Nessus Report

Report

16/Aug/2012:14:52:10 GMT

HomeFeed: Commercial use of the report is prohibited

Any time Nessus is used in a commercial environment you MUST maintain an active subscription to the ProfessionalFeed in order to be compliant with our license agreement: http://www.nessus.org/products/nessus-professionalfeed
Table Of Contents

Vulnerabilities By Host................................................................................................................................. 5

• 192.168.56.3................................................................................................................................................. 6

Vulnerabilities By Plugin.................................................................................................................................... 97

• 22964 (8) - Service Detection................................................................................................................................. 147
• 11111 (10) - RPC Services Enumeration........................................................................................................ 145
• 11219 (30) - Nessus SYN scanner......................................................................................................................... 143
• 53491 (1) - SSL / TLS Renegotiation DoS............................................................................................................. 142
• 42263 (1) - Unencrypted Telnet Server .................................................................................................................. 141
• 34850 (1) - Web Server Uses Basic Authentication Without HTTPS..................................................................... 140
• 10407 (1) - X Server Detection .............................................................................................................................. 139
• 34324 (2) - FTP Supports Clear Text Authentication ............................................................................................. 138
• 57608 (1) - SMB Signing Disabled ......................................................................................................................... 134
• 57582 (1) - SSL Self-Signed Certificate ................................................................................................................. 133
• 52611 (1) - SMTP Service STARTTLS Plaintext Command Injection .................................................................... 131
• 51425 (1) - phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9) ............................................................... 130
• 59088 (1) - PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution ........................................127
• 49142 (1) - phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7) ...................................................128
• 45411 (1) - SSL Certificate with Wrong Hostname................................................................................................ 126
• 46803 (1) - PHP expose.php Information Disclosure........................................................................................... 127
• 42873 (1) - SSL Medium Strength Cipher Suites Supported..................................................................................125
• 42256 (1) - NFS Shares World Readable.............................................................................................................124
• 59088 (1) - PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution ........................................127
• 42256 (1) - NFS Shares World Readable.............................................................................................................124
• 42873 (1) - SSL Medium Strength Cipher Suites Supported..................................................................................125
• 45411 (1) - SSL Certificate with Wrong Hostname................................................................................................ 126
• 46803 (1) - PHP expose.php Information Disclosure........................................................................................... 127
• 49142 (1) - phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7) ...................................................128
• 51192 (1) - SSL Certificate Cannot Be Trusted..................................................................................................129
• 51425 (1) - phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9) ............................................................... 130
• 52611 (1) - SMTP Service STARTTLS Plaintext Command Injection .................................................................... 131
• 57582 (1) - SSL Self-Signed Certificate ................................................................................................................. 133
• 57608 (1) - SMB Signing Disabled.........................................................................................................................134
• 57792 (1) - Apache HTTP Server httpOnly Cookie Information Disclosure............................................................ 135
• 26194 (2) - Web Server Uses Plain Text Authentication Forms.............................................................................136
• 34324 (2) - FTP Supports Clear Text Authentication.............................................................................................138
• 10407 (1) - X Server Detection..............................................................................................................................139
• 34850 (1) - Web Server Uses Basic Authentication Without HTTPS.....................................................................140
• 42263 (1) - Unencrypted Telnet Server..................................................................................................................141
• 53491 (1) - SSL / TLS Renegotiation DoS.............................................................................................................142
• 11219 (30) - Nessus SYN scanner.........................................................................................................................143
• 11111 (10) - RPC Services Enumeration.........................................................................................................145
• 22964 (8) - Service Detection............................................................................................................................147
Hosts Summary (Executive)..........................................................................................228

*192.168.56.3..............................................................................................................229
192.168.56.3

Scan Information
End time: Thu Aug 16 14:52:04 2012

Host Information
Netbios Name: METASPLOITABLE
IP: 192.168.56.3
MAC Address: 08:00:27:b9:7e:58
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Results Summary
<table>
<thead>
<tr>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Info</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>6</td>
<td>22</td>
<td>8</td>
<td>137</td>
<td>176</td>
</tr>
</tbody>
</table>

Results Details

0/icmp
10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis
It is possible to determine the exact time set on the remote host.

Description
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor
None

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

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

Ports
icmp/0
The difference between the local and remote clocks is -13832 seconds.

tcp
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
### 35716 - Ethernet Card Manufacturer Detection

**Synopsis**
The manufacturer can be deduced from the Ethernet OUI.

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

**See Also**

<table>
<thead>
<tr>
<th>Ports</th>
<th>tcp/0</th>
</tr>
</thead>
</table>

The following card manufacturers were identified:
- 08:00:27:b9:7e:58 : CADMUS COMPUTER SYSTEMS

### 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 script 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.

<table>
<thead>
<tr>
<th>Ports</th>
<th>tcp/0</th>
</tr>
</thead>
</table>

The linux distribution detected was:
- Ubuntu 8.04 (gutsy)
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, and sometimes its version.

Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2003/12/09, Modification date: 2012/04/06

Ports
tcp/0

Remote operating system : Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Confidence Level : 95
Method : SSH

Not all fingerprints could give a match - please email the following to os-signatures@nessus.org :
SinFP:
P1:B10113:F0x12:W5840:00204f0f:0000001:0000000:M1460:
P2:B10113:F0x12:W5792:00204f0f04020800:0000000:M1460:
P3:B10120:F0x04:W0:00:W0
P4:5002_7_p=3632
SMTP::220 metasploitable.localdomain ESMTTP Postfix (Ubuntu)
SSLcert::!C/CN:ubuntu804-base.localdomain/OU:Office for Complication of Otherwise Simple Affairs/CN:ubuntu804-base.localdomain/OU:Office for Complication of Otherwise Simple Affairs
ed093088706603bfd5dc237399b498da2d4d31c6
SSH:SSH-2.0-OpenSSH_4.7p1 Debian-Ubuntu

The remote host is running Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

54615 - Device Type

Synopsis
It is possible to guess the remote device type.

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

Solution
n/a

Risk Factor
None

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

Ports
tcp/0

Remote device type : general-purpose
Confidence level : 95

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: 2012/05/21

### Ports

| tcp/0 |

The remote operating system matched the following CPE:

- cpe:/o:canonical:ubuntu_linux:8.04

Following application CPE's matched on the remote system:

- cpe:/a:openbsd:openssh:4.7 -> OpenBSD OpenSSH 4.7
- cpe:/a:samba:samba:3.0.20 -> Samba 3.0.20
- cpe:/a:apache:http_server:2.2.8 -> Apache Software Foundation Apache HTTP Server 2.2.8
- cpe:/a:php:php:5.2.4 -> PHP 5.2.4
- cpe:/a:phpmyadmin:phpmyadmin:3.1.1 -> phpMYAdmin 3.1.1
- cpe:/a:isc:bind:9.4

### 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 plugin feed (HomeFeed or ProfessionalFeed)
- 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: 2012/04/18

#### Ports

| tcp/0 |

Information about this scan:

- Nessus version: 5.0.1
- Plugin feed version: 201208021939
- Type of plugin feed: HomeFeed (Non-commercial use only)
- Scanner IP: 192.168.56.1
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
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 : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2012/8/16 13:55
Scan duration : 3370 sec

0/udp
10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2012/02/23

Ports
udp/0

For your information, here is the traceroute from 192.168.56.1 to 192.168.56.3 :
192.168.56.1
192.168.56.3

21/tcp
55523 - vsftpd Smiley Face Backdoor

Synopsis

The remote FTP server contains a backdoor allowing execution of arbitrary code.

Description

The version of vsftpd running on the remote host has been compiled with a backdoor. Attempting to login with a username containing :) (a smiley face) triggers the backdoor, which results in a shell listening on TCP port 6200. The shell stops listening after a client connects to and disconnects from it. An unauthenticated, remote attacker could exploit this to execute arbitrary code as root.

See Also

http://pastebin.com/AetT9sS5

http://www.nessus.org/u?abcbc915

Solution

Validate and recompile a legitimate copy of the source code.

Risk Factor

Critical

CVSS Base Score

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

CVSS Temporal Score
Anonymous FTP Enabled

**Synopsis**
Anonymous logins are allowed on the remote FTP server.

**Description**
This FTP service allows anonymous logins. Any remote user may connect and authenticate without providing a password or unique credentials. This allows a user to access any files made available on the FTP server.

**Solution**
Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure sensitive content is not available.

**Risk Factor**
Medium

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

**References**

<table>
<thead>
<tr>
<th>CVE</th>
<th>CVE-1999-0497</th>
</tr>
</thead>
<tbody>
<tr>
<td>XREF</td>
<td>OSVDB:69</td>
</tr>
</tbody>
</table>

**Plugin Information:**
Publication date: 1999/06/22, Modification date: 2011/10/05

**Ports**
tcp/21

FTP Supports Clear Text Authentication

**Synopsis**
Authentication credentials might be intercepted.

**Description**
The remote FTP server allows the user's name and password to be transmitted in clear text, which could be intercepted by a network sniffer or a man-in-the-middle attack.

**Solution**
Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.

**Risk Factor**
Low

**CVSS Base Score**
8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
## 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### References

XREF  
CWE:522

XREF  
CWE:523

### Plugin Information:

Publication date: 2008/10/01, Modification date: 2012/02/22

### Ports

**tcp/21**

This FTP server does not support 'AUTH TLS'.

### 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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

#### Solution

Protect your target with an IP filter.

#### Risk Factor

None

### Ports

**tcp/21**

Port 21/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: 2012/07/09

### Ports

**tcp/21**

An FTP server is running on this port.

### 10092 - FTP Server Detection

#### Synopsis

An FTP server is listening on this port.

#### Description

It is possible to obtain the banner of the remote FTP server by connecting to the remote port.

#### Solution
52703 - vsftpd Detection

Synopsis
An FTP server is listening on the remote port.

Description
The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

See Also
http://vsftpd.beasts.org/

Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2011/03/17, Modification date: 2011/03/17

Ports
tcp/21

Source : 220 (vsFTPD 2.3.4)
Version : 2.3.4

22/tcp
32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis
The remote SSH host keys are weak.

Description
The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.
The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.
Attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

See Also
http://www.nessus.org/u?5d01bdab
http://www.nessus.org/u?f14f4224

Solution
Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor
Critical

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

CVSS Temporal Score
8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

<table>
<thead>
<tr>
<th>Reference</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>BID</td>
<td>29179</td>
</tr>
<tr>
<td>CVE</td>
<td>CVE-2008-0166</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:45029</td>
</tr>
<tr>
<td>XREF</td>
<td>CWE:310</td>
</tr>
</tbody>
</table>

Exploitable with
Core Impact (true)

Plugin Information:
Publication date: 2008/05/14, Modification date: 2011/03/21

Ports
tcp/22

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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution
Protect your target with an IP filter.

Risk Factor
None

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: 2012/07/09

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**
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_4.7p1 Debian-8ubuntu1
SSH supported authentication : publickey,password

**10881 - SSH Protocol Versions Supported**

**Synopsis**
A SSH server is running on the remote host.

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

**Solution**
n/a

**Risk Factor**
None

**Plugin Information:**
Publication date: 2002/03/06, Modification date: 2012/04/04

**Ports**
tcp/22

The remote SSH daemon supports the following versions of the SSH protocol :
- 1.99
- 2.0


**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:**
Ports
tcp/22
Give Nessus credentials to perform local checks.

23/tcp
42263 - Unencrypted Telnet Server

Synopsis
The remote Telnet server transmits traffic in cleartext.

Description
The remote host is running a Telnet server over an unencrypted channel. Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in cleartext. An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information. Use of SSH is preferred nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.

Solution
Disable this service and use SSH instead.

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: 2009/10/27, Modification date: 2011/09/15

Ports
tcp/23

Nessus collected the following banner from the remote Telnet server:

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

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login:
------------------------------- snip ------------------------------

11219 - Nessus SYN scanner

Synopsis
It is possible to determine which TCP ports are open.

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

Solution
Protect your target with an IP filter.
<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ports</strong></td>
<td>tcp/23</td>
</tr>
<tr>
<td></td>
<td>Port 23/tcp was found to be open</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plugin Information:</strong></td>
<td>Publication date: 2007/08/19, Modification date: 2012/07/09</td>
</tr>
<tr>
<td><strong>Ports</strong></td>
<td>tcp/23</td>
</tr>
<tr>
<td></td>
<td>A telnet server is running on this port.</td>
</tr>
</tbody>
</table>

**10281 - Telnet Server Detection**

**Synopsis**
A Telnet server is listening on the remote port.

**Description**
The remote host is running a Telnet server, a remote terminal server.

**Solution**
Disable this service if you do not use it.

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plugin Information:</strong></td>
<td>Publication date: 1999/10/12, Modification date: 2011/03/17</td>
</tr>
<tr>
<td><strong>Ports</strong></td>
<td>tcp/23</td>
</tr>
<tr>
<td></td>
<td>Here is the banner from the remote Telnet server:</td>
</tr>
<tr>
<td></td>
<td>snip</td>
</tr>
<tr>
<td></td>
<td>metasploitable</td>
</tr>
<tr>
<td></td>
<td>snip</td>
</tr>
</tbody>
</table>

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

| 25/tcp              | snip                        |
**57582 - SSL Self-Signed Certificate**

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

**Description**
The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man in the middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

**Solution**
Purchase or generate a proper certificate for this service.

**Risk Factor**
Medium

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

**Plugin Information:**
Publication date: 2012/01/17, Modification date: 2012/01/17

**Ports**
tcp/25

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

```plaintext
| Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain |
```

---

**51192 - SSL Certificate Cannot Be Trusted**

**Synopsis**
The SSL certificate for this service cannot be trusted.

**Description**
The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted. First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. Third, the certificate chain may contain a signature that either didn't match the certificate's information, or was not possible to verify. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain 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 Information:**
Publication date: 2010/12/15, Modification date: 2012/01/28

**Ports**
The following certificates were part of the certificate chain sent by the remote host, but have expired:

- **Subject**: C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain
- **Not After**: Apr 16 14:07:45 2010 GMT

The following certificates were at the top of the certificate chain sent by the remote host, but are signed by an unknown certificate authority:

- **Subject**: C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain
- **Issuer**: C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain

### 15901 - SSL Certificate Expiry

#### Synopsis

The remote server's SSL certificate has already expired.

#### Description

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

#### Solution

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

#### Risk Factor

Medium

#### CVSS Base Score

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

#### Plugin Information:

Publication date: 2004/12/03, Modification date: 2012/04/02

#### Ports

tcp/25

The SSL certificate has already expired:

- **Subject**: C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain
- **Issuer**: C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain
- **Not valid before**: Mar 17 14:07:45 2010 GMT
- **Not valid after**: Apr 16 14:07:45 2010 GMT

### 20007 - SSL Version 2 (v2) Protocol Detection

#### Synopsis

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

#### Description

The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

#### See Also


http://support.microsoft.com/kb/187498
Solution
Consult the application’s documentation to disable SSL 2.0 and use SSL 3.0, TLS 1.0, or higher instead.

Risk Factor
Medium

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

References
CVE
CVE-2005-2969

Plugin Information:
Publication date: 2005/10/12, Modification date: 2012/04/02

Ports
tcp/25

31705 - SSL Anonymous Cipher Suites Supported

Synopsis
The remote service supports the use of anonymous SSL ciphers.

Description
The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

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

Solution
Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk Factor
Medium

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

CVSS Temporal Score
3.6 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References
BID
28482

CVE
CVE-2007-1858

XREF
OSVDB:34882

Plugin Information:
Publication date: 2008/03/28, Modification date: 2012/04/02

Ports
tcp/25

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

<table>
<thead>
<tr>
<th>Low Strength Ciphers (&lt; 56-bit key)</th>
<th>SSLv3</th>
<th>TLSv1</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXP-ADH-DES-CBC-SHA</td>
<td>Kx=DH(512)</td>
<td>Au=None</td>
</tr>
<tr>
<td>EXP-ADH-RC4-MD5</td>
<td>Kx=DH(512)</td>
<td>Au=None</td>
</tr>
</tbody>
</table>
**Synopsis**

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

**Description**

The remote host supports the use of SSL ciphers that offer medium strength encryption, which we currently regard as those with key lengths at least 56 bits and less than 112 bits.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

**Solution**

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

**Risk Factor**

Medium

**CVSS Base Score**

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

**Plugin Information:**

Publication date: 2009/11/23, Modification date: 2012/04/02

**Ports**

tcp/25

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

**Medium Strength Ciphers (>= 56-bit and < 112-bit key)**

**SSLv2**
- DES-CBC-MD5
- DES-CBC-SHA

**SSLv3**
- ADH-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA

**TLSv1**
- ADH-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA

The fields above are:

- {OpenSSL ciphername}
- Kx={key exchange}
- Au={authentication}
- Enc={symmetric encryption method}
- Mac={message authentication code}
- {export flag}
26928 - SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

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

Solution

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

Risk Factor

Medium

CVSS Base Score

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

References

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

Plugin Information:

Publication date: 2007/10/08, Modification date: 2012/04/02

Ports
tcp/25

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

Low Strength Ciphers (< 56-bit key)

SSLv2
EXP-RC2-CBC-MD5 Kx=RSA (512)  Au=RSA  Enc=RC2 (40)  Mac=MD5  export
EXP-RC4-MD5 Kx=RSA (512)  Au=RSA  Enc=RC4 (40)  Mac=MD5  export

SSLv3
EXP-ADH-DES-CBC-SHA Kx=DH (512)  Au=None  Enc=DES (40)  Mac=SHA1  export
EXP-ADH-RC4-MD5 Kx=DH (512)  Au=None  Enc=RC4 (40)  Mac=MD5  export
EXP-EDH-RSA-DES-CBC-SHA Kx=DH (512)  Au=RSA  Enc=DES (40)  Mac=SHA1  export
EXP-DES-CBC-SHA Kx=RSA (512)  Au=RSA  Enc=DES (40)  Mac=SHA1  export
EXP-RC2-CBC-MD5 Kx=RSA (512)  Au=RSA  Enc=RC2 (40)  Mac=MD5  export
EXP-RC4-MD5 Kx=RSA (512)  Au=RSA  Enc=RC4 (40)  Mac=MD5  export

TLSv1
EXP-EDH-RSA-DES-CBC-SHA Kx=DH (512)  Au=RSA  Enc=DES (40)  Mac=SHA1  export
EXP-ADH-DES-CBC-SHA Kx=DH (512)  Au=None  Enc=DES (40)  Mac=SHA1  export
The fields above are:

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

### 52611 - SMTP Service STARTTLS Plaintext Command Injection

**Synopsis**
The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.

**Description**
The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.
Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

**See Also**


http://www.securityfocus.com/archive/1/516901/30/0/threaded

**Solution**
Contact the vendor to see if an update is available.

**Risk Factor**
Medium

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

**CVSS Temporal Score**
3.3 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

**References**

<table>
<thead>
<tr>
<th>BID</th>
<th>CVE-2011-0411</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>CVE-2011-1430</td>
</tr>
<tr>
<td>CVE</td>
<td>CVE-2011-1431</td>
</tr>
<tr>
<td>CVE</td>
<td>CVE-2011-1432</td>
</tr>
<tr>
<td>CVE</td>
<td>CVE-2011-1506</td>
</tr>
<tr>
<td>CVE</td>
<td>CVE-2011-2165</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:71020</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:71021</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:71854</td>
</tr>
</tbody>
</table>
Nessus sent the following two commands in a single packet:

```
STARTTLS
RSET
```

And the server sent the following two responses:

```
220 2.0.0 Ready to start TLS
250 2.0.0 Ok
```

**45411 - SSL Certificate with Wrong Hostname**

**Synopsis**

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

**Description**

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

**Solution**

Purchase or generate a proper certificate for this service.

**Risk Factor**

Medium

**CVSS Base Score**

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

---

The identity known by Nessus is:

192.168.56.3

The Common Name in the certificate is:

ubuntu804-base.localdomain

---

**53491 - SSL / TLS Renegotiation DoS**

**Synopsis**

The remote service allows repeated renegotiation of TLS / SSL connections.

**Description**

The remote service encrypts traffic using TLS / SSL and permits clients to renegotiate connections. The computational requirements for renegotiating a connection are asymmetrical between the client and the server, with the server performing several times more work. Since the remote host does not appear to limit the number of renegotiations for a single TLS / SSL connection, this permits a client to open several simultaneous connections and repeatedly renegotiate them, possibly leading to a denial of service condition.

**See Also**

http://www.ietf.org/mail-archive/web/tls/current/msg07553.html

Solution
Contact the vendor for specific patch information.

Risk Factor
Low

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

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

References

<table>
<thead>
<tr>
<th>BID</th>
<th>48626</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>CVE-2011-1473</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:73894</td>
</tr>
</tbody>
</table>

Plugin Information:
Publication date: 2011/05/04, Modification date: 2012/04/20

Ports
tcp/25

The remote host is vulnerable to renegotiation DoS over TLSv1 / SSLv3.

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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might
kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is
loaded.

Solution
Protect your target with an IP filter.

Risk Factor
None

Ports
tcp/25

Port 25/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
10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port. Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

42088 - SMTP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a plaintext to an encrypted communications channel.

See Also

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

Solution

n/a

Risk Factor

None

Here is the SMTP service's SSL certificate that Nessus was able to collect after sending a 'STARTTLS' command:

------------------------------ snip ------------------------------
Subject Name:
Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9 7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24 73 FF 3C E5 9E 3B 6D FC CB B1 AC FA 4C 4D 5E 9B 4C 99 54 0B D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF 8D 89 62 33 AF 65 BB 36 E1 9F C4 2C 73 C1 4E 2B A0 AB 14 4B 98 70 46 61 B1 B9 31 DF 8C 99 EE 75 6B 79 3C 4A 00 90 9D DC 99 OD 33 A4 B5 Exponent: 01 00 01
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A 0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F 1E B4 4F BE D4 BD DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49 68 35 19 7C 8C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 6B 83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53 A6 1E 30 DD AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C 15 6E 8D 3D 38 PF 6C CA 2E 75

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: 2012/06/23

Ports
tcp/25

This port supports SSLv2/SSLv3/TLSv1.0.

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: 2012/07/25

<table>
<thead>
<tr>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp/25</td>
</tr>
</tbody>
</table>

The host name known by Nessus is:

```
metasploitable
```

The Common Name in the certificate is:

```
ubuntu804-base.localdomain
```

### 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

<table>
<thead>
<tr>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp/25</td>
</tr>
</tbody>
</table>

**Subject Name:**

| Country: XX |
| State/Province: There is no such thing outside US |
| Locality: Everywhere |
| Organization: OCOSA |
| Organization Unit: Office for Complication of Otherwise Simple Affairs |
| Common Name: ubuntu804-base.localdomain |
| Email Address: root@ubuntu804-base.localdomain |

**Issuer Name:**

| Country: XX |
| State/Province: There is no such thing outside US |
| Locality: Everywhere |
| Organization: OCOSA |
| Organization Unit: Office for Complication of Otherwise Simple Affairs |
| Common Name: ubuntu804-base.localdomain |
| Email Address: root@ubuntu804-base.localdomain |

**Serial Number:** 00 FA F9 3A 4C 7F B6 B9 CC

**Version:** 1

**Signature Algorithm:** SHA-1 With RSA Encryption

**Not Valid Before:** Mar 17 14:07:45 2010 GMT

**Not Valid After:** Apr 16 14:07:45 2010 GMT
Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 AD AE 97
00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
1E 84 4F BE D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 6B
83 6A 53 4A 9C 27 CB AD B4 89 8D 29 OC B2 3C 1B 5C 67 CC 53
A6 1E 30 D0 AA 26 7B 1E 4E 40 B9 29 01 6C 2E BC A2 19 94 7C
15 6E 8D 30 3B F6 CA 2E 75

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
None

Plugin Information:
Publication date: 2006/06/05, Modification date: 2012/05/03

Ports
tcp/25

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

Low Strength Ciphers (< 56-bit key)

SSLv2
EXP-RC2-CBC-MD5
Kx=RSA(512)  Au=RSA  Enc=RC2(40)  Mac=MD5  export
EXP-RC4-MD5
Kx=RSA(512)  Au=RSA  Enc=RC4(40)  Mac=MD5  export

SSLv3
EXP-ADH-DES-CBC-SHA
Kx=DH(512)  Au=None  Enc=DES(40)  Mac=SHA1  export
EXP-ADH-RC4-MD5
Kx=DH(512)  Au=None  Enc=RC4(40)  Mac=MD5  export
EXP-EDH-RSA-DES-CBC-SHA
Kx=DH(512)  Au=RSA  Enc=DES(40)  Mac=SHA1  export
EXP-DES-CBC-SHA
Kx=RSA(512)  Au=RSA  Enc=DES(40)  Mac=SHA1  export
EXP-RC2-CBC-MD5
Kx=RSA(512)  Au=RSA  Enc=RC2(40)  Mac=MD5  export
EXP-RC4-MD5
Kx=RSA(512)  Au=RSA  Enc=RC4(40)  Mac=MD5  export

TLSv1
EXP-EDH-RSA-DES-CBC-SHA
Kx=DH(512)  Au=RSA  Enc=DES(40)  Mac=SHA1  export
EXP-ADH-DES-CBC-SHA
Kx=DH(512)  Au=None  Enc=DES(40)  Mac=SHA1  export
EXP-ADH-RC4-MD5
Kx=DH(512)  Au=None  Enc=RC4(40)  Mac=MD5  export
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/Perfect_forward_secrecy

Solution
n/a

Risk Factor
None

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

Ports
tcp/25

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

Low Strength Ciphers (< 56-bit key)
SSLv3
EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export

TLSv1
EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export

Medium Strength Ciphers (>= 56-bit and < 112-bit key)
SSLv3
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES(56) Mac=SHA1

TLSv1
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES(56) Mac=SHA1

High Strength Ciphers (>= 112-bit key)
SSLv3
EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES(168) 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

The fields above are:
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: 2012/04/19

Ports
tcp/25

This port supports resuming SSLv3 sessions.

50845 - OpenSSL Detection

Synopsis
The remote service appears to use OpenSSL to encrypt traffic.

Description
Based on its behavior, 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: 2012/04/02

Ports
tcp/25 53/tcp

53/tcp

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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution
Protect your target with an IP filter.

**Risk Factor**

None

**Ports**
tcp/53

Port 53/tcp was found to be open

### 11002 - DNS Server Detection

**Synopsis**

A DNS server is listening on the remote host.

**Description**

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

**See Also**

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

**Solution**

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

**Risk Factor**

None

**Plugin Information:**

Publication date: 2003/02/13, Modification date: 2011/03/11

**Ports**
tcp/53

### 10028 - DNS Server BIND version Directive Remote Version Disclosure

**Synopsis**

It is possible to obtain the version number of the remote DNS server.

**Description**

The remote host is running BIND or another DNS server that reports its version number when it receives a special request, for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

**Solution**
It is possible to hide the version number of bind by using the 'version' directive in the 'options' section in named.conf.

### Risk Factor
None

### References
XREF
OSVDB:23

### Plugin Information:
Publication date: 1999/10/12, Modification date: 2011/05/24

### Ports
udp/53

The version of the remote DNS server is:

9.4.2

#### 35373 - DNS Server DNSSEC Aware Resolver

**Synopsis**
The remote DNS resolver is DNSSEC-aware.

**Description**
The remote DNS resolver accepts DNSSEC options. This means that it may verify the authenticity of DNSSEC protected zones if it is configured to trust their keys.

**Solution**
n/a

### Risk Factor
None

### Plugin Information:
Publication date: 2009/01/15, Modification date: 2012/07/26

### Ports
udp/53

#### 35371 - DNS Server hostname.bind Map Hostname Disclosure

**Synopsis**
The DNS server discloses the remote host name.

**Description**
It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

**Solution**
It may be possible to disable this feature. Consult the vendor's documentation for more information.

### Risk Factor
None

### Plugin Information:
Publication date: 2009/01/15, Modification date: 2011/09/14

### Ports
udp/53

The remote host name is:

metasploitable

#### 69/udp

**11819 - TFTP Daemon Detection**

**Synopsis**
A TFTP server is listening on the remote port.
Description
The remote host is running a TFTP (Trivial File Transfer Protocol) daemon. TFTP is often used by routers and
diskless hosts to retrieve their configuration. It is also used by worms to propagate.

Solution
Disable this service if you do not use it.

Risk Factor
None

Plugin Information:
Publication date: 2003/08/13, Modification date: 2011/03/17

Ports
udp/69
80/tcp

Synopsis
The remote web server contains a version of PHP that allows arbitrary code execution.

Description
The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-
line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code,
reveal PHP source code, cause a system crash, etc.

See Also
http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
http://www.php.net/archive/2012.php#id2012-05-08-1
http://www.php.net/ChangeLog-5.php#5.3.13
http://www.php.net/ChangeLog-5.php#5.4.3

Solution
Upgrade to PHP 5.3.13 / 5.4.3 or later.

Risk Factor
High

CVSS Base Score
8.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:P/A:P)

CVSS Temporal Score
6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:P/A:P)

References
BID 53388
CVE CVE-2012-1823
CVE CVE-2012-2311
XREF OSVDB:81633
XREF EDB-ID:18834
XREF CERT-VU:520827

Exploitable with
Metasploit (true)

Plugin Information:
Publication date: 2012/05/14, Modification date: 2012/06/23
### Ports

| tcp/80 |

Nessus was able to verify the issue exists using the following request:

```
--snip--
POST /phpMyAdmin/themes/original/layout.inc.php?-d+allow_url_include%3don+-d+safe_mode%3doff+-d
+suhosin.simulation%3don+-d+open_basedir%3doff+-d+auto_prepend_file%3dphp%3a//input+-n HTTP/1.1
Host: 192.168.56.3
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Content-Length: 82
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

<?php echo 'php_cgi_query_string_code_execution-1345090228'; system('id'); die; ?>
--snip--
```

### 36171 - phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)

#### Synopsis

The remote web server contains a PHP application that may allow execution of arbitrary code.

#### Description

The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user supplied input before using it to generate a config file for the application. This version has the following vulnerabilities:

- The setup script inserts the unsanitized verbose server name into a C-style comment during config file generation.
- An attacker can save arbitrary data to the generated config file by altering the value of the 'textconfig' parameter during a POST request to config.php.

An unauthenticated, remote attacker may be able to leverage these issues to execute arbitrary PHP code.

#### See Also


#### Solution

Upgrade to phpMyAdmin 3.1.3.2 or apply the patches referenced in the project's advisory.

#### Risk Factor

High

#### CVSS Base Score

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

#### CVSS Temporal Score

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

#### References

<table>
<thead>
<tr>
<th>BID</th>
<th>34526</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>CVE-2009-1285</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:53685</td>
</tr>
<tr>
<td>XREF</td>
<td>Secunia:34727</td>
</tr>
<tr>
<td>XREF</td>
<td>CWE:94</td>
</tr>
</tbody>
</table>

#### Plugin Information:

- Publication date: 2009/04/16, Modification date: 2012/04/03

### Ports

| tcp/80 |

#### 55976 - Apache HTTP Server Byte Range DoS

#### Synopsis
The web server running on the remote host is affected by a denial of service vulnerability.

**Description**

The version of Apache HTTP Server running on the remote host is affected by a denial of service vulnerability. Making a series of HTTP requests with overlapping ranges in the Range or Request-Range request headers can result in memory and CPU exhaustion. A remote, unauthenticated attacker could exploit this to make the system unresponsive. Exploit code is publicly available and attacks have reportedly been observed in the wild.

**See Also**


http://www.gossamer-threads.com/lists/apache/dev/401638

http://www.nessus.org/u?404627ec

http://httpd.apache.org/security/CVE-2011-3192.txt

http://www.nessus.org/u?1538124a

http://www-01.ibm.com/support/docview.wss?uid=swg24030863

**Solution**

Upgrade to Apache httpd 2.2.21 or later, or use one of the workarounds in Apache's advisories for CVE-2011-3192. Version 2.2.20 fixed the issue, but also introduced a regression.

If the host is running a web server based on Apache httpd, contact the vendor for a fix.

**Risk Factor**

High

**CVSS Base Score**

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

**CVSS Temporal Score**

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

**References**

BID 49303

CVE CVE-2011-3192

XREF OSVDB:74721

XREF CERT:405811

XREF EDB-ID:17696

XREF EDB-ID:18221

**Plugin Information:**

Publication date: 2011/08/25, Modification date: 2012/07/18

**Ports**

tcp/80

Nessus determined the server is unpatched and is not using any of the suggested workarounds by making the following requests:

```
-------------------- Testing for workarounds --------------------
HEAD /mutillidae/framer.html HTTP/1.1
Host: 192.168.56.3
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Request-Range: bytes=5-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
Range: bytes=5-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
```
The remote web server contains a PHP script that is prone to an information disclosure attack.

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including:

- The username of the user who installed php and if they are a SUDO user.
- The IP address of the host.
- The version of the operating system.
- The web server version.
- The root directory of the web server.
- Configuration information about the remote PHP installation.

Solution

Remove the affected file(s).

Risk Factor

Medium

CVSS Base Score


Plugin Information:

Publication date: 2003/02/12, Modification date: 2011/03/15

Ports

tcp/80

Nessus discovered the following URLs that call phpinfo():

11229 - Web Server info.php / phpinfo.php Detection

Synopsis

The remote web server contains a PHP script that is prone to an information disclosure attack.

Description

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including:

- The username of the user who installed php and if they are a SUDO user.
- The IP address of the host.
- The version of the operating system.
- The web server version.
- The root directory of the web server.
- Configuration information about the remote PHP installation.

Solution

Remove the affected file(s).

Risk Factor

Medium

CVSS Base Score


Plugin Information:

Publication date: 2003/02/12, Modification date: 2011/03/15

Ports

tcp/80

Nessus discovered the following URLs that call phpinfo():
http://192.168.56.3/phpinfo.php
http://192.168.56.3/mutillidae/phpinfo.php

### 11213 - HTTP TRACE / TRACK Methods Allowed

#### Synopsis
Debugging functions are enabled on the remote web server.

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

#### See Also
- http://www.apacheweek.com/issues/03-01-24
- http://www.kb.cert.org/vuls/id/288308
- http://www.kb.cert.org/vuls/id/867593
- http://download.oracle.com/sunalerts/1000718.1.html

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

#### Risk Factor
Medium

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

#### CVSS Temporal Score
3.9 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

#### References
- **BID**: 9506, 9561, 11604, 33374, 37995
- **CVE**: CVE-2003-1567, CVE-2004-2320, CVE-2010-0386
- **OSVDB**: OSVDB:877, OSVDB:3726, OSVDB:5648, OSVDB:50485
- **CWE**: CWE:16

#### Plugin Information:
Publication date: 2003/01/23, Modification date: 2012/04/04

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

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

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

Nessus sent the following TRACE request:

```
------------------------------ snip ------------------------------
TRACE /Nessus1667296966.html HTTP/1.1
Connection: Close
Host: 192.168.56.3
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*;utf-8
------------------------------ snip ------------------------------
```

and received the following response from the remote server:

```
------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Wed, 15 Aug 2012 07:57:25 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http

TRACE /Nessus1667296966.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.56.3
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*;utf-8
------------------------------ snip ------------------------------
```

### 46803 - PHP expose_php Information Disclosure

**Synopsis**

The configuration of PHP on the remote host allows disclosure of sensitive information.

**Description**

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such an URL triggers an Easter egg built into PHP itself. Other such Easter eggs likely exist, but Nessus has not checked for them.

**See Also**

- http://www.0php.com/php_easter_egg.php

**Solution**

In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

**Risk Factor**

Medium

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

References

XREF OSVDB:12184

Plugin Information:

Publication date: 2010/06/03, Modification date: 2011/03/14

Ports
tcp/80

Nessus was able to verify the issue using the following URL:

http://192.168.56.3/phpMyAdmin/themes/original/layout.inc.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000

10056 - /doc Directory Browsable

Synopsis

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

Description

The /doc directory is browsable. /doc shows the contents of the /usr/doc directory, which reveals not only which programs are installed but also their versions.

See Also

http://projects.webappsec.org/Directory-Indexing

Solution

Use access restrictions for the /doc directory.

If you use Apache you might use this in your access.conf:

  <Directory /usr/doc>
    AllowOverride None
    order deny,allow
    deny from all
    allow from localhost
  </Directory>

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID 318

CVE CVE-1999-0678

XREF OSVDB:48

Plugin Information:

Publication date: 2000/01/03, Modification date: 2011/03/17

Ports
tcp/80

36083 - phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)

Synopsis

The remote web server contains a PHP script that is affected by multiple issues.

Description

The version of phpMyAdmin installed on the remote host fails to sanitize user supplied input to the 'file_path' parameter of the 'bsDisp_as_mime_type.php' script before using it to read a file and reporting it in dynamically-generated HTML. An unauthenticated, remote attacker may be able to leverage this issue to read arbitrary files, possibly from third-party hosts, or to inject arbitrary HTTP headers in responses sent to third-party users.

Note that the application is also reportedly affected by several other issues, although Nessus has not actually checked for them.
### Solution
Upgrade to phpMyAdmin 3.1.3.1 or apply the patch referenced in the project's advisory.

### Risk Factor
Medium

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

### CVSS Temporal Score
4.1 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### References

<table>
<thead>
<tr>
<th>BID</th>
<th>34253</th>
</tr>
</thead>
<tbody>
<tr>
<td>XREF</td>
<td>OSVDB:53226</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:53227</td>
</tr>
<tr>
<td>XREF</td>
<td>Secunia:34468</td>
</tr>
</tbody>
</table>

### Plugin Information:
Publication date: 2009/04/03, Modification date: 2012/06/08

### Ports

tcp/80

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>51425</td>
<td>phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)</td>
</tr>
</tbody>
</table>

### Synopsis
The remote web server hosts a PHP script that is prone to a cross-site scripting attack.

### Description
The version of phpMyAdmin fails to validate BBcode tags in user input to the 'error' parameter of the 'error.php' script before using it to generate dynamic HTML.

An attacker may be able to leverage this issue to inject arbitrary HTML or script code into a user’s browser to be executed within the security context of the affected site. For example, this could be used to cause a page with arbitrary text and a link to an external site to be displayed.

### See Also

### Solution
Upgrade to phpMyAdmin 3.4.0-beta1 or later.

### Risk Factor
Medium

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

### CVSS Temporal Score
3.6 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

### References

<table>
<thead>
<tr>
<th>BID</th>
<th>45633</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>CVE-2010-4480</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:69684</td>
</tr>
<tr>
<td>XREF</td>
<td>EDB-ID:15699</td>
</tr>
</tbody>
</table>

### Plugin Information:
49142 - phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)

**Synopsis**
The remote web server contains a PHP application that has a cross-site scripting vulnerability.

**Description**
The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user supplied input to the 'verbose server name' field. A remote attacker could exploit this by tricking a user into executing arbitrary script code.

**See Also**

**Solution**
Upgrade to phpMyAdmin 3.3.7 or later.

**Risk Factor**
Medium

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

**References**
CVE: CVE-2010-3263
OSVDB: 67851

---

57792 - Apache HTTP Server httpOnly Cookie Information Disclosure

**Synopsis**
The web server running on the remote host has an information disclosure vulnerability.

**Description**
The version of Apache HTTP Server running on the remote host has an information disclosure vulnerability. Sending a request with HTTP headers long enough to exceed the server limit causes the web server to respond with an HTTP 400. By default, the offending HTTP header and value are displayed on the 400 error page. When used in conjunction with other attacks (e.g., cross-site scripting), this could result in the compromise of httpOnly cookies.

**See Also**
http://fd.the-wildcat.de/apache_e36a9cf46c.php
http://httpd.apache.org/security/vulnerabilities_22.html
http://svn.apache.org/viewvc?view=revision&revision=1235454

**Solution**
Upgrade to Apache version 2.2.22 or later.
**Risk Factor**

Medium

**CVSS Base Score**

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

**CVSS Temporal Score**

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

**STIG Severity**

I

**References**

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>BID</td>
<td>51706</td>
</tr>
<tr>
<td>CVE</td>
<td>CVE-2012-0053</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:78556</td>
</tr>
<tr>
<td>XREF</td>
<td>EDB-ID:18442</td>
</tr>
<tr>
<td>XREF</td>
<td>IAVA:2012-A-0017</td>
</tr>
</tbody>
</table>

**Plugin Information:**

Publication date: 2012/02/02, Modification date: 2012/05/22

**Ports**

tcp/80

Nessus verified this by sending a request with a long Cookie header:

```
GET / HTTP/1.1
Host: 192.168.56.3
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA ...
       z8=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA ...
        [[...]]
```

**26194 - Web Server Uses Plain Text Authentication Forms**

**Synopsis**

The remote web server might transmit credentials in cleartext.

**Description**

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

**Solution**

Make sure that every sensitive form transmits content over HTTPS.

**Risk Factor**

Low

**CVSS Base Score**

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

**References**

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>XREF</td>
<td>CWE:522</td>
</tr>
<tr>
<td>XREF</td>
<td>CWE:523</td>
</tr>
<tr>
<td>XREF</td>
<td>CWE:718</td>
</tr>
</tbody>
</table>
Plugin Information:
Publication date: 2007/09/28, Modification date: 2011/09/15

Ports
tcp/80

Page : /phpMyAdmin/
Destination page : index.php
Input name : pma_password

Page : /phpMyAdmin/?D=A
Destination page : index.php
Input name : pma_password

Page : /twiki/TWikiDocumentation.html
Destination page : http://TWiki.org/cgi-bin/passwd/TWiki/WebHome
Input name : oldpassword
Input name : password
Input name : passwordA

Page : /twiki/TWikiDocumentation.html
Destination page : http://TWiki.org/cgi-bin/passwd/Main/WebHome
Input name : password
Input name : passwordA

Page : /dvwa/login.php
Destination page : login.php
Input name : password

Page : /twiki/bin/view/TWiki/TWikiDocumentation
Destination page : http://192.168.56.3/twiki/bin/passwd/TWiki/WebHome
Input name : oldpassword
Input name : password
Input name : passwordA

Page : /twiki/bin/view/TWiki/TWikiUserAuthentication
Destination page : http://192.168.56.3/twiki/bin/passwd/TWiki/WebHome
Input name : oldpassword
Input name : password
Input name : passwordA

Page : /twiki/bin/view/TWiki/TWikiUserAuthentication
Destination page : http://192.168.56.3/twiki/bin/passwd/Main/WebHome
Input name : password
Input name : passwordA

Page : /twiki/bin/rdiff/TWiki/TWikiDocumentation
Destination page : http://192.168.56.3/twiki/bin/passwd/TWiki/WebHome
Input name : oldpassword
Input name : password
Input name : passwordA

Page : /twiki/bin/rdiff/TWiki/TWikiDocumentation
Destination page : http://192.168.56.3/twiki/bin/passwd/Main/WebHome
Input name : password
Input name : passwordA
### 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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

**Ports**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>80</td>
</tr>
</tbody>
</table>

Port 80/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: 2012/07/09

**Ports**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>80</td>
</tr>
</tbody>
</table>

A web server is running on this port.

### 11032 - Web Server Directory Enumeration

**Synopsis**

It is possible to enumerate directories on the web server.

**Description**

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

**See Also**

http://projects.webappsec.org/Predictable-Resource-Location
### Solution

n/a

### Risk Factor

None

### References

**XREF**

OWASP:OWASP-CM-006

### Plugin Information:

**Publication date:** 2002/06/26, **Modification date:** 2012/04/14

### Ports

**tcp/80**

The following directories were discovered:

/cgi-bin, /doc, /text, /icons, /phpMyAdmin, /twiki/bin

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

### 10662 - Web mirroring

#### Synopsis

Nessus crawled the remote web site.

#### Description

This script makes a mirror of the remote web site(s) and extracts the list of CGIs that are used by the remote host. It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

#### Solution

n/a

#### Risk Factor

None

### Plugin Information:

**Publication date:** 2001/05/04, **Modification date:** 2012/06/07

### Ports

**tcp/80**

The following CGI have been discovered:

Syntax : cginame (arguments [default value])

/twiki/bin/view/Sandbox/WebTopicEditTemplate (unlock [on] )
/twiki/bin/upload/TWiki/TWikiSystemRequirements (filename [ ] filepath [ ] filecomment [ ] createlink [ ] hidefile [ ] )
/twiki/bin/oops/TWiki/WebIndex (template [oopsmore] param2 [1.2] param1 [1.2] )
/twiki/bin/view/TWiki/TWikiAuthentication (unlock [on] )
/twiki/bin/edit/TWiki/ColaNahaboo (t [1345017127] )
/twiki/bin/upload/Sandbox/WebPreferences (filename [ ] filepath [ ] filecomment [ ] createlink [ ] hidefile [ ] )
/twiki/bin/view/TWiki/Know/TopicClassification (skin [print] topic [ ] rev [1.2] )
/twiki/bin/edit/Main/BookView (topicparent [Main.TWikiVariables] )
/twiki/bin/edit/TWiki/CrisBailiff (t [1345017128] )
/twiki/bin/edit/Codev/UnchangeableTopicBug (topicparent [TWiki.TWikiHistory] )
/twiki/bin/view/TWiki/TWikiCodevTWikiDocumentation (unlock [on] )
/twiki/bin/rdiff/Main/LondonOffice (rev2 [1.2] rev1 [1.3] )
/twiki/bin/attach/TWiki/PreviewBackground (revInfo [1] filename [blankltgraybg.gif] )
/twiki/bin/oops/Codev/UnchangeableTopicBug (template [oopsnewweb] )
/twiki/bin/rdiff/TWiki/TWikiAccesControl (rev2 [1.26] rev1 [1.27] )
/twiki/bin/edit/Sandbox/TestTopic1 (t [1345017219] topicparent [Sandbox.WebHome] )
/twiki/bin/view/TWiki/WebChangesNotify (unlock [on] )
/twiki/bin/preview/Sandbox/WebChanges (text [ ] fortemplate [ ] topicparent [ ] cmd [ ] )
/twiki/bin/oops/Main/SupportGroup (template [oopsmore] param1 [1.1] param2 [1.1] )
/twiki/bin/edit/TWiki/TWikiBetaUpgradeNotes (topicparent [TWiki.TWikiUpgradeTo01Dec2001] )
49704 - External URLs

**Synopsis**

Links to external sites were gathered.

**Description**

Nessus gathered HREF links to external sites by crawling the remote web server.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2010/10/04, Modification date: 2011/08/19

**Ports**

tcp/80

200 external URLs were gathered on this web server:

- URL... - Seen on...
  - http://TWiki.SourceForge.net/ - /twiki/bin/rdiff/Main/WebHome
  - http://TWiki.SourceForge.net/cgi-bin/view/Codev/AttachedNotificationLinksBug - /twiki/bin/rdiff/TWiki/TWikiHistory
  - http://TWiki.SourceForge.net/cgi-bin/view/Codev/AuthenticationBasedOnGroups - /twiki/bin/rdiff/TWiki/TWikiHistory
  - http://TWiki.SourceForge.net/cgi-bin/view/Codev/BetterTWikiTagTemplateProcessing - /twiki/bin/rdiff/TWiki/TWikiHistory
  - http://TWiki.SourceForge.net/cgi-bin/view/Codev/FeatureEnhancementRequest - /twiki/bin/rdiff/TWiki/TWikiEnhancementRequests
  - http://TWiki.SourceForge.net/cgi-bin/view/Codev/FeatureToDo - /twiki/bin/rdiff/TWiki/TWikiPlannedFeatures
  - http://TWiki.SourceForge.net/cgi-bin/view/Codev/FeatureUnderConstruction - /twiki/bin/rdiff/TWiki/TWikiPlannedFeatures
  - http://TWiki.SourceForge.net/cgi-bin/view/Codev/UppercaseAttachments - /twiki/bin/rdiff/TWiki/TWikiHistory
  - http://TWiki.SourceForge.net/cgi-bin/view/Main/PoweredByTWikiLogo - /twiki/bin/rdiff/TWiki/TWikiInstallationGuide
  - http://TWiki.org/cgi-bin/view/Main/MikeMannix - /twiki/TWikiDocumentation.html
  - http://TWiki.org/cgi-bin/view/Main/WebHome - /twiki/TWikiInstallation.html
  - http://TWiki.org/cgi-bin/view/TWiki/AdminSkillsAssumptions - /twiki/TWikiInstallation.html
  - http://TWiki.org/cgi-bin/view/TWiki/MikeMannix - /twiki/TWikiInstallation.html
  - http://TWiki.org/cgi-bin/view/TWiki/PeterThoeny - /twiki/TWikiInstallation.html
  - http://TWiki.org/ [...]

39463 - HTTP Server Cookies Set

**Synopsis**

Some cookies have been set by the web server.

**Description**

HTTP cookies are pieces of information that are presented by web servers and are sent back by the browser. As HTTP is a stateless protocol, cookies are a possible mechanism to keep track of sessions. This plugin displays the list of the HTTP cookies that were set by the web server when it was crawled.

**Solution**
Risk Factor

None

Plugin Information:

Publication date: 2009/06/19, Modification date: 2011/03/15

Ports

tcp/80

<table>
<thead>
<tr>
<th>path</th>
<th>/phpMyAdmin/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>pma_fontsize</td>
</tr>
<tr>
<td>value</td>
<td>82%25</td>
</tr>
<tr>
<td>version</td>
<td>1</td>
</tr>
<tr>
<td>expires</td>
<td>Fri, 14-Sep-2012 07:48:01 GMT</td>
</tr>
<tr>
<td>secure</td>
<td>0</td>
</tr>
<tr>
<td>httponly</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>path</th>
<th>/phpMyAdmin/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>pma_lang</td>
</tr>
<tr>
<td>value</td>
<td>en-utf-8</td>
</tr>
<tr>
<td>version</td>
<td>1</td>
</tr>
<tr>
<td>expires</td>
<td>Fri, 14-Sep-2012 07:48:00 GMT</td>
</tr>
<tr>
<td>secure</td>
<td>0</td>
</tr>
<tr>
<td>httponly</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>path</th>
<th>/phpMyAdmin/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>pma_charset</td>
</tr>
<tr>
<td>value</td>
<td>utf-8</td>
</tr>
<tr>
<td>version</td>
<td>1</td>
</tr>
<tr>
<td>expires</td>
<td>Fri, 14-Sep-2012 07:48:00 GMT</td>
</tr>
<tr>
<td>secure</td>
<td>0</td>
</tr>
<tr>
<td>httponly</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>path</th>
<th>/phpMyAdmin/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>phpMyAdmin</td>
</tr>
<tr>
<td>value</td>
<td>8d9a4c7fa47f7b2b41100c0cb66c781839b39ad2</td>
</tr>
<tr>
<td>version</td>
<td>1</td>
</tr>
<tr>
<td>secure</td>
<td>0</td>
</tr>
<tr>
<td>httponly</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>path</th>
<th>/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>security</td>
</tr>
<tr>
<td>value</td>
<td>high</td>
</tr>
<tr>
<td>version</td>
<td>1</td>
</tr>
<tr>
<td>secure</td>
<td>0</td>
</tr>
<tr>
<td>httponly</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>path</th>
<th>/phpMyAdmin/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>pma_collation_connection</td>
</tr>
<tr>
<td>value</td>
<td>deleted</td>
</tr>
<tr>
<td>version</td>
<td>1</td>
</tr>
<tr>
<td>expires</td>
<td>Tue, 16-Aug-2011 07:48:00 GMT</td>
</tr>
<tr>
<td>secure</td>
<td>0</td>
</tr>
<tr>
<td>httponly</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>path</th>
<th>/phpMyAdmin/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>pma_theme</td>
</tr>
<tr>
<td>value</td>
<td>deleted</td>
</tr>
<tr>
<td>version</td>
<td>1</td>
</tr>
<tr>
<td>expires</td>
<td>Tue, 16-Aug-2011 07:48:00 GMT</td>
</tr>
<tr>
<td>secure</td>
<td>0</td>
</tr>
<tr>
<td>httponly</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>path</th>
<th>/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>PHPSESSID</td>
</tr>
<tr>
<td>value</td>
<td>92fdabbf75ff71126c6daad9d9785d3f</td>
</tr>
<tr>
<td>version</td>
<td>1</td>
</tr>
<tr>
<td>secure</td>
<td>0</td>
</tr>
<tr>
<td>httponly</td>
<td>0</td>
</tr>
</tbody>
</table>

49705 - Gathered email Addresses
Synopsis
e-mail addresses were gathered.

Description
Nessus gathered mailto: HREF links and extracted e-mail addresses by crawling the remote web server.

Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2010/10/04, Modification date: 2012/05/09

Ports
tcp/80

The following e-mail addresses have been gathered:

- 'Peter@Thoeny.com', referenced from:
  /twiki/bin/view/Main/PeterThoeny
  /twiki/bin/rdiff/TWiki/TWikiDocumentation
  /twiki/bin/rdiff/Know/WebNotify
  /twiki/bin/rdiff/TWiki/PeterThoeny
  /twiki/bin/rdiff/Main/WebNotify
  /twiki/bin/view/TWiki/TWikiDocumentation
  /twiki/bin/rdiff/Sandbox/WebNotify
  /twiki/bin/rdiff/TWiki/TWikiFuncModule
  /twiki/bin/rdiff/TWikiDocumentation.html
  /twiki/bin/rdiff/TWiki/WebNotify
  /twiki/bin/rdiff/TWiki/TWikiPreferences
  /twiki/bin/view/TWiki/TWikiFuncModule
  /twiki/bin/rdiff/Main/PeterThoeny

- 'john.talintyre@drkw.com', referenced from:
  /twiki/bin/rdiff/Main/JohnTalintyre

- 'name@domain.com', referenced from:
  /twiki/bin/rdiff/TWiki/TextFormattingRules

- 'webmaster@your.company', referenced from:
  /twiki/bin/attach/TWiki/SiteMap
  /twiki/bin/edit/Main/EngineeringGroup
  /twiki/bin/rdiff/TWiki/TWikiAccessControl
  /twiki/bin/edit/TWiki/WEBTWikiTemplates
  /twiki/bin/view/Know/WebNotify
  /twiki/bin/rdiff/Sandbox/WebHome
  /twiki/bin/edit/TWiki/TWikiAlphaRelease
  /twiki/bin/view/TWiki/AdminSkillsAssumptions
  /twiki/bin/view/TWiki/WikiNotation
  /twiki/bin/edit/Sandbox/TestTopic7
  /twiki/bin/rdiff/TWiki/BookView
  /twiki/bin/edit/TWiki/TWikiRegistration
  /twiki/bin/view/TWiki/RandyKramer
  /twiki/bin/rdiff/Main/TWikiVariables
  /twiki/bin/view/TWiki/TemplateWeb
  /twiki/bin/view/Main/
  /twiki/bin/attach/TWiki/StandardColors
  /twiki/bin/view/Know/OperatingSystem
  /twiki/bin/view/TWiki/WikiWikiClones
  /twiki/bin/rdiff/TWiki/HiddenAttachment
  /twiki/bin/edit/TWiki/TWikiCodecFeatureToDo
  /twiki/bin/edit/Main/UnlockTopic
  /twiki/bin/view/Know
  /twiki/bin/view/Know/PublicFAQ
  /twiki/bin/view/TWiki/AlWilliams
  /twiki/bin/edit/TWiki/WebTopicEditTemplate
  /twiki/bin/view/Know/WebTopicList
  /twiki/bin/edit/TWiki/TWikiCourseOutlineExample
42057 - Web Server Allows Password Auto-Completion

Synopsis

Auto-complete is not disabled on password fields.

Description

The remote web server contains at least HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

None

Plugin Information:

Publication date: 2009/10/07, Modification date: 2011/09/28

Ports

tcp/80

Page: /twiki/TWikiDocumentation.html
Destination Page: http://TWiki.org/cgi-bin/passwd/TWiki/WebHome
Input name: oldpassword
Input name: password
Input name: passwordA

Page: /twiki/TWikiDocumentation.html
Destination Page: http://TWiki.org/cgi-bin/passwd/Main/WebHome
Input name: password
Input name: passwordA

Page: /twiki/bin/view/TWiki/TWikiDocumentation
Destination Page: http://192.168.56.3/twiki/bin/passwd/TWiki/WebHome
Input name: oldpassword
Input name: password
Input name: passwordA

Page: /twiki/bin/view/TWiki/TWikiUserAuthentication
Destination Page: http://192.168.56.3/twiki/bin/passwd/TWiki/WebHome
Input name: oldpassword
Input name: password
Input name: passwordA

Page: /twiki/bin/view/TWiki/TWikiUserAuthentication

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: 2012/08/02

Ports
tcp/80
The remote web server type is:

Apache/2.2.8 (Ubuntu) DAV/2

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

### 43111 - HTTP Methods Allowed (per directory)

**Synopsis**

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

**Description**

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' - in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

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

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2009/12/10, Modification date: 2011/07/08

**Ports**

tcp/80

Based on the response to an OPTIONS request:

- HTTP methods COPY DELETE GET HEAD LOCK MOVE OPTIONS POST PROPFIND PROPPATCH TRACE UNLOCK are allowed on:
  
  /dav

- HTTP methods GET HEAD OPTIONS POST TRACE are allowed on:
  
  /doc
  /davva/davva
  /davva/davva/images
  /icons
  /mutillidae/documentation
  /mutillidae/images
  /mutillidae/javascript
  /mutillidae/javascript/ddsomSmoothMenu
  /docs/TWiki
  /p/pub/TWiki/TWikiTemplates
  /p/pub/ico
  /phpMyAdmin/themes
  /phpMyAdmin/themes/original
  /phpMyAdmin/themes/original/css
  /phpMyAdmin/themes/original/img
  /rdiff/TWiki
  /test
  /test/testoutput
  /twiki
  /twiki/changes
  /twiki/pub
  /twiki/pub/Know/IncorrectDllVersionW32PTh10DLL
  /twiki/pub/TWiki/FileAttachment
  /twiki/pub/TWiki/PreviewBackground
  /twiki/pub/TWiki/TWiki
  /twiki/pub/TWiki/TWikiDocGraphics
  /twiki/pub/TWiki/TWikiLogos
  /twiki/pub/TWiki/TWikiPreferences
  /twiki/pub/TWiki/TWikiTemplates
  /twiki/pub/TWiki/WabiSabi
  /twiki/pub/TWiki/WebHome
24004 - WebDAV Directory Enumeration

Synopsis
Several directories on the remote host are DAV-enabled.

Description
WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server. If you do not use this extension, you should disable it.

Solution
Disable DAV support if you do not use it.

Risk Factor
None

Plugin Information:
Publication date: 2007/01/11, Modification date: 2011/03/14

Ports
tcp/80

The following directories are DAV enabled:
- /dav/

17219 - phpMyAdmin Detection

Synopsis
The remote web server contains a database management application written in PHP.

Description
The remote host is running phpMyAdmin, a web-based MySQL administration tool written in PHP.

See Also
http://www.phpmyadmin.net/home_page/index.php

Solution
Make sure the use of this program is in accordance with your corporate security policy.

Risk Factor
None

Plugin Information:
Publication date: 2005/02/25, Modification date: 2011/04/18

Ports
tcp/80

The following instance of phpMyAdmin was detected on the remote host:

Version : 3.1.1
URL : http://192.168.56.3/phpMyAdmin/

11419 - Web Server Office File Inventory

Synopsis
The remote web server hosts office-related files.

Description
This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution
Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

**Risk Factor**
None

**Plugin Information:**
Publication date: 2003/03/19, Modification date: 2011/12/28

**Ports**
tcp/80

The following office-related files are available on the remote server:

- Adobe Acrobat files (.pdf):
  /mutillidae/documentation/mutillidae-installation-on-xampp-win7.pdf

**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/80

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

Date: Wed, 15 Aug 2012 07:57:17 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

**11424 - WebDAV Detection**

**Synopsis**
The remote server is running with WebDAV enabled.

**Description**
WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.
If you do not use this extension, you should disable it.

**Solution**

**Risk Factor**
### 40984 - Browsable Web Directories

**Synopsis**

Some directories on the remote web server are browsable.

**Description**

Miscellaneous Nessus plugins identified directories on this web server that are browsable.

**See Also**

http://projects.webappsec.org/Directory-Indexing

**Solution**

Make sure that browseable directories do not leak confidential informative or give access to sensitive resources. And use access restrictions or disable directory indexing for any that do.

**Risk Factor**

None

---

### 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
### 111/tcp

**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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

### Ports

tcp/111

Port 111/tcp was found to be open

**Synopsis**

An ONC RPC portmapper is running on the remote host.

**Description**

The RPC portmapper is running on this port.
The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

**Solution**

n/a

**Risk Factor**

None

### Plugin Information:

Publication date: 2009/06/25, Modification date: 2012/02/02

### Ports

tcp/80

Give Nessus credentials to perform local checks.

**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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

### Ports

tcp/111

**53335 - RPC portmapper (TCP)**

**Synopsis**

An ONC RPC portmapper is running on the remote host.

**Description**

The RPC portmapper is running on this port.
The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

**Solution**

n/a

**Risk Factor**

None

### Plugin Information:

Publication date: 2011/04/08, Modification date: 2011/08/29

### Ports

tcp/111

**11111 - RPC Services Enumeration**

**Synopsis**

An ONC RPC service is running on the remote host.

**Description**

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

**Solution**

n/a

**Risk Factor**

None

### Plugin Information:
Portmapper is running on TCP port 111.

**Synopsis**
An ONC RPC portmapper is running on the remote host.

**Description**
The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

**Solution**
n/a

**Risk Factor**
None

**References**
CVE
CVE-1999-0632

---

RPC Services Enumeration is available on UDP port 111.

**Synopsis**
An ONC RPC service is running on the remote host.

**Description**
By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

**Solution**
n/a

**Risk Factor**
None

---

NetBIOS SMB Remote Host Information Disclosure is available on UDP port 137.

**Synopsis**
It is possible to obtain the network name of the remote host.

**Description**
The remote host listens on UDP port 137 or TCP port 445 and replies to NetBIOS nbtscan or SMB requests.
Note that this plugin gathers information to be used in other plugins but does not itself generate a report.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 1999/10/12, Modification date: 2012/02/10

**Ports**

udp/137

The following 7 NetBIOS names have been gathered:

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

This SMB server seems to be a SAMBA server (MAC address is NULL).

**139/tcp**

**11011 - Microsoft Windows SMB Service Detection**

**Synopsis**

A file / print sharing service is listening on the remote host.

**Description**

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2002/06/05, Modification date: 2012/01/31

**Ports**

tcp/139

An SMB server is running on this port.

**11219 - Nessus SYN scanner**

**Synopsis**

It is possible to determine which TCP ports are open.

**Description**

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

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

**Ports**

tcp/139
### 25216 - Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow

**Synopsis**

It is possible to execute code on the remote host through Samba.

**Description**

The version of the Samba server installed on the remote host is affected by multiple heap overflow vulnerabilities, which can be exploited remotely to execute code with the privileges of the Samba daemon.

**See Also**


**Solution**

Upgrade to Samba version 3.0.25 or later.

**Risk Factor**

Critical

**CVSS Base Score**

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

**References**

<table>
<thead>
<tr>
<th>BID</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>23973</td>
<td></td>
</tr>
<tr>
<td>24195</td>
<td></td>
</tr>
<tr>
<td>24196</td>
<td></td>
</tr>
<tr>
<td>24197</td>
<td></td>
</tr>
<tr>
<td>24198</td>
<td></td>
</tr>
<tr>
<td>CVE</td>
<td>CVE-2007-2446</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:34699</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:34731</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:34732</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:34733</td>
</tr>
</tbody>
</table>

**Exploitable with**

- CANVAS (true)
- Metasploit (true)

**Plugin Information:**

Publication date: 2007/05/15, Modification date: 2011/04/13

### 42411 - Microsoft Windows SMB Shares Unprivileged Access

**Synopsis**

It is possible to access a network share.

**Description**

The remote has one or more Windows shares that can be accessed through the network with the given credentials. Depending on the share rights, it may allow an attacker to read/write confidential data.

**Solution**

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

**Risk Factor**
### 57608 - SMB Signing Disabled

**Synopsis**

Signing is disabled on the remote SMB server.

**Description**

Signing is disabled on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

**See Also**

http://support.microsoft.com/kb/887429

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

http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

**Solution**

Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

**Risk Factor**

Medium

**CVSS Base Score**

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

**Plugin Information:**

Publication date: 2012/01/19, Modification date: 2012/03/05

**Ports**

- tcp/445
- 11011 - Microsoft Windows SMB Service Detection
A file / print sharing service is listening on the remote host.

**Description**

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2002/06/05, Modification date: 2012/01/31

**Ports**

tcp/445

A CIFS server is running on this port.

### 25240 - Samba Server Detection

**Synopsis**

An SMB server is running on the remote host.

**Description**

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

**See Also**

http://www.samba.org/

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2007/05/16, Modification date: 2011/09/14

**Ports**

tcp/445

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

**Synopsis**

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

**Description**

It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2001/10/17, Modification date: 2011/03/17

**Ports**

tcp/445

The remote Operating System is : Unix
The remote native lan manager is : Samba 3.0.20-Debian
The remote SMB Domain Name is : METASPLOITABLE

### 10394 - Microsoft Windows SMB Log In Possible

**Synopsis**
It is possible to log into the remote host.

**Description**

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

**See Also**

http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP

http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

**Solution**

n/a

**Risk Factor**

None

**Exploitable with**

Metasploit (true)

**Plugin Information:**

Publication date: 2000/05/09, Modification date: 2012/03/06

**Ports**

<table>
<thead>
<tr>
<th>tcp/445</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 445/tcp was found to be open</td>
</tr>
</tbody>
</table>

**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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

**Ports**

<table>
<thead>
<tr>
<th>tcp/445</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 445/tcp was found to be open</td>
</tr>
</tbody>
</table>

**10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure**

**Synopsis**

It is possible to obtain network information.

**Description**

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

**Solution**

n/a

**Risk Factor**

None

**References**
XREF

Plugin Information:
Publication date: 2000/05/09, Modification date: 2011/09/14

Ports
tcp/445

Here is the browse list of the remote host:

METASPLOITABLE ( os : 0.0 )

60119 - Microsoft Windows SMB Share Permissions Enumeration

Synopsis
It is possible to enumerate the permissions of remote network shares.

Description
By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2012/07/25, Modification date: 2012/07/25

Ports
tcp/445

Share path : \METASPLOITABLE\print$
Local path : C:\var\lib\samba\printers
Comment : Printer Drivers

Share path : \METASPLOITABLE\tmp
Local path : C:\tmp
Comment : oh noes!

Share path : \METASPLOITABLE\opt
Local path : C:\tmp

Share path : \METASPLOITABLE\IPC$
Local path : C:\tmp
Comment : IPC Service (metasploitable server (Samba 3.0.20-Debian))

Share path : \METASPLOITABLE\ADMIN$
Local path : C:\tmp
Comment : IPC Service (metasploitable server (Samba 3.0.20-Debian))

17651 - Microsoft Windows SMB : Obtains the Password Policy

Synopsis
It is possible to retrieve the remote host's password policy using the supplied credentials.

Description
Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution
n/a

Risk Factor
The following password policy is defined on the remote host:

- Minimum password len: 5
- Password history len: 0
- Maximum password age (d): No limit
- Password must meet complexity requirements: Disabled
- Minimum password age (d): 0
- Forced logoff time (s): Not set
- Locked account time (s): 1800
- Time between failed logon (s): 1800
- Number of invalid logon before locked out (s): 0

**10395 - Microsoft Windows SMB Shares Enumeration**

**Synopsis**

It is possible to enumerate remote network shares.

**Description**

By connecting to the remote host, Nessus was able to enumerate the network share names.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2000/05/09, Modification date: 2012/07/09

**Ports**

tcp/445

Here are the SMB shares available on the remote host when logged as a NULL session:

- print$
- tmp
- opt
- IPC$
- ADMIN$

**10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration**

**Synopsis**

It is possible to obtain the host SID for the remote host.

**Description**

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).

The host SID can then be used to get the list of local users.

**See Also**


**Solution**

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

**Risk Factor**

None

**Plugin Information:**

Publication date: 2002/02/13, Modification date: 2011/09/15
The remote host SID value is:
1-5-21-1042354039-2475377354-766472396

The value of 'RestrictAnonymous' setting is: unknown

10860 - SMB Use Host SID to Enumerate Local Users

Synopsis
It is possible to enumerate local users.

Description
Using the host security identifier (SID), it is possible to enumerate local users on the remote Windows system.

Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2002/02/13, Modification date: 2011/09/15

Ports
tcp/445

- Administrator (id 500, Administrator account)
- nobody (id 501, Guest account)
- root (id 1000)
- root (id 1001)
- daemon (id 1002)
- daemon (id 1003)
- bin (id 1004)
- bin (id 1005)
- sys (id 1006)
- sys (id 1007)
- sync (id 1008)
- adm (id 1009)
- games (id 1010)
- tty (id 1011)
- man (id 1012)
- disk (id 1013)
- lp (id 1014)
- lp (id 1015)
- mail (id 1016)
- mail (id 1017)
- news (id 1018)
- news (id 1019)
- uucp (id 1020)
- uucp (id 1021)
- man (id 1025)
- proxy (id 1026)
- proxy (id 1027)
- kmem (id 1031)
- dialout (id 1041)
- fax (id 1043)
- voice (id 1045)
- cdrom (id 1049)
- floppy (id 1051)
- tape (id 1053)
- sudo (id 1055)
- audio (id 1059)
- dip (id 1061)
- www-data (id 1066)
- www-data (id 1067)
- backup (id 1068)
- backup (id 1069)
- operator (id 1075)
- list (id 1076)
Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

### 512/tcp

#### 10203 - rexec Service Detection

**Synopsis**

The rexec service is listening on the remote port.

**Description**

The rexec service is open. This service is design to allow users of a network to execute commands remotely. However, rexec does not provide any good means of authentication, so it may be abused by an attacker to scan a third party host.

**Solution**

Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

**Risk Factor**

Medium

**CVSS Base Score**

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

**References**

<table>
<thead>
<tr>
<th><strong>CVE</strong></th>
<th>CVE-1999-0618</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>XREF</strong></td>
<td>OSVDB:9721</td>
</tr>
</tbody>
</table>

**Plugin Information:**

Publication date: 1999/08/31, Modification date: 2011/03/11

**Ports**

tcp/512

#### 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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

**Ports**
**10205 - rlogin Service Detection**

**Synopsis**
The rlogin service is listening on the remote port.

**Description**
The remote host is running the 'rlogin' service. This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the rlogin client and the rlogin server. This includes logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files. You should disable this service and use ssh instead.

**Solution**
Comment out the 'login' line in /etc/inetd.conf

**Risk Factor**
High

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

**References**
- CVE: CVE-1999-0651
- XREF: OSVDB:193

**Plugin Information:**
Publication date: 1999/08/30, Modification date: 2011/04/01

**Ports**
tcp/513

**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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**
Protect your target with an IP filter.

**Risk Factor**
None

**Ports**
tcp/513

**Note:**
Port 513/tcp was found to be open.
It shall be reasonably quick even against a firewalled target. Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

**Ports**

tcp/514

Port 514/tcp was found to be open

**11154 - Unknown Service Detection: Banner Retrieval**

**Synopsis**

There is an unknown service running on the remote host.

**Description**

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2002/11/18, Modification date: 2012/06/22

**Ports**

tcp/514

If you know what this service is and think the banner could be used to identify it, please send a description of the service along with the following output to svc-signatures@nessus.org:

```
Port   : 514
Type   : spontaneous
Banner :
0x00:  01 67 65 6E 61 6D 65 69 6E 66 6F 3A 20 54 65    .getnameinfo: Te
0x10:  6D 70 6F 72 61 72 79 20 66 61 69 6C 75 72 65 20    mporary failure
0x20:  69 6E 20 6E 61 6D 65 20 72 65 73 6F 6C 75 74 69    in name resoluti
0x30:  6F 6E 0A                                           on.
```

**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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

**Ports**

tcp/1099
### 22227 - RMI Registry Detection

**Synopsis**
An RMI registry is listening on the remote host.

**Description**
The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

**See Also**
- [http://java.sun.com/j2se/1.5.0/docs/guide/rmi/spec/rmiTOC.html](http://java.sun.com/j2se/1.5.0/docs/guide/rmi/spec/rmiTOC.html)
- [http://java.sun.com/j2se/1.5.0/docs/guide/rmi/spec/rmi-protocol3.html](http://java.sun.com/j2se/1.5.0/docs/guide/rmi/spec/rmi-protocol3.html)

**Solution**

n/a

**Risk Factor**
None

**Plugin Information:**
- Publication date: 2006/08/16, Modification date: 2011/03/11

**Ports**
tcp/1099

The remote RMI registry currently does not have information about any objects.

### 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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**
Protect your target with an IP filter.

**Risk Factor**
None

**Ports**
tcp/1524

Port 1524/tcp was found to be open

### 11154 - Unknown Service Detection: Banner Retrieval

**Synopsis**
There is an unknown service running on the remote host.

**Description**
Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

**Solution**

n/a

**Risk Factor**
None

**Plugin Information:**
Ports
tcp/1524

If you know what this service is and think the banner could be used to identify it, please send a description of the service along with the following output to svc-signatures@nessus.org:

Port : 1524
Type : spontaneous
Banner :
0x00:  72 6F 6F 74 40 6D 65 74 61 73 70 6C 6F 69 74 61
c9 40 6D 65 74 61 73 70 6C 6F 69 74 61 62 6C 65 3A
c9 2F 23 root@metasploita ble:/#

2049/tcp
42256 - NFS Shares World Readable

Synopsis
The remote NFS server exports world readable shares.

Description
The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

See Also
http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

Solution
Place the appropriate restrictions on all NFS shares.

Risk Factor
Medium

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

References
XREF OSVDB:339

Plugin Information:
Publication date: 2009/10/26, Modification date: 2011/03/21

Ports
tcp/2049

The following shares have no access restrictions:
/ *

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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution
Protect your target with an IP filter.

Risk Factor
None
Port 2049/tcp was found to be open.

### 11111 - RPC Services Enumeration

#### Synopsis

An ONC RPC service is running on the remote host.

#### Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

#### Solution

n/a

#### Risk Factor

None

#### Plugin Information:

Publication date: 2002/08/24, Modification date: 2011/05/24

The following RPC services are available on TCP port 2049:

- program: 100003 (nfs), version: 2
- program: 100003 (nfs), version: 3
- program: 100003 (nfs), version: 4

### 10437 - NFS Share Export List

#### Synopsis

The remote NFS server exports a list of shares.

#### Description

This plugin retrieves the list of NFS exported shares.

#### See Also

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

#### Solution

Ensure each share is intended to be exported.

#### Risk Factor

None

#### Plugin Information:

Publication date: 2000/06/07, Modification date: 2011/05/24

Here is the export list of 192.168.56.3:

/ *

### 2049/udp

11356 - NFS Exported Share Information Disclosure

#### Synopsis

It is possible to access NFS shares on the remote host.

#### Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

#### Solution
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

### Risk Factor
Medium

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

### References

<table>
<thead>
<tr>
<th>Type</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>CVE-1999-0170</td>
</tr>
<tr>
<td>CVE</td>
<td>CVE-1999-0211</td>
</tr>
<tr>
<td>CVE</td>
<td>CVE-1999-0554</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:339</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:8750</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:11516</td>
</tr>
</tbody>
</table>

### Plugin Information:
Publication date: 2003/03/12, Modification date: 2011/05/24

### Ports

**udp/2049**

The following NFS shares could be mounted:

```
+ /  
  + Contents of / :  
  - initrd  
  - media  
  - bin  
  - lost+found  
  - mnt  
  - sbin  
  - initrd.img  
  - home  
  - lib  
  - usr  
  - proc  
  - root  
  - sys  
  - boot  
  - nohup.out  
  - etc  
  - dev  
  - ..  
  - vmlinuz  
  - opt  
  - var  
  - cdrom  
  - tmp  
  - .  
  - srv
```

### 11111 - RPC Services Enumeration

#### Synopsis
An ONC RPC service is running on the remote host.

#### Description
By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

#### Solution
<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>None</th>
</tr>
</thead>
</table>

**Plugin Information:**
Publication date: 2002/08/24, Modification date: 2011/05/24

**Ports**

**udp/2049**

The following RPC services are available on UDP port 2049:
- program: 100003 (nfs), version: 2
- program: 100003 (nfs), version: 3
- program: 100003 (nfs), version: 4

**2121/tcp**

### 34324 - FTP Supports Clear Text Authentication

**Synopsis**
Authentication credentials might be intercepted.

**Description**
The remote FTP server allows the user's name and password to be transmitted in clear text, which could be intercepted by a network sniffer or a man-in-the-middle attack.

**Solution**
Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.

**Risk Factor**
Low

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

**References**
- XREF CWE:522
- XREF CWE:523

**Plugin Information:**
Publication date: 2008/10/01, Modification date: 2012/02/22

**Ports**

**tcp/2121**

This FTP server does not support 'AUTH TLS'.

### 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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**
Protect your target with an IP filter.

**Risk Factor**
None
Port 2121/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: 2012/07/09

### 10092 - FTP Server Detection

**Synopsis**
An FTP server is listening on this port.

**Description**
It is possible to obtain the banner of the remote FTP server by connecting to the remote port.

**Solution**
N/A

**Risk Factor**
None

**Plugin Information:**
Publication date: 1999/10/12, Modification date: 2011/03/15

### 39519 - Backported Security Patch Detection (FTP)

**Synopsis**
Security patches are backported.

**Description**
Security patches may have been 'backported' to the remote FTP 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

---

The remote FTP banner is:

```
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.56.3]
```
### 10481 - MySQL Unpassworded Account Check

**Synopsis**

The remote database server can be accessed without a password.

**Description**

It is possible to connect to the remote MySQL database server using an unpassworded account. This may allow an attacker to launch further attacks against the database.

**See Also**


**Solution**

Disable or set a password for the affected account.

**Risk Factor**

High

**CVSS Base Score**

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

**CVSS Temporal Score**

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

**References**

- BID: 11704
- CVE: CVE-2002-1809
- CVE: CVE-2004-1532
- XREF: OSVDB:380
- XREF: OSVDB:16026
It shall be reasonably quick even against a firewalled target. Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Ports

- **tcp/3306**: Port 3306/tcp was found to be open

#### 11153 - Service Detection (HELP Request)

**Synopsis**

The remote service could be identified.

**Description**

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a "HELP" request.

**Solution**

n/a

**Risk Factor**

None

#### Plugin Information:

- Publication date: 2002/11/18, Modification date: 2012/06/29

### Ports

- **tcp/3306**: A MySQL server is running on this port.

#### 10719 - MySQL Server Detection

**Synopsis**

A database server is listening on the remote port.

**Description**

The remote host is running MySQL, an open-source database server.

**Solution**

n/a

**Risk Factor**

None

#### Plugin Information:

- Publication date: 2001/08/13, Modification date: 2011/09/14

### Ports

- **tcp/3306**: Version: 5.0.51a-3ubuntu5, Protocol: 10, Server Status: SERVER_STATUS_AUTOCOMMIT, Server Capabilities: CLIENT_LONG_FLAG (Get all column flags), CLIENT_CONNECT_WITH_DB (One can specify db on connect), CLIENT_COMPRESS (Can use compression protocol), CLIENT_PROTOCOL_41 (New 4.1 protocol), CLIENT_SSL (Switch to SSL after handshake), CLIENT_TRANSACTIONS (Client knows about transactions), CLIENT_SECURE_CONNECTION (New 4.1 authentication)

### 3632/tcp
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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might
kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is
loaded.

Solution
Protect your target with an IP filter.

Risk Factor
None

Ports
tcp/3632
Port 3632/tcp was found to be open

tcp/5432
Port 5432/tcp was found to be open

5432/tcp

26024 - PostgreSQL Server Detection

Synopsis
A database service is listening on the remote host.

Description
The remote service is a PostgreSQL database server, or a derivative such as EnterpriseDB.

See Also
http://www.postgresql.org/

Solution
Limit incoming traffic to this port if desired.

Risk Factor
None

Plugin Information:
Publication date: 2007/09/14, Modification date: 2011/03/11

Ports
tcp/5432

5900/tcp
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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution
Protect your target with an IP filter.

Risk Factor
None

Ports
tcp/5900

Port 5900/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: 2012/07/09

Ports
tcp/5900

A vnc server is running on this port.

10342 - VNC Software Detection

Synopsis
The remote host is running a remote display software (VNC).

Description
The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) protocol to provide remote access to graphical user interfaces and thus permits a console on the remote host to be displayed on another.

See Also
http://en.wikipedia.org/wiki/Vnc

Solution
Make sure use of this software is done in accordance with your organization's security policy and filter incoming traffic to this port.

Risk Factor
None

Plugin Information:
Publication date: 2000/03/07, Modification date: 2011/04/01

Ports
tcp/5900
The highest RFB protocol version supported by the server is : 3.3

19288 - VNC Server Security Type Detection

Synopsis
A VNC server is running on the remote host.

Description
This script checks the remote VNC server protocol version and the available 'security types'.

Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2005/07/22, Modification date: 2011/12/06

Ports
tcp/5900

The remote VNC server chose security type #2 (VNC authentication)

6000/tcp

10407 - X Server Detection

Synopsis
An X11 server is listening on the remote host

Description
The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.
Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Solution
Restrict access to this port. If the X11 client/server facility is not used, disable TCP entirely.

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: 2000/05/12, Modification date: 2011/03/11

Ports
tcp/6000

X11 Version : 11.0

11219 - Nessus SYN scanner

Synopsis
It is possible to determine which TCP ports are open.

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

Solution
Protect your target with an IP filter.
**Risk Factor**

None

**Ports**

* tcp/6000

Port 6000/tcp was found to be open

**6667/tcp**

**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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

**Ports**

* tcp/6667

Port 6667/tcp was found to be open

**17975 - Service Detection (GET request)**

**Synopsis**

The remote service could be identified.

**Description**

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

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2005/04/06, Modification date: 2012/07/24

**Ports**

* tcp/6667

An IRC daemon is listening on this port.
### Ports

**tcp/6697**

- **Port 6697/tcp was found to be open**

#### 17975 - Service Detection (GET request)

**Synopsis**

The remote service could be identified.

**Description**

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

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2005/04/06, Modification date: 2012/07/24

---

**Ports**

**tcp/6697**

An IRC daemon is listening on this port.

---

**Ports**

**tcp/8009**

- **Port 8009/tcp was found to be open**

#### 8009/tcp

**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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

---

**Ports**

**tcp/8009**

- **Port 8009/tcp was found to be open**

#### 21186 - AJP Connector Detection

**Synopsis**

There is an AJP connector listening on the remote host.

**Description**

The remote host is running an AJP (Apache JServ Protocol) connector, a service by which a standalone web server such as Apache communicates over TCP with a Java servlet container such as Tomcat.

**See Also**


**Solution**

n/a

**Risk Factor**

None
### 34850 - Web Server Uses Basic Authentication Without HTTPS

#### Synopsis
The remote web server seems to transmit credentials in clear text.

#### Description
The remote web server contains web pages that are protected by 'Basic' authentication over plain text.
An attacker eavesdropping the traffic might obtain logins and passwords of valid users.

#### Solution
Make sure that HTTP authentication is transmitted over HTTPS.

#### Risk Factor
Low

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

---

### 26194 - Web Server Uses Plain Text Authentication Forms

#### Synopsis
The remote web server might transmit credentials in cleartext.

#### Description
The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.
An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

#### Solution
Make sure that every sensitive form transmits content over HTTPS.

#### Risk Factor
Low

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

---

### References

<table>
<thead>
<tr>
<th>Reference</th>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>XREF</td>
<td>522</td>
</tr>
<tr>
<td>XREF</td>
<td>523</td>
</tr>
<tr>
<td>XREF</td>
<td>718</td>
</tr>
</tbody>
</table>
### 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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

**Ports**

**tcp/8180**

- Port 8180/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

---

### 11422 - Web Server Unconfigured - Default Install Page Present

**Synopsis**

The remote web server is not configured or is not properly configured.

**Description**

The remote web server uses its default welcome page. It probably means that this server is not used at all or is serving content that is meant to be hidden.

**Solution**

Disable this service if you do not use it.
### 11032 - Web Server Directory Enumeration

#### Synopsis

It is possible to enumerate directories on the remote web server.

#### Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

#### See Also

http://projects.webappsec.org/Predictable-Resource-Location

#### Solution

n/a

#### Risk Factor

None

#### References

XREF OWASP:OWASP-CM-006

#### Plugin Information:

Publication date: 2002/06/26, Modification date: 2012/04/14

#### Ports

tcp/8180

The following directories were discovered:
/admin, /jsp-examples, /servlets-examples

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards.

The following directories require authentication:
/host-manager/html, /manager/html

### 10662 - Web mirroring

#### Synopsis

Nessus crawled the remote web site.

#### Description

This script makes a mirror of the remote web site(s) and extracts the list of CGIs that are used by the remote host. It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

#### Solution

n/a

#### Risk Factor

None

#### Plugin Information:

Publication date: 2001/05/04, Modification date: 2012/06/07
Ports
tcp/8180

The following CGI have been discovered:

Syntax: cginame (arguments [default value])

/jsp-examples/error/err.jsp (name [infiniti] submit [Submit])
/jsp-examples/jsp2/el/implicit-objects.jsp (foo [bar])
/admin/j_security_check;jsessionid=7D67332B1F9E09E36034C53277903FD2 (j_username [] j_password [])
/servlets-examples/servlet/SessionExample (dataname [foo] datavalue [bar])
/jsp-examples/jsp2/el/functions.jsp (foo [JSP+2.0])
/jsp-examples/num/numguess.jsp (guess [])
/jsp-examples/colors/colrs.jsp (action [Submit] action [Hint])
/jsp-examples/cal/cal.jsp (name [] email [] action [Submit])
/jsp-examples/sessions/carts.jsp (item [] submit [add] submit [remove])
/servlets-examples/servlet/SessionExample;jsessionid=D57E0D62FC5D04F537A8A955FF5DB393 (dataname [])
/servlets-examples/servlet/RequestParamExample (firstname [] lastname [])

49704 - External URLs

Synopsis
Links to external sites were gathered.

Description
Nessus gathered HREF links to external sites by crawling the remote web server.

Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2010/10/04, Modification date: 2011/08/19

Ports
tcp/8180

1 external URL was gathered on this web server:
URL... - Seen on...

irc://irc.freenode.net/ - /

39463 - HTTP Server Cookies Set

Synopsis
Some cookies have been set by the web server.

Description
HTTP cookies are pieces of information that are presented by web servers and are sent back by the browser.
As HTTP is a stateless protocol, cookies are a possible mechanism to keep track of sessions.
This plugin displays the list of the HTTP cookies that were set by the web server when it was crawled.

Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2009/06/19, Modification date: 2011/03/15

Ports
tcp/8180
This cookie was set by Tomcat (servlet/jsp engine):
path    = /servlets-examples
name    = JSESSIONID
value   = D57E0D62FC5D04F537A8A955FF5DB393
version = 1
secure  = 0
httponly = 0

This cookie was set by Tomcat (servlet/jsp engine):
path    = /jsp-examples
name    = JSESSIONID
value   = 41BF97DBAB77D119E3DABB0945C79B5
version = 1
secure  = 0
httponly = 0

This cookie was set by Tomcat (servlet/jsp engine):
path    = /admin
name    = JSESSIONID
value   = 7D67332B1F9E09E36034C53277903FD2
version = 1
secure  = 0
httponly = 0

49705 - Gathered email Addresses

Synopsis
description was gathered.

Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2010/10/04, Modification date: 2012/05/09

Ports
tcp/8180

The following email addresses have been gathered:

- 'users@tomcat.apache.org', referenced from:
  /tomcat-docs/architecture/index.html
  /tomcat-docs/architecture/printer/
  /tomcat-docs/architecture/printer/index.html

- 'yoavs@apache.org', referenced from:
  /tomcat-docs/appdev/
  /tomcat-docs/appdev/printer/
  /tomcat-docs/appdev/printer/index.html

- 'craigmcc@apache.org', referenced from:
  /tomcat-docs/architecture/printer/index.html
  /tomcat-docs/architecture/
  /tomcat-docs/architecture/printer/
  /tomcat-docs/architecture/index.html

- 'fhanik@apache.org', referenced from:
  /tomcat-docs/architecture/printer/index.html
  /tomcat-docs/architecture/
  /tomcat-docs/architecture/printer/

- 'jfarcand@apache.org', referenced from:
  /tomcat-docs/architecture/
  /tomcat-docs/architecture/printer/index.html
### 40665 - Protected Web Page Detection

**Synopsis**

Some web pages require authentication.

**Description**

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available:

- Basic is the simplest but the credentials are sent in clear text.
- NTLM provides an SSO in MS environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.
- Digest is a cryptographically strong scheme. Credentials are never sent in clear text. They may still be cracked by a dictionary attack though.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2009/08/21, Modification date: 2011/03/15

**Ports**

tcp/8180

The following pages are protected by the Basic authentication scheme:

- /manager/html
- /host-manager/html
- /manager/status

### 42057 - Web Server Allows Password Auto-Completion

**Synopsis**

Auto-complete is not disabled on password fields.

**Description**

The remote web server contains at least HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.

**Solution**

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

**Risk Factor**

None

**Plugin Information:**

Publication date: 2009/10/07, Modification date: 2011/09/28

**Ports**

tcp/8180

Page: /admin/
Destination Page: j_security_check;jsessionid=7D67332B1F9E09E36034C53277903FD2
Input name: j_password
### 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: 2012/08/02

**Ports**
tcp/8180

The remote web server type is:
- Coyote HTTP/1.1 Connector

### 43111 - HTTP Methods Allowed (per directory)

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

**Description**
By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501. Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

**Solution**
n/a

**Risk Factor**
None

**Plugin Information:**
- Publication date: 2009/12/10, Modification date: 2011/07/08

**Ports**
tcp/8180

Based on the response to an OPTIONS request:

- HTTP methods COPY DELETE GET HEAD LOCK MOVE POST PROPFIND PROPPATCH TRACE UNLOCK OPTIONS are allowed on:
  - /webdav

- HTTP methods DELETE HEAD OPTIONS POST PUT TRACE GET are allowed on:
  - /admin/images
  - /include
  - /jsp-examples
  - /jsp-examples/cal
  - /jsp-examples/checkbox
  - /jsp-examples/colors
  - /jsp-examples/dates
  - /jsp-examples/error
  - /jsp-examples/forward
  - /jsp-examples/images
  - /jsp-examples/include
  - /jsp-examples/jsp2/el
24004 - WebDAV Directory Enumeration

**Synopsis**

Several directories on the remote host are DAV-enabled.

**Description**

WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server. If you do not use this extension, you should disable it.

**Solution**

Disable DAV support if you do not use it.

**Risk Factor**

None

**Plugin Information:**

Publication date: 2007/01/11. Modification date: 2011/03/14

**Ports**

TCP/8180

The following directories are DAV enabled:
- /webdav/

39446 - Apache Tomcat Default Error Page Version Detection

**Synopsis**
The remote web server reports its version number on error pages.

**Description**
Apache Tomcat appears to be running on the remote host and reporting its version number on the default error pages. An attacker could use this information to mount further attacks.

**See Also**
http://wiki.apache.org/tomcat/FAQ/Miscellaneous#Q6

**Solution**
Replace the default error pages with custom error pages to hide the version number. Refer to the Apache wiki or the Java Servlet Specification for more information.

**Risk Factor**
None

**Plugin Information:**
Publication date: 2009/06/18, Modification date: 2011/09/29

**Ports**
tcp/8180

Nessus found the following version information on an Apache Tomcat 404 page or in the HTTP Server header:

<table>
<thead>
<tr>
<th>Source</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache Tomcat/5.5</td>
<td>5.5</td>
</tr>
</tbody>
</table>

**11419 - Web Server Office File Inventory**

**Synopsis**
The remote web server hosts office-related files.

**Description**
This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

**Solution**
Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

**Risk Factor**
None

**Plugin Information:**
Publication date: 2003/03/19, Modification date: 2011/12/28

**Ports**
tcp/8180

The following office-related files are available on the remote server:

- Adobe Acrobat files (.pdf):
  - /tomcat-docs/architecture/requestProcess/requestProcess.pdf
  - /tomcat-docs/architecture/startup/serverStartup.pdf

**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**
**Risk Factor**
None

**Plugin Information:**
Publication date: 2007/01/30, Modification date: 2011/05/31

**Ports**
tcp/8180

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

Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Wed, 15 Aug 2012 07:57:17 GMT
Connection: close

**20108 - Web Server / Application favicon.ico Vendor Fingerprinting**

**Synopsis**
The remote web server contains a graphic image that is prone to information disclosure.

**Description**
The 'favicon.ico' file found on the remote web server belongs to a popular web server. This may be used to fingerprint the web server.

**Solution**
Remove the 'favicon.ico' file or create a custom one for your site.

**Risk Factor**
None

**References**

**Plugin Information:**
Publication date: 2005/10/28, Modification date: 2012/04/12

**Ports**
tcp/8180

The MD5 fingerprint for 'favicon.ico' suggests the web server is Apache Tomcat 5.5.26 or Alfresco Community.

**8787/tcp**

**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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**
Protect your target with an IP filter.

**Risk Factor**
None
Port 8787/tcp was found to be open.

### 11154 - Unknown Service Detection: Banner Retrieval

#### Synopsis
There is an unknown service running on the remote host.

#### Description
Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

#### Solution
n/a

#### Risk Factor
None

#### Plugin Information:
- Publication date: 2002/11/18, Modification date: 2012/06/22

If you know what this service is and think the banner could be used to identify it, please send a description of the service along with the following output to svc-signatures@nessus.org:

```
Port   : 8787
Type   : get_http
Banner :
```

```
0x0000:  00 00 00 03 04 08 46 00 00 03 A1 04 08 6F 3A 16    ......F......o:.
0x0010:  44 52 62 3A 3A 44 52 62 43 6F 6E 6E 45 72 72 6F    DRb::DRbConnErro
0x0020:  r:.bt["/usr/1
0x0030:  69 62 2F 72 75 62 3A 3A 3A 35 37 33 69 6E 20 60 6C    ib/ruby/573:in `l
0x0040:  6F 61 64 27 22 2F 2F 75 73 72 2F 6C 69 62 2F 72    oad"//usr/lib/r
0x0050:  75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2F    uby/1.8/drb/db.
0x0060:  64 72 62 2E 72 62 3A 35 37 33 68 6E 20 60 6F 61    drb.rb:573:in `r
0x0070:  64 27 22 2F 2F 75 73 72 2F 6C 69 62 2F 72    uby//usr/lib/
0x0080:  75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2F    ruby/1.8/drb/db.
0x0090:  64 72 62 2E 72 62 3A 35 37 33 69 6E 20 60 72 75    drb.rb:573:in `r
0x00A0:  65 73 74 74 72 27 22 37 2F 75 73 72 2F 6C 69 62    ecv_request"7/usr/lib/
0x00B0:  2F 72 75 62 3A 3A 3A 35 37 33 3A 3A 69 6E 20 60 6C    2F/drdb:573:in `l
0x00C0:  6F 61 64 27 22 2F 2F 75 73 72 2F 6C 69 62 2F 72    oad"//usr/lib/r
0x00D0:  75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2F    uby/1.8/drb/db.
0x00E0:  64 72 62 2E 72 62 3A 35 37 33 3A 3A 69 6E 20 60 72    drb.rb:911:in `r
0x00F0:  6F 64 27 22 2F 2F 75 73 72 2F 6C 69 62 2F 72    oad"//usr/lib/
0x0100:  75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2F    ruby/1.8/drb/db.
0x0110:  64 72 62 2E 72 62 3A 35 37 33 3A 3A 69 6E 20 60 72    drb.rb:1530:in `r
0x0120:  6F 64 27 22 2F 2F 75 73 72 2F 6C 69 62 2F 72    oad"//usr/lib/
0x0130:  75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2F    ruby/1.8/drb/db.
0x0140:  64 72 62 2E 72 62 3A 35 37 33 3A 3A 69 6E 20 60 72    drb.rb:1542:in `r
0x0150:  6F 64 27 22 2F 2F 75 73 72 2F 6C 69 62 2F 72    oad"//usr/lib/
0x0160:  75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2F    ruby/1.8/drb/db.
0x0170:  64 72 62 2E 72 62 3A 35 37 33 3A 3A 69 6E 20 60 72    drb.rb:1552:in `r
0x0180:  6F 64 27 22 2F 2F 75 73 72 2F 6C 69 62 2F 72    oad"//usr/lib/
0x0190:  75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2F    ruby/1.8/drb/db.
0x01A0:  64 72 62 2E 72 62 3A 35 37 33 3A 3A 69 6E 20 60 72    drb.rb:1573:in `r
0x01B0:  6F 64 27 22 2F 2F 75 73 72 2F 6C 69 62 2F 72    oad"//usr/lib/
```

#### 33649/udp

### 11111 - RPC Services Enumeration

#### Synopsis
An ONC RPC service is running on the remote host.

#### Description
By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

#### Solution
n/a

#### Risk Factor
None

#### Plugin Information:
- Publication date: 2002/11/18, Modification date: 2012/06/22

An ONC RPC service is running on the remote host.
The following RPC services are available on UDP port 33649:

- program: 100005 (mountd), version: 1
- program: 100005 (mountd), version: 2
- program: 100005 (mountd), version: 3

### 37000/tcp

**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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

### Ports
tcp/37000

Port 37000/tcp was found to be open.

**11111 - RPC Services Enumeration**

**Synopsis**

An ONC RPC service is running on the remote host.

**Description**

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2002/08/24, Modification date: 2011/05/24

### Ports
tcp/37000

The following RPC services are available on TCP port 37000:

- program: 100005 (mountd), version: 1
- program: 100005 (mountd), version: 2
- program: 100005 (mountd), version: 3

### 44501/tcp

**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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

**Ports**

tcp/44501

| Port 44501/tcp was found to be open |

### 11111 - RPC Services Enumeration

**Synopsis**

An ONC RPC service is running on the remote host.

**Description**

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2002/08/24, Modification date: 2011/05/24

**Ports**

tcp/44501

The following RPC services are available on TCP port 44501:

- program: 100021 (nlockmgr), version: 1
- program: 100021 (nlockmgr), version: 3
- program: 100021 (nlockmgr), version: 4

udp/48701

### 11111 - RPC Services Enumeration

**Synopsis**

An ONC RPC service is running on the remote host.

**Description**

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2002/08/24, Modification date: 2011/05/24

**Ports**

udp/48701

The following RPC services are available on UDP port 48701:
### 51571/tcp

**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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

**Ports**

- **tcp/51571**
  
  Port 51571/tcp was found to be open

### 57176/tcp

**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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

**Ports**

- **tcp/57176**
  
  Port 57176/tcp was found to be open

### 11111 - RPC Services Enumeration

**Synopsis**

An ONC RPC service is running on the remote host.

**Description**

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2002/08/24, Modification date: 2011/05/24

**Ports**

- **tcp/57176**
The following RPC services are available on TCP port 57176:

- program: 100024 (status), version: 1
- program: 11111, version: 1

### Synopsis

An ONC RPC service is running on the remote host.

### Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2002/08/24, Modification date: 2011/05/24

### Ports

udp/58930

The following RPC services are available on UDP port 58930:

- program: 100021 (nlockmgr), version: 1
- program: 100021 (nlockmgr), version: 3
- program: 100021 (nlockmgr), version: 4
Synopsis
   It is possible to execute code on the remote host through Samba.

Description
   The version of the Samba server installed on the remote host is affected by multiple heap overflow vulnerabilities, which can be exploited remotely to execute code with the privileges of the Samba daemon.

See Also

Solution
   Upgrade to Samba version 3.0.25 or later.

Risk Factor
   Critical

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

References
   BID 23973
   BID 24195
   BID 24196
   BID 24197
   BID 24198
   CVE CVE-2007-2446
   XREF OSVDB:34699
   XREF OSVDB:34731
   XREF OSVDB:34732
   XREF OSVDB:34733

Exploitable with
   CANVAS (true) Metasploit (true)

Plugin Information:
   Publication date: 2007/05/15, Modification date: 2011/04/13

Hosts
   192.168.56.3 (tcp/445)
**Synopsis**

The remote SSH host keys are weak.

**Description**

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL. An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

**See Also**

http://www.nessus.org/u?5d01bdab

http://www.nessus.org/u?f14f4224

**Solution**

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

**Risk Factor**

Critical

**CVSS Base Score**

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

**CVSS Temporal Score**

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

**References**

<table>
<thead>
<tr>
<th>BID</th>
<th>29179</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>CVE-2008-0166</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:45029</td>
</tr>
<tr>
<td>XREF</td>
<td>CWE:310</td>
</tr>
</tbody>
</table>

**Exploitable with**

Core Impact (true)

**Plugin Information:**

Publication date: 2008/05/14, Modification date: 2011/03/21

**Hosts**

192.168.56.3 (tcp/22)
Synopsis
The remote FTP server contains a backdoor allowing execution of arbitrary code.

Description
The version of vsftpd running on the remote host has been compiled with a backdoor. Attempting to login with a username containing :) (a smiley face) triggers the backdoor, which results in a shell listening on TCP port 6200. The shell stops listening after a client connects to and disconnects from it.
An unauthenticated, remote attacker could exploit this to execute arbitrary code as root.

See Also
http://pastebin.com/AetT9sS5
http://www.nessus.org/u?abcbc915

Solution
Validate and recompile a legitimate copy of the source code.

Risk Factor
Critical

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

CVSS Temporal Score
8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References
BID 48539
XREF OSVDB:73573
XREF EDB-ID:17491

Exploitable with
Metasploit (true)

Plugin Information:
Publication date: 2011/07/06, Modification date: 2011/10/24

Hosts
192.168.56.3 (tcp/21)

Nessus executed "id" which returned the following output :
uid=0(root) gid=0(root)
### 10205 (1) - rlogin Service Detection

#### Synopsis

The rlogin service is listening on the remote port.

#### Description

The remote host is running the 'rlogin' service. This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the rlogin client and the rloginserver. This includes logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files. You should disable this service and use ssh instead.

#### Solution

Comment out the 'login' line in /etc/inetd.conf

#### Risk Factor

High

#### CVSS Base Score

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

#### References

**CVE**

CVE-1999-0651

**XREF**

OSVDB:193

#### Plugin Information:

Publication date: 1999/08/30, Modification date: 2011/04/01

#### Hosts

192.168.56.3 (tcp/513)
Synopsis
The remote database server can be accessed without a password.

Description
It is possible to connect to the remote MySQL database server using an unpassworded account. This may allow an attacker to launch further attacks against the database.

See Also

Solution
Disable or set a password for the affected account.

Risk Factor
High

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

CVSS Temporal Score
7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References
BID 11704
CVE CVE-2002-1809
CVE CVE-2004-1532
XREF OSVDB:380
XREF OSVDB:16026

Plugin Information:
Publication date: 2000/07/27, Modification date: 2012/03/28

Hosts
192.168.56.3 (tcp/3306)

The 'root' account does not have a password.

Here is the list of databases on the remote server:

- information_schema
- dvwa
- metasploit
- mysql
- owasp10
- tikiwiki
- tikiwiki195
Synopsis
The remote web server contains a PHP application that may allow execution of arbitrary code.

Description
The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user supplied input before using it to generate a config file for the application. This version has the following vulnerabilities:
- The setup script inserts the unsanitized verbose server name into a C-style comment during config file generation.
- An attacker can save arbitrary data to the generated config file by altering the value of the 'textconfig' parameter during a POST request to config.php.
An unauthenticated, remote attacker may be able to leverage these issues to execute arbitrary PHP code.

See Also

Solution
Upgrade to phpMyAdmin 3.1.3.2 or apply the patches referenced in the project's advisory.

Risk Factor
High

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

CVSS Temporal Score
6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References
BID 34526
CVE CVE-2009-1285
XREF OSVDB:53685
XREF Secunia:34727
XREF CWE:94

Plugin Information:
Publication date: 2009/04/16, Modification date: 2012/04/03

Hosts
192.168.56.3 (tcp/80)
**Synopsis**

It is possible to access a network share.

**Description**

The remote has one or more Windows shares that can be accessed through the network with the given credentials. Depending on the share rights, it may allow an attacker to read/write confidential data.

**Solution**

To restrict access under Windows, open Explorer, do a right click on each share, go to the ‘sharing’ tab, and click on ‘permissions’.

**Risk Factor**

High

**CVSS Base Score**

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

**CVSS Temporal Score**

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

**References**

<table>
<thead>
<tr>
<th>BID</th>
<th>CVE</th>
<th>CVE</th>
<th>XREF</th>
</tr>
</thead>
</table>

**Plugin Information:**

Publication date: 2009/11/06, Modification date: 2011/03/27

**Hosts**

**192.168.56.3 (tcp/445)**

The following shares can be accessed using a NULL session:

- tmp  - (readable,writable)
  + Content of this share:
    
    ..
    
    4511.jsvc_up
    .ICE-unix
    .X11-unix
    .X0-lock
55976 (1) - Apache HTTP Server Byte Range DoS

Synopsis
The web server running on the remote host is affected by a denial of service vulnerability.

Description
The version of Apache HTTP Server running on the remote host is affected by a denial of service vulnerability. Making a series of HTTP requests with overlapping ranges in the Range or Request-Range request headers can result in memory and CPU exhaustion. A remote, unauthenticated attacker could exploit this to make the system unresponsive. Exploit code is publicly available and attacks have reportedly been observed in the wild.

See Also
http://www.gossamer-threads.com/lists/apache/dev/401638
http://httpd.apache.org/security/CVE-2011-3192.txt
http://www.nessus.org/u?1538124a
http://www-01.ibm.com/support/docview.wss?uid=swg24030863

Solution
Upgrade to Apache httpd 2.2.21 or later, or use one of the workarounds in Apache's advisories for CVE-2011-3192. Version 2.2.20 fixed the issue, but also introduced a regression. If the host is running a web server based on Apache httpd, contact the vendor for a fix.

Risk Factor
High

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

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

References
BID 49303
CVE CVE-2011-3192
XREF OSVDB:74721
XREF CERT:405811
XREF EDB-ID:17696
XREF EDB-ID:18221

Plugin Information:
Publication date: 2011/08/25, Modification date: 2012/07/18

Hosts
192.168.56.3 (tcp/80)

Nessus determined the server is unpatched and is not using any of the suggested workarounds by making the following requests:

--------------------- Testing for workarounds ---------------------
HEAD /mutillidae/framer.html HTTP/1.1
Host: 192.168.56.3
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en

105
### Synopsis
The remote web server contains a version of PHP that allows arbitrary code execution.

### Description
The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.

### See Also
- [http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/](http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/)
- [http://www.php.net/ChangeLog-5.php#5.3.13](http://www.php.net/ChangeLog-5.php#5.3.13)
- [http://www.php.net/ChangeLog-5.php#5.4.3](http://www.php.net/ChangeLog-5.php#5.4.3)

### Solution
Upgrade to PHP 5.3.13 / 5.4.3 or later.

### Risk Factor
High

### CVSS Base Score
- **8.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:P/A:P)**

### CVSS Temporal Score
- **6.9 (CVSS2#AV:N/AC:M/Au:N/C:C/I:P/A:P)**

### References
- **BID**: 53388
- **CVE**: CVE-2012-1823
- **CVE**: CVE-2012-2311
- **XREF**: OSVDB:81633
- **XREF**: EDB-ID:18834
- **XREF**: CERT-VU:520827

### Exploitable with
Metasploit (true)

### Plugin Information:
- **Publication date**: 2012/05/14, **Modification date**: 2012/06/23

### Hosts
- **192.168.56.3 (tcp/80)**

Nessus was able to verify the issue exists using the following request:

```plaintext
POST /phpMyAdmin/themes/original/layout.inc.php?--d+allow_url_include%3don+-d+safe_mode%3doff+-d+suhosin.simulation%3don+-d+open_basedir%3doff+-d+auto_prepend_file%3dphp%3a//input+-n HTTP/1.1
Host: 192.168.56.3
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Content-Length: 82
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
```
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

```php
<?php echo 'php_cgi_query_string_code_execution-1345090228'; system('id'); die; ?>
```

--- snip ---
### Synopsis
The remote web server is affected by an information disclosure vulnerability.

### Description
The `/doc` directory is browsable. `/doc` shows the contents of the `/usr/doc` directory, which reveals not only which programs are installed but also their versions.

### See Also
http://projects.webappsec.org/Directory-Indexing

### Solution
Use access restrictions for the `/doc` directory.
If you use Apache you might use this in your `access.conf`:
```apache
<Directory /usr/doc>
    AllowOverride None
    order deny,allow
    deny from all
    allow from localhost
</Directory>
```

### Risk Factor
Medium

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

### CVSS Temporal Score
4.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### References
<table>
<thead>
<tr>
<th>BID</th>
<th>318</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>CVE-1999-0678</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:48</td>
</tr>
</tbody>
</table>

### Plugin Information:
Publication date: 2000/01/03, Modification date: 2011/03/17

### Hosts
192.168.56.3 (tcp/80)
### 10079 (1) - Anonymous FTP Enabled

#### Synopsis
Anonymous logins are allowed on the remote FTP server.

#### Description
This FTP service allows anonymous logins. Any remote user may connect and authenticate without providing a password or unique credentials. This allows a user to access any files made available on the FTP server.

#### Solution
Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure sensitive content is not available.

#### Risk Factor
Medium

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

#### References
- **CVE**: CVE-1999-0497
- **XREF**: OSVDB:69

#### Plugin Information:
Publication date: 1999/06/22, Modification date: 2011/10/05

#### Hosts
192.168.56.3 (tcp/21)
**Synopsis**

The rexecd service is listening on the remote port.

**Description**

The rexecd service is open. This service is designed to allow users of a network to execute commands remotely. However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third party host.

**Solution**

comment out the 'exec' line in /etc/inetd.conf and restart the inetd process

**Risk Factor**

Medium

**CVSS Base Score**

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

**References**

- CVE
  - CVE-1999-0618
- XREF
  - OSVDB:9721

**Plugin Information:**

Publication date: 1999/08/31, Modification date: 2011/03/11

**Hosts**

192.168.56.3 (tcp/512)
11213 (1) - HTTP TRACE / TRACK Methods Allowed

**Synopsis**
Debugging functions are enabled on the remote web server.

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

**See Also**
http://www.apacheweek.com/issues/03-01-24
http://www.kb.cert.org/vuls/id/288308
http://www.kb.cert.org/vuls/id/867593
http://download.oracle.com/sunalerts/1000718.1.html

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

**Risk Factor**
Medium

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

**CVSS Temporal Score**
3.9 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

**References**

<table>
<thead>
<tr>
<th>BID</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9506</td>
<td></td>
</tr>
<tr>
<td>9561</td>
<td></td>
</tr>
<tr>
<td>11604</td>
<td></td>
</tr>
<tr>
<td>33374</td>
<td></td>
</tr>
<tr>
<td>37995</td>
<td></td>
</tr>
<tr>
<td>CVE</td>
<td>CVE-2003-1567</td>
</tr>
<tr>
<td>CVE</td>
<td>CVE-2004-2320</td>
</tr>
<tr>
<td>CVE</td>
<td>CVE-2010-0386</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:877</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:3726</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:5648</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:50485</td>
</tr>
<tr>
<td>XREF</td>
<td>CWE:16</td>
</tr>
</tbody>
</table>

**Plugin Information:**
Publication date: 2003/01/23, Modification date: 2012/04/04

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

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

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

Nessus sent the following TRACE request:

```
------------------------------ snip ------------------------------
TRACE /Nessus1667296966.html HTTP/1.1
Connection: Close
Host: 192.168.56.3
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*;utf-8
------------------------------ snip ------------------------------
```

and received the following response from the remote server:

```
------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Wed, 15 Aug 2012 07:57:25 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http

TRACE /Nessus1667296966.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.56.3
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*;utf-8
------------------------------ snip ------------------------------
```
Summary: The remote web server contains a PHP script that is prone to an information disclosure attack.

Description:
Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including:
- The username of the user who installed php and if they are a SUDO user.
- The IP address of the host.
- The version of the operating system.
- The web server version.
- The root directory of the web server.
- Configuration information about the remote PHP installation.

Solution:
Remove the affected file(s).

Risk Factor:
Medium

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

Plugin Information:
Publication date: 2003/02/12, Modification date: 2011/03/15

Hosts:
192.168.56.3 (tcp/80)

Nessus discovered the following URLs that call phpinfo():
11356 (1) - NFS Exported Share Information Disclosure

**Synopsis**
It is possible to access NFS shares on the remote host.

**Description**
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

**Solution**
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

**Risk Factor**
Medium

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

**References**
- CVE-1999-0170
- CVE-1999-0211
- CVE-1999-0554
- OSVDB:339
- OSVDB:8750
- OSVDB:11516

**Plugin Information:**
Publication date: 2003/03/12, Modification date: 2011/05/24

**Hosts**
192.168.56.3 (udp/2049)

The following NFS shares could be mounted:

+ /
  + Contents of / :
  - initrd
  - media
  - bin
  - lost+found
  - mnt
  - sbin
  - initrd.img
  - home
  - lib
  - usr
  - proc
  - root
  - sys
  - boot
  - nohup.out
  - etc
  - dev
  - ..
  - vmlinux
  - opt
  - var
  - cdrom
  - tmp
  - .
  - srv
## 15901 (1) - SSL Certificate Expiry

### Synopsis
The remote server's SSL certificate has already expired.

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

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

### Risk Factor
Medium

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

### Plugin Information:
Publication date: 2004/12/03, Modification date: 2012/04/02

### Hosts
192.168.56.3 (tcp/25)

The SSL certificate has already expired:

---

Subject: C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain  
Issuer: C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain  
Not valid before: Mar 17 14:07:45 2010 GMT  
Not valid after: Apr 16 14:07:45 2010 GMT
### 20007 (1) - SSL Version 2 (v2) Protocol Detection

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

**Description**
The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

**See Also**
- http://support.microsoft.com/kb/187498
- http://www.linux4beginners.info/node/disable-sslv2

**Solution**
Consult the application's documentation to disable SSL 2.0 and use SSL 3.0, TLS 1.0, or higher instead.

**Risk Factor**
Medium

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

**References**

<table>
<thead>
<tr>
<th>CVE</th>
<th>CVE-2005-2969</th>
</tr>
</thead>
</table>

**Plugin Information:**
- Publication date: 2005/10/12, Modification date: 2012/04/02

**Hosts**

| 192.168.56.3 (tcp/25) |
**Synopsis**

The remote service supports the use of weak SSL ciphers.

**Description**

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all. Note: This is considerably easier to exploit if the attacker is on the same physical network.

**See Also**

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

**Solution**

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

**Risk Factor**

Medium

**CVSS Base Score**

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

**References**

<table>
<thead>
<tr>
<th>XREF</th>
<th>CWE</th>
<th>XREF</th>
<th>CWE</th>
<th>XREF</th>
<th>CWE</th>
<th>XREF</th>
<th>CWE</th>
<th>XREF</th>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSLv2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXP-RC2-CBC-MD5</td>
<td>Kx=RSA(512)</td>
<td>Au=RSA</td>
<td>Enc=RC2(40)</td>
<td>Mac=MD5</td>
<td>export</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXP-RC4-MD5</td>
<td>Kx=RSA(512)</td>
<td>Au=RSA</td>
<td>Enc=RC4(40)</td>
<td>Mac=MD5</td>
<td>export</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSLv3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXP-ADH-DES-CBC-SHA</td>
<td>Kx=DH(512)</td>
<td>Au=None</td>
<td>Enc=DES(40)</td>
<td>Mac=SHA1</td>
<td>export</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXP-ADH-RC4-MD5</td>
<td>Kx=DH(512)</td>
<td>Au=None</td>
<td>Enc=RC4(40)</td>
<td>Mac=MD5</td>
<td>export</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXP-EDH-RSA-DES-CBC-SHA</td>
<td>Kx=DH(512)</td>
<td>Au=RSA</td>
<td>Enc=DES(40)</td>
<td>Mac=SHA1</td>
<td>export</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXP-DES-CBC-SHA</td>
<td>Kx=RSA(512)</td>
<td>Au=RSA</td>
<td>Enc=DES(40)</td>
<td>Mac=SHA1</td>
<td>export</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXP-RC2-CBC-MD5</td>
<td>Kx=RSA(512)</td>
<td>Au=RSA</td>
<td>Enc=RC2(40)</td>
<td>Mac=MD5</td>
<td>export</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXP-RC4-MD5</td>
<td>Kx=RSA(512)</td>
<td>Au=RSA</td>
<td>Enc=RC4(40)</td>
<td>Mac=MD5</td>
<td>export</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLSv1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXP-EDH-RSA-DES-CBC-SHA</td>
<td>Kx=DH(512)</td>
<td>Au=RSA</td>
<td>Enc=DES(40)</td>
<td>Mac=SHA1</td>
<td>export</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXP-ADH-DES-CBC-SHA</td>
<td>Kx=DH(512)</td>
<td>Au=None</td>
<td>Enc=DES(40)</td>
<td>Mac=SHA1</td>
<td>export</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXP-ADH-RC4-MD5</td>
<td>Kx=DH(512)</td>
<td>Au=None</td>
<td>Enc=RC4(40)</td>
<td>Mac=MD5</td>
<td>export</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXP-DES-CBC-SHA</td>
<td>Kx=RSA(512)</td>
<td>Au=RSA</td>
<td>Enc=DES(40)</td>
<td>Mac=SHA1</td>
<td>export</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Plugin Information:**

Publication date: 2007/10/08, Modification date: 2012/04/02

**Hosts**

192.168.56.3 (tcp/25)

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

**Low Strength Ciphers (< 56-bit key)**

**SSLv2**

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Key Type</th>
<th>Authentication</th>
<th>Encryption</th>
<th>Hash</th>
<th>Export</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXP-RC2-CBC-MD5</td>
<td>Kx=RSA(512)</td>
<td>Au=RSA</td>
<td>Enc=RC2(40)</td>
<td>Mac=MD5</td>
<td>export</td>
</tr>
<tr>
<td>EXP-RC4-MD5</td>
<td>Kx=RSA(512)</td>
<td>Au=RSA</td>
<td>Enc=RC4(40)</td>
<td>Mac=MD5</td>
<td>export</td>
</tr>
</tbody>
</table>

**SSLv3**

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Key Type</th>
<th>Authentication</th>
<th>Encryption</th>
<th>Hash</th>
<th>Export</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXP-ADH-DES-CBC-SHA</td>
<td>Kx=DH(512)</td>
<td>Au=None</td>
<td>Enc=DES(40)</td>
<td>Mac=SHA1</td>
<td>export</td>
</tr>
<tr>
<td>EXP-ADH-RC4-MD5</td>
<td>Kx=DH(512)</td>
<td>Au=None</td>
<td>Enc=RC4(40)</td>
<td>Mac=MD5</td>
<td>export</td>
</tr>
<tr>
<td>EXP-EDH-RSA-DES-CBC-SHA</td>
<td>Kx=DH(512)</td>
<td>Au=RSA</td>
<td>Enc=DES(40)</td>
<td>Mac=SHA1</td>
<td>export</td>
</tr>
<tr>
<td>EXP-DES-CBC-SHA</td>
<td>Kx=RSA(512)</td>
<td>Au=RSA</td>
<td>Enc=DES(40)</td>
<td>Mac=SHA1</td>
<td>export</td>
</tr>
<tr>
<td>EXP-RC2-CBC-MD5</td>
<td>Kx=RSA(512)</td>
<td>Au=RSA</td>
<td>Enc=RC2(40)</td>
<td>Mac=MD5</td>
<td>export</td>
</tr>
<tr>
<td>EXP-RC4-MD5</td>
<td>Kx=RSA(512)</td>
<td>Au=RSA</td>
<td>Enc=RC4(40)</td>
<td>Mac=MD5</td>
<td>export</td>
</tr>
</tbody>
</table>

**TLSv1**

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Key Type</th>
<th>Authentication</th>
<th>Encryption</th>
<th>Hash</th>
<th>Export</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXP-EDH-RSA-DES-CBC-SHA</td>
<td>Kx=DH(512)</td>
<td>Au=RSA</td>
<td>Enc=DES(40)</td>
<td>Mac=SHA1</td>
<td>export</td>
</tr>
<tr>
<td>EXP-ADH-DES-CBC-SHA</td>
<td>Kx=DH(512)</td>
<td>Au=None</td>
<td>Enc=DES(40)</td>
<td>Mac=SHA1</td>
<td>export</td>
</tr>
<tr>
<td>EXP-ADH-RC4-MD5</td>
<td>Kx=DH(512)</td>
<td>Au=None</td>
<td>Enc=RC4(40)</td>
<td>Mac=MD5</td>
<td>export</td>
</tr>
<tr>
<td>EXP-DES-CBC-SHA</td>
<td>Kx=RSA(512)</td>
<td>Au=RSA</td>
<td>Enc=DES(40)</td>
<td>Mac=SHA1</td>
<td>export</td>
</tr>
</tbody>
</table>
The fields above are:

(OpenSSL ciphername)
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
(export flag)
## 31705 (1) - SSL Anonymous Cipher Suites Supported

### Synopsis

The remote service supports the use of anonymous SSL ciphers.

### Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host’s identity and renders the service vulnerable to a man-in-the-middle attack.

*Note: This is considerably easier to exploit if the attacker is on the same physical network.*

### See Also

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

### Solution

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

### Risk Factor

Medium

### CVSS Base Score

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

### CVSS Temporal Score

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

### References

<table>
<thead>
<tr>
<th>BID</th>
<th>28482</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>CVE-2007-1858</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:34882</td>
</tr>
</tbody>
</table>

### Plugin Information:

Publication date: 2008/03/28, Modification date: 2012/04/02

### Hosts

**192.168.56.3 (tcp/25)**

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

**Low Strength Ciphers (< 56-bit key)**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Cipher</th>
<th>Key</th>
<th>Auth</th>
<th>Enc</th>
<th>Mac</th>
<th>Export</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSLv3</td>
<td>EXP-ADH-DES-CBC-SHA</td>
<td>Kx=DH (512)</td>
<td>Au=None</td>
<td>Enc=DES (40)</td>
<td>Mac=SHA1</td>
<td>export</td>
</tr>
<tr>
<td>SSLv3</td>
<td>EXP-ADH-RC4-MD5</td>
<td>Kx=DH (512)</td>
<td>Au=None</td>
<td>Enc=RC4 (40)</td>
<td>Mac=MD5</td>
<td>export</td>
</tr>
<tr>
<td>TLSv1</td>
<td>EXP-ADH-DES-CBC-SHA</td>
<td>Kx=DH (512)</td>
<td>Au=None</td>
<td>Enc=DES (40)</td>
<td>Mac=SHA1</td>
<td>export</td>
</tr>
<tr>
<td>TLSv1</td>
<td>EXP-ADH-RC4-MD5</td>
<td>Kx=DH (512)</td>
<td>Au=None</td>
<td>Enc=RC4 (40)</td>
<td>Mac=MD5</td>
<td>export</td>
</tr>
</tbody>
</table>

**Medium Strength Ciphers (>= 56-bit and < 112-bit key)**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Cipher</th>
<th>Key</th>
<th>Auth</th>
<th>Enc</th>
<th>Mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSLv3</td>
<td>ADH-DES-CBC-SHA</td>
<td>Kx=DH</td>
<td>Au=None</td>
<td>Enc=DES (56)</td>
<td>Mac=SHA1</td>
</tr>
<tr>
<td>TLSv1</td>
<td>ADH-DES-CBC-SHA</td>
<td>Kx=DH</td>
<td>Au=None</td>
<td>Enc=DES (56)</td>
<td>Mac=SHA1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Cipher</th>
<th>Key</th>
<th>Auth</th>
<th>Enc</th>
<th>Mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSLv3</td>
<td>ADH-DES-CBC3-SHA</td>
<td>Kx=DH</td>
<td>Au=None</td>
<td>Enc=3DES (168)</td>
<td>Mac=SHA1</td>
</tr>
<tr>
<td>SSLv3</td>
<td>ADH-RC4-MD5</td>
<td>Kx=DH</td>
<td>Au=None</td>
<td>Enc=RC4 (128)</td>
<td>Mac=MD5</td>
</tr>
<tr>
<td>TLSv1</td>
<td>ADH-DES-CBC3-SHA</td>
<td>Kx=DH</td>
<td>Au=None</td>
<td>Enc=3DES (168)</td>
<td>Mac=SHA1</td>
</tr>
<tr>
<td>TLSv1</td>
<td>ADH-AES128-SHA</td>
<td>Kx=DH</td>
<td>Au=None</td>
<td>Enc=AES (128)</td>
<td>Mac=SHA1</td>
</tr>
<tr>
<td>TLSv1</td>
<td>ADH-AES256-SHA</td>
<td>Kx=DH</td>
<td>Au=None</td>
<td>Enc=AES (256)</td>
<td>Mac=SHA1</td>
</tr>
<tr>
<td>TLSv1</td>
<td>ADH-RC4-MD5</td>
<td>Kx=DH</td>
<td>Au=None</td>
<td>Enc=RC4 (128)</td>
<td>Mac=MD5</td>
</tr>
</tbody>
</table>
The fields above are:

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
The remote web server contains a PHP script that is affected by multiple issues.

The version of phpMyAdmin installed on the remote host fails to sanitize user supplied input to the 'file_path' parameter of the 'bs_disp_as_mime_type.php' script before using it to read a file and reporting it in dynamically-generated HTML. An unauthenticated, remote attacker may be able to leverage this issue to read arbitrary files, possibly from third-party hosts, or to inject arbitrary HTTP headers in responses sent to third-party users. Note that the application is also reportedly affected by several other issues, although Nessus has not actually checked for them.

See Also


Solution

Upgrade to phpMyAdmin 3.1.3.1 or apply the patch referenced in the project's advisory.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID 34253
XREF OSVDB:53226
XREF OSVDB:53227
XREF Secunia:34468

Plugin Information:

Publication date: 2009/04/03, Modification date: 2012/06/08

Hosts

192.168.56.3 (tcp/80)
### 42256 (1) - NFS Shares World Readable

#### Synopsis
The remote NFS server exports world readable shares.

#### Description
The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

#### See Also
http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

#### Solution
Place the appropriate restrictions on all NFS shares.

#### Risk Factor
Medium

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

#### References
XREF OSVDB:339

#### Plugin Information:
Publication date: 2009/10/26, Modification date: 2011/03/21

#### Hosts
192.168.56.3 (tcp/2049)

The following shares have no access restrictions:

/ *
**Synopsis**

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

**Description**

The remote host supports the use of SSL ciphers that offer medium strength encryption, which we currently regard as those with key lengths at least 56 bits and less than 112 bits.

**Note:** This is considerably easier to exploit if the attacker is on the same physical network.

**Solution**

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

**Risk Factor**

Medium

**CVSS Base Score**

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

**Plugin Information:**

Publication date: 2009/11/23, Modification date: 2012/04/02

**Hosts**

192.168.56.3 (tcp/25)

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

Medium Strength Ciphers (>= 56-bit and < 112-bit key)

<table>
<thead>
<tr>
<th>SSLv2</th>
<th>Kx=RSA</th>
<th>Au=RSA</th>
<th>Enc=DES(56)</th>
<th>Mac=MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES-CBC-MD5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSLv3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADH-DES-CBC-SHA</td>
<td>Kx=DH</td>
<td>Au=None</td>
<td>Enc=DES(56)</td>
<td>Mac=SHA1</td>
</tr>
<tr>
<td>EDH-RSA-DES-CBC-SHA</td>
<td>Kx=DH</td>
<td>Au=RSA</td>
<td>Enc=DES(56)</td>
<td>Mac=SHA1</td>
</tr>
<tr>
<td>DES-CBC-SHA</td>
<td>Kx=RSA</td>
<td>Au=RSA</td>
<td>Enc=DES(56)</td>
<td>Mac=SHA1</td>
</tr>
<tr>
<td>TLSv1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDH-RSA-DES-CBC-SHA</td>
<td>Kx=DH</td>
<td>Au=RSA</td>
<td>Enc=DES(56)</td>
<td>Mac=SHA1</td>
</tr>
<tr>
<td>ADH-DES-CBC-SHA</td>
<td>Kx=DH</td>
<td>Au=None</td>
<td>Enc=DES(56)</td>
<td>Mac=SHA1</td>
</tr>
<tr>
<td>DES-CBC-SHA</td>
<td>Kx=RSA</td>
<td>Au=RSA</td>
<td>Enc=DES(56)</td>
<td>Mac=SHA1</td>
</tr>
</tbody>
</table>

The fields above are:

(OpenSSL ciphername)
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
(export flag)
45411 (1) - SSL Certificate with Wrong Hostname

**Synopsis**

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

**Description**

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

**Solution**

Purchase or generate a proper certificate for this service.

**Risk Factor**

Medium

**CVSS Base Score**

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

**Plugin Information:**

Publication date: 2010/04/03, Modification date: 2012/07/25

**Hosts**

192.168.56.3 (tcp/25)

The identity known by Nessus is:

192.168.56.3

The Common Name in the certificate is:

ubuntu804-base.localdomain
Synopsis
The configuration of PHP on the remote host allows disclosure of sensitive information.

Description
The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such an URL triggers an Easter egg built into PHP itself. Other such Easter eggs likely exist, but Nessus has not checked for them.

See Also
http://www.0php.com/php_easter_egg.php
http://seclists.org/webappsec/2004/q4/324

Solution
In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

Risk Factor
Medium

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

References
XREF OSVDB:12184

Plugin Information:
Publication date: 2010/06/03, Modification date: 2011/03/14

Hosts
192.168.56.3 (tcp/80)

Nessus was able to verify the issue using the following URL:
http://192.168.56.3/phpMyAdmin/themes/original/layout.inc.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
Synopsis
The remote web server contains a PHP application that has a cross-site scripting vulnerability.

Description
The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user supplied input to the 'verbose server name' field.
A remote attacker could exploit this by tricking a user into executing arbitrary script code.

See Also

Solution
Upgrade to phpMyAdmin 3.3.7 or later.

Risk Factor
Medium

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

References
CVE
CVE-2010-3263

XREF
OSVDB:67851

Plugin Information:
Publication date: 2010/09/08, Modification date: 2012/03/28

Hosts
192.168.56.3 (tcp/80)

By making a series of requests, Nessus was able to determine the following phpMyAdmin installation is vulnerable:

http://192.168.56.3/phpMyAdmin/
**51192 (1) - SSL Certificate Cannot Be Trusted**

**Synopsis**

The SSL certificate for this service cannot be trusted.

**Description**

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted. First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. Third, the certificate chain may contain a signature that either didn't match the certificate's information, or was not possible to verify. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize. If the remote host is a public host in production, any break in the chain 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 Information:**

Publication date: 2010/12/15, Modification date: 2012/01/28

**Hosts**

192.168.56.3 (tcp/25)

The following certificates were part of the certificate chain sent by the remote host, but have expired:

<table>
<thead>
<tr>
<th>Subject</th>
<th>C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=<a href="mailto:root@ubuntu804-base.localdomain">root@ubuntu804-base.localdomain</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Not After</td>
<td>Apr 16 14:07:45 2010 GMT</td>
</tr>
</tbody>
</table>

The following certificates were at the top of the certificate chain sent by the remote host, but are signed by an unknown certificate authority:

<table>
<thead>
<tr>
<th>Subject</th>
<th>C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=<a href="mailto:root@ubuntu804-base.localdomain">root@ubuntu804-base.localdomain</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuer</td>
<td>C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=<a href="mailto:root@ubuntu804-base.localdomain">root@ubuntu804-base.localdomain</a></td>
</tr>
</tbody>
</table>


Synopsis

The remote web server hosts a PHP script that is prone to a cross-site scripting attack.

Description

The version of phpMyAdmin fails to validate BBcode tags in user input to the 'error' parameter of the 'error.php' script before using it to generate dynamic HTML.
An attacker may be able to leverage this issue to inject arbitrary HTML or script code into a user's browser to be executed within the security context of the affected site. For example, this could be used to cause a page with arbitrary text and a link to an external site to be displayed.

See Also


Solution

Upgrade to phpMyAdmin 3.4.0-beta1 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID 45633
CVE CVE-2010-4480
XREF OSVDB:69684
XREF EDB-ID:15699

Plugin Information:

Publication date: 2011/01/06, Modification date: 2011/10/24

Hosts

192.168.56.3 (tcp/80)

Nessus was able to exploit the issue using the following URL:

52611 (1) - SMTP Service STARTTLS Plaintext Command Injection

Synopsis
The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.

Description
The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase. Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

See Also
http://www.securityfocus.com/archive/1/516901/30/0/threaded

Solution
Contact the vendor to see if an update is available.

Risk Factor
Medium

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

CVSS Temporal Score
3.3 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

References
BID 46767
CVE CVE-2011-0411
CVE CVE-2011-1430
CVE CVE-2011-1431
CVE CVE-2011-1432
CVE CVE-2011-1506
CVE CVE-2011-2165
XREF OSVDB:71020
XREF OSVDB:71021
XREF OSVDB:71854
XREF OSVDB:71946
XREF OSVDB:73251
XREF OSVDB:75014
XREF OSVDB:75256
XREF CERT:555316

Plugin Information:
Publication date: 2011/03/10, Modification date: 2012/06/14

Hosts
Nessus sent the following two commands in a single packet:

STARTTLS\nR\n
And the server sent the following two responses:

220 2.0.0 Ready to start TLS
250 2.0.0 Ok
57582 (1) - SSL Self-Signed Certificate

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

Description
The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man in the middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution
Purchase or generate a proper certificate for this service.

Risk Factor
Medium

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

Plugin Information:
Publication date: 2012/01/17, Modification date: 2012/01/17

Hosts
192.168.56.3 (tcp/25)

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

| Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain |
**57608 (1) - SMB Signing Disabled**

**Synopsis**
Signing is disabled on the remote SMB server.

**Description**
Signing is disabled on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

**See Also**
- http://support.microsoft.com/kb/887429
- http://www.nessus.org/u?74b80723

**Solution**
Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

**Risk Factor**
Medium

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

**Plugin Information:**
Publication date: 2012/01/19, Modification date: 2012/03/05

**Hosts**
192.168.56.3 (tcp/445)
Synopsis
The web server running on the remote host has an information disclosure vulnerability.

Description
The version of Apache HTTP Server running on the remote host has an information disclosure vulnerability. Sending a request with HTTP headers long enough to exceed the server limit causes the web server to respond with an HTTP 400. By default, the offending HTTP header and value are displayed on the 400 error page. When used in conjunction with other attacks (e.g., cross-site scripting), this could result in the compromise of httpOnly cookies.

See Also
http://fd.the-wildcat.de/apache_e36a9cf46c.php
http://httpd.apache.org/security/vulnerabilities_22.html
http://svn.apache.org/viewvc?view=revision&revision=1235454

Solution
Upgrade to Apache version 2.2.22 or later.

Risk Factor
Medium

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

CVSS Temporal Score
3.6 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

STIG Severity
I

References
BID 51706
CVE CVE-2012-0053
XREF OSVDB:78556
XREF EDB-ID:18442
XREF IAVA:2012-A-0017

Plugin Information:
Publication date: 2012/02/02, Modification date: 2012/05/22

Hosts
192.168.56.3 (tcp/80)

Nessus verified this by sending a request with a long Cookie header:

GET / HTTP/1.1
Host: 192.168.56.3
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA ... AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA; z8=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA ...
[...]
**26194 (2) - Web Server Uses Plain Text Authentication Forms**

**Synopsis**

The remote web server might transmit credentials in cleartext.

**Description**

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

**Solution**

Make sure that every sensitive form transmits content over HTTPS.

**Risk Factor**

Low

**CVSS Base Score**

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

**References**

XREF CWE:522

XREF CWE:523

XREF CWE:718

XREF CWE:724

**Plugin Information:**

Publication date: 2007/09/28, Modification date: 2011/09/15

**Hosts**

192.168.56.3 (tcp/80)

Page : /phpMyAdmin/
Destination page : index.php
Input name : pma_password

Page : /phpMyAdmin/?D=A
Destination page : index.php
Input name : pma_password

Page : /twiki/TWikiDocumentation.html
Destination page : http://TWiki.org/cgi-bin/passwd/TWiki/WebHome
Input name : oldpassword
Input name : password
Input name : passwordA

Page : /twiki/TWikiDocumentation.html
Destination page : http://TWiki.org/cgi-bin/passwd/Main/WebHome
Input name : password
Input name : passwordA

Page : /dvwa/login.php
Destination page : login.php
Input name : password

Page : /twiki/bin/view/TWiki/TWikiDocumentation
Destination page : http://192.168.56.3/twiki/bin/passwd/TWiki/WebHome
Input name : oldpassword
Input name : password
Input name : passwordA
34324 (2) - FTP Supports Clear Text Authentication

Synopsis
Authentication credentials might be intercepted.

Description
The remote FTP server allows the user's name and password to be transmitted in clear text, which could be intercepted by a network sniffer or a man-in-the-middle attack.

Solution
Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.

Risk Factor
Low

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

References
XREF CWE:522
XREF CWE:523

Plugin Information:
Publication date: 2008/10/01, Modification date: 2012/02/22

Hosts
192.168.56.3 (tcp/21)

This FTP server does not support 'AUTH TLS'.

192.168.56.3 (tcp/2121)

This FTP server does not support 'AUTH TLS'.

XREF CWE:522
XREF CWE:523
### Synopsis
An X11 server is listening on the remote host

### Description
The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.
Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

### Solution
Restrict access to this port. If the X11 client/server facility is not used, disable TCP entirely.

### 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: 2000/05/12, Modification date: 2011/03/11

### Hosts
192.168.56.3 (tcp/6000)

X11 Version : 11.0
Synopsis
The remote web server seems to transmit credentials in clear text.

Description
The remote web server contains web pages that are protected by 'Basic' authentication over plain text.
An attacker eavesdropping the traffic might obtain logins and passwords of valid users.

Solution
Make sure that HTTP authentication is transmitted over HTTPS.

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: 2008/11/21, Modification date: 2011/09/15

Hosts
192.168.56.3 (tcp/8180)

The following pages are protected.
/manager/html/ realm="Tomcat Manager Application"
/host-manager/html/ realm="Tomcat Host Manager Application"
/manager/status/ realm="Tomcat Manager Application"
42263 (1) - Unencrypted Telnet Server

Synopsis
The remote Telnet server transmits traffic in cleartext.

Description
The remote host is running a Telnet server over an unencrypted channel. Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in cleartext. An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information. Use of SSH is preferred nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.

Solution
Disable this service and use SSH instead.

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: 2009/10/27, Modification date: 2011/09/15

Hosts
192.168.56.3 (tcp/23)

Nessus collected the following banner from the remote Telnet server:

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

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:
-------------------------------- snip --------------------------------
The remote service allows repeated renegotiation of TLS / SSL connections.

The computational requirements for renegotiating a connection are asymmetrical between the client and the server, with the server performing several times more work. Since the remote host does not appear to limit the number of renegotiations for a single TLS / SSL connection, this permits a client to open several simultaneous connections and repeatedly renegotiate them, possibly leading to a denial of service condition.

Contact the vendor for specific patch information.

Low

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

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

CVE-2011-1473

OSVDB:73894

The remote host is vulnerable to renegotiation DoS over TLSv1 / SSLv3.
11219 (30) - 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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution
Protect your target with an IP filter.

Risk Factor
None

Hosts
192.168.56.3 (tcp/21)
Port 21/tcp was found to be open
192.168.56.3 (tcp/22)
Port 22/tcp was found to be open
192.168.56.3 (tcp/23)
Port 23/tcp was found to be open
192.168.56.3 (tcp/25)
Port 25/tcp was found to be open
192.168.56.3 (tcp/53)
Port 53/tcp was found to be open
192.168.56.3 (tcp/80)
Port 80/tcp was found to be open
192.168.56.3 (tcp/111)
Port 111/tcp was found to be open
192.168.56.3 (tcp/139)
Port 139/tcp was found to be open
192.168.56.3 (tcp/445)
Port 445/tcp was found to be open
192.168.56.3 (tcp/512)
Port 512/tcp was found to be open
192.168.56.3 (tcp/513)
Port 513/tcp was found to be open
192.168.56.3 (tcp/514)
Port 514/tcp was found to be open
192.168.56.3 (tcp/1099)
Port 1099/tcp was found to be open
192.168.56.3 (tcp/1524)
Port 1524/tcp was found to be open
192.168.56.3 (tcp/2049)
Port 2049/tcp was found to be open
192.168.56.3 (tcp/2121)
Port 2121/tcp was found to be open
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.56.3</td>
<td>3306/tcp</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>3632/tcp</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>5432/tcp</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>5900/tcp</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>6000/tcp</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>6667/tcp</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>6697/tcp</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>8009/tcp</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>8180/tcp</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>8787/tcp</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>37000/tcp</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>44501/tcp</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>51571/tcp</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>57176/tcp</td>
</tr>
</tbody>
</table>
### 11111 (10) - RPC Services Enumeration

**Synopsis**
An ONC RPC service is running on the remote host.

**Description**
By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

**Solution**
\[n/a\]

**Risk Factor**
None

**Plugin Information:**
Publication date: 2002/08/24, Modification date: 2011/05/24

**Hosts**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Port Type</th>
<th>Port Number</th>
<th>Services Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.56.3</td>
<td>TCP</td>
<td>111</td>
<td>- program: 100000 (portmapper), version: 2</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>UDP</td>
<td>111</td>
<td>- program: 100000 (portmapper), version: 2</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>TCP</td>
<td>2049</td>
<td>- program: 100003 (nfs), version: 2</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>UDP</td>
<td>2049</td>
<td>- program: 100003 (nfs), version: 2</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>UDP</td>
<td>2049</td>
<td>- program: 100003 (nfs), version: 2</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>UDP</td>
<td>2049</td>
<td>- program: 100003 (nfs), version: 2</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>UDP</td>
<td>33649</td>
<td>- program: 100005 (mountd), version: 1</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>TCP</td>
<td>37000</td>
<td>- program: 100005 (mountd), version: 1</td>
</tr>
<tr>
<td>192.168.56.3</td>
<td>TCP</td>
<td>44501</td>
<td>- program: 100021 (nlockmgr), version: 1</td>
</tr>
</tbody>
</table>
- program: 100021 (nlockmgr), version: 3
- program: 100021 (nlockmgr), version: 4

192.168.56.3 (udp/48701)

The following RPC services are available on UDP port 48701:
- program: 100024 (status), version: 1

192.168.56.3 (tcp/57176)

The following RPC services are available on TCP port 57176:
- program: 100024 (status), version: 1

192.168.56.3 (udp/58930)

The following RPC services are available on UDP port 58930:
- program: 100021 (nlockmgr), version: 1
- program: 100021 (nlockmgr), version: 3
- program: 100021 (nlockmgr), version: 4
**22964 (8) - 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: 2012/07/09

**Hosts**

192.168.56.3 (tcp/21)

An FTP server is running on this port.

192.168.56.3 (tcp/22)

An SSH server is running on this port.

192.168.56.3 (tcp/23)

A telnet server is running on this port.

192.168.56.3 (tcp/25)

An SMTP server is running on this port.

192.168.56.3 (tcp/80)

A web server is running on this port.

192.168.56.3 (tcp/2121)

An FTP server is running on this port.

192.168.56.3 (tcp/5900)

A vnc server is running on this port.

192.168.56.3 (tcp/8180)

A web server is running on this port.
There is an unknown service running on the remote host.

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

If you know what this service is and think the banner could be used to identify it, please send a description of the service along with the following output to svc-signatures@nessus.org:

192.168.56.3 (tcp/514)

Port : 514
Type : spontaneous
Banner:
0x00:  01 67 65 74 6E 61 6D 65 69 6E 66 6F 3A 20 54 65    .getnameinfo: Te
0x10:  6D 70 6F 72 61 72 79 20 66 61 69 6C 75 72 65 20  
mпорary failure
0x20:  69 6E 20 6E 61 6D 65 20 72 65 73 6F 6C 75 74 69  
in name resoluti
0x30:  on.

192.168.56.3 (tcp/1524)

Port : 1524
Type : spontaneous
Banner:
0x00:  72 6F 6F 74 40 6D 65 74 61 73 70 6C 6F 69 74 61  
root@metasploita
0x10:  ble:/#

192.168.56.3 (tcp/8787)

Port : 8787
Type : get_http
Banner:
0x0000:  00 00 00 03 04 08 46 00 03 A1 04 08 6F 3A 16      ......F......o:.
0x0010:  44 52 62 3A 3A 44 52 62 43 6F 6E 6E 45 72 72 6F    Drb:DrbConnErro
0x0020:  72 07 3A 07 62 74 5B 17 22 2F 2F 75 73 72 2F 6C    r:.bt[..]//usr/
0x0030:  69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F    ib/ruby/1.8/drb/
0x0040:  64 72 62 2E 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F    drb.rb:573:in `l
0x0050:  69 6E 20 60 69 6E 69 74 5F 77 69 74 68 5F 63 6C    oad''7/usr/l
0x0060:  69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F    ib/ruby/1.8/drb/
0x0070:  64 72 62 2E 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F    drb.rb:911:in `r
0x0080:  65 63 76 5F 72 65 71 75 65 73 74 27 22 37 2F 75  
cesv_request"7/usr/
0x0090:  73 72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F  
rib/ruby/1.8/drb/
0x00A0:  64 72 62 2E 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F    drb.rb:1530:
0x00B0:  65 63 76 5F 72 65 71 75 65 73 74 27 22 3C 2F 75  
ecv_request""/u
0x00C0:  73 72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F  
src/lib/ruby/1.8/
0x00D0:  64 72 62 2F 64 72 75 62 2E 72 62 2E 72 62 3A 31 35 33 33 30 3A  
0x00E0:  69 6E 20 60 69 6E 69 74 5F 77 69 74 68 5F 63 6C    in `init_with_co
### 10092 (2) - FTP Server Detection

<table>
<thead>
<tr>
<th><strong>Synopsis</strong></th>
<th>An FTP server is listening on this port.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>It is possible to obtain the banner of the remote FTP server by connecting to the remote port.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
<td>None</td>
</tr>
</tbody>
</table>

### Plugin Information:

- Publication date: 1999/10/12, Modification date: 2011/03/15

### Hosts

<table>
<thead>
<tr>
<th>192.168.56.3 (tcp/21)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The remote FTP banner is:</td>
</tr>
<tr>
<td>220 (vsFTPd 2.3.4)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>192.168.56.3 (tcp/2121)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The remote FTP banner is:</td>
</tr>
<tr>
<td>220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.56.3]</td>
</tr>
</tbody>
</table>
### 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: 2012/08/02

### Hosts

<table>
<thead>
<tr>
<th>Host</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.56.3 (tcp/80)</td>
<td>The remote web server type is:</td>
</tr>
<tr>
<td></td>
<td>Apache/2.2.8 (Ubuntu) DAV/2</td>
</tr>
<tr>
<td></td>
<td>You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.</td>
</tr>
<tr>
<td>192.168.56.3 (tcp/8180)</td>
<td>The remote web server type is:</td>
</tr>
<tr>
<td></td>
<td>Coyote HTTP/1.1 Connector</td>
</tr>
</tbody>
</table>


# 10662 (2) - Web mirroring

## Synopsis

Nessus crawled the remote web site.

## Description

This script makes a mirror of the remote web site(s) and extracts the list of CGIs that are used by the remote host. It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

## Solution

n/a

## Risk Factor

None

## Plugin Information:

Publication date: 2001/05/04, Modification date: 2012/06/07

## Hosts

192.168.56.3 (tcp/80)

The following CGI have been discovered:

Syntax: cginame (arguments [default value])

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/twiki/bin/view/Sandbox/WebTopicEditTemplate</td>
<td>unlock [on]</td>
</tr>
<tr>
<td>/twiki/bin/upload/TWiki/TWikiSystemRequirements</td>
<td>(filename [] filepath [] filecomment [] createlink []) hidefile []</td>
</tr>
<tr>
<td>/twiki/bin/clops/TWiki/WebIndex</td>
<td>(template [clopsmore] param2 [1.2] param1 [1.2])</td>
</tr>
<tr>
<td>/twiki/bin/view/TWiki/TWikiAuthentication</td>
<td>(unlock [on])</td>
</tr>
<tr>
<td>/twiki/edit/TWiki/ColanNahaboo</td>
<td>(t [1345017127])</td>
</tr>
<tr>
<td>/twiki/bin/upload/Sandbox/WebPreferences</td>
<td>(filename [] filepath [] filecomment [] createlink []) hidefile []</td>
</tr>
<tr>
<td>/twiki/bin/view/Know/TopicClassification</td>
<td>(skin [print] topic [] rev [1.2])</td>
</tr>
<tr>
<td>/twiki/edit/Main/BookView</td>
<td>(topicparent [Main.TWikiVariables])</td>
</tr>
<tr>
<td>/twiki/edit/TWiki/CrisBailiff</td>
<td>(t [1345017128])</td>
</tr>
<tr>
<td>/twiki/edit/Codev/UnchangeableTopicBug</td>
<td>(topicparent [TWiki.TWikiHistory])</td>
</tr>
<tr>
<td>/twiki/bin/view/TWiki/TWikiDocumentation</td>
<td>(unlock [on])</td>
</tr>
<tr>
<td>/twiki/bin/rdiff/Main/LondonOffice</td>
<td>(rev2 [1.2] rev1 [1.3])</td>
</tr>
<tr>
<td>/twiki/bin/attach/TWiki/PreviewBackground</td>
<td>(revInfo [1] filename [blankltgraybg.gif])</td>
</tr>
<tr>
<td>/twiki/bin/clops/Codev/UnchangeableTopicBug</td>
<td>(template [copsnowweb])</td>
</tr>
<tr>
<td>/twiki/bin/view/TWiki/DefaultPlugin</td>
<td>(skin [print] topic [] rev [1.4] unlock [on])</td>
</tr>
<tr>
<td>/twiki/bin/rdiff/TWiki/TWikiAccessControl</td>
<td>(rev2 [1.26] rev1 [1.27])</td>
</tr>
<tr>
<td>/twiki/edit/Sandbox/TextTopic1</td>
<td>(t [1345017219]) topicparent [Sandbox.WebHome]</td>
</tr>
<tr>
<td>/twiki/view/TWiki/WebChangesNotify</td>
<td>(unlock [on])</td>
</tr>
<tr>
<td>/twiki/bin/rdiff/Sandbox/WebChanges</td>
<td>(text [] fortemplate [] topicparent [] cmd [])</td>
</tr>
<tr>
<td>/twiki/bin/clops/Main/SupportGroup</td>
<td>(template [copsmore] param1 [1.1] param2 [1.1])</td>
</tr>
<tr>
<td>/twiki/edit/TWiki/TWikiBetaUpgradeNotes</td>
<td>(topicparent [TWiki.TWikiUpgradeTo01Dec2001])</td>
</tr>
<tr>
<td>/twiki/bin/rdiff/Know/WebIndex</td>
<td>(rev1 [1.2] rev2 [1.1])</td>
</tr>
<tr>
<td>/twiki/bin/upload/TWiki/WindowsInstallCookbook</td>
<td>(filename [] filepath [] filecomment [] createlink []) hidefile []</td>
</tr>
<tr>
<td>/twiki/bin/view/Main/TokyoOffice</td>
<td>(skin [print] topic [] rev [1.2] unlock [on])</td>
</tr>
<tr>
<td>/twiki/bin/edit/Sandbox/WebTopicList</td>
<td>(t [1345016962])</td>
</tr>
</tbody>
</table>

192.168.56.3 (tcp/8180)

The following CGI have been discovered:

Syntax: cginame (arguments [default value])

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/jsp-examples/error/err.jsp</td>
<td>(name [infiniti] submit [Submit])</td>
</tr>
<tr>
<td>/jsp-examples/jsp2/el/implicit-objects.jsp</td>
<td>(foo [bar])</td>
</tr>
<tr>
<td>/admin/_j_security_check;jsessionid=7D67332B1F9E09E36034C53277903FD2</td>
<td>(j_username [] j_password [])</td>
</tr>
<tr>
<td>/servlets-examples/servlet/SessionExample</td>
<td>(dataname [foo] datavalue [bar])</td>
</tr>
<tr>
<td>/jsp-examples/jsp2/el/functions.jsp</td>
<td>(foo [JSP+2.0])</td>
</tr>
<tr>
<td>/jsp-examples/num/numguess.jsp</td>
<td>(guess [])</td>
</tr>
<tr>
<td>/jsp-examples/colors/colors.jsp</td>
<td>(action [Submit] action [Hint])</td>
</tr>
<tr>
<td>/jsp-examples/cal/call.jsp</td>
<td>(name [] email [] action [Submit])</td>
</tr>
<tr>
<td>/jsp-examples/sessions/carts.jsp</td>
<td>(item [] submit [add] submit [remove])</td>
</tr>
</tbody>
</table>
11002 (2) - DNS Server Detection

**Synopsis**
A DNS server is listening on the remote host.

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

**See Also**
http://en.wikipedia.org/wiki/Domain_Name_System

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

**Risk Factor**
None

**Plugin Information:**
Publication date: 2003/02/13, Modification date: 2011/03/11

**Hosts**
192.168.56.3 (tcp/53)
192.168.56.3 (udp/53)
<table>
<thead>
<tr>
<th><strong>11011 (2) - Microsoft Windows SMB Service Detection</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synopsis</strong></td>
</tr>
<tr>
<td>A file / print sharing service is listening on the remote host.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
</tr>
<tr>
<td>n/a</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Plugin Information:</strong></td>
</tr>
<tr>
<td>Publication date: 2002/06/05, Modification date: 2012/01/31</td>
</tr>
<tr>
<td><strong>Hosts</strong></td>
</tr>
<tr>
<td><strong>192.168.56.3 (tcp/139)</strong></td>
</tr>
<tr>
<td>An SMB server is running on this port.</td>
</tr>
<tr>
<td><strong>192.168.56.3 (tcp/445)</strong></td>
</tr>
<tr>
<td>A CIFS server is running on this port.</td>
</tr>
</tbody>
</table>
**Synopsis**

It is possible to enumerate directories on the web server.

**Description**

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

**See Also**

http://projects.webappsec.org/Predictable-Resource-Location

**Solution**

n/a

**Risk Factor**

None

**References**

XREF  OWASP:OWASP-CM-006

**Plugin Information:**

Publication date: 2002/06/26, Modification date: 2012/04/14

**Hosts**

192.168.56.3 (tcp/80)

The following directories were discovered:
/cgi-bin, /doc, /test, /icons, /phpMyAdmin, /twiki/bin

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

192.168.56.3 (tcp/8180)

The following directories were discovered:
/admin, /jsp-examples, /servlets-examples

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

The following directories require authentication:
/host-manager/html, /manager/html
## 11419 (2) - Web Server Office File Inventory

### Synopsis
The remote web server hosts office-related files.

### Description
This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

### Solution
Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

### Risk Factor
None

### Plugin Information:
Publication date: 2003/03/19, Modification date: 2011/12/28

### Hosts

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.56.3</td>
<td>(tcp/80)</td>
</tr>
</tbody>
</table>

The following office-related files are available on the remote server:

- Adobe Acrobat files (.pdf):
  /mutillidae/documentation/mutillidae-installation-on-xampp-win7.pdf

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.56.3</td>
<td>(tcp/8180)</td>
</tr>
</tbody>
</table>

The following office-related files are available on the remote server:

- Adobe Acrobat files (.pdf):
  /tomcat-docs/architecture/requestProcess/requestProcess.pdf
  /tomcat-docs/architecture/startup/serverStartup.pdf
### 17975 (2) - Service Detection (GET request)

<table>
<thead>
<tr>
<th><strong>Synopsis</strong></th>
<th>The remote service could be identified.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
<td>None</td>
</tr>
</tbody>
</table>

**Plugin Information:**
Publication date: 2005/04/06, Modification date: 2012/07/24

<table>
<thead>
<tr>
<th><strong>Hosts</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>192.168.56.3 (tcp/6667)</strong></td>
<td>An IRC daemon is listening on this port.</td>
</tr>
<tr>
<td><strong>192.168.56.3 (tcp/6697)</strong></td>
<td>An IRC daemon is listening on this port.</td>
</tr>
</tbody>
</table>
**24004 (2) - WebDAV Directory Enumeration**

**Synopsis**
Several directories on the remote host are DAV-enabled.

**Description**
WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server. If you do not use this extension, you should disable it.

**Solution**
Disable DAV support if you do not use it.

**Risk Factor**
None

**Plugin Information:**
Publication date: 2007/01/11, Modification date: 2011/03/14

**Hosts**

**192.168.56.3 (tcp/80)**
The following directories are DAV enabled:
- /dav/

**192.168.56.3 (tcp/8180)**
The following directories are DAV enabled:
- /webdav/
### 24260 (2) - 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

192.168.56.3 (tcp/80)

<table>
<thead>
<tr>
<th>Protocol version</th>
<th>HTTP/1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>no</td>
</tr>
<tr>
<td>Keep-Alive</td>
<td>yes</td>
</tr>
<tr>
<td>Options allowed</td>
<td>(Not implemented)</td>
</tr>
<tr>
<td>Headers</td>
<td></td>
</tr>
</tbody>
</table>

- **Date**: Wed, 15 Aug 2012 07:57:17 GMT
- **Server**: Apache/2.2.8 (Ubuntu) DAV/2
- **X-Powered-By**: PHP/5.2.4-2ubuntu5.10
- **Keep-Alive**: timeout=15, max=100
- **Connection**: Keep-Alive
- **Transfer-Encoding**: chunked
- **Content-Type**: text/html

192.168.56.3 (tcp/8180)

<table>
<thead>
<tr>
<th>Protocol version</th>
<th>HTTP/1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>no</td>
</tr>
<tr>
<td>Keep-Alive</td>
<td>no</td>
</tr>
<tr>
<td>Options allowed</td>
<td>GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS</td>
</tr>
<tr>
<td>Headers</td>
<td></td>
</tr>
</tbody>
</table>

- **Server**: Apache-Coyote/1.1
- **Content-Type**: text/html;charset=ISO-8859-1
- **Date**: Wed, 15 Aug 2012 07:57:17 GMT
- **Connection**: close
**Synopsis**

Some cookies have been set by the web server.

**Description**

HTTP cookies are pieces of information that are presented by web servers and are sent back by the browser. As HTTP is a stateless protocol, cookies are a possible mechanism to keep track of sessions. This plugin displays the list of the HTTP cookies that were set by the web server when it was crawled.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2009/06/19, Modification date: 2011/03/15

**Hosts**

192.168.56.3 (tcp/80)

<table>
<thead>
<tr>
<th>path</th>
<th>/phpMyAdmin/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>pma_fontsize</td>
</tr>
<tr>
<td>value</td>
<td>82%25</td>
</tr>
<tr>
<td>version</td>
<td>1</td>
</tr>
<tr>
<td>expires</td>
<td>Fri, 14-Sep-2012 07:48:01 GMT</td>
</tr>
<tr>
<td>secure</td>
<td>0</td>
</tr>
<tr>
<td>httponly</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>path</th>
<th>/phpMyAdmin/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>pma_lang</td>
</tr>
<tr>
<td>value</td>
<td>en-utf-8</td>
</tr>
<tr>
<td>version</td>
<td>1</td>
</tr>
<tr>
<td>expires</td>
<td>Fri, 14-Sep-2012 07:48:00 GMT</td>
</tr>
<tr>
<td>secure</td>
<td>0</td>
</tr>
<tr>
<td>httponly</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>path</th>
<th>/phpMyAdmin/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>pma_charset</td>
</tr>
<tr>
<td>value</td>
<td>utf-8</td>
</tr>
<tr>
<td>version</td>
<td>1</td>
</tr>
<tr>
<td>expires</td>
<td>Fri, 14-Sep-2012 07:48:00 GMT</td>
</tr>
<tr>
<td>secure</td>
<td>0</td>
</tr>
<tr>
<td>httponly</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>path</th>
<th>/phpMyAdmin/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>phpMyAdmin</td>
</tr>
<tr>
<td>value</td>
<td>8d9a4c7fa47f7b2b41100c0cb66c781839b39ad2</td>
</tr>
<tr>
<td>version</td>
<td>1</td>
</tr>
<tr>
<td>secure</td>
<td>0</td>
</tr>
<tr>
<td>httponly</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>path</th>
<th>/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>security</td>
</tr>
<tr>
<td>value</td>
<td>high</td>
</tr>
<tr>
<td>version</td>
<td>1</td>
</tr>
<tr>
<td>secure</td>
<td>0</td>
</tr>
<tr>
<td>httponly</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>path</th>
<th>/phpMyAdmin/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>pma_collation_connection</td>
</tr>
<tr>
<td>value</td>
<td>deleted</td>
</tr>
<tr>
<td>version</td>
<td>1</td>
</tr>
<tr>
<td>expires</td>
<td>Tue, 16-Aug-2011 07:48:00 GMT</td>
</tr>
<tr>
<td>secure</td>
<td>0</td>
</tr>
<tr>
<td>httponly</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>path</th>
<th>/phpMyAdmin/</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>pma_theme</td>
</tr>
<tr>
<td>value</td>
<td>deleted</td>
</tr>
</tbody>
</table>
version = 1
expires = Tue, 16-Aug-2011 07:48:00 GMT
secure = 0
httponly = 0

path = /
name = PHPSESSID
value = 92fdabbf75ff71126c6daad9d9785d3f
version = 1
secure = 0
httponly = 0

This cookie was set by Tomcat(servlet/jsp engine) :
path = /servlets-examples
name = JSESSIONID
value = D57E0062FC5D04F537A8A955F5DB393
version = 1
secure = 0
httponly = 0

This cookie was set by Tomcat(servlet/jsp engine) :
path = /jsp-examples
name = JSESSIONID
value = 41BF97DBAB77D119E3DABB0945C79B5
version = 1
secure = 0
httponly = 0

This cookie was set by Tomcat(servlet/jsp engine) :
path = /admin
name = JSESSIONID
value = 7D67332B1F9E09E36034C53277903FD2
version = 1
secure = 0
httponly = 0

192.168.56.3 (tcp/8180)

This cookie was set by Tomcat(servlet/jsp engine) :
path = /servlets-examples
name = JSESSIONID
value = D57E0062FC5D04F537A8A955F5DB393
version = 1
secure = 0
httponly = 0

This cookie was set by Tomcat(servlet/jsp engine) :
path = /jsp-examples
name = JSESSIONID
value = 41BF97DBAB77D119E3DABB0945C79B5
version = 1
secure = 0
httponly = 0

This cookie was set by Tomcat(servlet/jsp engine) :
path = /admin
name = JSESSIONID
value = 7D67332B1F9E09E36034C53277903FD2
version = 1
secure = 0
httponly = 0
42057 (2) - Web Server Allows Password Auto-Completion

**Synopsis**
Auto-complete is not disabled on password fields.

**Description**
The remote web server contains at least HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.
While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.

**Solution**
Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

**Risk Factor**
None

**Plugin Information:**
Publication date: 2009/10/07, Modification date: 2011/09/28

**Hosts**

**192.168.56.3 (tcp/80)**

Page : /twiki/TWikiDocumentation.html
Destination Page : http://TWiki.org/cgi-bin/passwd/TWiki/WebHome
Input name : oldpassword
Input name : password
Input name : passwordA

Page : /twiki/TWikiDocumentation.html
Destination Page : http://TWiki.org/cgi-bin/passwd/Main/WebHome
Input name : password
Input name : passwordA

Page : /twiki/bin/view/TWiki/TWikiDocumentation
Destination Page : http://192.168.56.3/twiki/bin/passwd/TWiki/WebHome
Input name : oldpassword
Input name : password
Input name : passwordA

Page : /twiki/bin/view/TWiki/TWikiDocumentation
Destination Page : http://192.168.56.3/twiki/bin/passwd/Main/WebHome
Input name : password
Input name : passwordA

Page : /twiki/bin/view/TWiki/TWikiUserAuthentication
Destination Page : http://192.168.56.3/twiki/bin/passwd/TWiki/WebHome
Input name : oldpassword
Input name : password
Input name : passwordA

Page : /twiki/bin/view/TWiki/TWikiUserAuthentication
Destination Page : http://192.168.56.3/twiki/bin/passwd/Main/WebHome
Input name : password
Input name : passwordA
Page : /twiki/bin/rdiff/TWiki/TWikiDocumentation
Destination Page : http://192.168.56.3/twiki/bin/passwd/TWiki/WebHome
Input name : oldpassword
Input name : password
Input name : passwordA

Page : /twiki/bin/rdiff/TWiki/TWikiDocumentation
Destination Page : http://192.168.56.3/twiki/bin/passwd/Main/WebHome
Input name : password
Input name : passwordA

Page : /twiki/bin/view/TWiki/TWikiRegistrationPub
Destination Page : http://192.168.56.3/twiki/bin/register/Main/WebHome
Input name : Twk1Password
Input name : Twk1Confirm

Page : /twiki/bin/rdiff/TWiki/TWikiRegistrationPub
Destination Page : http://192.168.56.3/twiki/bin/register
Input name : Twk1Password
Input name : Twk1Password
Input name : Twk1Confirm
Input name : Twk1Confirm
Input name : Twk1Password
Input name : Twk1Confirm

Page : /twiki/bin/view/TWiki/ChangePassword
Destination Page : http://192.168.56.3/twiki/bin/passwd/TWiki/WebHome
Input name : oldpassword
Input name : password
Input name : passwordA

Page  

192.168.56.3 (tcp/8180)

Page : /admin/
Destination Page : j_security_check;jsessionid=7D67332B1F9E09E36D34C53277903FD2
Input name : j_password
**43111 (2) - HTTP Methods Allowed (per directory)**

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

**Description**
By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

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

**Solution**

n/a

**Risk Factor**
None

**Plugin Information:**
Publication date: 2009/12/10, Modification date: 2011/07/08

**Hosts**

<table>
<thead>
<tr>
<th>192.168.56.3 (tcp/80)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the response to an OPTIONS request :</td>
</tr>
</tbody>
</table>

- HTTP methods COPY DELETE GET HEAD LOCK MOVE OPTIONS POST PROPFIND PROPPATCH TRACE UNLOCK are allowed on :

  /dav

- HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

  /doc
  /dvwa/dvwa
  /dvwa/dvwa/images
  /icons
  /mutillidae/documentation
  /mutillidae/images
  /mutillidae/javascript
  /mutillidae/javascript/ddsmoothmenu
  /oops/TWiki
  /p/pub/TWiki/TWikiTemplates
  /p/pub/icn
  /phpMyAdmin/themes
  /phpMyAdmin/themes/original
  /phpMyAdmin/themes/original/css
  /phpMyAdmin/themes/original/img
  /rdiff/TWiki
  /test
  /test/testoutput
  /twiki
  /twiki/changes
  /twiki/pub
  /twiki/pub/Know/IncorrectDllVersionW32PTH10DLL
  /twiki/pub/TWiki/PreviewBackground
  /twiki/pub/TWiki/TWiki
  /twiki/pub/TWiki/TWikiDocGraphics
  /twiki/pub/TWiki/TWikiLogos
  /twiki/pub/TWiki/TWikiPreferences
  /twiki/pub/TWiki/TWikiTemplates
  /twiki/pub/TWiki/WabiSabi
  /twiki/pub/TWiki/WebHome
  /twiki/pub/icn
  /twiki/search/Know
  /twiki/search/Main
  /twiki/view/Main
  /view/TWiki
192.168.56.3 (tcp/8180)

Based on the response to an OPTIONS request:

- HTTP methods: COPY DELETE GET HEAD LOCK MOVE POST PROPFIND
  PROPPATCH TRACE UNLOCK OPTIONS are allowed on:
  /webdav

- HTTP methods: DELETE HEAD OPTIONS POST PUT TRACE GET
  are allowed on:
  /admin/images
  /include
  /jsp-examples/cal
  /jsp-examples/checkbox
  /jsp-examples/colors
  /jsp-examples/dates
  /jsp-examples/error
  /jsp-examples/forward
  /jsp-examples/images
  /jsp-examples/include
  /jsp-examples/jsp2/el
  /jsp-examples/jsp2/jspattribute
  /jsp-examples/jsp2/jspx
  /jsp-examples/jsp2/misc
  /jsp-examples/jsp2/simpletag
  /jsp-examples/jsp2/tagfiles
  /jsp-examples/jsp2/taglib
  /jsp-examples/jsp2/tagserv
  /jsp-examples/num
  /jsp-examples/plugin
  /jsp-examples/sessions
  /jsp-examples/simpletag
  /jsp-examples/snp
  /jsp-examples/tagplugin
  /jsp-examples/xml
  /manager
  /servlets-examples
  /servlets-examples/images
  /servlets-examples/servlet
  /tomcat-docs
  /tomcat-docs/appdev
  /tomcat-docs/appdev/printer
  /tomcat-docs/appdev/sample
  /tomcat-docs/architecture
  /tomcat-docs/architecture/printer
  /tomcat-docs/architecture/requestProcess
  /tomcat-docs/architecture/startup
  /tomcat-docs/catalina/docs/api
  /tomcat-docs/catalina/docs/api/org/apache/catalina
  /tomcat-docs/catalina/docs/api/org/apache/catalina/core
  /tomcat-docs/catalina/docs/api/org/apache/catalina/funcspecs
  /tomcat-docs/catalina/docs/api/org/apache/catalina/funcspecs/printer
  /tomcat-docs/config
  /tomcat-docs/config/printer
  /tomcat-docs/images
  /tomcat-docs/jasper/docs/api
  /tomcat-docs/jspapi
  /tomcat-docs/jspapi/java/servlet/jsp
  /tomcat-docs/jspapi/java/servlet/jsp/el
  /tomcat-docs/jspapi/java/servlet/jsp/tagext
  /tomcat-docs/jspapi/java/servlet/jsp/tagext/doc-files
  /tomcat-docs/jspapi/resources
  /tomcat-docs/printer
  /tomcat-docs/servletapi
  /tomcat-docs/servletapi/java/servlet
  /tomcat-docs/servletapi/java/servlet/http
  /tomcat-docs/servletapi/resources
## Synopsis

Links to external sites were gathered.

## Description

Nessus gathered HREF links to external sites by crawling the remote web server.

## Solution

n/a

## Risk Factor

None

## Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/08/19

### Hosts

**192.168.56.3 (tcp/80)**

200 external URLs were gathered on this web server:

<table>
<thead>
<tr>
<th>URL...</th>
<th>- Seen on...</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://TWiki.SourceForge.net/">http://TWiki.SourceForge.net/</a></td>
<td>- /twiki/bin/rdiff/Main/WebHome</td>
</tr>
<tr>
<td><a href="http://TWiki.SourceForge.net/cgi-bin/view/Codev/AttachedNotificationLinksBug">http://TWiki.SourceForge.net/cgi-bin/view/Codev/AttachedNotificationLinksBug</a></td>
<td>- /twiki/bin/rdiff/TWiki/TWikiHistory</td>
</tr>
<tr>
<td><a href="http://TWiki.SourceForge.net/cgi-bin/view/Codev/AuthenticationBasedOnGroups">http://TWiki.SourceForge.net/cgi-bin/view/Codev/AuthenticationBasedOnGroups</a></td>
<td>- /twiki/bin/rdiff/TWiki/TWikiHistory</td>
</tr>
<tr>
<td><a href="http://TWiki.SourceForge.net/cgi-bin/view/Codev/BetterTWikiTagTemplateProcessing">http://TWiki.SourceForge.net/cgi-bin/view/Codev/BetterTWikiTagTemplateProcessing</a></td>
<td>- /twiki/bin/rdiff/TWiki/TWikiHistory</td>
</tr>
<tr>
<td><a href="http://TWiki.SourceForge.net/cgi-bin/view/Codev/FeatureEnhancementRequest">http://TWiki.SourceForge.net/cgi-bin/view/Codev/FeatureEnhancementRequest</a></td>
<td>- /twiki/bin/rdiff/TWiki/TWikiEnhancementRequests</td>
</tr>
<tr>
<td><a href="http://TWiki.SourceForge.net/cgi-bin/view/Codev/FeatureToDo">http://TWiki.SourceForge.net/cgi-bin/view/Codev/FeatureToDo</a></td>
<td>- /twiki/bin/rdiff/TWiki/TWikiPlannedFeatures</td>
</tr>
<tr>
<td><a href="http://TWiki.SourceForge.net/cgi-bin/view/Codev/FeatureUnderConstruction">http://TWiki.SourceForge.net/cgi-bin/view/Codev/FeatureUnderConstruction</a></td>
<td>- /twiki/bin/rdiff/TWiki/TWikiPlannedFeatures</td>
</tr>
<tr>
<td><a href="http://TWiki.SourceForge.net/cgi-bin/view/Main/PoweredByTWikiLogo">http://TWiki.SourceForge.net/cgi-bin/view/Main/PoweredByTWikiLogo</a></td>
<td>- /twiki/bin/rdiff/TWiki/TWikiHistory</td>
</tr>
<tr>
<td><a href="http://TWiki.org/cgi-bin/view/Main/MikeMannix">http://TWiki.org/cgi-bin/view/Main/MikeMannix</a></td>
<td>- /twiki/TWikiInstallationGuide</td>
</tr>
<tr>
<td><a href="http://TWiki.org/cgi-bin/view/Main/RichardDonkin">http://TWiki.org/cgi-bin/view/Main/RichardDonkin</a></td>
<td>- /twiki/TWikiDocumentation.html</td>
</tr>
<tr>
<td><a href="http://TWiki.org/cgi-bin/view/Main/TWikiAdminGroup">http://TWiki.org/cgi-bin/view/Main/TWikiAdminGroup</a></td>
<td>- /twiki/TWikiDocumentation.html</td>
</tr>
<tr>
<td><a href="http://TWiki.org/cgi-bin/view/Main/WebHome">http://TWiki.org/cgi-bin/view/Main/WebHome</a></td>
<td>- /twiki/TWikiDocumentation.html</td>
</tr>
<tr>
<td><a href="http://TWiki.org/cgi-bin/view/TWiki/AdminSkillsAssumptions">http://TWiki.org/cgi-bin/view/TWiki/AdminSkillsAssumptions</a></td>
<td>- /twiki/TWikiDocumentation.html</td>
</tr>
<tr>
<td><a href="http://TWiki.org/cgi-bin/view/TWiki/AppendixFileSystem">http://TWiki.org/cgi-bin/view/TWiki/AppendixFileSystem</a></td>
<td>- /twiki/TWikiDocumentation.html</td>
</tr>
<tr>
<td><a href="http://TWiki.org/cgi-bin/view/TWiki/FeatureEnhancementRequests">http://TWiki.org/cgi-bin/view/TWiki/FeatureEnhancementRequests</a></td>
<td>- /twiki/TWikiDocumentation.html</td>
</tr>
<tr>
<td><a href="http://TWiki.org/cgi-bin/view/TWiki/MikeMannix">http://TWiki.org/cgi-bin/view/TWiki/MikeMannix</a></td>
<td>- /twiki/TWikiDocumentation.html</td>
</tr>
<tr>
<td><a href="http://TWiki.org/cgi-bin/view/TWiki/PeterThoeny">http://TWiki.org/cgi-bin/view/TWiki/PeterThoeny</a></td>
<td>- /twiki/TWikiDocumentation.html</td>
</tr>
<tr>
<td><a href="http://TWiki.org/cgi-bin/view/TWiki/NewUserTemplate">http://TWiki.org/cgi-bin/view/TWiki/NewUserTemplate</a></td>
<td>- /twiki/TWikiDocumentation.html</td>
</tr>
</tbody>
</table>

**192.168.56.3 (tcp/8180)**

1 external URL was gathered on this web server:

<table>
<thead>
<tr>
<th>URL...</th>
<th>- Seen on...</th>
</tr>
</thead>
<tbody>
<tr>
<td>irc://irc.freenode.net/</td>
<td>- /</td>
</tr>
</tbody>
</table>

167
## Synopsis

Email addresses were gathered.

## Description

Nessus gathered mailto: HREF links and extracted email addresses by crawling the remote web server.

## Solution

N/A

## Risk Factor

None

## Plugin Information:

Publication date: 2010/10/04, Modification date: 2012/05/09

## Hosts

192.168.56.3 (tcp/80)

The following email addresses have been gathered:

- 'Peter@Thoeny.com', referenced from:
  /twiki/bin/view/Main/PeterThoeny
  /twiki/bin/rdiff/TWiki/TWikiDocumentation
  /twiki/bin/rdiff/Know/WebNotify
  /twiki/bin/rdiff/TWiki/PeterThoeny
  /twiki/bin/rdiff/Main/WebNotify
  /twiki/bin/view/TWiki/TWikiDocumentation
  /twiki/bin/rdiff/Sandbox/WebNotify
  /twiki/bin/rdiff/TWiki/TWikiFuncModule
  /twiki/bin/rdiff/TWiki/TWikiFunctionModule.html
  /twiki/bin/rdiff/TWiki/WebNotify
  /twiki/bin/rdiff/TWiki/TWikiPreferences
  /twiki/bin/view/TWiki/TWikiFuncModule
  /twiki/bin/rdiff/Main/PeterThoeny

- 'john.talintyre@drkw.com', referenced from:
  /twiki/bin/rdiff/Main/JohnTalintyre

- 'name@domain.com', referenced from:
  /twiki/bin/rdiff/TWiki/TextFormattingRules

- 'webmaster@your.company', referenced from:
  /twiki/bin/attach/TWiki/SiteMap
  /twiki/bin/edit/Main/EngineeringGroup
  /twiki/bin/rdiff/TWiki/TWikiAccessControl
  /twiki/bin/edit/TWiki/WEBTWikiTemplates
  /twiki/bin/view/Know/WebNotify
  /twiki/bin/rdiff/Sandbox/WebNotify
  /twiki/bin/edit/TWiki/TWikiAlphaRelease
  /twiki/bin/view/TWiki/AdminSkillsAssumptions
  /twiki/bin/view/TWiki/wikiNotation
  /twiki/bin/edit/Sandbox/TestTopic7
  /twiki/bin/rdiff/TWiki/BookView
  /twiki/bin/edit/TWiki/TWikiRegistration
  /twiki/bin/view/TWiki/RandyKramer
  /twiki/bin/rdiff/Main/TWikiVariables
  /twiki/bin/view/TWiki/TemplateWeb
  /twiki/bin/view/Main/
  /twiki/bin/attach/TWiki/StandardColors
  /twiki/bin/view/Know/OperatingSystem
  /twiki/bin/view/TWiki/wikiWikiClones
  /twiki/bin/rdiff/TWiki/HiddenAttachment
  /twiki/bin/edit/TWiki/TWikiCodecFeatureToDo
  /twiki/bin/edit/Main/UnlockTopic
  /twiki/bin/view/Know
  /twiki/bin/view/Know/PublicFAQ
  /twiki/bin/view/TWiki/AlWilliams
The following email addresses have been gathered:

- 'users@tomcat.apache.org', referenced from:
  /tomcat-docs/architecture/index.html
  /tomcat-docs/architecture/printer/
  /tomcat-docs/architecture/printer/index.html

- 'yoavs@apache.org', referenced from:
  /tomcat-docs/appdev/
  /tomcat-docs/appdev/printer/
  /tomcat-docs/appdev/printer/index.html
  /tomcat-docs/appdev/index.html

- 'craigmcc@apache.org', referenced from:
  /tomcat-docs/architecture/printer/index.html
  /tomcat-docs/architecture/
  /tomcat-docs/architecture/printer/
  /tomcat-docs/architecture/index.html

- 'fhanik@apache.org', referenced from:
  /tomcat-docs/architecture/printer/index.html
  /tomcat-docs/architecture/
  /tomcat-docs/architecture/printer/
  /tomcat-docs/architecture/index.html

- 'jfarcand@apache.org', referenced from:
  /tomcat-docs/architecture/printer/index.html
  /tomcat-docs/architecture/
  /tomcat-docs/architecture/printer/
  /tomcat-docs/architecture/index.html

- 'dev@tomcat.apache.org', referenced from:
  /
**Synopsis**

It is possible to obtain the version number of the remote DNS server.

**Description**

The remote host is running BIND or another DNS server that reports its version number when it receives a special request, for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

**Solution**

It is possible to hide the version number of bind by using the 'version' directive in the 'options' section in named.conf

**Risk Factor**

None

**References**

XREF

OSVDB:23

**Plugin Information:**

Publication date: 1999/10/12, Modification date: 2011/05/24

**Hosts**

192.168.56.3 (udp/53)

The version of the remote DNS server is:

9.4.2
**Synopsis**

It is possible to determine the exact time set on the remote host.

**Description**

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

**Solution**

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

**Risk Factor**

None

**References**

<table>
<thead>
<tr>
<th>CVE</th>
<th>CVE-1999-0524</th>
</tr>
</thead>
<tbody>
<tr>
<td>XREF</td>
<td>OSVDB:94</td>
</tr>
<tr>
<td>XREF</td>
<td>CWE:200</td>
</tr>
</tbody>
</table>

**Plugin Information:**

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

**Hosts**

192.168.56.3 (icmp/0)

The difference between the local and remote clocks is -13832 seconds.
**10150 (1) - Windows NetBIOS / SMB Remote Host Information Disclosure**

**Synopsis**

It is possible to obtain the network name of the remote host.

**Description**

The remote host listens on UDP port 137 or TCP port 445 and replies to NetBIOS nbtscan or SMB requests. Note that this plugin gathers information to be used in other plugins but does not itself generate a report.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 1999/10/12, Modification date: 2012/02/10

**Hosts**

**192.168.56.3 (udp/137)**

The following 7 NetBIOS names have been gathered:

- **METASPLOITABLE** = Computer name
- **METASPLOITABLE** = Messenger Service
- **METASPLOITABLE** = File Server Service
- **__MSBROWSE__** = Master Browser
- **WORKGROUP** = Workgroup / Domain name
- **WORKGROUP** = Master Browser
- **WORKGROUP** = Browser Service Elections

This SMB server seems to be a SAMBA server (MAC address is NULL).
**Synopsis**
An ONC RPC portmapper is running on the remote host.

**Description**
The RPC portmapper is running on this port.
The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

**Solution**
n/a

**Risk Factor**
None

**References**
CVE
CVE-1999-0632

**Plugin Information:**
Publication date: 1999/08/19, Modification date: 2011/11/15

**Hosts**
192.168.56.3 (udp/111)
<table>
<thead>
<tr>
<th><strong>10263 (1) - SMTP Server Detection</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synopsis</strong></td>
</tr>
<tr>
<td>An SMTP server is listening on the remote port.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>The remote host is running a mail (SMTP) server on this port. Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
</tr>
<tr>
<td>Disable this service if you do not use it, or filter incoming traffic to this port.</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Plugin Information:</strong></td>
</tr>
<tr>
<td>Publication date: 1999/10/12, Modification date: 2011/03/11</td>
</tr>
<tr>
<td><strong>Hosts</strong></td>
</tr>
<tr>
<td>192.168.56.3 (tcp/25)</td>
</tr>
</tbody>
</table>

Remote SMTP server banner:

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
<table>
<thead>
<tr>
<th><strong>10267 (1) - SSH Server Type and Version Information</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synopsis</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Solution</strong></td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
</tr>
<tr>
<td><strong>Plugin Information:</strong></td>
</tr>
<tr>
<td><strong>Hosts</strong></td>
</tr>
</tbody>
</table>

SSH version : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1  
SSH supported authentication : publickey,password
10281 (1) - Telnet Server Detection

Synopsis

A Telnet server is listening on the remote port.

Description

The remote host is running a Telnet server, a remote terminal server.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/03/17

Hosts

192.168.56.3 (tcp/23)

Here is the banner from the remote Telnet server:

________________________________ snip _____________________________

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:
________________________________ snip _____________________________
### 10287 (1) - Traceroute Information

<table>
<thead>
<tr>
<th><strong>Synopsis</strong></th>
<th>It was possible to obtain traceroute information.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Makes a traceroute to the remote host.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Plugin Information:</strong></td>
<td>Publication date: 1999/11/27, Modification date: 2012/02/23</td>
</tr>
<tr>
<td><strong>Hosts</strong></td>
<td><strong>192.168.56.3 (udp/0)</strong></td>
</tr>
</tbody>
</table>
| | For your information, here is the traceroute from 192.168.56.1 to 192.168.56.3:
| | 192.168.56.1
| | 192.168.56.3 |
### 10342 (1) - VNC Software Detection

**Synopsis**

The remote host is running a remote display software (VNC).

**Description**

The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) protocol to provide remote access to graphical user interfaces and thus permits a console on the remote host to be displayed on another.

**See Also**

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

**Solution**

Make sure use of this software is done in accordance with your organization's security policy and filter incoming traffic to this port.

**Risk Factor**

None

**Plugin Information:**

Publication date: 2000/03/07, Modification date: 2011/04/01

**Hosts**

192.168.56.3 (tcp/5900)

The highest RFB protocol version supported by the server is:

3.3
**Synopsis**
It is possible to log into the remote host.

**Description**
The remote host is running Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts:
- NULL session
- Guest account
- Given Credentials

**See Also**
http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

**Solution**
n/a

**Risk Factor**
None

**Exploitable with**
Metasploit (true)

**Plugin Information:**
Publication date: 2000/05/09, Modification date: 2012/03/06

**Hosts**
192.168.56.3 (tcp/445)
- NULL sessions are enabled on the remote host
### Microsoft Windows SMB Shares Enumeration

#### Synopsis
It is possible to enumerate remote network shares.

#### Description
By connecting to the remote host, Nessus was able to enumerate the network share names.

#### Solution
n/a

#### Risk Factor
None

#### Plugin Information:
Publication date: 2000/05/09, Modification date: 2012/07/09

#### Hosts
192.168.56.3 (tcp/445)

Here are the SMB shares available on the remote host when logged as a NULL session:

- print$
- tmp
- opt
- IPC$
- ADMIN$
### Synopsis
It is possible to obtain network information.

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

### Solution
n/a

### Risk Factor
None

### References

#### XREF
- OSVDB:300

### Plugin Information:
- Publication date: 2000/05/09, Modification date: 2011/09/14

### Hosts

#### 192.168.56.3 (tcp/445)

Here is the browse list of the remote host:

METASPOITABLE ( os : 0.0 )
## 10437 (1) - NFS Share Export List

<table>
<thead>
<tr>
<th><strong>Synopsis</strong></th>
<th>The remote NFS server exports a list of shares.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>This plugin retrieves the list of NFS exported shares.</td>
</tr>
</tbody>
</table>

### See Also

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

### Solution

Ensure each share is intended to be exported.

### Risk Factor

None

### Plugin Information:

Publication date: 2000/06/07, Modification date: 2011/05/24

### Hosts

**192.168.56.3 (tcp/2049)**

Here is the export list of 192.168.56.3:

/ *
10719 (1) - MySQL Server Detection

**Synopsis**

A database server is listening on the remote port.

**Description**

The remote host is running MySQL, an open-source database server.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2001/08/13, Modification date: 2011/09/14

**Hosts**

192.168.56.3 (tcp/3306)

Version : 5.0.51a-3ubuntu5
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :

- CLIENT_LONG_FLAG (Get all column flags)
- CLIENT_CONNECT_WITH_DB (One can specify db on connect)
- CLIENT_COMPRESS (Can use compression protocol)
- CLIENT_PROTOCOL_41 (New 4.1 protocol)
- CLIENT_SSL (Switch to SSL after handshake)
- CLIENT_TRANSACTIONS (Client knows about transactions)
- CLIENT_SECURE_CONNECTION (New 4.1 authentication)
### Synopsis
It is possible to obtain information about the remote operating system.

### Description
It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445.

### Solution
n/a

### Risk Factor
None

### Plugin Information:
Publication date: 2001/10/17, Modification date: 2011/03/17

### Hosts
192.168.56.3 (tcp/445)
- The remote Operating System is: Unix
- The remote native lan manager is: Samba 3.0.20-Debian
- The remote SMB Domain Name is: METASPLOITABLE
<table>
<thead>
<tr>
<th><strong>Synopsis</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>It is possible to obtain the host SID for the remote host.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier). The host SID can then be used to get the list of local users.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>See Also</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Solution</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value. Refer to the 'See also' section for guidance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Risk Factor</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Plugin Information:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Publication date: 2002/02/13, Modification date: 2011/09/15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Hosts</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>192.168.56.3 (tcp/445)</strong></td>
</tr>
</tbody>
</table>

The remote host SID value is: 
1-5-21-1042354039-2475377354-766472396

The value of 'RestrictAnonymous' setting is: unknown
Synopsis
It is possible to enumerate local users.

Description
Using the host security identifier (SID), it is possible to enumerate local users on the remote Windows system.

Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2002/02/13, Modification date: 2011/09/15

Hosts
192.168.56.3 (tcp/445)

- Administrator (id 500, Administrator account)
- nobody (id 501, Guest account)
- root (id 1000)
- root (id 1001)
- daemon (id 1002)
- daemon (id 1003)
- bin (id 1004)
- bin (id 1005)
- sys (id 1006)
- sys (id 1007)
- sync (id 1008)
- adm (id 1009)
- games (id 1010)
- tty (id 1011)
- man (id 1012)
- disk (id 1013)
- lp (id 1014)
- lp (id 1015)
- mail (id 1016)
- mail (id 1017)
- news (id 1018)
- news (id 1019)
- uucp (id 1020)
- uucp (id 1021)
- man (id 1025)
- proxy (id 1026)
- proxy (id 1027)
- kmem (id 1031)
- dialout (id 1041)
- fax (id 1043)
- voice (id 1045)
- cdrom (id 1049)
- floppy (id 1051)
- tape (id 1053)
- sudo (id 1055)
- audio (id 1059)
- dip (id 1061)
- www-data (id 1066)
- www-data (id 1067)
- backup (id 1068)
- backup (id 1069)
- operator (id 1075)
- list (id 1076)
- list (id 1077)
- irc (id 1078)
- irc (id 1079)
- src (id 1081)
- gnats (id 1082)
- gnats (id 1083)
- shadow (id 1085)
- utmp (id 1087)
- video (id 1089)
- sasl (id 1091)
- plugdev (id 1093)
- staff (id 1101)
- games (id 1121)
- libuuid (id 1200)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.
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

192.168.56.3 (tcp/25)

Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
73 FF 3C E5 9E 3B 6D PC C8 B1 AC FA 4C 4D 5E 98 4C 99 54 0B
D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
BD 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A FA F8 17 6A
0C CF 66 AA A7 65 2F 4B 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
1E B4 4F 8E D4 BD DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
68 35 19 75 OC DA 53 23 8B 88 19 2D 74 26 C1 22 65 EE 11 6B
83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
15 6E 8D 3D 38 F6 CA 2E 75
### 10881 (1) - SSH Protocol Versions Supported

<table>
<thead>
<tr>
<th><strong>Synopsis</strong></th>
<th>A SSH server is running on the remote host.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
<td>None</td>
</tr>
</tbody>
</table>

#### Plugin Information:
Publication date: 2002/03/06, Modification date: 2012/04/04

#### Hosts
192.168.56.3 (tcp/22)

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

- 1.99
- 2.0

### 11153 (1) - Service Detection (HELP Request)

<table>
<thead>
<tr>
<th><strong>Synopsis</strong></th>
<th>The remote service could be identified.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
<td>None</td>
</tr>
</tbody>
</table>

**Plugin Information:**
- Publication date: 2002/11/18, Modification date: 2012/06/29

**Hosts**
- **192.168.56.3 (tcp/3306)**

A MySQL server is running on this port.
### 11422 (1) - Web Server Unconfigured - Default Install Page Present

<table>
<thead>
<tr>
<th><strong>Synopsis</strong></th>
<th>The remote web server is not configured or is not properly configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>The remote web server uses its default welcome page. It probably means that this server is not used at all or is serving content that is meant to be hidden.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>Disable this service if you do not use it.</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>References</strong></td>
<td>XREF OSVDB:2117</td>
</tr>
</tbody>
</table>

**Plugin Information:**
Publication date: 2003/03/20, Modification date: 2011/08/12

### Hosts

<table>
<thead>
<tr>
<th><strong>192.168.56.3 (tcp/8180)</strong></th>
</tr>
</thead>
</table>

The default welcome page is from Tomcat.
<table>
<thead>
<tr>
<th><strong>11424 (1) - WebDAV Detection</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synopsis</strong></td>
</tr>
<tr>
<td>The remote server is running with WebDAV enabled.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| WebDAV is an industry standard extension to the HTTP specification.  
If you do not use this extension, you should disable it. |
| **Solution**                     |
| **Risk Factor**                  |
| None                             |
| **Plugin Information:**          |
| Publication date: 2003/03/20, Modification date: 2011/03/14 |
| **Hosts**                        |
| 192.168.56.3 (tcp/80)            |
TFTP Daemon Detection

Synopsis
A TFTP server is listening on the remote port.

Description
The remote host is running a TFTP (Trivial File Transfer Protocol) daemon. TFTP is often used by routers and diskless hosts to retrieve their configuration. It is also used by worms to propagate.

Solution
Disable this service if you do not use it.

Risk Factor
None

Plugin Information:
Publication date: 2003/08/13, Modification date: 2011/03/17

Hosts
192.168.56.3 (udp/69)
### 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, and sometimes its version.

### Solution
n/a

### Risk Factor
None

### Plugin Information:
Publication date: 2003/12/09, Modification date: 2012/04/06

### Hosts

<table>
<thead>
<tr>
<th>192.168.56.3 (tcp/0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote operating system : Linux Kernel 2.6 on Ubuntu 8.04 (hardy)</td>
</tr>
<tr>
<td>Confidence Level : 95</td>
</tr>
<tr>
<td>Method : SSH</td>
</tr>
</tbody>
</table>

Not all fingerprints could give a match – please email the following to os-signatures@nessus.org :

SinFP:
P1:B10113:F0x12:W5840:000204ffff:M1460:
P2:B10113:F0x12:W5792:000204ffff0402080affffffff4445414401030305:M1460:
P3:B10120:F0x04:W0:O0:M0
P4:5002_7_p=3632

SMTP:!:220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

ed093088706603bfd5dc237399b498da2d4d31c6

SSH:SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

The remote host is running Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
192.168.56.3 (tcp/80)

The following instance of phpMyAdmin was detected on the remote host:

Version : 3.1.1
URL : http://192.168.56.3/phpMyAdmin/
17651 (1) - Microsoft Windows SMB : Obtains the Password Policy

**Synopsis**

It is possible to retrieve the remote host's password policy using the supplied credentials.

**Description**

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information:**

Publication date: 2005/03/30, Modification date: 2011/03/04

**Hosts**

192.168.56.3 (tcp/445)

The following password policy is defined on the remote host:

- Minimum password len: 5
- Password history len: 0
- Maximum password age (d): No limit
- Password must meet complexity requirements: Disabled
- Minimum password age (d): 0
- Forced logoff time (s): Not set
- Locked account time (s): 1800
- Time between failed logon (s): 1800
- Number of invalid logon before locked out (s): 0
Synopsis
The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description
This script 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: 2012/07/02

Hosts
192.168.56.3 (tcp/0)

The linux distribution detected was:
- Ubuntu 8.04 (gutsy)
<table>
<thead>
<tr>
<th>19288 (1) - VNC Server Security Type Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synopsis</strong></td>
</tr>
<tr>
<td>A VNC server is running on the remote host.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This script checks the remote VNC server protocol version and the available 'security types'.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
</tr>
<tr>
<td>n/a</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Plugin Information:</strong></td>
</tr>
<tr>
<td>Publication date: 2005/07/22, Modification date: 2011/12/06</td>
</tr>
<tr>
<td><strong>Hosts</strong></td>
</tr>
<tr>
<td>192.168.56.3 (tcp/5900)</td>
</tr>
</tbody>
</table>

The remote VNC server chose security type #2 (VNC authentication)
19506 (1) - Nessus Scan Information

<table>
<thead>
<tr>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information about the Nessus scan.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This script displays, for each tested host, information about the scan itself:</td>
</tr>
<tr>
<td>- The version of the plugin set</td>
</tr>
<tr>
<td>- The type of plugin feed (HomeFeed or ProfessionalFeed)</td>
</tr>
<tr>
<td>- The version of the Nessus Engine</td>
</tr>
<tr>
<td>- The port scanner(s) used</td>
</tr>
<tr>
<td>- The port range scanned</td>
</tr>
<tr>
<td>- Whether credentialed or third-party patch management checks are possible</td>
</tr>
<tr>
<td>- The date of the scan</td>
</tr>
<tr>
<td>- The duration of the scan</td>
</tr>
<tr>
<td>- The number of hosts scanned in parallel</td>
</tr>
<tr>
<td>- The number of checks done in parallel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Plugin Information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publication date: 2005/08/26, Modification date: 2012/04/18</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.56.3 (tcp/0)</td>
</tr>
</tbody>
</table>

Information about this scan:

Nessus version : 5.0.1
Plugin feed version : 201208021939
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.56.1
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
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 : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2012/8/16 13:55
Scan duration : 3370 sec
Synopsis
The remote web server contains a graphic image that is prone to information disclosure.

Description
The 'favicon.ico' file found on the remote web server belongs to a popular web server. This may be used to fingerprint the web server.

Solution
Remove the 'favicon.ico' file or create a custom one for your site.

Risk Factor
None

References
XREF OSVDB:39272

Plugin Information:
Publication date: 2005/10/28, Modification date: 2012/04/12

Hosts
192.168.56.3 (tcp/8180)

The MD5 fingerprint for 'favicon.ico' suggests the web server is Apache Tomcat 5.5.26 or Alfresco Community.
21186 (1) - AJP Connector Detection

Synopsis
There is an AJP connector listening on the remote host.

Description
The remote host is running an AJP (Apache JServ Protocol) connector, a service by which a standalone web server such as Apache communicates over TCP with a Java servlet container such as Tomcat.

See Also
http://tomcat.apache.org/connectors-doc/


Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2006/04/05, Modification date: 2011/03/11

Hosts
192.168.56.3 (tcp/8009)

The connector listing on this port supports the ajp13 protocol.
### 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: 2012/05/03

**Hosts**

192.168.56.3 (tcp/25)

---

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

#### Low Strength Ciphers (< 56-bit key)

**SSLv2**

- EXP-RC2-CBC-MD5  
  - Kx=RSA(512)  
  - Au=RSA  
  - Enc=RC2(40)  
  - Mac=MD5  
  - export

- EXP-RC4-MD5  
  - Kx=RSA(512)  
  - Au=RSA  
  - Enc=RC4(40)  
  - Mac=MD5  
  - export

**SSLv3**

- EXP-ADH-DES-CBC-SHA  
  - Kx=DH(512)  
  - Au=None  
  - Enc=DES(40)  
  - Mac=SHA1  
  - export

- EXP-ADH-RC4-MD5  
  - Kx=DH(512)  
  - Au=None  
  - Enc=RC4(40)  
  - Mac=MD5  
  - export

- EXP-EDH-RSA-DES-CBC-SHA  
  - Kx=DH(512)  
  - Au=RSA  
  - Enc=DES(40)  
  - Mac=SHA1  
  - export

- EXP-DES-CBC-SHA  
  - Kx=RSA(512)  
  - Au=RSA  
  - Enc=DES(40)  
  - Mac=SHA1  
  - export

- EXP-RC2-CBC-MD5  
  - Kx=RSA(512)  
  - Au=RSA  
  - Enc=RC2(40)  
  - Mac=MD5  
  - export

- EXP-RC4-MD5  
  - Kx=RSA(512)  
  - Au=RSA  
  - Enc=RC4(40)  
  - Mac=MD5  
  - export

**TLSv1**

- EXP-EDH-RSA-DES-CBC-SHA  
  - Kx=DH(512)  
  - Au=RSA  
  - Enc=DES(40)  
  - Mac=SHA1  
  - export

- EXP-ADH-DES-CBC-SHA  
  - Kx=DH(512)  
  - Au=None  
  - Enc=DES(40)  
  - Mac=SHA1  
  - export

- EXP-ADH-RC4-MD5  
  - Kx=DH(512)  
  - Au=None  
  - Enc=RC4(40)  
  - Mac=MD5  
  - export

- EXP-DES-CBC-SHA  
  - Kx=RSA(512)  
  - Au=RSA  
  - Enc=DES(40)  
  - Mac=SHA1  
  - export

- EXP-RC2-CBC-MD5  
  - Kx=RSA(512)  
  - Au=RSA  
  - Enc=RC2(40)  
  - Mac=MD5  
  - export

- EXP-RC4-MD5  
  - Kx=RSA(512)  
  - Au=RSA  
  - Enc=RC4(40)  
  - Mac=MD5  
  - export

#### Medium Strength Ciphers (>= 56-bit and < 112-bit key)

**SSLv2**

- DES-CBC-MD5  
  - Kx=RSA  
  - Au=RSA  
  - Enc=DES(56)  
  - Mac=MD5

**SSLv3**

- ADH-DES-CBC-SHA  
  - Kx=DH  
  - Au=None  
  - Enc=DES(56)  
  - Mac=SHA1

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

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

**TLSv1**

- EDH-RSA-DES-CBC-SHA  
  - Kx=DH  
  - Au=RSA  
  - Enc=DES(56)  
  - [...]
**Synopsis**
An RMI registry is listening on the remote host.

**Description**
The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

**See Also**
- http://java.sun.com/j2se/1.5.0/docs/guide/rmi/spec/rmiTOC.html
- http://java.sun.com/j2se/1.5.0/docs/guide/rmi/spec/rmi-protocol3.html

**Solution**
n/a

**Risk Factor**
None

**Plugin Information:**
Publication date: 2006/08/16, Modification date: 2011/03/11

**Hosts**
192.168.56.3 (tcp/1099)

The remote RMI registry currently does not have information about any objects.
### 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**

192.168.56.3 (tcp/0)
<table>
<thead>
<tr>
<th><strong>25240 (1) - Samba Server Detection</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synopsis</strong></td>
</tr>
<tr>
<td>An SMB server is running on the remote host.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>The remote host is running Samba, a CIFS/SMB server for Linux and Unix.</td>
</tr>
<tr>
<td><strong>See Also</strong></td>
</tr>
<tr>
<td><strong>Solution</strong></td>
</tr>
<tr>
<td>n/a</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Plugin Information:</strong></td>
</tr>
<tr>
<td>Publication date: 2007/05/16, Modification date: 2011/09/14</td>
</tr>
<tr>
<td><strong>Hosts</strong></td>
</tr>
<tr>
<td>192.168.56.3 (tcp/445)</td>
</tr>
</tbody>
</table>
### 26024 (1) - PostgreSQL Server Detection

<table>
<thead>
<tr>
<th><strong>Synopsis</strong></th>
<th>A database service is listening on the remote host.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th>The remote service is a PostgreSQL database server, or a derivative such as EnterpriseDB.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>See Also</strong></th>
<th><a href="http://www.postgresql.org/">http://www.postgresql.org/</a></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Solution</strong></th>
<th>Limit incoming traffic to this port if desired.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Risk Factor</strong></th>
<th>None</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Plugin Information:</strong></th>
<th>Publication date: 2007/09/14, Modification date: 2011/03/11</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Hosts</strong></th>
<th>192.168.56.3 (tcp/5432)</th>
</tr>
</thead>
</table>
**35371 (1) - DNS Server hostname.bind Map Hostname Disclosure**

**Synopsis**
The DNS server discloses the remote host name.

**Description**
It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

**Solution**
It may be possible to disable this feature. Consult the vendor's documentation for more information.

**Risk Factor**
None

**Plugin Information:**
Publication date: 2009/01/15, Modification date: 2011/09/14

**Hosts**
192.168.56.3 (udp/53)

The remote host name is:

metasploitable
| **35373 (1) - DNS Server DNSSEC Aware Resolver** |
| **Synopsis** |
| The remote DNS resolver is DNSSEC-aware. |
| **Description** |
| The remote DNS resolver accepts DNSSEC options. This means that it may verify the authenticity of DNSSEC protected zones if it is configured to trust their keys. |
| **Solution** |
| n/a |
| **Risk Factor** |
| None |
| **Plugin Information:** |
| Publication date: 2009/01/15, Modification date: 2012/07/26 |
| **Hosts** |
| 192.168.56.3 (udp/53) |
Synopsis
The manufacturer can be deduced from the Ethernet OUI.

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

See Also
http://standards.ieee.org/faqs/OUI.html

Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2009/02/19, Modification date: 2011/03/27

Hosts
192.168.56.3 (tcp/0)

The following card manufacturers were identified:

08:00:27:b9:7e:58 : CADMUS COMPUTER SYSTEMS
The remote web server reports its version number on error pages.

Apache Tomcat appears to be running on the remote host and reporting its version number on the default error pages. A remote attacker could use this information to mount further attacks.

Replace the default error pages with custom error pages to hide the version number. Refer to the Apache wiki or the Java Servlet Specification for more information.

None

Nessus found the following version information on an Apache Tomcat 404 page or in the HTTP Server header:

Source : <title>Apache Tomcat/5.5
Version : 5.5
<table>
<thead>
<tr>
<th>39519 (1) - Backported Security Patch Detection (FTP)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synopsis</strong></td>
</tr>
<tr>
<td>Security patches are backported.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Security patches may have been 'backported' to the remote FTP 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.</td>
</tr>
<tr>
<td><strong>See Also</strong></td>
</tr>
<tr>
<td><a href="http://www.nessus.org/u?d636c8c7">http://www.nessus.org/u?d636c8c7</a></td>
</tr>
<tr>
<td><strong>Solution</strong></td>
</tr>
<tr>
<td>N/A</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Plugin Information:</strong></td>
</tr>
<tr>
<td>Publication date: 2009/06/25, Modification date: 2012/02/02</td>
</tr>
<tr>
<td><strong>Hosts</strong></td>
</tr>
<tr>
<td>192.168.56.3 (tcp/2121)</td>
</tr>
</tbody>
</table>

Give Nessus credentials to perform local checks.
### 39520 (1) - Backported Security Patch Detection (SSH)

<table>
<thead>
<tr>
<th><strong>Synopsis</strong></th>
<th>Security patches are backported.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>See Also</strong></td>
<td><a href="http://www.nessus.org/u?d636c8c7">http://www.nessus.org/u?d636c8c7</a></td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Plugin Information:</strong></td>
<td>Publication date: 2009/06/25, Modification date: 2012/02/02</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Hosts</strong></th>
<th><strong>192.168.56.3 (tcp/22)</strong></th>
</tr>
</thead>
</table>

*Give Nessus credentials to perform local checks.*
<table>
<thead>
<tr>
<th><strong>39521 (1) - Backported Security Patch Detection (WWW)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synopsis</strong></td>
</tr>
<tr>
<td>Security patches are backported.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td><strong>See Also</strong></td>
</tr>
<tr>
<td><a href="http://www.nessus.org/u?d636c8c7">http://www.nessus.org/u?d636c8c7</a></td>
</tr>
<tr>
<td><strong>Solution</strong></td>
</tr>
<tr>
<td>N/A</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Plugin Information:</strong></td>
</tr>
<tr>
<td>Publication date: 2009/06/25, Modification date: 2012/02/02</td>
</tr>
<tr>
<td><strong>Hosts</strong></td>
</tr>
<tr>
<td>192.168.56.3 (tcp/80)</td>
</tr>
</tbody>
</table>

Give Nessus credentials to perform local checks.
40665 (1) - Protected Web Page Detection

Synopsis
Some web pages require authentication.

Description
The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available:
- Basic is the simplest but the credential are sent in clear text.
- NTLM provides an SSO in MS environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.
- Digest is a cryptographically strong scheme. Credentials are never sent in clear text. They may still be cracked by a dictionary attack though.

Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2009/08/21, Modification date: 2011/03/15

Hosts
192.168.56.3 (tcp/8180)

The following pages are protected by the Basic authentication scheme:

/manager/html
/host-manager/html
/manager/status
40984 (1) - Browsable Web Directories

Synopsis
Some directories on the remote web server are browsable.

Description
Miscellaneous Nessus plugins identified directories on this web server that are browsable.

See Also
http://projects.webappsec.org/Directory-Indexing

Solution
Make sure that browsable directories do not leak confidential informative or give access to sensitive resources. And use access restrictions or disable directory indexing for any that do.

Risk Factor
None

Plugin Information:
Publication date: 2009/09/15, Modification date: 2011/04/29

Hosts
192.168.56.3 (tcp/80)

The following directories are browsable:

http://192.168.56.3/twiki/bin/view/TWiki/TWikiInstallationGuide
http://192.168.56.3/mutillidae/documentation/
http://192.168.56.3/mutillidae/images/
http://192.168.56.3/mutillidae/javascript/ddsmoothmenu/
http://192.168.56.3/mutillidae/javascript/
http://192.168.56.3/phpMyAdmin/themes/original/img/
http://192.168.56.3/dav/
http://192.168.56.3/test/
http://192.168.56.3/twiki/TWikiDocumentation.html
http://192.168.56.3/test/testoutput/
http://192.168.56.3/twiki/bin/view/TWiki/TWikiDocumentation
http://192.168.56.3/twiki/bin/rdiff/TWiki/TWikiInstallationGuide
http://192.168.56.3/twiki/bin/rdiff/TWiki/TWikiDocumentation
http://192.168.56.3/phpMyAdmin/themes/original/
http://192.168.56.3/dvwa/dvwa/images/
http://192.168.56.3/twiki/bin/edit/TWiki/TWikiInstallationGuide
http://192.168.56.3/doc/
**Synopsis**
The remote mail service supports encrypting traffic.

**Description**
The remote SMTP service supports the use of the 'STARTTLS' command to switch from a plaintext to an encrypted communications channel.

**See Also**
http://en.wikipedia.org/wiki/STARTTLS

**Solution**
n/a

**Risk Factor**
None

**Plugin Information:**
Publication date: 2009/10/09, Modification date: 2011/12/14

**Hosts**
192.168.56.3 (tcp/25)

Here is the SMTP service's SSL certificate that Nessus was able to collect after sending a 'STARTTLS' command:

```
Subject Name:
Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:
Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC
Version: 1
Signature Algorithm: SHA-1 With RSA Encryption
Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:
Algorithm: RSA Encryption
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B 6E 7C 75 DA 71 B1 3C A9
7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
73 FF 3C E5 9E 3B 6D FC CB B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
D7 A8 4A 50 8A 9A DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
98 70 46 61 B8 D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 AD AE 97
08 90 9D DC 99 00 33 A4 B5
Exponent: 01 00 01
```
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: 2012/07/25

**Hosts**

192.168.56.3 (tcp/25)

The host name known by Nessus is:

metasploitable

The Common Name in the certificate is:

ubuntu804-base.localdomain
### 45590 (1) - 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: 2012/05/21

#### Hosts

**192.168.56.3 (tcp/0)**

The remote operating system matched the following CPE:

- **cpe:/o:canonical:ubuntu_linux:8.04**

Following application CPE's matched on the remote system:

- **cpe:/a:openbsd:openssh:4.7** → OpenBSD OpenSSH 4.7
- **cpe:/a:samba:samba:3.0.20** → Samba 3.0.20
- **cpe:/a:apache:http_server:2.2.8** → Apache Software Foundation Apache HTTP Server 2.2.8
- **cpe:/a:php:php:5.2.4** → PHP 5.2.4
- **cpe:/a:phpmyadmin:phpmyadmin:3.1.1** → phpMyAdmin 3.1.1
- **cpe:/a:isc:bind:9.4**
<table>
<thead>
<tr>
<th><strong>50845 (1) - OpenSSL Detection</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synopsis</strong></td>
</tr>
<tr>
<td>The remote service appears to use OpenSSL to encrypt traffic.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Based on its behavior, 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).</td>
</tr>
<tr>
<td><strong>See Also</strong></td>
</tr>
<tr>
<td><a href="http://www.openssl.org">http://www.openssl.org</a></td>
</tr>
<tr>
<td><strong>Solution</strong></td>
</tr>
<tr>
<td>n/a</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Plugin Information:</strong></td>
</tr>
<tr>
<td>Publication date: 2010/11/30, Modification date: 2012/04/02</td>
</tr>
<tr>
<td><strong>Hosts</strong></td>
</tr>
<tr>
<td>192.168.56.3 (tcp/25)</td>
</tr>
</tbody>
</table>
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: 2012/04/19

Hosts
192.168.56.3 (tcp/25)

This port supports resuming SSLv3 sessions.
<table>
<thead>
<tr>
<th>Plugin Information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publication date: 2011/03/17, Modification date: 2011/03/17</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.56.3 (tcp/21)</td>
</tr>
<tr>
<td>Source : 220 (vsFTPd 2.3.4)</td>
</tr>
<tr>
<td>Version : 2.3.4</td>
</tr>
<tr>
<td><strong>53335 (1) - RPC portmapper (TCP)</strong></td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td><strong>Synopsis</strong></td>
</tr>
<tr>
<td>An ONC RPC portmapper is running on the remote host.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| The RPC portmapper is running on this port.  
The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request. |
| **Solution**                        |
| n/a                                 |
| **Risk Factor**                     |
| None                                |
| **Plugin Information:**             |
| Publication date: 2011/04/08,  Modification date: 2011/08/29 |
| **Hosts**                           |
| 192.168.56.3 (tcp/111)               |
### 54615 (1) - Device Type

<table>
<thead>
<tr>
<th><strong>Synopsis</strong></th>
<th>It is possible to guess the remote device type.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Based on the remote operating system, it is possible to determine what the remote system type is (e.g., a printer, router, general-purpose computer, etc.).</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Plugin Information:</strong></td>
<td>Publication date: 2011/05/23, Modification date: 2011/05/23</td>
</tr>
<tr>
<td><strong>Hosts</strong></td>
<td><strong>192.168.56.3 (tcp/0)</strong></td>
</tr>
<tr>
<td></td>
<td>Remote device type: general-purpose</td>
</tr>
<tr>
<td></td>
<td>Confidence level: 95</td>
</tr>
<tr>
<td><strong>56984 (1) - SSL / TLS Versions Supported</strong></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Synopsis</strong></td>
<td></td>
</tr>
<tr>
<td>The remote service encrypts communications.</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.</td>
<td></td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td></td>
</tr>
<tr>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Plugin Information:</strong></td>
<td></td>
</tr>
<tr>
<td>Publication date: 2011/12/01, Modification date: 2012/06/23</td>
<td></td>
</tr>
<tr>
<td><strong>Hosts</strong></td>
<td></td>
</tr>
<tr>
<td>192.168.56.3 (tcp/25)</td>
<td></td>
</tr>
</tbody>
</table>

This port supports SSLv2/SSLv3/TLSv1.0.
The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

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/Perfect_forward_secrecy

Solution
n/a

Risk Factor
None

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

Hosts
192.168.56.3 (tcp/25)

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

### Low Strength Ciphers (< 56-bit key)

- **SSLv3**
  - EXP-EDH-RSA-DES-CBC-SHA
  - Kx=DH (512)
  - Au=RSA
  - Enc=DES (40)
  - Mac=SHA1
  - export

- **TLSv1**
  - EXP-EDH-RSA-DES-CBC-SHA
  - Kx=DH (512)
  - Au=RSA
  - Enc=DES (40)
  - Mac=SHA1
  - export

### Medium Strength Ciphers (>= 56-bit and < 112-bit key)

- **SSLv3**
  - EDH-RSA-DES-CBC-SHA
  - Kx=DH
  - Au=RSA
  - Enc=DES (56)
  - Mac=SHA1

- **TLSv1**
  - EDH-RSA-DES-CBC-SHA
  - Kx=DH
  - Au=RSA
  - Enc=DES (56)
  - Mac=SHA1

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

- **SSLv3**
  - EDH-RSA-DES-CBC3-SHA
  - Kx=DH
  - Au=RSA
  - Enc=3DES (168)
  - 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

The fields above are:

- (OpenSSL ciphername)
- Kx={key exchange}
- Au={authentication}
- Enc={symmetric encryption method}
- Mac={message authentication code}
- {export flag}
Synopsis
It is possible to enumerate the permissions of remote network shares.

Description
By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

Solution
n/a

Risk Factor
None

Plugin Information:
Publication date: 2012/07/25, Modification date: 2012/07/25

Hosts
192.168.56.3 (tcp/445)

Share path : \METASPLOITABLE\print$
Local path : C:\var\lib\samba\printers
Comment : Printer Drivers

Share path : \METASPLOITABLE\tmp
Local path : C:\tmp
Comment : oh noes!

Share path : \METASPLOITABLE\opt
Local path : C:\tmp

Share path : \METASPLOITABLE\IPC$
Local path : C:\tmp
Comment : IPC Service (metasploitable server (Samba 3.0.20-Debian))

Share path : \METASPLOITABLE\ADMIN$
Local path : C:\tmp
Comment : IPC Service (metasploitable server (Samba 3.0.20-Debian))
<table>
<thead>
<tr>
<th>Details</th>
<th>Plugin Id</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Critical (10.0)</strong></td>
<td>25216</td>
<td>Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow</td>
</tr>
<tr>
<td><strong>Critical (10.0)</strong></td>
<td>32314</td>
<td>Debian OpenSSH/OpenSSL Package Random Number Generator Weakness</td>
</tr>
<tr>
<td><strong>Critical (10.0)</strong></td>
<td>55523</td>
<td>vsftpd Smiley Face Backdoor</td>
</tr>
<tr>
<td><strong>High (8.3)</strong></td>
<td>59088</td>
<td>PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution</td>
</tr>
<tr>
<td><strong>High (7.8)</strong></td>
<td>55976</td>
<td>Apache HTTP Server Byte Range DoS</td>
</tr>
<tr>
<td><strong>High (7.5)</strong></td>
<td>10205</td>
<td>rlogin Service Detection</td>
</tr>
<tr>
<td><strong>High (7.5)</strong></td>
<td>10481</td>
<td>MySQL Unpassworded Account Check</td>
</tr>
<tr>
<td><strong>High (7.5)</strong></td>
<td>36171</td>
<td>phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)</td>
</tr>
<tr>
<td><strong>High (7.5)</strong></td>
<td>42411</td>
<td>Microsoft Windows SMB Shares Unprivileged Access</td>
</tr>
<tr>
<td><strong>Medium (6.4)</strong></td>
<td>11356</td>
<td>NFS Exported Share Information Disclosure</td>
</tr>
<tr>
<td><strong>Medium (6.4)</strong></td>
<td>51192</td>
<td>SSL Certificate Cannot Be Trusted</td>
</tr>
<tr>
<td><strong>Medium (6.4)</strong></td>
<td>57582</td>
<td>SSL Self-Signed Certificate</td>
</tr>
<tr>
<td><strong>Medium (5.0)</strong></td>
<td>10056</td>
<td>/doc Directory Browsable</td>
</tr>
<tr>
<td><strong>Medium (5.0)</strong></td>
<td>10079</td>
<td>Anonymous FTP Enabled</td>
</tr>
<tr>
<td><strong>Medium (5.0)</strong></td>
<td>10203</td>
<td>rexec Service Detection</td>
</tr>
<tr>
<td><strong>Medium (5.0)</strong></td>
<td>11229</td>
<td>Web Server info.php / phpinfo.php Detection</td>
</tr>
<tr>
<td><strong>Medium (5.0)</strong></td>
<td>15901</td>
<td>SSL Certificate Expiry</td>
</tr>
<tr>
<td><strong>Medium (5.0)</strong></td>
<td>20007</td>
<td>SSL Version 2 (v2) Protocol Detection</td>
</tr>
<tr>
<td><strong>Medium (5.0)</strong></td>
<td>36083</td>
<td>phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)</td>
</tr>
<tr>
<td><strong>Medium (5.0)</strong></td>
<td>42256</td>
<td>NFS Shares World Readable</td>
</tr>
<tr>
<td><strong>Medium (5.0)</strong></td>
<td>45411</td>
<td>SSL Certificate with Wrong Hostname</td>
</tr>
<tr>
<td><strong>Medium (5.0)</strong></td>
<td>46803</td>
<td>PHP expose_php Information Disclosure</td>
</tr>
<tr>
<td><strong>Medium (5.0)</strong></td>
<td>57608</td>
<td>SMB Signing Disabled</td>
</tr>
<tr>
<td><strong>Medium (4.3)</strong></td>
<td>11213</td>
<td>HTTP TRACE / TRACK Methods Allowed</td>
</tr>
<tr>
<td><strong>Medium (4.3)</strong></td>
<td>26928</td>
<td>SSL Weak Cipher Suites Supported</td>
</tr>
<tr>
<td>Level</td>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Medium (4.3)</td>
<td>31705</td>
<td>SSL Anonymous Cipher Suites Supported</td>
</tr>
<tr>
<td>Medium (4.3)</td>
<td>42873</td>
<td>SSL Medium Strength Cipher Suites Supported</td>
</tr>
<tr>
<td>Medium (4.3)</td>
<td>49142</td>
<td>phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)</td>
</tr>
<tr>
<td>Medium (4.3)</td>
<td>51425</td>
<td>phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)</td>
</tr>
<tr>
<td>Medium (4.3)</td>
<td>57792</td>
<td>Apache HTTP Server httpOnly Cookie Information Disclosure</td>
</tr>
<tr>
<td>Medium (4.3)</td>
<td>52611</td>
<td>SMTP Service STARTTLS Plaintext Command Injection</td>
</tr>
<tr>
<td>Low (4.0)</td>
<td>52611</td>
<td>X Server Detection</td>
</tr>
<tr>
<td>Low (2.6)</td>
<td>10407</td>
<td>Web Server Uses Plain Text Authentication Forms</td>
</tr>
<tr>
<td>Low (2.6)</td>
<td>26194</td>
<td>FTP Supports Clear Text Authentication</td>
</tr>
<tr>
<td>Low (2.6)</td>
<td>34324</td>
<td>Web Server Uses Basic Authentication Without HTTPS</td>
</tr>
<tr>
<td>Low (2.6)</td>
<td>34850</td>
<td>Unencrypted Telnet Server</td>
</tr>
<tr>
<td>Low (2.6)</td>
<td>42263</td>
<td>SSL / TLS Renegotiation DoS</td>
</tr>
<tr>
<td>Info</td>
<td>10092</td>
<td>FTP Server Detection</td>
</tr>
<tr>
<td>Info</td>
<td>10107</td>
<td>HTTP Server Type and Version</td>
</tr>
<tr>
<td>Info</td>
<td>10114</td>
<td>ICMP Timestamp Request Remote Date Disclosure</td>
</tr>
<tr>
<td>Info</td>
<td>10150</td>
<td>Windows NetBIOS / SMB Remote Host Information Disclosure</td>
</tr>
<tr>
<td>Info</td>
<td>10223</td>
<td>RPC portmapper Service Detection</td>
</tr>
<tr>
<td>Info</td>
<td>10263</td>
<td>SMTP Server Detection</td>
</tr>
<tr>
<td>Info</td>
<td>10267</td>
<td>SSH Server Type and Version Information</td>
</tr>
<tr>
<td>Info</td>
<td>10281</td>
<td>Telnet Server Detection</td>
</tr>
<tr>
<td>Info</td>
<td>10287</td>
<td>Traceroute Information</td>
</tr>
<tr>
<td>Info</td>
<td>10342</td>
<td>VNC Software Detection</td>
</tr>
<tr>
<td>Info</td>
<td>10394</td>
<td>Microsoft Windows SMB Log In Possible</td>
</tr>
<tr>
<td>Info</td>
<td>10395</td>
<td>Microsoft Windows SMB Shares Enumeration</td>
</tr>
<tr>
<td>Info</td>
<td>10397</td>
<td>Microsoft Windows SMB LanMan Pipe Server Listing Disclosure</td>
</tr>
<tr>
<td>Info</td>
<td>10437</td>
<td>NFS Share Export List</td>
</tr>
<tr>
<td>Info</td>
<td>10662</td>
<td>Web mirroring</td>
</tr>
<tr>
<td>Info</td>
<td>10719</td>
<td>MySQL Server Detection</td>
</tr>
<tr>
<td>Info</td>
<td>10785</td>
<td>Microsoft Windows SMB NativeLanManager Remote System Information Disclosure</td>
</tr>
<tr>
<td>Info</td>
<td>10859</td>
<td>Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration</td>
</tr>
<tr>
<td>Info</td>
<td>10860</td>
<td>SMB Use Host SID to Enumerate Local Users</td>
</tr>
<tr>
<td>Info</td>
<td>10863</td>
<td>SSL Certificate Information</td>
</tr>
<tr>
<td>Info</td>
<td>10881</td>
<td>SSH Protocol Versions Supported</td>
</tr>
<tr>
<td>Info</td>
<td>11002</td>
<td>DNS Server Detection</td>
</tr>
<tr>
<td>Info</td>
<td>11011</td>
<td>Microsoft Windows SMB Service Detection</td>
</tr>
<tr>
<td>Info</td>
<td>11032</td>
<td>Web Server Directory Enumeration</td>
</tr>
<tr>
<td>Info</td>
<td>11111</td>
<td>RPC Services Enumeration</td>
</tr>
<tr>
<td>Info</td>
<td>11153</td>
<td>Service Detection (HELP Request)</td>
</tr>
<tr>
<td>Info</td>
<td>11154</td>
<td>Unknown Service Detection: Banner Retrieval</td>
</tr>
<tr>
<td>Info</td>
<td>11219</td>
<td>Nessus SYN scanner</td>
</tr>
<tr>
<td>Info</td>
<td>11419</td>
<td>Web Server Office File Inventory</td>
</tr>
<tr>
<td>Info</td>
<td>11422</td>
<td>Web Server Unconfigured - Default Install Page Present</td>
</tr>
<tr>
<td>Info</td>
<td>11424</td>
<td>WebDAV Detection</td>
</tr>
<tr>
<td>Info</td>
<td>11819</td>
<td>TFTP Daemon Detection</td>
</tr>
<tr>
<td>Info</td>
<td>11936</td>
<td>OS Identification</td>
</tr>
<tr>
<td>Info</td>
<td>17219</td>
<td>phpMyAdmin Detection</td>
</tr>
<tr>
<td>Info</td>
<td>17651</td>
<td>Microsoft Windows SMB: Obtains the Password Policy</td>
</tr>
<tr>
<td>Info</td>
<td>17975</td>
<td>Service Detection (GET request)</td>
</tr>
<tr>
<td>Info</td>
<td>18261</td>
<td>Apache Banner Linux Distribution Disclosure</td>
</tr>
<tr>
<td>Info</td>
<td>19288</td>
<td>VNC Server Security Type Detection</td>
</tr>
<tr>
<td>Info</td>
<td>19506</td>
<td>Nessus Scan Information</td>
</tr>
<tr>
<td>Info</td>
<td>20108</td>
<td>Web Server / Application favicon.ico Vendor Fingerprinting</td>
</tr>
<tr>
<td>Info</td>
<td>21186</td>
<td>AJP Connector Detection</td>
</tr>
<tr>
<td>Info</td>
<td>21643</td>
<td>SSL Cipher Suites Supported</td>
</tr>
<tr>
<td>Info</td>
<td>22227</td>
<td>RMI Registry Detection</td>
</tr>
<tr>
<td>Info</td>
<td>22964</td>
<td>Service Detection</td>
</tr>
<tr>
<td>Info</td>
<td>24004</td>
<td>WebDAV Directory Enumeration</td>
</tr>
<tr>
<td>Info</td>
<td>24260</td>
<td>HyperText Transfer Protocol (HTTP) Information</td>
</tr>
<tr>
<td>Info</td>
<td>25220</td>
<td>TCP/IP Timestamps Supported</td>
</tr>
<tr>
<td>Info</td>
<td>25240</td>
<td>Samba Server Detection</td>
</tr>
<tr>
<td>Info</td>
<td>26024</td>
<td>PostgreSQL Server Detection</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>35371</td>
<td>DNS Server hostname.bind Map Hostname Disclosure</td>
<td></td>
</tr>
<tr>
<td>35373</td>
<td>DNS Server DNSSEC Aware Resolver</td>
<td></td>
</tr>
<tr>
<td>35716</td>
<td>Ethernet Card Manufacturer Detection</td>
<td></td>
</tr>
<tr>
<td>39446</td>
<td>Apache Tomcat Default Error Page Version Detection</td>
<td></td>
</tr>
<tr>
<td>39463</td>
<td>HTTP Server Cookies Set</td>
<td></td>
</tr>
<tr>
<td>39519</td>
<td>Backported Security Patch Detection (FTP)</td>
<td></td>
</tr>
<tr>
<td>39520</td>
<td>Backported Security Patch Detection (SSH)</td>
<td></td>
</tr>
<tr>
<td>39521</td>
<td>Backported Security Patch Detection (WWW)</td>
<td></td>
</tr>
<tr>
<td>40665</td>
<td>Protected Web Page Detection</td>
<td></td>
</tr>
<tr>
<td>40984</td>
<td>Browsable Web Directories</td>
<td></td>
</tr>
<tr>
<td>42057</td>
<td>Web Server Allows Password Auto-Completion</td>
<td></td>
</tr>
<tr>
<td>42088</td>
<td>SMTP Service STARTTLS Command Support</td>
<td></td>
</tr>
<tr>
<td>43111</td>
<td>HTTP Methods Allowed (per directory)</td>
<td></td>
</tr>
<tr>
<td>45410</td>
<td>SSL Certificate commonName Mismatch</td>
<td></td>
</tr>
<tr>
<td>45590</td>
<td>Common Platform Enumeration (CPE)</td>
<td></td>
</tr>
<tr>
<td>49704</td>
<td>External URLs</td>
<td></td>
</tr>
<tr>
<td>49705</td>
<td>Gathered email Addresses</td>
<td></td>
</tr>
<tr>
<td>50845</td>
<td>OpenSSL Detection</td>
<td></td>
</tr>
<tr>
<td>51891</td>
<td>SSL Session Resume Supported</td>
<td></td>
</tr>
<tr>
<td>52703</td>
<td>vsftpd Detection</td>
<td></td>
</tr>
<tr>
<td>53335</td>
<td>RPC portmapper (TCP)</td>
<td></td>
</tr>
<tr>
<td>54615</td>
<td>Device Type</td>
<td></td>
</tr>
<tr>
<td>56984</td>
<td>SSL / TLS Versions Supported</td>
<td></td>
</tr>
<tr>
<td>57041</td>
<td>SSL Perfect Forward Secrecy Cipher Suites Supported</td>
<td></td>
</tr>
<tr>
<td>60119</td>
<td>Microsoft Windows SMB Share Permissions Enumeration</td>
<td></td>
</tr>
</tbody>
</table>