TO:

FROM: ARND.SPIERING@AS-INFORMATIK.NET

SUBJECT: ASTARO FIREWALL SCAN MIT NESSUS AUS BACKTRACK 5 R1

DATE: 24.11.2011

Inhalt

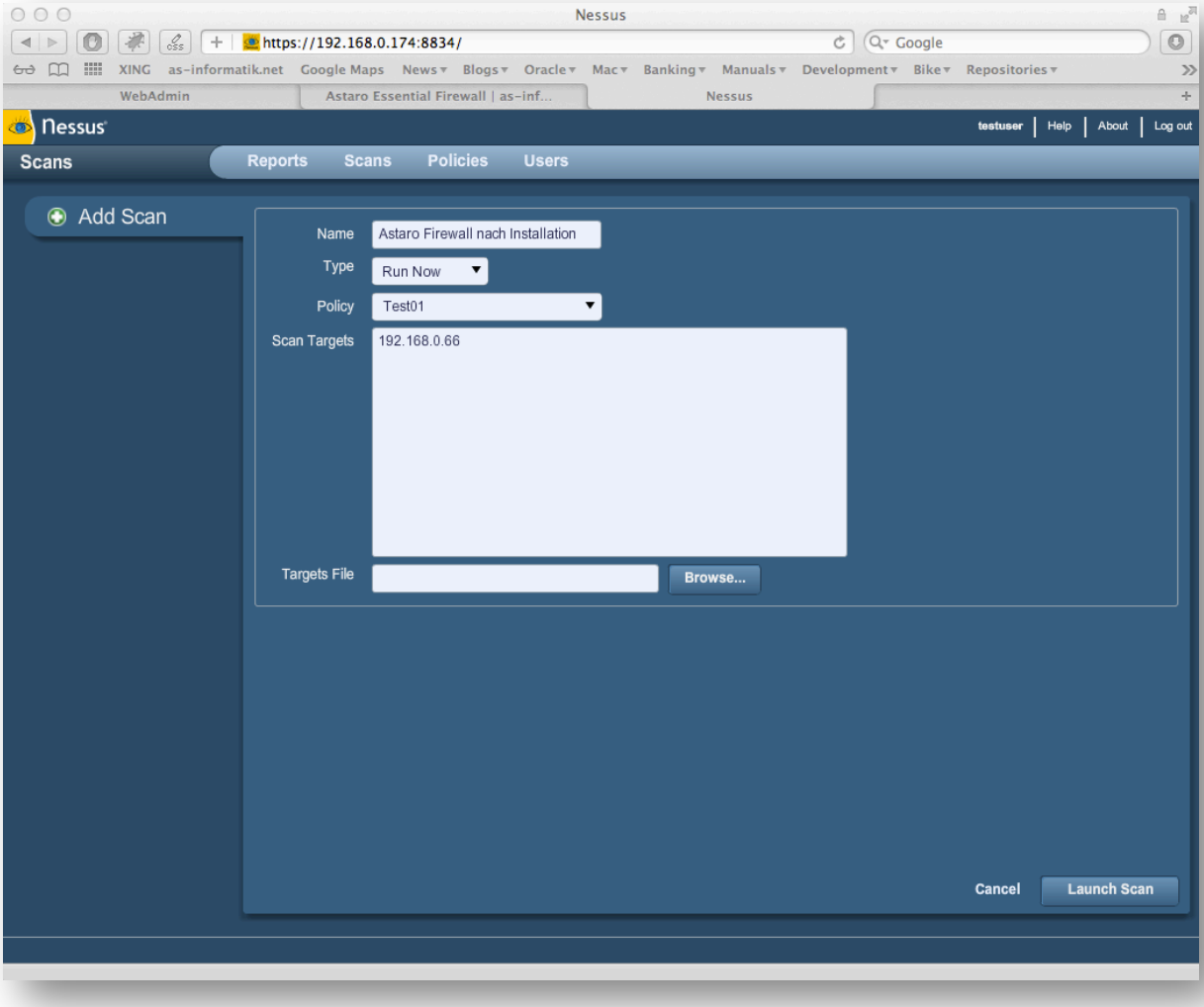
Dieses Dokument beschreibt einen Nessus Scan einer Astaro Firewall direkt nach der Installation.

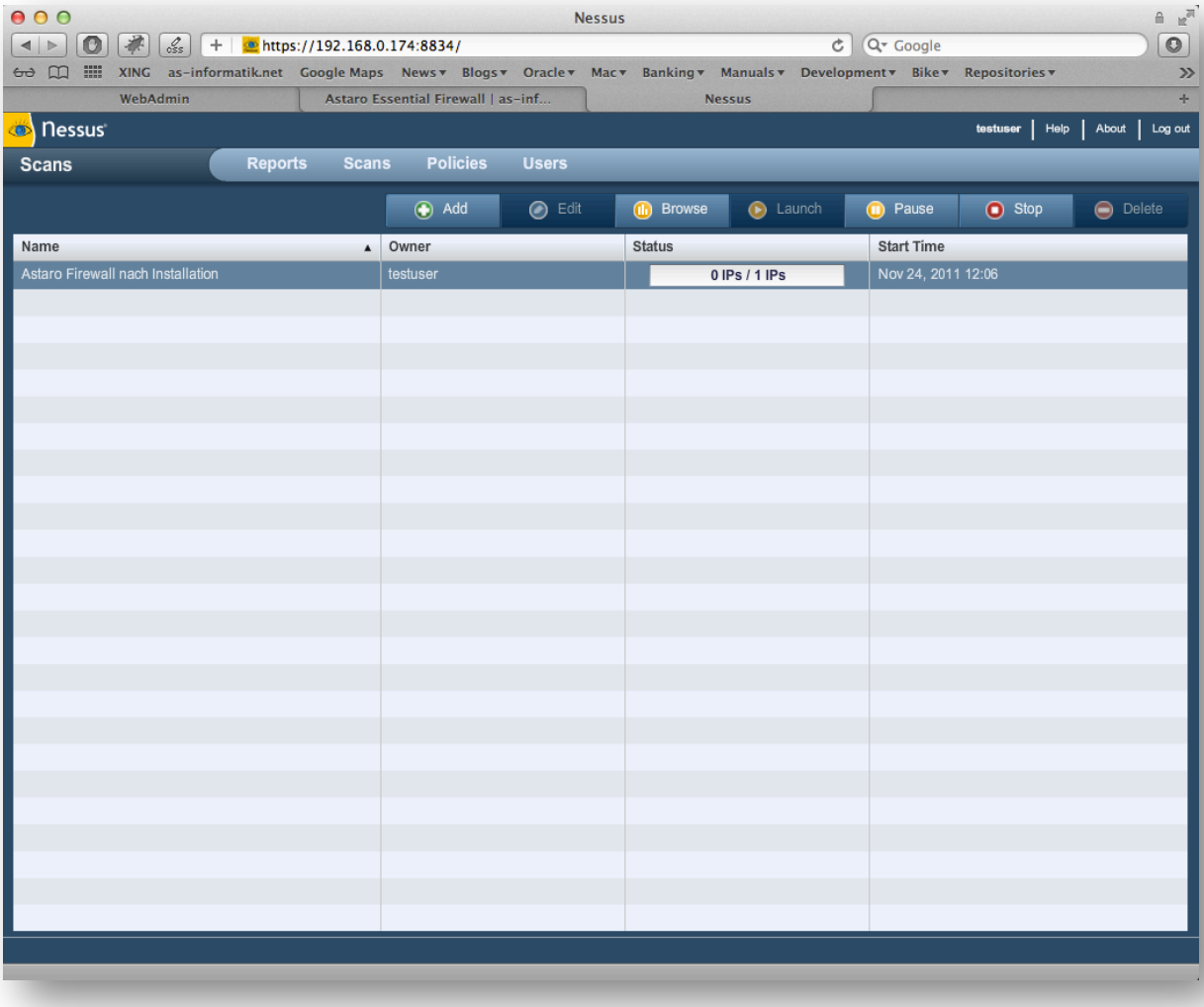
Die Parameter der Installation sind in diesem Artikel zu finden:

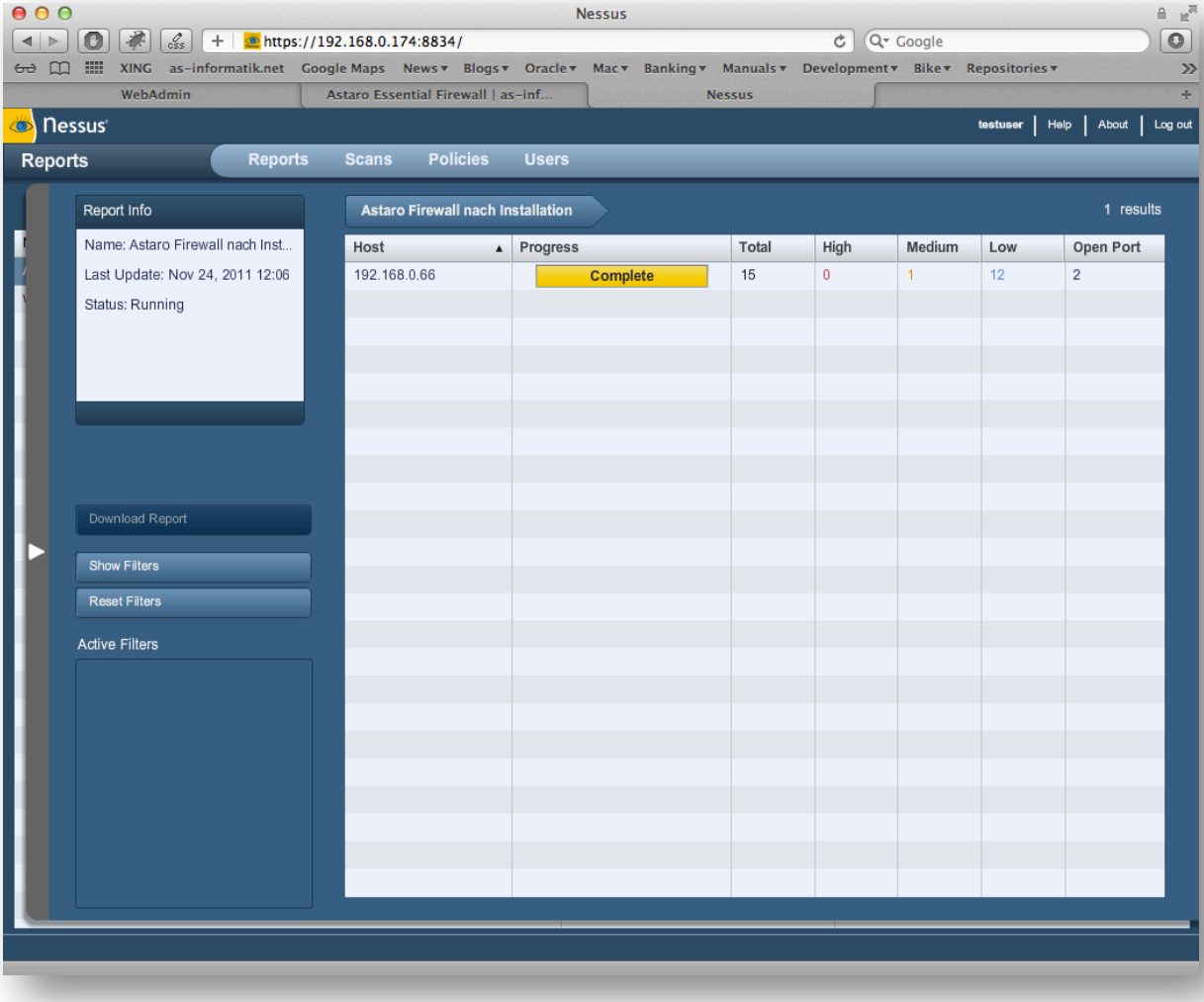
http://www.as-informatik.net/wordpress/2011/11/24/astaro-essentials-firewall/

Der Nessus Scanner ist in BackTrack 5 R1 enthalten und über ein Web Interface zu konfigurieren.


Nessus
https://192.168.0.174:8834/
Google
XING
as-informatik.net
Google Maps
News
Blogs
Oracle
Mac
Banking
Manuals
Development
Bike
Repositories
WebAdmin
Artikel ‹ as-informatik.net — Wor...
Nessus
Nessus®
HF
HomeFeed
Username
Password
Log In
TENABLE
Network Security


Nessus
https://192.168.0.174:8834/
Google
XING
as-informatik.net
Google Maps
News
Blogs
Oracle
Mac
Banking
Manuals
Development
Bike
Repositories
WebAdmin
Astaro Essential Firewall | as-inf...
Nessus
Nessus
testuser
Help
About
Log out
Scans
Reports
Scans
Policies
Users
Add Scan
Name
Astaro Firewall nach Installation
Type
Run Now
Policy
Test01
Scan Targets
192.168.0.66
Targets File
Browse...
Cancel
Launch Scan


Nessus
https://192.168.0.174:8834/
Google
XING as-informatik.net Google Maps News Blogs Oracle Mac Banking Manuals Development Bike Repositories
WebAdmin
Astaro Essential Firewall | as-inf...
Nessus
Nessus
testuser | Help | About | Log out
Scans
Reports Scans Policies Users
Add Edit Browse Launch Pause Stop Delete
Name
Owner
Status
Start Time
Astaro Firewall nach Installation
testuser
0 IPs / 1 IPs
Nov 24, 2011 12:06



HINWEIS: Der Eintrag Medium Risk resultiert aus dem Zertifikat der Astaro Firewall. An dieser Stelle kann das Zertifikat nicht als gültig angesehen werden, da es sich um ein lokales Zertifikat handelt. Dieser Punkt ist also zu vernachlässigen.

Alle weiteren Punkte werden mit dem Risk Factor NONE bewertet, stellen also keine Gefahr dar.

Nessus Scan Ergebnis als Report

NESSUS REPORT

List of PlugIn IDs

The following plugin IDs have problems associated with them. Select the ID to review more detail.

PLUGIN ID#	#	PLUGIN NAME	SEVERITY
51192	1	SSL Certificate signed with an unknown Certificate Authority	Medium Severity problem(s) found
54615	1	Device Type	Low Severity problem(s) found
51891	1	SSL Session Resume Supported	Low Severity problem(s) found
45590	1	Common Platform Enumeration (CPE)	Low Severity problem(s) found
35716	1	Ethernet Card Manufacturer Detection	Low Severity problem(s) found
25220	1	TCP/IP Timestamps Supported	Low Severity problem(s) found
24260	1	HyperText Transfer Protocol (HTTP) Information	Low Severity problem(s) found
21643	1	SSL Cipher Suites Supported	Low Severity problem(s) found
19506	1	Nessus Scan Information	Low Severity problem(s) found
15588	1	Web Server SSL Port HTTP Traffic Detection	Low Severity problem(s) found
11936	1	OS Identification	Low Severity problem(s) found
10287	1	Traceroute Information	Low Severity problem(s) found
10107	1	HTTP Server Type and Version	Low Severity problem(s) found

PORT WWW (4444/TCP)

Plugin ID: **24260**

HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

List of Hosts

192.168.0.66

Plugin Output

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

  Date: Thu, 24 Nov 2011 11:11:20 GMT
  Server: Apache
  Expires: Thursday, 01-Jan-1970 00:00:01 GMT
  Pragma: no-cache
  Vary: Accept-Encoding
  Connection: close
  Transfer-Encoding: chunked
  Content-Type: text/html; charset=utf-8
```

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 publication date: 2007/01/30
Plugin last modification date: 2011/05/31

PORT (0/TCP)

Plugin ID: **19506**

Nessus Scan Information

Synopsis

Information about the Nessus scan.

List of Hosts

192.168.0.66

Plugin Output

```
Information about this scan :

Nessus version : 4.4.1
Plugin feed version : 201111160037
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.0.174
Port scanner(s) : nessus_tcp_scanner 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
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2011/11/24 12:06
Scan duration : 374 sec
```

Description

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

- The version of the plugin set
- The type of plugin feed (HomeFeed or ProfessionalFeed)
- The version of the Nessus Engine

- The port scanner(s) used
- The port range scanned
- 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 publication date: 2005/08/26
Plugin last modification date: 2011/09/21

PORT (0/TCP)

Plugin ID: **25220**
TCP/IP Timestamps Supported

Synopsis
The remote service implements TCP timestamps.
List of Hosts
192.168.0.66

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.

Solution
n/a

See also
http://www.ietf.org/rfc/rfc1323.txt

Risk Factor
None

Plugin publication date: 2007/05/16
Plugin last modification date: 2011/03/20

PORT WWW (4444/TCP)

Plugin ID: **21643**
SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

List of Hosts

192.168.0.66

Plugin Output

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

  High Strength Ciphers (>= 112-bit key)
    SSLv3
      EDH-RSA-DES-CBC3-SHA       Kx=DH         Au=RSA     Enc=3DES(168)
Mac=SHA1
      DES-CBC3-SHA               Kx=RSA        Au=RSA     Enc=3DES(168)
Mac=SHA1
      RC4-MD5                    Kx=RSA        Au=RSA     Enc=RC4(128)
Mac=MD5
      RC4-SHA                    Kx=RSA        Au=RSA     Enc=RC4(128)
Mac=SHA1
    TLSv1
      EDH-RSA-DES-CBC3-SHA       Kx=DH         Au=RSA     Enc=3DES(168)
Mac=SHA1
      DHE-RSA-AES128-SHA         Kx=DH         Au=RSA     Enc=AES(128)
Mac=SHA1
      DHE-RSA-AES256-SHA         Kx=DH         Au=RSA     Enc=AES(256)
Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA    Kx=DH         Au=RSA     Enc=Camellia(128)
Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA    Kx=DH         Au=RSA     Enc=Camellia(256)
Mac=SHA1
      DES-CBC3-SHA               Kx=RSA        Au=RSA     Enc=3DES(168)
Mac=SHA1
      AES128-SHA                 Kx=RSA        Au=RSA     Enc=AES(128)
```

```
Mac=SHA1
      AES256-SHA                Kx=RSA        Au=RSA     Enc=AES(256)
Mac=SHA1
      CAMELLIA128-SHA           Kx=RSA        Au=RSA     Enc=Camellia(128)
Mac=SHA1
      CAMELLIA256-SHA           Kx=RSA        Au=RSA     Enc=Camellia(256)
Mac=SHA1
      RC4-MD5                   Kx=RSA        Au=RSA     Enc=RC4(128)
Mac=MD5
      RC4-SHA                   Kx=RSA        Au=RSA     Enc=RC4(128)
Mac=SHA1

The fields above are :

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

Description

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

Solution

n/a

See also

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

Risk Factor

None

Plugin publication date: 2006/06/05
Plugin last modification date: 2011/06/07

PORT WWW (4444/TCP)

Plugin ID: **10107**

HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

List of Hosts

192.168.0.66

Plugin Output

```
The remote web server type is :

Apache
and the 'ServerTokens' directive is ProductOnly
Apache does not offer a way to hide the server type.
```

Description

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

Solution

n/a

Risk Factor

None

Plugin publication date: 2000/01/04
Plugin last modification date: 2011/04/21

PORT WWW (4444/TCP)

Plugin ID: **51192**

SSL Certificate signed with an unknown Certificate Authority

Synopsis

The SSL certificate for this service is signed by an unknown\certificate authority.

List of Hosts

192.168.0.66

Plugin Output

```
*** ERROR: Unknown root CA in the chain:

Country: de

Locality: Herne

Organization: as-informatik.net

Common Name: as-informatik.net WebAdmin CA

Email Address: admin@as-informatik.net



Certificate chain:

|-Country: de

|-Locality: Herne

|-Organization: as-informatik.net

|-Common Name: ASGE01

|
```

Description

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

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

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

Plugin publication date: 2010/12/15
Plugin last modification date: 2011/10/26

PORT (0/TCP)

Plugin ID: **54615**

Device Type

Synopsis
It is possible to guess the remote device type.
List of Hosts
192.168.0.66

Plugin Output
```
Remote device type : general-purpose
Confidence level : 70
```

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 publication date: 2011/05/23
Plugin last modification date: 2011/05/23

PORT (0/UDP)

Plugin ID: **10287**
Traceroute Information

Synopsis
It was possible to obtain traceroute information.
List of Hosts
192.168.0.66

Plugin Output
```
For your information, here is the traceroute from 192.168.0.174 to 192.168.0.66 :
192.168.0.174
192.168.0.66
```

Description

Makes a traceroute to the remote host.

Solution
n/a

Risk Factor
None

Plugin publication date: 1999/11/27
Plugin last modification date: 2011/03/21

PORT (0/TCP)

Plugin ID: **11936**
OS Identification

Synopsis
It is possible to guess the remote operating system.
List of Hosts
192.168.0.66

Plugin Output

```
Remote operating system : Linux Kernel 2.6
Confidence Level : 70
Method : SinFP


The remote host is running Linux Kernel 2.6
```

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, and sometimes its version.

Solution
N/A

Risk Factor
None

Plugin publication date: 2003/12/09
Plugin last modification date: 2011/09/23

PORT (0/TCP)

Plugin ID: **35716**
Ethernet Card Manufacturer Detection

Synopsis
The manufacturer can be deduced from the Ethernet OUI.
List of Hosts
192.168.0.66

Plugin Output

```
The following card manufacturers were identified :

08:00:27:d3:e2:7f : CADMUS COMPUTER SYSTEMS
```

Description

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

Solution
n/a

See also
http://standards.ieee.org/faqs/OUI.html
http://standards.ieee.org/regauth/oui/index.shtml

Risk Factor

None

Plugin publication date: 2009/02/19
Plugin last modification date: 2011/03/27

PORT WWW (4444/TCP)

Plugin ID: **15588**
Web Server SSL Port HTTP Traffic Detection

Synopsis
An SSL detection issue might impede the Nessus Scan.
List of Hosts
192.168.0.66

Description

Nessus has discovered that it is talking in plain HTTP on a SSL port.

Nessus has corrected this issue by enabling HTTPS for this port only. However if other SSL ports are used on the remote host, they might be skipped.

Solution
Enable SSL tests in the 'Services' preference setting, or increase the timeouts if this option is already set and the plugin missed this port.

Risk Factor
None

Plugin publication date: 2004/11/01
Plugin last modification date: 2011/04/01

PORT WWW (4444/TCP)

Plugin ID: **51891**
SSL Session Resume Supported

Synopsis
The remote host allows resuming SSL sessions.

List of Hosts
192.168.0.66

Plugin Output

```
This port supports resuming SSLv3 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 publication date: 2011/02/07
Plugin last modification date: 2011/10/21

PORT (0/TCP)

Plugin ID: **45590**
Common Platform Enumeration (CPE)

Synopsis
It is possible to enumerate CPE names that matched on the remote\system.
List of Hosts
192.168.0.66

Plugin Output

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

  cpe:/o:linux:linux_kernel:2.6
```

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.

Solution

n/a

See also

http://cpe.mitre.org/

Risk Factor

None

Plugin publication date: 2010/04/21
Plugin last modification date: 2011/10/20

192.168.0.66	
Scan Time	
Start time:	Thu Nov 24 12:06:09 2011
End time:	Thu Nov 24 12:12:23 2011
Number of vulnerabilities	
High	
Medium	1
Low	12

Remote Host Information	
Operating System:	Linux Kernel 2.6
IP address:	192.168.0.66

MAC addresses:	08:00:27:d3:e2:7f