 10.0.100.234:58470      10.0.100.30:137         ESTABLISHED
raw6       0      0 :::58                   :::*                    7
raw6       0      0 :::58                   :::*                    7
raw6       0      0 :::58                   :::*                    7
raw6       0      0 :::58                   :::*                    7
raw6       0      0 :::58                   :::*                    7
raw6       0      0 :::58                   :::*          [...]
```

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:

Publication date: 2013/02/13, Modification date: 2016/08/05

Ports

tcp/0

```
tcp4 (listen)
  src: [host=0.0.0.0, port=22]
  dst: [host=0.0.0.0, port=*]

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

tcp4 (established)
  src: [host=10.99.0.234, port=8834]
  dst: [host=77.74.137.114, port=32658]

tcp4 (established)
  src: [host=10.99.0.234, port=8834]
  dst: [host=77.74.137.114, port=50512]

tcp4 (established)
  src: [host=10.99.0.234, port=8834]
  dst: [host=77.74.137.114, port=8887]

tcp4 (established)
  src: [host=10.0.100.234, port=45976]
  dst: [host=10.0.100.91, port=80]

tcp4 (established)
  src: [host=10.0.100.234, port=39486]
  dst: [host=10.0.100.91, port=23]

tcp4 (established)
  src: [host=10.99.0.234, port=8834]
  dst: [host=77.74.137.114, port=55829]

tcp4 (established)
  src: [host=10.99.0.234, port=8834]
  dst: [host=77.74.137.114, port=51269]

tcp6 (listen)
  src: [host=::, port=22]
  dst: [host=::, port=*]

tcp6 (listen)
  src: [host=::, port=8834]
  dst: [host=::, port=*]

udp4 (established)
  src: [host=10.0.100.234, port=36209]
  dst: [host=10.0.100.10, port=53]

udp4 (established)
  src: [host=10.0.100.234, port=60803]
  dst: [host=10.0.100.50, port=137]

udp4 (listen)
  src: [host=0.0.0.0, port=68]
  dst: [host=0.0.0.0, port=*]

udp4 (established)
  src: [host=10.0.100.234, port=45424]
  dst: [host=10.0.100.20, port=161]

udp4 (established)
  src: [host=10.0.100.234, port=41432]
  dst: [host=10.0.100.10, port=161]

udp4 (established)
  src: [host=10.0.100.234, port=58311]
  dst: [host=10.0.100.1, port=161]
```

```
udp4 (established)
  src: [host=10.0.100.234, port=58470]
  dst: [host=10.0.100.30, port=137]

udp6 (listen)
  src: [host=::, port=58]
  dst: [host=::, port=*]

udp6 (listen)
  src: [host=::, port=58]
  dst: [host=::, port=*]

udp6 (listen)
  src: [host=::, port=58]
  dst: [host=::, port=*]

udp6 (listen)
  src: [host=::, port=58]
  dst: [host=::, port=*]

udp6 (listen)
  src: [host=::, port=58]
  dst: [host=::, port=*]

udp6 (listen)
  src: [host=::, port=58]
  dst: [host=::, port=*]

udp6 (listen)
  src: [host=::, port=58]
  dst: [h [...]
```

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:

Publication date: 2017/05/30, Modification date: 2017/11/17

Ports

tcp/0

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

The output of "uname -a" is :
Linux kali 4.12.0-kali1-amd64 #1 SMP Debian 4.12.6-1kali6 (2017-08-30) x86_64 GNU/Linux

We are able to run commands on the remote host, but are unable to
currently identify it in this plugin.

Runtime : 0.14351 seconds
```

22/tcp

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2017/11/17

Ports

tcp/22

```

SSH version : SSH-2.0-OpenSSH_7.5p1 Debian-10
SSH supported authentication : publickey,password
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/03/06, Modification date: 2017/05/30

Ports

tcp/22

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

  - 1.99
  - 2.0
```

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.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/08/15, Modification date: 2017/08/25

Ports

tcp/22

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/22

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

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.
Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2017/08/28

Ports

tcp/22

```

  Process ID   : 7436
  Executable   : /usr/sbin/sshd
  Command line : /usr/sbin/sshd -D
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/28, Modification date: 2017/08/28

Ports

tcp/22

```

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256
  curve25519-sha256@libssh.org
```

```
    diffie-hellman-group-exchange-sha256
    diffie-hellman-group14-sha1
    diffie-hellman-group14-sha256
    diffie-hellman-group16-sha512
    diffie-hellman-group18-sha512
    ecdh-sha2-nistp256
    ecdh-sha2-nistp384
    ecdh-sha2-nistp521

  The server supports the following options for server_host_key_algorithms :

    ecdsa-sha2-nistp256
    rsa-sha2-256
    rsa-sha2-512
    ssh-ed25519
    ssh-rsa

  The server supports the following options for encryption_algorithms_client_to_server :

    aes128-ctr
    aes128-gcm@openssh.com
    aes192-ctr
    aes256-ctr
    aes256-gcm@openssh.com
    chacha20-poly1305@openssh.com

  The server supports the following options for encryption_algorithms_server_to_client :

    aes128-ctr
    aes128-gcm@openssh.com
    aes192-ctr
    aes256-ctr
    aes256-gcm@openssh.com
    chacha20-poly1305@openssh.com

  The server supports the following options for mac_algorithms_client_to_server :

    hmac-sha1
    hmac-sha1-etm@openssh.com
    hmac-sha2-256
    hmac-sha2-256-etm@openssh.com
    hmac-sha2-512
    hmac-sha2-512-etm@openssh.com
    umac-128-etm@openssh.com
    umac-128@openssh.com
    umac-64-etm@openssh.com
    umac-64@openssh.com

  The server supports the following options for mac_algorithms_server_to_client :

    hmac-sha1
    hmac-sha1-etm@openssh.com
    hmac-sha2-256
    hmac-sha2-256-etm@openssh.com
    hmac-sha2-512
    hmac-sha2-512-etm@openssh.com
    umac-128-etm@openssh.com
    umac-128@openssh.com
    umac-64-etm@openssh.com
    umac-64@openssh.com

  The server supports the following options for compression_algorithms_client_to_server :

    none
    zlib@openssh.com

  The server supports the following options for compression_algorithms_server_to_client :

    none
    zlib@openssh.com
```

68/udp

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.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/08/15, Modification date: 2017/08/25

Ports

udp/68

```
Port 68/udp was found to be open
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.
Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2017/08/28

Ports

udp/68

```
  Process ID   : 1784
  Executable   : /sbin/dhclient
  Command line : /sbin/dhclient -d -q -sf /usr/lib/NetworkManager/nm-dhcp-helper -pf /run/
dhclient-eth3.pid -lf /var/lib/NetworkManager/dhclient-cec9324d-e7a6-3273-9745-438b95233ba7-
eth3.lease -cf /var/lib/NetworkManager/dhclient-eth3.conf eth3
```

8834/tcp

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:

Publication date: 2010/12/15, Modification date: 2017/05/18

Ports

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=kali
|-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:

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

Ports

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:

Publication date: 1999/10/12, Modification date: 2016/02/25

Ports

tcp/8834

```
  URL               : https://kali:8834/
  Version           : 6.11.2
  Nessus UI Version : 6.11.2
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2015/12/30

Ports

tcp/8834

```
Subject Name:

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

Issuer Name:

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

Serial Number: 00 86 F1

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 20 11:55:46 2017 GMT
Not Valid After: Nov 19 11:55:46 2021 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C1 99 EE 33 5E C9 FB 8C 6B 29 DA FD 05 62 20 65 BC 82 FC
            39 2F CC 8D 4D 8A 23 70 6B 7A 74 F7 10 0D 4F 3D 0B 05 18 12
            02 81 1D 8F DC 49 00 99 FB 00 22 CE A7 9F 90 52 C8 5C 5F 3E
            D1 7E 5B 27 5A F6 6D 3E A7 81 D8 09 13 F6 5D 2D F6 F1 CC DC
            59 05 CF D0 22 FE BB 93 AD 60 CC B1 42 09 81 BB C8 F4 D4 3E
            EB 01 18 B4 F0 13 33 84 F0 04 23 FE D1 43 8F B8 5D 6F 73 BA
            0C 0C 9F 3D 68 32 30 4A CE DB 02 71 4F 48 C5 00 1D C8 8A 4D
            07 55 0D 67 B6 41 86 DD 16 73 98 07 C3 76 F9 B4 4D BA 76 90
            7C EB E8 5F 0E 28 DE 0D 39 B8 9B DE 86 27 3D 9C ED CF 79 58
            9A 65 BE 2D D2 E5 38 59 58 47 4C E4 02 74 E5 8C 3F FC D3 27
            92 4E 8C 1E 7B A4 7E A8 CB 24 5C 89 DB 55 11 B8 BF D1 0A 28
            C2 47 6E 6D 19 7E BB 87 F5 8A C7 88 01 AA 2E C4 D6 AA 54 BA
            62 57 E5 35 EB B1 87 EA DA 52 FF C1 F7 12 CE 02 01
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 5C 67 C2 00 AA 92 06 5D 95 4F D4 4A 88 77 E0 B3 95 64 34
           30 5A D3 29 C3 0A 09 EA EA 18 33 0C C8 DE C5 FE 96 BB 8F 00
           3E 38 04 FD 79 77 52 BE 9B 97 E5 45 62 AB BF F4 1D 28 69 71
           6D 72 55 D7 BA 57 6A 1A 06 A4 00 D2 D3 8A 53 97 5A DA FD 89
           0D AA 15 31 80 7D 1D 97 DB 10 CA 41 57 82 F4 AF 22 2F B2 20
           D6 09 AE 52 4F 04 EB DE 35 85 73 5A 3C A0 69 BA 12 25 22 FC
           93 7E 56 A0 7D F6  [...]
```

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.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/08/15, Modification date: 2017/08/25

Ports

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:

Publication date: 2006/06/05, Modification date: 2017/11/13

Ports

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:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

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:

Publication date: 2007/01/30, Modification date: 2017/11/13

Ports

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: 2d8f1cb96bb1d7fc42ef9974628f2a2f
  Content-Type: text/html
  Date: : Fri, 08 Dec 2017 14:42:18 GMT
  Connection: close
  Server: NessusWWW
  Content-Length: 575
  Expires: 0
  Pragma: 

Response Body :

<!doctype html>
<html lang="en">
    <head>
        <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <meta charset="utf-8" />
        <!--[if lt IE 11]>
            <script>
                window.location = '/unsupported6.html';
            </script>
        <![endif]-->
        <title>Nessus</title>
        <link rel="stylesheet" href="nessus6.css?v=1507563878131" />
        <script src="nessus6.js?v=1507563878132"></script>
    </head>
    <body>
    </body>
</html>
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.
Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2017/08/28

Ports

tcp/8834

```
  Process ID   : 7814
  Executable   : /opt/nessus/sbin/nessusd
  Command line : nessusd -q
```

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:

Publication date: 2011/12/01, Modification date: 2017/11/06

Ports

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:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

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:

Publication date: 2015/07/02, Modification date: 2015/07/02

Ports

tcp/8834

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

10.0.100.251

Scan Information

Start time:	Fri Dec 8 16:41:31 2017
End time:	Fri Dec 8 17:59:01 2017

Host Information

IP:	10.0.100.251
MAC Address:	00:50:56:01:32:c5
OS:	Linux Kernel 3.16 on Debian 8.0 (jessie)

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	19	19

Results Details

0/icmp

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:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is 2 seconds.
```

0/tcp

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:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```
Remote operating system : Linux Kernel 3.16 on Debian 8.0 (jessie)
Confidence level : 95
Method : SSH


The remote host is running Linux Kernel 3.16 on Debian 8.0 (jessie)
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 10.0.100.234
Port scanner(s) : nessus_udp_scanner nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
```

```
Scan Start Date : 2017/12/8 16:41 EET
Scan duration : 4647 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

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

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:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

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:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:01:32:c5 : VMware, 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:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

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

  cpe:/o:debian:debian_linux:8.0 -> Debian Linux 8.0 (Jessie)

Following application CPE matched on the remote system :

  cpe:/a:openbsd:openssh:6.7 -> OpenBSD OpenSSH 6.7
```

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:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 95
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2017/08/22

Ports

udp/0

```
For your information, here is the traceroute from 10.0.100.234 to 10.0.100.251 :
10.0.100.234
10.0.100.251

Hop Count: 1
```

22/tcp

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2017/11/17

Ports

tcp/22

```

SSH version : SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u1
SSH supported authentication : publickey,password
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/22

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

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/03/06, Modification date: 2017/05/30

Ports

tcp/22

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

  - 1.99
  - 2.0
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/22

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

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

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

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

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

Ports

tcp/22

```
Give Nessus credentials to perform local checks.
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/28, Modification date: 2017/08/28

Ports

tcp/22

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

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

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  ssh-dss
  ssh-ed25519
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
```

```
    hmac-sha2-256-etm@openssh.com
    hmac-sha2-512
    hmac-sha2-512-etm@openssh.com
    umac-128-etm@openssh.com
    umac-128@openssh.com
    umac-64-etm@openssh.com
    umac-64@openssh.com

  The server supports the following options for mac_algorithms_server_to_client :

    hmac-sha1
    hmac-sha1-etm@openssh.com
    hmac-sha2-256
    hmac-sha2-256-etm@openssh.com
    hmac-sha2-512
    hmac-sha2-512-etm@openssh.com
    umac-128-etm@openssh.com
    umac-128@openssh.com
    umac-64-etm@openssh.com
    umac-64@openssh.com

  The server supports the following options for compression_algorithms_client_to_server :

    none
    zlib@openssh.com

  The server supports the following options for compression_algorithms_server_to_client :

    none
    zlib@openssh.com
```

69/udp

11819 - TFTP Daemon Detection

Synopsis

A TFTP server is listening on the remote port.

Description

The remote host is running a TFTP (Trivial File Transfer Protocol) daemon. TFTP is often used by routers and diskless hosts to retrieve their configuration. It can also be used by worms to propagate.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information:

Publication date: 2003/08/13, Modification date: 2016/02/22

Ports

udp/69

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/69

```
Port 69/udp was found to be open
```

5353/udp

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/5353

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

66717 - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.
This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information:

Publication date: 2013/05/31, Modification date: 2013/05/31

Ports

udp/5353

```
Nessus was able to extract the following information :

  - mDNS hostname       : kalics3-2.local.

  - Advertised services :
    o Service name      : kalics3-2 [00:50:56:01:32:c5]._workstation._tcp.local.
      Port number       : 9
    o Service name      : kalics3-2._udisks-ssh._tcp.local.
      Port number       : 22

  - CPU type            : X86_64
  - OS                  : LINUX
```