Network Vulnerability Scan Report

September 23, 2014

Prepared for:

234 Marshall Street, Suite 14
Redwood City, CA 94063

T (650) 260-8638
E support@daric.com

http://www.daric.com/

Prepared by:

Nessus Enterprise Advisory Solutions
Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

Table Of Contents

Hosts Summary (Executive)

Scope:

The internal and external vulnerability scans are used as a tool to gather data to assess the effectiveness of current security control measures taken at the system level of Daric's network. The internal scan took place within the Daric Virtual Private Cloud (Daric VPC) vpc1pa23b network in the Amazon Web Services us-east-1b cloud server region. This network contains a web server linked to the domain www.daric.com at 54.209.69.129 (i-ad801846) and a database server supporting the core Daric web application, firewalled from HTTP access and access from outside the VPC at private IP address 10.0.0.158 (i-a0fc644b). The Nessus scanner was placed inside the Daric VPC. The purpose of the internal test was to bypass external security controls and counter measures to get a detailed look at system configurations. The external scan's purpose is to see the security posture through the eyes of the Internet user. The IP address chosen for the scanner was 54.167.204.1.

The Daric web server (i-ad801846) is open on ports 443 and 80 to 0.0.0.0/0, and closed off on other ports except 22 with login credentials and 3306 to the Daric database server (i-a0fc644b). The Daric database server is open only through 22 with administrative login credentials and 3306 to 54.209.69.129 (i-ad801846).

The vulnerability scan has three phases: network discovery, vulnerability assessment, and manual checks (optional). The first two phases require the use of scanning tools. The tool used to scan the VPC was Nessus Enterprise Scanner. The Network Discovery phase involved discovery of live hosts on the targeted network. The only two hosts provisioned on the network are the two hosts discussed in this report. The tool nmap was used to determine hosts on the network, and the output from phase one was inputted into phase two, where Nessus Enterprise Scanner was then used to scan these hosts for vulnerabilities, and vulnerabilities are identified below. Potential vulnerabilities identified in the internal scan are shown in blue as "info" vulnerabilities, while vulnerabilities identified in the external scan are assigned "low," "medium," "high" and "critical" risk ratings. Phase three was only conducted on the external scan to verify findings.

Findings:

The results from the internal scan and the external scan are listed below. No serious informational vulnerabilities were found, and all vulnerabilities identified in the external scan were assessed a "low" risk rating.

Duke Confidential – For Internal Use Only. Do Not Distribute

i-a0fc644b

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	2	23	25

Details

Severity	Plugin Id	Name
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10267	SSH Server Type and Version Information
Info	10881	SSH Protocol Versions Supported
Info	10884	Network Time Protocol (NTP) Server Detection
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	12634	Authenticated Check: OS Name and Installed Package Enumeration
Info	14272	netstat portscanner (SSH)
Info	19506	Nessus Scan Information
Info	22869	Software Enumeration (SSH)
Info	22964	Service Detection
Info	25202	Enumerate IPv6 Interfaces via SSH
Info	25203	Enumerate IPv4 Interfaces via SSH
Info	25221	Remote listeners enumeration (Linux / AIX)
Info	33276	Enumerate MAC Addresses via SSH
Info	39520	Backported Security Patch Detection (SSH)
Info	45590	Common Platform Enumeration (CPE)
Info	46215	Inconsistent Hostname and IP Address
Info	54615	Device Type
Info	55472	Device Hostname
Info	56468	Time of Last System Startup
Info	58651	Netstat Active Connections
Info	64582	Netstat Connection Information
Info	70657	SSH Algorithms and Languages Supported

Bank Confidential – For Internal Use Only. Do Not Distribute

i-ad801846

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	23	24

Details

Severity	Plugin Id	Name
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	39521	Backported Security Patch Detection (WWW)
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	46215	Inconsistent Hostname and IP Address
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

Duke Confidential - For Internal Use Only. Do Not Distribute

Vulnerabilities By Host

Date Confidential - For Internal Use Only. Do Not Distribute

i-a0fc644b

Scan Information

Start time:	Tue Sep 23 03:10:55 2014
End time:	Tue Sep 23 03:11:16 2014

Host Information

DNS Name:	i-a0fc644b
IP:	10.150.73.77
MAC Address:	22:00:0B:0E:A1:66
OS:	Linux Kernel 3.10.35-43.137.amzn1.x86_64 on Amazon Linux AMI on Amazon Linux AMI 2014.03

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	2	27	29

Results Details

0/tcp

64582 - Netstat Connection Information

Synopsis

Nessus is 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: 2013/06/18

Ports

tcp/0

```
tcp4 (listen)
  src: [host=127.0.0.1, port=8834]
  dst: [host=0.0.0.0, port=*]

tcp4 (listen)
  src: [host=0.0.0.0, port=22]
  dst: [host=0.0.0.0, port=*]

tcp4 (listen)
  src: [host=127.0.0.1, port=25]
  dst: [host=0.0.0.0, port=*]

tcp6 (listen)
  src: [host=::, port=22]
  dst: [host=::, port=*]

udp4 (listen)
  src: [host=0.0.0.0, port=68]
  dst: [host=0.0.0.0, port=*]

udp4 (listen)
  src: [host=10.150.73.77, port=123]
  dst: [host=0.0.0.0, port=*]
```

Data Confidential - For Internal Use Only. Do Not Distribute

```
udp4 (listen)
  src: [host=127.0.0.1, port=123]
  dst: [host=0.0.0.0, port=*]

udp4 (listen)
  src: [host=0.0.0.0, port=123]
  dst: [host=0.0.0.0, port=*]
```

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: 2012/04/10

Ports

tcp/0

```
Netstat output :
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 127.0.0.1:8834              0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
udp        0      0 0.0.0.0:68                  0.0.0.0:*
udp        0      0 10.150.73.77:123            0.0.0.0:*
udp        0      0 127.0.0.1:123               0.0.0.0:*
udp        0      0 0.0.0.0:123                 0.0.0.0:*
```

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 FQDN of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/02/11, Modification date: 2012/09/28

Ports

tcp/0

```
10.150.73.77 resolves as i-a0fc644b.
```

46215 - Inconsistent Hostname and IP Address

Synopsis

The remote host's hostname is not consistent with DNS information.

Description

Data Confidential - For Internal Use Only. Do Not Distribute

The name of this machine either does not resolve or resolves to a different IP address.
This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host.
As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

Solution

Fix the reverse DNS or host file.

Risk Factor

None

Plugin Information:

Publication date: 2010/05/03, Modification date: 2011/10/06

Ports

tcp/0

```
The host name 'i-a0fc644b' does not resolve to an IP address
```

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: 2014/09/19

Ports

tcp/0

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

The output of "uname -a" is :
Linux ip-10-150-73-77 3.10.35-43.137.amzn1.x86_64 #1 SMP Wed Apr 2 09:36:59 UTC 2014 x86_64 x86_64
 x86_64 GNU/Linux

The remote Amazon Linux AMI system is :
Amazon Linux AMI release 2014.03

Local security checks have been enabled for this host.
```

25203 - Enumerate IPv4 Interfaces via SSH

Synopsis

This plugin enumerates IPv4 interfaces on a remote host.

Description

By connecting to the remote host via SSH with the supplied credentials, this plugin enumerates network interfaces configured with IPv4 addresses.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information:

Duke Confidential - For Internal Use Only. Do Not Distribute

Publication date: 2007/05/11, Modification date: 2011/03/21

Ports
tcp/0

```
The following IPv4 addresses are set on the remote host :

 - 10.150.73.77 (on interface eth0)
 - 127.0.0.1 (on interface lo)
```

22869 - Software Enumeration (SSH)

Synopsis

It is possible to enumerate installed software on the remote host, via SSH.

Description

This plugin lists the software installed on the remote host by calling the appropriate command (rpm -qa on RPM-based Linux distributions, qpkg, dpkg, etc...)

Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2006/10/15, Modification date: 2014/07/28

Ports
tcp/0

```
Here is the list of packages installed on the remote Amazon Linux AMI system :

  Nessus-5.2.6-es6|(none)
  PyYAML-3.10-3.6.amzn1|(none)
  acl-2.2.49-6.9.amzn1|(none)
  acpid-1.0.10-2.1.6.amzn1|(none)
  alsa-lib-1.0.22-3.9.amzn1|(none)
  at-3.1.10-43.8.amzn1|(none)
  attr-2.4.44-7.9.amzn1|(none)
  audit-2.3.2-3.19.amzn1|(none)
  audit-libs-2.3.2-3.19.amzn1|(none)
  authconfig-6.1.12-13.17.amzn1|(none)
  aws-amitools-ec2-1.5.2-0.0.amzn1|(none)
  aws-apitools-as-1.0.61.4-1.0.amzn1|(none)
  aws-apitools-common-1.1.0-1.8.amzn1|(none)
  aws-apitools-ec2-1.6.13.0-1.1.amzn1|(none)
  aws-apitools-elb-1.0.34.0-1.0.amzn1|(none)
  aws-apitools-iam-1.5.0-1.2.amzn1|(none)
  aws-apitools-mon-1.0.20.0-1.0.amzn1|(none)
  aws-apitools-rds-1.15.001-1.0.amzn1|(none)
  aws-cfn-bootstrap-1.3-17.amzn1|(none)
  aws-cli-1.3.6-1.0.amzn1|(none)
  basesystem-10.0-4.9.amzn1|(none)
  bash-4.1.2-15.17.amzn1|(none)
  bc-1.06.95-1.10.amzn1|(none)
  bind-libs-9.8.2-0.23.rc1.32.amzn1|32
  bind-utils-9.8.2-0.23.rc1.32.amzn1|32
  bzip2-1.0.6-8.12.amzn1|(none)
  bzip2-libs-1.0.6-8.12.amzn1|(none)
  ca-certificates-2013.1.94-65.0.9.amzn1|(none)
  chkconfig-1.3.49.3-2.10.amzn1|(none)
  cloud-disk-utils-0.27-1.3.amzn1|(none)
  cloud-init-0.7.2-7.20.amzn1|(none)
  coreutils-8.21-13.31.amzn1|(none)
  cpio-2.10-11.11.amzn1|(none) cracklib-
  2.8.16-4.11.amzn1|(none) cracklib-
  dicts-2.8.16-4.11.amzn1|(none) cronie-
  1.4.4-12.6.amzn1|(none)
  cronie-anacron-1.4.4-12.6.amzn1|(none)
  crontabs-1.10-33.9.amzn1|(none)
  cryptsetup-1.6.2-2.11.amzn1|(none)
```

Duke Confidential - For Internal Use Only. Do Not Distribute

```
cryptsetup-libs-1.6.2-2.11.amzn1|(none)
curl-7.36.0-2.44.amzn1|(none)
cyrus-sasl-2.1.23-13.13.amzn1|(none)
cyrus-sasl-lib-2.1.23-13.13.amzn1|(none)
cyrus-sasl-plain-2.1.23-13.13.amzn1|(none)
dash-0.5.5.1-4.5.amzn1|(none)
db4-4.7.25-18.11.amzn1|(none)
db4-utils-4.7.25-18.11.amzn1|(none)
dbus-1.6.12-5.25.amzn1|1
dbus-libs-1.6.12-5.25.amzn1|1
dejavu-fonts-common-2.33-5.8.amzn1|(none)
dejavu-sans-fonts-2.33-5.8.amzn1|(none)
dejavu-serif-fonts-2.33-5.8.amzn1|(none)
device-mapper-1.02.79- [...]
```

33276 - Enumerate MAC Addresses via SSH

Synopsis

This plugin enumerates MAC addresses on a remote host.

Description

By connecting to the remote host via SSH with the supplied credentials, this plugin enumerates MAC addresses.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information:

Publication date: 2008/06/30, Modification date: 2012/03/27

Ports

tcp/0

```
The following MAC address exists on the remote host :

  - 22:00:0B:0E:A1:66 (interface eth0)
```

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: 2014/07/25

Ports

tcp/0

```
reboot   system boot  3.10.35-43.137.a Tue Sep 23 00:54 - 03:11  (02:16)
reboot   system boot  3.10.35-43.137.a Tue Sep 23 00:19 - 00:52  (00:32)
reboot   system boot  3.10.35-43.137.a Tue Sep 23 00:06 - 00:15  (00:09)
reboot   system boot  3.10.35-43.137.a Wed May 28 20:01 - 13:52  (17:51)

wtmp begins Wed May 28 20:01:15 2014
```

25202 - Enumerate IPv6 Interfaces via SSH

Synopsis

This plugin enumerates IPv6 interfaces on a remote host.

Description

Data Confidential - For Internal Use Only. Do Not Distribute

By connecting to the remote host via SSH with the supplied credentials, this plugin enumerates network interfaces configured with IPv6 addresses.

Solution

Disable IPv6 if you do not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Plugin Information:

Publication date: 2007/05/11, Modification date: 2011/03/21

Ports

tcp/0

```
The following IPv6 interfaces are set on the remote host :

 - fe80::2000:bff:fe0e:a166 (on interface eth0)
 - ::1 (on interface lo)
```

55472 - Device Hostname

Synopsis

It is 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: 2014/01/07

Ports

tcp/0

```
  Hostname : ip-10-150-73-77
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2014/02/19

Ports

tcp/0

```
Remote operating system : Linux Kernel 3.10.35-43.137.amzn1.x86_64 on Amazon Linux AMI on Amazon
 Linux AMI 2014.03
Confidence Level : 100
Method : LinuxDistribution
```

Data Confidential - For Internal Use Only. Do Not Distribute

```
The remote host is running Linux Kernel 3.10.35-43.137.amzn1.x86_64 on Amazon Linux AMI on Amazon
 Linux AMI 2014.03
```

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 : 100
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It is 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/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2014/09/19

Ports

tcp/0

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

  cpe:/o:linux:linux_kernel:3.10.35.43

Following application CPE matched on the remote system :

  cpe:/a:openbsd:openssh:6.2 -> OpenBSD OpenSSH 6.2
```

19506 - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script 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

Duke Confidential - For Internal Use Only. Do Not Distribute

- 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: 2014/07/29

Ports

tcp/0

```
Information about this scan :

Nessus version : 5.2.7
Plugin feed version : 201409221716
Scanner edition used : Nessus
Scan policy used : Basic Scan
Scanner IP : 10.150.73.77
Port scanner(s) : netstat
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes (on the localhost)
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2014/9/23 3:10 UTC
Scan duration : 21 sec
```

22/tcp

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

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

Duke Confidential - For Internal Use Only. Do Not Distribute

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: 2014/01/28

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

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

Description

The 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 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: 2014/07/08

Ports

tcp/22

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

Data Confidential - For Internal Use Only. Do Not Distribute

```
  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com

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

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
```

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/08/15, Modification date: 2014/05/23

Ports

tcp/22

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

22964 - Service Detection

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 an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2014/07/24

Ports

tcp/22

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

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

Duke Confidential - For Internal Use Only. Do Not Distribute

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/10/24

Ports

tcp/22

```
SSH version : SSH-2.0-OpenSSH_6.2
SSH supported authentication : publickey
```

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: 2014/04/04

Ports

tcp/22

```
Nessus negotiated the following encryption algorithm with the server : aes128-cbc

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
  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-rsa

The server supports the following options for encryption_algorithms_client_to_server :

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

Duke Confidential - For Internal Use Only. Do Not Distribute

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

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  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-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-ripemd160
  hmac-ripemd160-etm@openssh.com
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
  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-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-ripemd160
  hmac-ripemd160-etm@openssh.com
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512- [...]
```

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: 2013/10/21

Duke Confidential - For Internal Use Only. Do Not Distribute

Ports
tcp/22

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

  - 1.99
  - 2.0


SSHv2 host key fingerprint : 1a:0f:a7:68:d7:b7:7a:bb:59:10:18:b2:dc:c5:99:f2
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it is possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, it is possible to obtain the name of the process listening on the remote port.
Note that this 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: 2014/06/04

Ports
tcp/22

```
Process id   : 1248
Executable   : /usr/sbin/sshd
Command line : /usr/sbin/sshd
```

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

http://www.nessus.org/u?d636c8c7

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2013/04/03

Ports
tcp/22

```
Local checks have been enabled.
```

68/udp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Data Confidential - For Internal Use Only. Do Not Distribute

Description

This plugin runs 'netstat' on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/08/15, Modification date: 2014/05/23

Ports

udp/68

```
Port 68/udp was found to be open
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it is possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, it is possible to obtain the name of the process listening on the remote port.
Note that this 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: 2014/06/04

Ports

udp/68

```
  Process id   : 1071
  Executable   : /sbin/dhclient
  Command line : /sbin/dhclient -q -lf /var/lib/dhclient/dhclient-eth0.leases -pf /var/run/
dhclient-eth0.pid eth0
```

123/udp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/08/15, Modification date: 2014/05/23

Ports

udp/123

```
Port 123/udp was found to be open
```

10884 - Network Time Protocol (NTP) Server Detection

Data Confidential - For Internal Use Only. Do Not Distribute

Synopsis

An NTP server is listening on the remote host.

Description

An NTP (Network Time Protocol) server is listening on this port. It provides information about the current date and time of the remote system and may provide system information.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/03/13, Modification date: 2011/03/11

Ports

udp/123

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it is possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, it is possible to obtain the name of the process listening on the remote port.
Note that this 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: 2014/06/04

Ports

udp/123

```
Process id   : 1266
Executable   : /usr/sbin/ntpd
Command line : ntpd -u ntp:ntp -p /var/run/ntpd.pid -g
```

Duke Confidential - For Internal Use Only. Do Not Distribute

i-ad801846

Scan Information

Start time:	Tue Sep 23 03:10:55 2014
End time:	Tue Sep 23 03:16:57 2014

Host Information

DNS Name:	i-ad801846
IP:	10.146.251.12
OS:	Linux Kernel 3.0 on Ubuntu 12.04 (precise), Linux Kernel 3.5 on Ubuntu 12.10 (quantal), Linux Kernel 3.8 on Ubuntu 13.04 (raring)

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	24	25

Results Details

0/tcp

46215 - Inconsistent Hostname and IP Address

Synopsis

The remote host's hostname is not consistent with DNS information.

Description

The name of this machine either does not resolve or resolves to a different IP address.
This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host.
As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

Solution

Fix the reverse DNS or host file.

Risk Factor

None

Plugin Information:

Publication date: 2010/05/03, Modification date: 2011/10/06

Ports

tcp/0

```
The host name 'i-ad801846' does not resolve to an IP address
```

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:

Duke Confidential - For Internal Use Only. Do Not Distribute

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

Ports
tcp/0

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 FQDN of the remote host.

Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2004/02/11, Modification date: 2012/09/28

Ports
tcp/0

```
10.146.251.12 resolves as i-ad801846.
```

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
This plugin extracts the banner of the Apache web server, and attempts to 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.

Risk Factor
None

Plugin Information:
Publication date: 2005/05/15, Modification date: 2014/07/29

Ports
tcp/0

```
The Linux distribution detected was :
 - Ubuntu 12.04 (precise)
 - Ubuntu 12.10 (quantal)
 - Ubuntu 13.04 (raring)
```

11936 - OS Identification

Synopsis
It is possible to guess the remote operating system.

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

Solution
n/a

Risk Factor
None

Plugin Information:

Duke Confidential - For Internal Use Only. Do Not Distribute

Publication date: 2003/12/09, Modification date: 2014/02/19

Ports
tcp/0

```
Remote operating system : Linux Kernel 3.0 on Ubuntu 12.04 (precise)
Linux Kernel 3.5 on Ubuntu 12.10 (quantal)
Linux Kernel 3.8 on Ubuntu 13.04 (raring)
Confidence Level : 85
Method : HTTP


The remote host is running one of these operating systems :
Linux Kernel 3.0 on Ubuntu 12.04 (precise)
Linux Kernel 3.5 on Ubuntu 12.10 (quantal)
Linux Kernel 3.8 on Ubuntu 13.04 (raring)
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It is 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/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2014/09/19

Ports
tcp/0

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

  cpe:/o:canonical:ubuntu_linux:12.04
  cpe:/o:canonical:ubuntu_linux:12.10 -> Canonical Ubuntu Linux 12.10
  cpe:/o:canonical:ubuntu_linux:13.04 -> Canonical Ubuntu Linux 13.04

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:

Data Confidential - For Internal Use Only. Do Not Distribute

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

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 85
```

19506 - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script 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: 2014/07/29

Ports

tcp/0

```
Information about this scan :

Nessus version : 5.2.7
Plugin feed version : 201409221716
Scanner edition used : Nessus
Scan policy used : Basic Scan
Scanner IP : 10.150.73.77
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2014/9/23 3:10 UTC
Scan duration : 362 sec
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Duke Confidential - For Internal Use Only. Do Not Distribute

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports

udp/0

```
For your information, here is the traceroute from 10.150.73.77 to 10.146.251.12 :
10.150.73.77
?
10.146.251.12
```

443/tcp

65821 - SSL RC4 Cipher Suites Supported

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/

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

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

References

BID	58796
CVE	CVE-2013-2566
XREF	OSVDB:91162

Plugin Information:

Publication date: 2013/04/05, Modification date: 2014/02/27

Ports

tcp/443

```
Here is the list of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)
```

Duke Confidential - For Internal Use Only. Do Not Distribute

```
    TLSv1
      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}
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/443

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

22964 - Service Detection

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 an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2014/07/24

Ports

tcp/443

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

tcp/443

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

22964 - Service Detection

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 an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2014/07/24

Ports

tcp/443

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

tcp/443

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

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: 2014/08/01

Ports

tcp/443

```
The remote web server type is :

Apache/2.2.22 (Ubuntu)

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

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: 2011/05/31

Ports

tcp/443

```
Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :
```

Data Confidential - For Internal Use Only. Do Not Distribute

```
Date: Tue, 23 Sep 2014 03:15:25 GMT
Server: Apache/2.2.22 (Ubuntu)
Vary: Cookie,Accept-Encoding
Content-Type: text/html; charset=utf-8
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This script 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: 2014/04/14

Ports

tcp/443

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

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

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

http://tools.ietf.org/html/rfc3749

Duke Confidential - For Internal Use Only. Do Not Distribute

http://tools.ietf.org/html/rfc3943

http://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2013/10/18

Ports

tcp/443

```
Nessus was able to confirm that the following compression method is
supported by the target :

  NULL (0x00)
```

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: 2012/04/02

Ports

tcp/443

```
Subject Name:

Organization Unit: Domain Control Validated
Common Name: www.patientadvance.com

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: GoDaddy.com, Inc.
Organization Unit: http://certs.godaddy.com/repository/
Common Name: Go Daddy Secure Certificate Authority - G2

Serial Number: 2B 37 6E 24 BD E3 88

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 11 08:57:02 2014 GMT
Not Valid After: Feb 11 08:57:02 2017 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 D9 6A EB 08 B2 85 2E C4 DA 28 FC 05 3A 2B C6 7D 5C 68 D1
            91 DF 92 9F A3 94 34 F2 E3 B7 02 C0 68 8C D4 32 40 02 A8 3B
            F0 79 1D 75 E7 B5 B3 7F 33 AE 56 3C B6 86 C0 28 12 5A F0 46
```

Data Confidential - For Internal Use Only. Do Not Distribute

```
            3B BE 14 53 79 35 82 59 36 54 42 13 42 3D EB 8A 20 11 2A 84
            54 D3 1B D0 42 BC 45 6C 85 CE 82 8B D0 1C CA FB 1C 76 FC A1
            94 3D 9F F2 27 CB 33 8B D2 4B E9 70 59 0B 12 A1 59 C6 06 10
            67 BF B7 EF 7A B2 2E 20 A5 53 32 65 E1 30 19 0B CE CE EA 86
            CA 3E C8 29 87 35 35 B5 7B 3D F8 EB 9A 2E 06 B1 39 AC C6 DC
            FC E9 59 B9 C5 1A B9 5D E1 15 61 4E 81 38 67 E3 B7 18 88 81
            08 3F 40 64 3E 88 46 45 A6 54 C6 04 83 AE 83 19 B2 E9 1E 20
            7C 30 CB C6 A2 C8 E8 47 0F 98 A9 A5 45 02 BA 54 CA CC 02 04
            49 2C DE 40 0D 4F FC 5D AA 1F 21 B7 DE CE 02 B2 C3 9F 94 4E
            D8 E8 83 DA 58 B1 91 2A E9 90 AF 46 F9 73 0D E0 95
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 47 5A F1 A5 B4 86 D2 B7 F5 39 E7 A9 DD DA 98 21 D0 E5 C5
           16 9B D8 DD 2A 73 5E ED 92 76 4B 8C 20 15 61 48 E1 AE 73 21
           33 04 69 47 D0 E1 F6 9C 4D E0 E0 11 89 AA FB CF 4F C5 6F F2
           B9 B7 01 78 C2 5A A2 6E 55 C2 72 28 F8 13 BA FF DE 1B 69 3C
           5A 68 E9 B4 94 08 06 FE 1B 96 E1 E7 91 56 88 00 70 E3 4E 6E
           D6 E7 65 97 74 DD 52 AA 74 E4 AA 94 A0 35 67 FC E5 39 B9 2B
           51 34 6B FE CC 16 9E E2 E8 77 D5 34 41 [...]
```

45410 - SSL Certificate commonName Mismatch

Synopsis

The SSL certificate commonName does not match the host name.

Description

This service presents an SSL certificate for which the 'commonName' (CN) does not match the host name on which the service listens.

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2010/04/03, Modification date: 2012/09/30

Ports

tcp/443

```
The host name known by Nessus is :

  i-ad801846

The Common Name in the certificate is :

  www.patientadvance.com

The Subject Alternate Names in the certificate are :

  patientadvance.com
  www.patientadvance.com
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

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

Solution

n/a

Risk Factor

Data Confidential - For Internal Use Only. Do Not Distribute

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2014/07/08

Ports

tcp/443

```
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)
     EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
     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
     DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        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-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1
     SEED-SHA                     Kx=RSA         Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1
     DHE-RSA-AES128-SHA256        Kx=DHE         Au=RSA      Enc=AES128-CBC           Mac=SHA256

     DHE-RSA-AES256-SHA256        Kx=DHE         Au=RSA      Enc=AES256-CBC           Mac=SHA256

     RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES128-CBC           Mac=SHA256

     RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES256-CBC           Mac=SHA256
     DHE-RSA-AES128-SHA256        Kx=DHE         Au=RSA      Enc=AES-GCM(128)         Mac=SHA256

     DHE-RSA-AES256-SHA384        Kx=DHE         Au=RSA      Enc=AES-GCM(256)         Mac=SHA3
 [...]
```

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Ports

tcp/443

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

  High Strength Ciphers (>= 112-bit key)
```

Data Confidential - For Internal Use Only. Do Not Distribute

```
  TLSv1
    EDH-RSA-DES-CBC3-SHA          Kx=DH          Au=RSA      Enc=3DES-CBC(168)         Mac=SHA1
    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
    DHE-RSA-AES128-SHA256         Kx=DHE         Au=RSA      Enc=AES128-CBC            Mac=SHA256

    DHE-RSA-AES256-SHA256         Kx=DHE         Au=RSA      Enc=AES256-CBC            Mac=SHA256


  TLSv12
    DHE-RSA-AES128-SHA256         Kx= HE         Au=RSA      Enc=AES-GCM(128)          Mac=SHA256

    DHE-RSA-AES256-SHA384         Kx= HE         Au=RSA      Enc=AES-GCM(256)          Mac=SHA384


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/443

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

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      EDH-RSA-DES-CBC3-SHA        Kx=DH          Au=RSA      Enc=3DES-CBC(168)         Mac=SHA1
      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
      DES-CBC3-SHA                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)         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
```

Dark Confidential - For Internal Use Only. Do Not Distribute

```
  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
  DHE-RSA-AES128-SHA256        Kx=DHE      Au=RSA      Enc=AES128-CBC           Mac=SHA256

  DHE-RSA-AES256-SHA256        Kx=DHE      Au=RSA      Enc=AES256-CBC           Mac=SHA256

  RSA-AES128-SHA256            Kx=RSA      Au=RSA      Enc=AES128-CBC           Mac=SHA256

  RSA-AES256-SHA256            Kx=RSA      Au=RSA      Enc=AES256-CBC           Mac=SHA256


The fields above are :

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

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.
```

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

http://www.nessus.org/u?d636c8c7

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2013/10/02

Ports

tcp/443

Duke Confidential - For Internal Use Only. Do Not Distribute

Give Nessus credentials to perform local checks.

Duke Confidential - For Internal Use Only. Do Not Distribute

Vulnerabilities By Plugin

Bank Confidential - For Internal Use Only. Do Not Distribute

65821 (1) - SSL RC4 Cipher Suites Supported

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/

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

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

References

BID	58796
CVE	CVE-2013-2566
XREF	OSVDB:91162

Plugin Information:

Publication date: 2013/04/05, Modification date: 2014/02/27

Hosts

i-ad801846 (tcp/443)

```
Here is the list of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      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}
```

Duke Confidential - For Internal Use Only. Do Not Distribute

70658 (1) - 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

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

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: 2014/01/28

Hosts

i-a0fc644b (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
```

Duke Confidential - For Internal Use Only. Do Not Distribute

71049 (1) - SSH Weak MAC Algorithms Enabled

Synopsis

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

Description

The 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 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: 2014/07/08

Hosts

i-a0fc644b (tcp/22)

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

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com

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

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
```

Duke Confidential - For Internal Use Only. Do Not Distribute

14272 (3) - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/08/15, Modification date: 2014/05/23

Hosts

i-a0fc644b (tcp/22)

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

i-a0fc644b (udp/68)

```
Port 68/udp was found to be open
```

i-a0fc644b (udp/123)

```
Port 123/udp was found to be open
```

Data Confidential - For Internal Use Only. Do Not Distribute

22964 (3) - Service Detection

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 an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2014/07/24

Hosts

i-a0fc644b (tcp/22)

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

i-ad801846 (tcp/443)

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

i-ad801846 (tcp/443)

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

Duke Confidential - For Internal Use Only. Do Not Distribute

25221 (3) - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it is possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, it is possible to obtain the name of the process listening on the remote port.
Note that this 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: 2014/06/04

Hosts

i-a0fc644b (tcp/22)

```
  Process id   : 1248
  Executable   : /usr/sbin/sshd
  Command line : /usr/sbin/sshd
```

i-a0fc644b (udp/68)

```
  Process id   : 1071
  Executable   : /sbin/dhclient
  Command line : /sbin/dhclient -q -lf /var/lib/dhclient/dhclient-eth0.leases -pf /var/run/
dhclient-eth0.pid eth0
```

i-a0fc644b (udp/123)

```
  Process id   : 1266
  Executable   : /usr/sbin/ntpd
  Command line : ntpd -u ntp:ntp -p /var/run/ntpd.pid -g
```

Data Confidential - For Internal Use Only. Do Not Distribute

11936 (2) - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2014/02/19

Hosts

i-a0fc644b (tcp/0)

```
Remote operating system : Linux Kernel 3.10.35-43.137.amzn1.x86_64 on Amazon Linux AMI on Amazon
 Linux AMI 2014.03
Confidence Level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 3.10.35-43.137.amzn1.x86_64 on Amazon Linux AMI on Amazon
 Linux AMI 2014.03
```

i-ad801846 (tcp/0)

```
Remote operating system : Linux Kernel 3.0 on Ubuntu 12.04 (precise)
Linux Kernel 3.5 on Ubuntu 12.10 (quantal)
Linux Kernel 3.8 on Ubuntu 13.04 (raring)
Confidence Level : 85
Method : HTTP


The remote host is running one of these operating systems :
Linux Kernel 3.0 on Ubuntu 12.04 (precise)
Linux Kernel 3.5 on Ubuntu 12.10 (quantal)
Linux Kernel 3.8 on Ubuntu 13.04 (raring)
```

Duke Confidential - For Internal Use Only. Do Not Distribute

12053 (2) - 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 FQDN of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/02/11, Modification date: 2012/09/28

Hosts

i-a0fc644b (tcp/0)

```
10.150.73.77 resolves as i-a0fc644b.
```

i-ad801846 (tcp/0)

```
10.146.251.12 resolves as i-ad801846.
```

Duke Confidential - For Internal Use Only. Do Not Distribute

19506 (2) - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script 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: 2014/07/29

Hosts

i-a0fc644b (tcp/0)

```
Information about this scan :

Nessus version : 5.2.7
Plugin feed version : 201409221716
Scanner edition used : Nessus
Scan policy used : Basic Scan
Scanner IP : 10.150.73.77
Port scanner(s) : netstat
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes (on the localhost)
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2014/9/23 3:10 UTC
Scan duration : 21 sec
```

i-ad801846 (tcp/0)

```
Information about this scan :

Nessus version : 5.2.7
Plugin feed version : 201409221716
Scanner edition used : Nessus
Scan policy used : Basic Scan
Scanner IP : 10.150.73.77
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
```

Duke Confidential - For Internal Use Only. Do Not Distribute

```
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 : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2014/9/23 3:10 UTC
Scan duration : 362 sec
```

Duke Confidential - For Internal Use Only. Do Not Distribute

45590 (2) - Common Platform Enumeration (CPE)

Synopsis

It is 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/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2014/09/19

Hosts

i-a0fc644b (tcp/0)

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

  cpe:/o:linux:linux_kernel:3.10.35.43

Following application CPE matched on the remote system :

  cpe:/a:openbsd:openssh:6.2 -> OpenBSD OpenSSH 6.2
```

i-ad801846 (tcp/0)

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

  cpe:/o:canonical:ubuntu_linux:12.04
  cpe:/o:canonical:ubuntu_linux:12.10 -> Canonical Ubuntu Linux 12.10
  cpe:/o:canonical:ubuntu_linux:13.04 -> Canonical Ubuntu Linux 13.04

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
```

Data Confidential - For Internal Use Only. Do Not Distribute

46215 (2) - Inconsistent Hostname and IP Address

Synopsis

The remote host's hostname is not consistent with DNS information.

Description

The name of this machine either does not resolve or resolves to a different IP address.
This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host.
As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

Solution

Fix the reverse DNS or host file.

Risk Factor

None

Plugin Information:

Publication date: 2010/05/03, Modification date: 2011/10/06

Hosts

i-a0fc644b (tcp/0)

```
The host name 'i-a0fc644b' does not resolve to an IP address
```

i-ad801846 (tcp/0)

```
The host name 'i-ad801846' does not resolve to an IP address
```

54615 (2) - 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

Hosts

i-a0fc644b (tcp/0)

```
Remote device type : general-purpose
Confidence level : 100
```

i-ad801846 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 85
```

10107 (1) - 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: 2014/08/01

Hosts

i-ad801846 (tcp/443)

```
The remote web server type is :

Apache/2.2.22 (Ubuntu)

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

10267 (1) - 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: 2011/10/24

Hosts

i-a0fc644b (tcp/22)

```
SSH version : SSH-2.0-OpenSSH_6.2
SSH supported authentication : publickey
```

10287 (1) - 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: 2013/04/11

Hosts

i-ad801846 (udp/0)

```
For your information, here is the traceroute from 10.150.73.77 to 10.146.251.12 :
10.150.73.77
?
10.146.251.12
```

10863 (1) - 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: 2012/04/02

Hosts

i-ad801846 (tcp/443)

```
Subject Name:

Organization Unit: Domain Control Validated
Common Name: www.patientadvance.com

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: GoDaddy.com, Inc.
Organization Unit: http://certs.godaddy.com/repository/
Common Name: Go Daddy Secure Certificate Authority - G2

Serial Number: 2B 37 6E 24 BD E3 88

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 11 08:57:02 2014 GMT
Not Valid After: Feb 11 08:57:02 2017 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 D9 6A EB 08 B2 85 2E C4 DA 28 FC 05 3A 2B C6 7D 5C 68 D1
            91 DF 92 9F A3 94 34 F2 E3 B7 02 C0 68 8C D4 32 40 02 A8 3B
            F0 79 1D 75 E7 B5 B3 7F 33 AE 56 3C B6 86 C0 28 12 5A F0 46
            3B BE 14 53 79 35 82 59 36 54 42 13 42 3D EB 8A 20 11 2A 84
            54 D3 1B D0 42 BC 45 6C 85 CE 82 8B D0 1C CA FB 1C 76 FC A1
            94 3D 9F F2 27 CB 33 8B D2 4B E9 70 59 0B 12 A1 59 C6 06 10
            67 BF B7 EF 7A B2 2E 20 A5 53 32 65 E1 30 19 0B CE CE EA 86
            CA 3E C8 29 87 35 35 B5 7B 3D F8 EB 9A 2E 06 B1 39 AC C6 DC
            FC E9 59 B9 C5 1A B9 5D E1 15 61 4E 81 38 67 E3 B7 18 88 81
            08 3F 40 64 3E 88 46 45 A6 54 C6 04 83 AE 83 19 B2 E9 1E 20
            7C 30 CB C6 A2 C8 E8 47 0F 98 A9 A5 45 02 BA 54 CA CC 02 04
            49 2C DE 40 0D 4F FC 5D AA 1F 21 B7 DE CE 02 B2 C3 9F 94 4E
            D8 E8 83 DA 58 B1 91 2A E9 90 AF 46 F9 73 0D E0 95
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 47 5A F1 A5 B4 86 D2 B7 F5 39 E7 A9 DD DA 98 21 D0 E5 C5
           16 9B D8 DD 2A 73 5E ED 92 76 4B 8C 20 15 61 48 E1 AE 73 21
           33 04 69 47 D0 E1 F6 9C 4D E0 E0 11 89 AA FB CF 4F C5 6F F2
           B9 B7 01 78 C2 5A A2 6E 55 C2 72 28 F8 13 BA FF DE 1B 69 3C
           5A 68 E9 B4 94 08 06 FE 1B 96 E1 E7 91 56 88 00 70 E3 4E 6E
           D6 E7 65 97 74 DD 52 AA 74 E4 AA 94 A0 35 67 FC E5 39 B9 2B
           51 34 6B FE CC 16 9E E2 E8 77 D5 34 41 [...]
```

10881 (1) - 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: 2013/10/21

Hosts

i-a0fc644b (tcp/22)

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

  - 1.99
  - 2.0


SSHv2 host key fingerprint : 1a:0f:a7:68:d7:b7:7a:bb:59:10:18:b2:dc:c5:99:f2
```

10884 (1) - Network Time Protocol (NTP) Server Detection

Synopsis

An NTP server is listening on the remote host.

Description

An NTP (Network Time Protocol) server is listening on this port. It provides information about the current date and time of the remote system and may provide system information.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/03/13, Modification date: 2011/03/11

Hosts

i-a0fc644b (udp/123)

11219 (1) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Hosts

i-ad801846 (tcp/443)

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

12634 (1) - 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: 2014/09/19

Hosts

i-a0fc644b (tcp/0)

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

The output of "uname -a" is :
Linux ip-10-150-73-77 3.10.35-43.137.amzn1.x86_64 #1 SMP Wed Apr 2 09:36:59 UTC 2014 x86_64 x86_64
 x86_64 GNU/Linux

The remote Amazon Linux AMI system is :
Amazon Linux AMI release 2014.03

Local security checks have been enabled for this host.
```

18261 (1) - 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

This plugin extracts the banner of the Apache web server, and attempts to 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.

Risk Factor

None

Plugin Information:

Publication date: 2005/05/15, Modification date: 2014/07/29

Hosts

i-ad801846 (tcp/0)

```
The Linux distribution detected was :
 - Ubuntu 12.04 (precise)
 - Ubuntu 12.10 (quantal)
 - Ubuntu 13.04 (raring)
```

21643 (1) - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2014/07/08

Hosts

i-ad801846 (tcp/443)

```
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)
     EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
     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
     DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        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-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1
     SEED-SHA                     Kx=RSA         Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1
     DHE-RSA-AES128-SHA256        Kx=DHE         Au=RSA      Enc=AES128-CBC           Mac=SHA256

     DHE-RSA-AES256-SHA256        Kx=DHE         Au=RSA      Enc=AES256-CBC           Mac=SHA256

     RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES128-CBC           Mac=SHA256

     RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES256-CBC           Mac=SHA256
     DHE-RSA-AES128-SHA256        Kx=DHE         Au=RSA      Enc=AES-GCM(128)         Mac=SHA256

     DHE-RSA-AES256-SHA384        Kx=DHE         Au=RSA      Enc=AES-GCM(256)         Mac=SHA3
 [...]
```

22869 (1) - Software Enumeration (SSH)

Synopsis

It is possible to enumerate installed software on the remote host, via SSH.

Description

This plugin lists the software installed on the remote host by calling the appropriate command (rpm -qa on RPM-based Linux distributions, qpkg, dpkg, etc...)

Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2006/10/15, Modification date: 2014/07/28

Hosts

i-a0fc644b (tcp/0)

```
Here is the list of packages installed on the remote Amazon Linux AMI system :

  Nessus-5.2.6-es6|(none)
  PyYAML-3.10-3.6.amzn1|(none)
  acl-2.2.49-6.9.amzn1|(none)
  acpid-1.0.10-2.1.6.amzn1|(none)
  alsa-lib-1.0.22-3.9.amzn1|(none)
  at-3.1.10-43.8.amzn1|(none)
  attr-2.4.44-7.9.amzn1|(none)
  audit-2.3.2-3.19.amzn1|(none)
  audit-libs-2.3.2-3.19.amzn1|(none)
  authconfig-6.1.12-13.17.amzn1|(none)
  aws-amitools-ec2-1.5.2-0.0.amzn1|(none)
  aws-apitools-as-1.0.61.4-1.0.amzn1|(none)
  aws-apitools-common-1.1.0-1.8.amzn1|(none)
  aws-apitools-ec2-1.6.13.0-1.1.amzn1|(none)
  aws-apitools-elb-1.0.34.0-1.0.amzn1|(none)
  aws-apitools-iam-1.5.0-1.2.amzn1|(none)
  aws-apitools-mon-1.0.20.0-1.0.amzn1|(none)
  aws-apitools-rds-1.15.001-1.0.amzn1|(none)
  aws-cfn-bootstrap-1.3-17.amzn1|(none)
  aws-cli-1.3.6-1.0.amzn1|(none)
  basesystem-10.0-4.9.amzn1|(none)
  bash-4.1.2-15.17.amzn1|(none)
  bc-1.06.95-1.10.amzn1|(none)
  bind-libs-9.8.2-0.23.rc1.32.amzn1|32
  bind-utils-9.8.2-0.23.rc1.32.amzn1|32
  bzip2-1.0.6-8.12.amzn1|(none)
  bzip2-libs-1.0.6-8.12.amzn1|(none)
  ca-certificates-2013.1.94-65.0.9.amzn1|(none)
  chkconfig-1.3.49.3-2.10.amzn1|(none)
  cloud-disk-utils-0.27-1.3.amzn1|(none)
  cloud-init-0.7.2-7.20.amzn1|(none)
  coreutils-8.21-13.31.amzn1|(none)
  cpio-2.10-11.11.amzn1|(none)
  cracklib-2.8.16-4.11.amzn1|(none)
  cracklib-dicts-2.8.16-4.11.amzn1|(none)
  cronie-1.4.4-12.6.amzn1|(none)
  cronie-anacron-1.4.4-12.6.amzn1|(none)
  crontabs-1.10-33.9.amzn1|(none)
  cryptsetup-1.6.2-2.11.amzn1|(none)
  cryptsetup-libs-1.6.2-2.11.amzn1|(none)
  curl-7.36.0-2.44.amzn1|(none)
  cyrus-sasl-2.1.23-13.13.amzn1|(none)
  cyrus-sasl-lib-2.1.23-13.13.amzn1|(none)
  cyrus-sasl-plain-2.1.23-13.13.amzn1|(none)
  dash-0.5.5.1-4.5.amzn1|(none)
  db4-4.7.25-18.11.amzn1|(none)
  db4-utils-4.7.25-18.11.amzn1|(none)
  dbus-1.6.12-5.25.amzn1|1
```

```
dbus-libs-1.6.12-5.25.amzn1|1
dejavu-fonts-common-2.33-5.8.amzn1|(none)
dejavu-sans-fonts-2.33-5.8.amzn1|(none)
dejavu-serif-fonts-2.33-5.8.amzn1|(none)
device-mapper-1.02.79- [...]
```

24260 (1) - 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: 2011/05/31

Hosts

i-ad801846 (tcp/443)

```
Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Tue, 23 Sep 2014 03:15:25 GMT
  Server: Apache/2.2.22 (Ubuntu)
  Vary: Cookie,Accept-Encoding
  Content-Type: text/html; charset=utf-8
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Transfer-Encoding: chunked
```

25202 (1) - Enumerate IPv6 Interfaces via SSH

Synopsis

This plugin enumerates IPv6 interfaces on a remote host.

Description

By connecting to the remote host via SSH with the supplied credentials, this plugin enumerates network interfaces configured with IPv6 addresses.

Solution

Disable IPv6 if you do not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Plugin Information:

Publication date: 2007/05/11, Modification date: 2011/03/21

Hosts

i-a0fc644b (tcp/0)

```
The following IPv6 interfaces are set on the remote host :

 - fe80::2000:bff:fe0e:a166 (on interface eth0)
 - ::1 (on interface lo)
```

25203 (1) - Enumerate IPv4 Interfaces via SSH

Synopsis

This plugin enumerates IPv4 interfaces on a remote host.

Description

By connecting to the remote host via SSH with the supplied credentials, this plugin enumerates network interfaces configured with IPv4 addresses.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information:

Publication date: 2007/05/11, Modification date: 2011/03/21

Hosts

i-a0fc644b (tcp/0)

```
The following IPv4 addresses are set on the remote host :

 - 10.150.73.77 (on interface eth0)
 - 127.0.0.1 (on interface lo)
```

25220 (1) - 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

Hosts

i-ad801846 (tcp/0)

33276 (1) - Enumerate MAC Addresses via SSH

Synopsis

This plugin enumerates MAC addresses on a remote host.

Description

By connecting to the remote host via SSH with the supplied credentials, this plugin enumerates MAC addresses.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information:

Publication date: 2008/06/30, Modification date: 2012/03/27

Hosts

i-a0fc644b (tcp/0)

```
The following MAC address exists on the remote host :

  - 22:00:0B:0E:A1:66 (interface eth0)
```

39520 (1) - 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

http://www.nessus.org/u?d636c8c7

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2013/04/03

Hosts

i-a0fc644b (tcp/22)

```
Local checks have been enabled.
```

39521 (1) - 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

http://www.nessus.org/u?d636c8c7

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2013/10/02

Hosts

i-ad801846 (tcp/443)

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

45410 (1) - SSL Certificate commonName Mismatch

Synopsis

The SSL certificate commonName does not match the host name.

Description

This service presents an SSL certificate for which the 'commonName'
(CN) does not match the host name on which the service listens.

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2010/04/03, Modification date: 2012/09/30

Hosts

i-ad801846 (tcp/443)

```
The host name known by Nessus is :

  i-ad801846

The Common Name in the certificate is :

  www.patientadvance.com

The Subject Alternate Names in the certificate are :

  patientadvance.com
  www.patientadvance.com
```

50845 (1) - 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

Hosts

i-ad801846 (tcp/443)

51891 (1) - 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

Hosts

i-ad801846 (tcp/443)

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

55472 (1) - Device Hostname

Synopsis

It is 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: 2014/01/07

Hosts

i-a0fc644b (tcp/0)

```
Hostname : ip-10-150-73-77
```

56468 (1) - 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: 2014/07/25

Hosts

i-a0fc644b (tcp/0)

```
reboot   system boot  3.10.35-43.137.a Tue Sep 23 00:54 - 03:11  (02:16)
reboot   system boot  3.10.35-43.137.a Tue Sep 23 00:19 - 00:52  (00:32)
reboot   system boot  3.10.35-43.137.a Tue Sep 23 00:06 - 00:15  (00:09)
reboot   system boot  3.10.35-43.137.a Wed May 28 20:01 - 13:52  (17:51)

wtmp begins Wed May 28 20:01:15 2014
```

56984 (1) - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This script 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: 2014/04/14

Hosts

i-ad801846 (tcp/443)

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

57041 (1) - 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

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Hosts

i-ad801846 (tcp/443)

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

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      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
      DHE-RSA-AES128-SHA256        Kx=DHE         Au=RSA      Enc=AES128-CBC           Mac=SHA256

      DHE-RSA-AES256-SHA256        Kx=DHE         Au=RSA      Enc=AES256-CBC           Mac=SHA256


    TLSv12
      DHE-RSA-AES128-SHA256        Kx=DHE         Au=RSA      Enc=AES-GCM(128)         Mac=SHA256

      DHE-RSA-AES256-SHA384        Kx=DHE         Au=RSA      Enc=AES-GCM(256)         Mac=SHA384


The fields above are :

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

58651 (1) - 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: 2012/04/10

Hosts

i-a0fc644b (tcp/0)

```
Netstat output :
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 127.0.0.1:8834              0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
udp        0      0 0.0.0.0:68                  0.0.0.0:*
udp        0      0 10.150.73.77:123            0.0.0.0:*
udp        0      0 127.0.0.1:123               0.0.0.0:*
udp        0      0 0.0.0.0:123                 0.0.0.0:*
```

62563 (1) - 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

http://tools.ietf.org/html/rfc3749

http://tools.ietf.org/html/rfc3943

http://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2013/10/18

Hosts

i-ad801846 (tcp/443)

```
Nessus was able to confirm that the following compression method is
supported by the target :

  NULL (0x00)
```

64582 (1) - Netstat Connection Information

Synopsis

Nessus is 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: 2013/06/18

Hosts

i-a0fc644b (tcp/0)

```
tcp4 (listen)
  src: [host=127.0.0.1, port=8834]
  dst: [host=0.0.0.0, port=*]

tcp4 (listen)
  src: [host=0.0.0.0, port=22]
  dst: [host=0.0.0.0, port=*]

tcp4 (listen)
  src: [host=127.0.0.1, port=25]
  dst: [host=0.0.0.0, port=*]

tcp6 (listen)
  src: [host=::, port=22]
  dst: [host=::, port=*]

udp4 (listen)
  src: [host=0.0.0.0, port=68]
  dst: [host=0.0.0.0, port=*]

udp4 (listen)
  src: [host=10.150.73.77, port=123]
  dst: [host=0.0.0.0, port=*]

udp4 (listen)
  src: [host=127.0.0.1, port=123]
  dst: [host=0.0.0.0, port=*]

udp4 (listen)
  src: [host=0.0.0.0, port=123]
  dst: [host=0.0.0.0, port=*]
```

70544 (1) - 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

Hosts

i-ad801846 (tcp/443)

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

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      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
      DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        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
      DHE-RSA-AES128-SHA256        Kx=DHE         Au=RSA      Enc=AES128-CBC           Mac=SHA256

      DHE-RSA-AES256-SHA256        Kx=DHE         Au=RSA      Enc=AES256-CBC           Mac=SHA256

      RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES128-CBC           Mac=SHA256

      RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES256-CBC           Mac=SHA256


The fields above are :

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

70657 (1) - 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: 2014/04/04

Hosts

i-a0fc644b (tcp/22)

```
Nessus negotiated the following encryption algorithm with the server : aes128-cbc

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
  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-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  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
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  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-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-ripemd160
  hmac-ripemd160-etm@openssh.com
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
  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-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-ripemd160
  hmac-ripemd160-etm@openssh.com
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512- [...]
```

Remediations

Suggested Remediations