



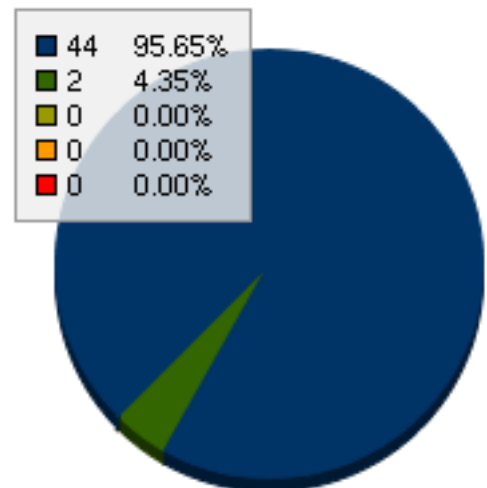
<b>Analysis Date</b>	Friday - August 01, 2008
<b>Type of Analysis</b>	Payment Card Industry (PCI) - PCI
<b>Scan Date(s)</b>	Wednesday - July 30, 2008
<b>Technical Attention Priority</b>	40%
<b>Security Threats Discovered</b>	46 (Low risk and greater)
<b>Severe Threats Discovered</b>	0
<b>Scanned By</b>	EXTERNAL (69.16.180.10, 69.16.180.2, 69.16.180.6)

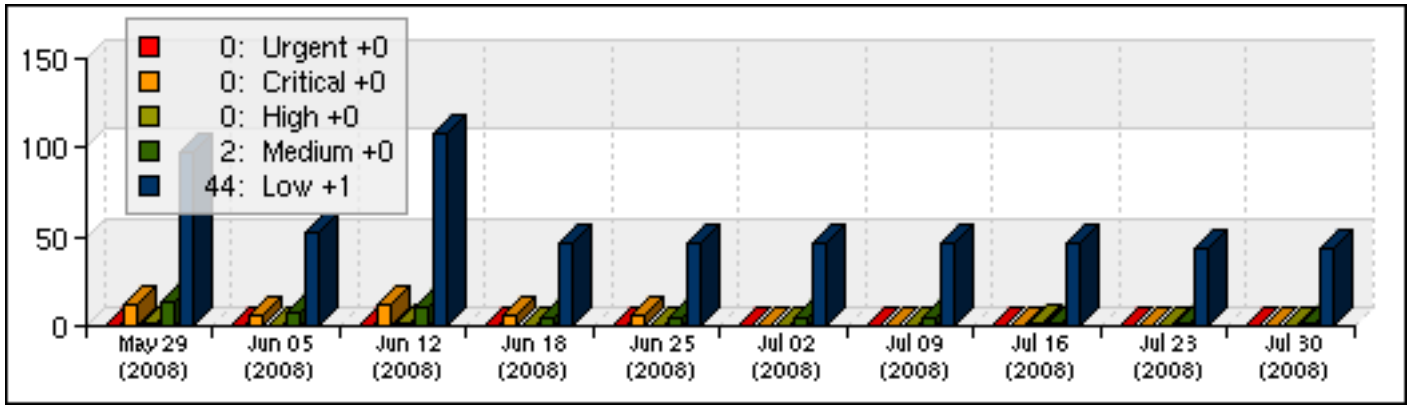
## Target Description

128.177.21.90

## Overview

This ControlScan assessment was performed against a total of 1 hosts. The charts below provide details on the number of threats discovered for each risk classification and the number of threats found for up to the last 10 scans of all the hosts in this network are shown below. Drastic changes indicate that something has impacted the security posture of these hosts and should be looked into immediately.





# Payment Card Industry (PCI) Executive Summary

Starting July 30, 2008 at 18:02 GMT through July 30, 2008 at 22:38 GMT, your PCI approved scanning vendor performed a compliant scan of the network components/hosts referenced on the cover page of this document. The purpose of the PCI scan is to provide the computer personnel with feedback on the security posture of the network and to verify compliance with the PCI standard. The purpose of this document is to provide the findings of the PCI scan.

This report was generated by your PCI approved scanning vendor, ControlScan, under certificate number 4078-01-02 in the framework of the PCI data security initiative.

## PCI Compliance Status

The tested network was found to be **in compliance** with the PCI standard. This means that all of the components of the network successfully met the PCI compliance requirements. The following table shows each component of the network and the compliance status for each component.

Component	Compliance Status
128.177.21.90	Passed
Global Compliance ( Passed=1 : Failed=0 )	Passed - In Compliance

# Attestation of Compliance

The merchant must complete this Attestation of Compliance as a declaration of the merchant's compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections.

## Part 1. Qualified Security Assessor Company Information (if applicable)

**Company Name:** rackaid LLC

**QSA Contact Name:** Jeff Huckaby

**Title:**

**Telephone:** 877-435-2444x100

**E-mail:** support@rackaid.com

**Business Address:** 1533 San Marco Blvd

**City:** Jacksonville

**State/Province:** FL

**Zip:** 32207

**Country:** United States

**URL:** <http://www.rackaid.com/>

## Part 2. Merchant Organization Information

**Company Name:** Rackaid LLC

**DBA(s):** rackAID

**Contact Name:** Jeff Huckaby

**Title:**

**Telephone:** 877435-2444x100

**E-mail:** marketing@rackaid.com

**Business Address:** 1533 N. Hogan Street

**City:** Jacksonville

**State/Province:** FL

**Zip:** 32207

**Country:** United States

**URL:** http://www.rackaid.com/

### Part 2a. Type of merchant business (check all that apply):

- |   |  |   |
|---|--|---|
| <input type="checkbox"/> Retailer                 | <input type="checkbox"/> Telecommunication     | <input type="checkbox"/> Grocery and Supermarkets |
| <input type="checkbox"/> Petroleum                | <input checked="" type="checkbox"/> E-Commerce | <input type="checkbox"/> Mail/Telephone-Order     |
| <input type="checkbox"/> Others (please specify): |  |   |

List facilities and locations included in PCI DSS review: Office, Datacenter

### Part 2b. Relationships

Does your company have a relationship with one or more third-party service providers (e.g. gateways, web-hosting companies, airline booking agents, loyalty program agents, etc)?

Yes  No

Does your company have a relationship with more than one acquirer?

Yes  No

### Part 2c. Transaction Processing

Payment application in use: Quickbooks Pro Merchant Services version 2007

### Part 3. PCI DSS Validation

Based on the results noted in the SAQ dated below, Rackaid LLC asserts the following compliance status (check one):

- Compliant:** All sections of the PCI SAQ are complete, all questions answered affirmatively, resulting in an overall compliant rating; **and** a passing scan has been completed by a PCI SSC Approved Scan Vendor, thereby Rackaid LLC has demonstrated full compliance with the PCI DSS.
  
- Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions are answered "yes" resulting in an overall non-compliant rating, **or** a passing scan has not been completed by a PCI SSC Approved Scan Vendor, thereby Rackaid LLC has not demonstrated full compliance with the PCI DSS.

**Target Date for Compliance:**

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

### Part 3a. Confirmation of Compliant Status

**Merchant confirms:**

- PCI DSS Self-Assessment Questionnaire A, Version 1.1, was completed according to the instructions therein.
- All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
- I have confirmed with my POS vendor that my POS system does not store sensitive authentication data after authorization
- I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.
- No evidence of magnetic stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage subsequent to transaction authorization was found on ANY systems reviewed during this assessment.

### Part 3b. Merchant Acknowledgement

-- Digitally Signed --	2008-07-03
<hr/>	
Signature of Merchant Executive Officer	Date
Jeff Huckaby	none
<hr/>	
Merchant Executive Officer Name	Title
rackaid	
<hr/>	
Merchant Company Represented	

## Part 4. Action Plan for Non-Compliant Status

Please select the appropriate "Compliance Status" for each requirement. If you answer "No" to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.

PCI DSS Requirement	Compliant		Remediation Date and Actions
1. Install and maintain a firewall configuration to protect cardholder data	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
2. Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
3. Protect stored cardholder data	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
4. Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
5. Use and regularly update anti-virus software	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
6. Develop and maintain secure systems and applications	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
7. Restrict access to cardholder data by business need to know	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
8. Assign a unique ID to each person with computer access	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
9. Restrict physical access to cardholder data	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
10. Track and monitor all access to network resources and cardholder data	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
11. Regularly test security systems and processes	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
12. Maintain a policy that addresses information security	<input type="checkbox"/> Yes	<input type="checkbox"/> No	

# PCI Self-Assessment Questionnaire

This section displays the results of the Self-Assessment Questionnaire (SAQ) A, Version 1.1.

9. Restrict physical access to cardholder data	Compliant
<b>9.6.</b> Are all paper and electronic media that contain cardholder data physically secure? ( <i>Such media includes computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes.</i> )	<b>Yes</b>
<b>9.7.a.</b> Is strict control maintained over the internal or external distribution of any kind of media that contains cardholder data?	<b>Yes</b>
<b>9.7.b.</b> Do controls include the following:	
<b>9.7.b.1.</b> Is the media classified so it can be identified as confidential?	<b>Yes</b>
<b>9.7.b.2.</b> Is the media sent by secured courier or other delivery method that can be accurately tracked?	<b>Yes</b>
<b>9.8.</b> Are processes and procedures in place to ensure management approval is obtained prior to moving any and all media from a secured area (especially when media is distributed to individuals)?	<b>Yes</b>
<b>9.9.</b> Is strict control maintained over the storage and accessibility of media that contains cardholder data?	<b>Yes</b>
<b>9.10.</b> Is media containing cardholder data destroyed when it is no longer needed for business or legal reasons? Destruction should be as follows:	<b>Yes</b>
<b>9.10.1.</b> Are hardcopy materials cross-cut shredded, incinerated, or pulped?	<b>Yes</b>

12. Maintain a policy that addresses information security for employees and contractors	Compliant
<b>12.8.</b> Contractually, are the following required if cardholder data is shared with service providers?	
<b>12.8.1.</b> That service providers must adhere to the PCI DSS requirements?	<b>Yes</b>
<b>12.8.2.</b> An agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses?	<b>Yes</b>

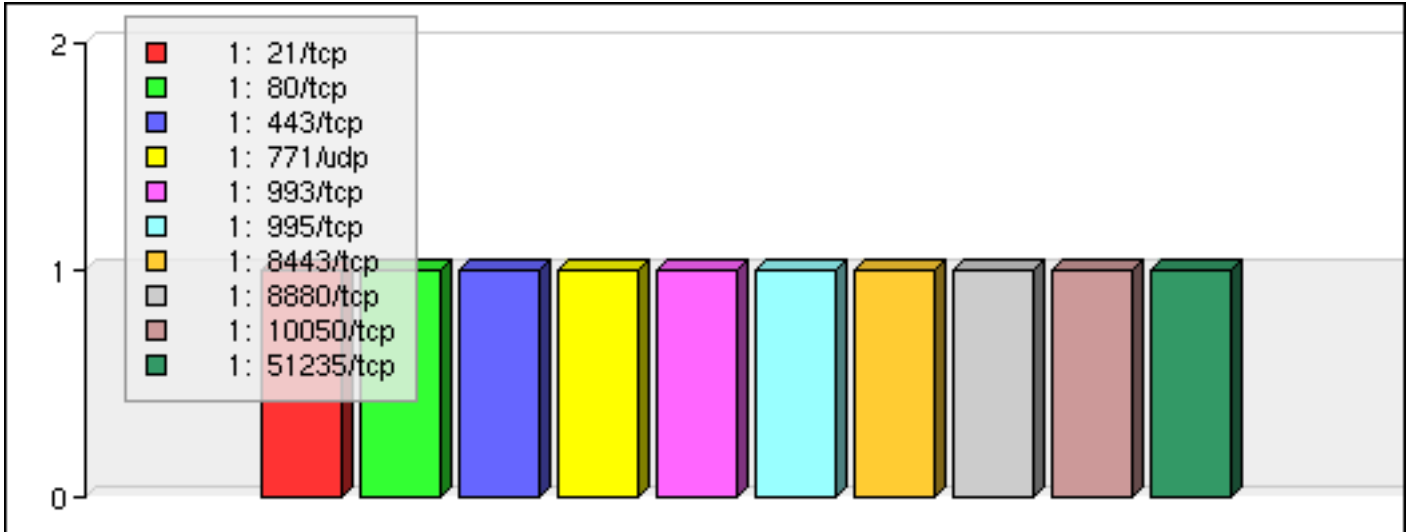
## Vulnerable Hosts

This ControlScan analysis scanned 1 total IP addresses. Of those, 1 host was found active with outstanding vulnerabilities or open ports. The following table provides a brief summary about each of these active hosts and their analysis data.

Scanner: EXTERNAL							
Host	Ports	Urgent	Critical	High	Medium	Low	Threats
128.177.21.90 - Infoblox NIOS 4.1r5	23	0	0	0	2	44	46

## Discovered Open Ports (Nmap)

This assessment discovered a total of 23 distinct open network ports on the hosts in this report. This does not mean each open port is a security threat, but it does show some possible points of entry to your network that an attacker could potentially leverage. It is generally considered good practice to keep the number of open ports to a minimum. Sometimes hackers will target computers with a large number of open network ports because they may be more susceptible to attack. Minimizing the number of open network ports will help to minimize this risk and make your network less "attractive" to hackers and attacks.



Number of Hosts vs. Open Ports

The following table shows a cross-reference of all discovered security threats by port number and risk factor. This analysis will help to determine which port represents the greatest overall risk to the target system. The most vulnerable port has been highlighted.

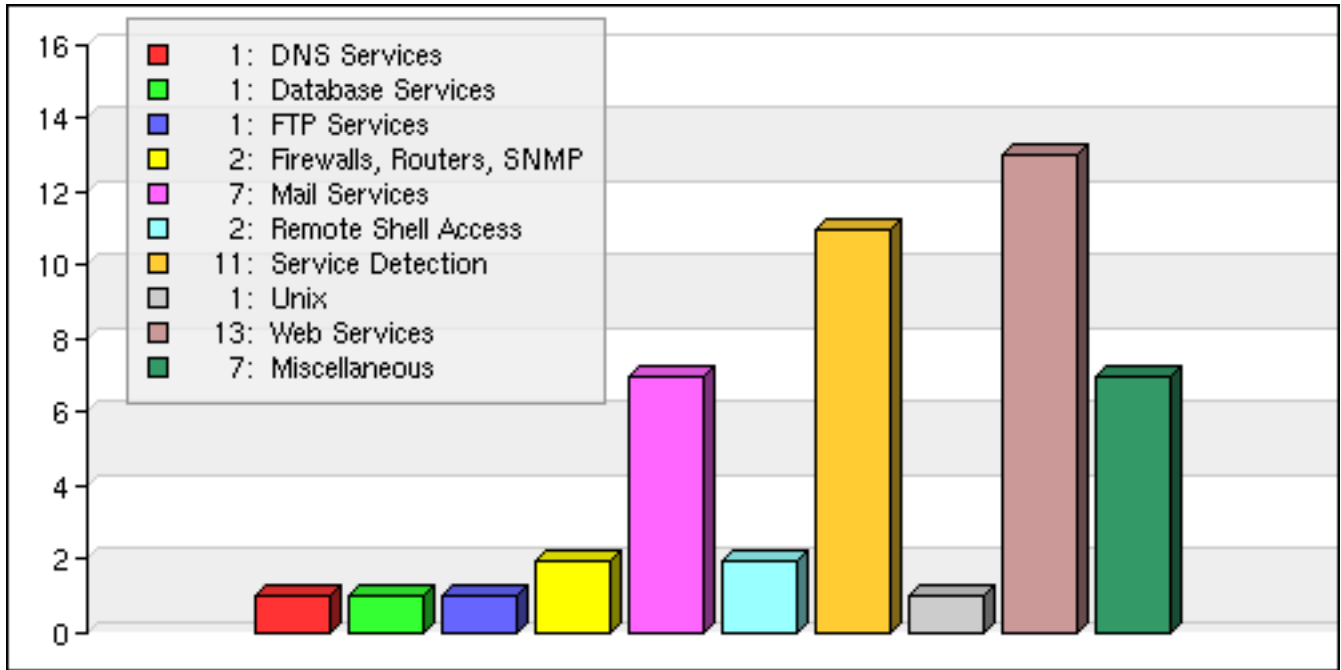
Host: 128.177.21.90

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
tcp		0	0	0	0	4	4
icmp		0	0	0	0	1	1
21 tcp	PROFTPD 1.3.1	0	0	0	0	1	1
22 tcp	OPENSSSH 4.3 (PROTOCOL 2.0)	0	0	0	0	2	2
25 tcp	QMAIL SMTPD	0	0	0	0	2	2
80 tcp	APACHE HTTPD 2.2.3 ((CENTOS))	0	0	0	0	2	2
106 tcp	POPPASSD	0	0	0	0	1	1
110 tcp	COURIER POP3D	0	0	0	1	1	2
111 udp	SUNRPC	0	0	0	0	0	0
111 tcp	2 (RPC #100000)	0	0	0	0	2	2
143 tcp	COURIER IMAPD (RELEASED 2004)	0	0	0	0	1	1
443 tcp	APACHE HTTPD 2.2.3 ((CENTOS))	0	0	0	1	5	6
771 udp	RTIP	0	0	0	0	1	1

774 tcp	1 (RPC #100024)	0	0	0	0	1	1
904 tcp	VMWARE GSX AUTHENTICATION DAEMON 1.10 (USES VNC)	0	0	0	0	1	1
993 tcp	COURIER IMAPD (RELEASED 2004)	0	0	0	0	3	3
995 tcp	COURIER POP3D	0	0	0	0	3	3
3306 tcp	MYSQL 5.0.45	0	0	0	0	2	2
5353 udp	UNKNOWN	0	0	0	0	1	1
8443 tcp	APACHE HTTPD	0	0	0	0	5	5
8880 tcp	APACHE HTTPD	0	0	0	0	3	3
10050 tcp	TCPWRAPPED	0	0	0	0	0	0
51235 tcp	PYTHON SIMPLEXMLRPCSERVER (BASEHTTP 0.3; PYTHON 2.4.3)	0	0	0	0	2	2

## Vulnerable Threat Families

The 46 total discovered vulnerabilities are spread across 10 families of threat classifications. The graph below shows the most frequently occurring threat families discovered on this network. Also, a complete list of every threat classification along with the number of vulnerabilities discovered is in the table below. The most vulnerable family has been highlighted.



Number of Discovered Threats vs. Family Classifications

Family	Urgent	Critical	High	Medium	Low	Total
DNS Services	0	0	0	0	1	1
Database Services	0	0	0	0	1	1
FTP Services	0	0	0	0	1	1
Firewalls, Routers, SNMP	0	0	0	0	2	2
Mail Services	0	0	0	1	6	7
Miscellaneous	0	0	0	1	6	7
Remote Shell Access	0	0	0	0	2	2
Service Detection	0	0	0	0	11	11
Unix	0	0	0	0	1	1
Web Services	0	0	0	0	13	13

## Discovered Security Threat Summaries

This section provides a simple one-line summary of each discovered potential security threat on each host in this network. These summaries are grouped by host and sorted by risk factor. The full analysis report for each host is linked to the IP address.

Host: 128.177.21.90

Risk	Port	Protocol	ID	Summary
Medium	110	tcp	15855	POP3 Unencrypted Cleartext Logins
Medium	443	tcp	20007	Deprecated SSL Protocol Usage
Low	---	tcp	14788	IP protocols scan
Low	---	tcp	11936	OS Identification
Low	---	tcp	18261	Linux Distribution Detection
Low	---	icmp	10114	icmp timestamp request
Low	---	tcp	25220	TCP timestamps
Low	21	tcp	10092	FTP Server Detection
Low	22	tcp	10881	SSH protocol versions supported
Low	22	tcp	10267	SSH Server type and version
Low	25	tcp	10263	SMTP Server Detection
Low	25	tcp	11421	smtpscan
Low	80	tcp	24260	HyperText Transfer Protocol Information
Low	80	tcp	10107	HTTP Server type and version
Low	106	tcp	14773	Identifies services like FTP, SMTP, NNTP...
Low	110	tcp	10185	POP Server Detection
Low	111	tcp	11111	RPC Services Enumeration
Low	111	tcp	10223	RPC portmapper
Low	143	tcp	11414	Get the IMAP Banner

<b>Low</b>	443	tcp	24260	HyperText Transfer Protocol Information
<b>Low</b>	443	tcp	16338	Mailman Detection
<b>Low</b>	443	tcp	10107	HTTP Server type and version
<b>Low</b>	443	tcp	21643	Supported SSL Ciphers Suites
<b>Low</b>	443	tcp	10863	SSL Certificate
<b>Low</b>	771	udp	11111	RPC Services Enumeration
<b>Low</b>	774	tcp	11111	RPC Services Enumeration
<b>Low</b>	904	tcp	20301	VMware ESX/GSX Server detection
<b>Low</b>	993	tcp	21643	Supported SSL Ciphers Suites
<b>Low</b>	993	tcp	11414	Get the IMAP Banner
<b>Low</b>	993	tcp	10863	SSL Certificate
<b>Low</b>	995	tcp	10185	POP Server Detection
<b>Low</b>	995	tcp	21643	Supported SSL Ciphers Suites
<b>Low</b>	995	tcp	10863	SSL Certificate
<b>Low</b>	3306	tcp	10719	MySQL Server detection
<b>Low</b>	3306	tcp	11153	Service Identification (2nd pass)
<b>Low</b>	5353	udp	12218	mDNS Detection
<b>Low</b>	8443	tcp	10766	Apache Remote Username Enumeration Vulnerability
<b>Low</b>	8443	tcp	24260	HyperText Transfer Protocol Information
<b>Low</b>	8443	tcp	10107	HTTP Server type and version
<b>Low</b>	8443	tcp	21643	Supported SSL Ciphers Suites
<b>Low</b>	8443	tcp	10863	SSL Certificate
<b>Low</b>	8880	tcp	10766	Apache Remote Username Enumeration Vulnerability
<b>Low</b>	8880	tcp	24260	HyperText Transfer Protocol Information

<b>Low</b>	8880	tcp	10107	HTTP Server type and version
<b>Low</b>	51235	tcp	24260	HyperText Transfer Protocol Information
<b>Low</b>	51235	tcp	10107	HTTP Server type and version

## Discovered Security Threats Details

This section provides all the details about each discovered potential security threat for all of the hosts in this assessment. These details are grouped by host and ordered by risk factor.

Host: 128.177.21.90

### POP3 Unencrypted Cleartext Logins

	Risk	Port/Protocol	ID
<b>Family:</b> Mail Services	Medium	110/tcp	15855

#### Solution:

Contact your vendor for a fix or encrypt traffic with SSL / TLS using stunnel.

#### Description:

The remote host is running a POP3 daemon that allows cleartext logins over unencrypted connections. An attacker can uncover user names and passwords by sniffing traffic to the POP3 daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used.

#### Cross-References:

[OSVDB-3119](#)

## Deprecated SSL Protocol Usage

**Family:** Miscellaneous

Risk	Port/Protocol	ID
Medium	443/tcp	20007

### Synopsis:

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

### Solution:

Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.

### 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.

### Cross-References:

<http://www.schneier.com/paper-ssl.pdf>

### CVSS(2) Base Score:

5.0

### CVSS(2) Base Vector:

AV:N/AC:L/Au:N/C:P/I:N/A:N

## IP protocols scan

**Family:** Firewalls, Routers, SNMP

Risk	Port/Protocol	ID
Low	---/tcp	14788

### Description:

The following IP protocols are accepted on this host:

- 1 ICMP
- 2 IGMP
- 6 TCP
- 17 UDP
- 41 IPv6

## OS Identification

**Family:** Service Detection

Risk	Port/Protocol	ID
Low	---/tcp	11936

### Description:

Remote operating system : Linux Kernel 2.6 on CentOS 5  
Confidence Level : 95  
Method : HTTP

The remote host is running Linux Kernel 2.6 on CentOS 5

## Linux Distribution Detection

**Family:** Miscellaneous

Risk	Port/Protocol	ID
Low	---/tcp	18261

### Description:

Using the remote HTTP banner, it is possible to guess that the Linux distribution installed on the remote host is :

- CentOS 5

## icmp timestamp request

**Family:** Firewalls, Routers, SNMP

Risk	Port/Protocol	ID
Low	---/icmp	10114

### Synopsis:

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

### Solution:

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

### Description:

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentication protocols.

The difference between the local and remote clocks is 15403 seconds

### Cross-References:

[CVE-CVE-1999-0524](#)

## TCP timestamps

**Family:** Miscellaneous

Risk	Port/Protocol	ID
Low	---/tcp	25220

### 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.

### Cross-References:

<http://www.ietf.org/rfc/rfc1323.txt>

## FTP Server Detection

**Family:** FTP Services

Risk	Port/Protocol	ID
Low	21/tcp	10092

### 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.

The remote FTP banner is :

220 ProFTPD 1.3.1 Server (ProFTPD) [128.177.21.90]

## SSH protocol versions supported

Risk	Port/Protocol	ID
Low	22/tcp	10881

**Family:** Remote Shell Access

### Synopsis:

An SSH server is running on the remote host.

### Description:

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

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

- . 1.99
- . 2.0

SSHv2 host key fingerprint : eb:df:c0:fe:ae:fb:65:78:60:96:38:00:ee:8d:4b:29

## SSH Server type and version

Risk	Port/Protocol	ID
Low	22/tcp	10267

**Family:** Remote Shell Access

### 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.

SSH version : SSH-2.0-OpenSSH\_4.3

SSH supported authentication : publickey,gssapi-with-mic,password

## SMTP Server Detection

**Family:** Mail Services

Risk	Port/Protocol	ID
Low	25/tcp	10263

### Synopsis:

An SMTP server is listening on the remote port.

### Solution:

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

Remote SMTP server banner :

220 plesk.rackaid.com ESMTP

## smtpscan

**Family:** Mail Services

Risk	Port/Protocol	ID
Low	25/tcp	11421

### Description:

This server could be fingerprinted as being:

Qmail 1.0.3

## HyperText Transfer Protocol Information

Risk	Port/Protocol	ID
Low	80/tcp	24260

**Family:** Web Services

### Synopsis:

Some information about the remote HTTP configuration can be extracted.

### Solution:

None.

### 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

Protocol version : HTTP/1.1

SSL : no

Pipelining : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Date: Wed, 30 Jul 2008 14:06:26 GMT

Server: Apache/2.2.3 (CentOS)

Content-Length: 321

Connection: close

Content-Type: text/html; charset=iso-8859-1

## HTTP Server type and version

Risk	Port/Protocol	ID
Low	80/tcp	10107

**Family:** Web Services

### 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.

The remote web server type is :

Apache/2.2.3 (CentOS)

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

## Identifies services like FTP, SMTP, NNTP...

**Family:** Service Detection

**Risk**

**Low**

**Port/Protocol**

106/tcp

**ID**

14773

### Description:

A POP3PW server is running on this port

## POP Server Detection

**Family:** Mail Services

**Risk**

**Low**

**Port/Protocol**

110/tcp

**ID**

10185

### Synopsis:

A POP server is listening on the remote port

### Solution:

Disable this service if you do not use it.

### Description:

The remote host is running a POP server.

Remote POP server banner :

+OK Hello there. <28019.1217426141@localhost.localdomain >

## RPC Services Enumeration

**Family:** Service Detection

**Risk**

**Low**

**Port/Protocol**

111/tcp

**ID**

11111

### 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.

The following RPC services are available on TCP port 111 :

- program: 100000 (portmapper), version: 2

## RPC portmapper

**Family:** Unix

Risk	Port/Protocol	ID
Low	111/tcp	10223

### Synopsis:

An ONC RPC portmapper is running on the remote host.

### Description:

The RPC portmapper is running on this port.

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

## Get the IMAP Banner

**Family:** Mail Services

Risk	Port/Protocol	ID
Low	143/tcp	11414

### Synopsis:

An IMAP server is running on the remote host.

### Description:

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

The remote imap server banner is :

```
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT  
THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS] Courier-IMAP ready. Copyright  
1998-2004 Double Precision, Inc. See COPYING for distribution information.
```

## HyperText Transfer Protocol Information

**Family:** Web Services

Risk	Port/Protocol	ID
Low	443/tcp	24260

### Synopsis:

Some information about the remote HTTP configuration can be extracted.

### Solution:

None.

### 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

Protocol version : HTTP/1.1

SSL : yes

Pipelining : no

Keep-Alive : no

Options allowed : GET,HEAD,POST,OPTIONS

Headers :

Date: Wed, 30 Jul 2008 14:06:26 GMT

Server: Apache/2.2.3 (CentOS)

Last-Modified: Fri, 02 May 2008 23:50:19 GMT

ETag: "1498014-dc3-b5f64c0"

Accept-Ranges: bytes

Content-Length: 3523

Connection: close

Content-Type: text/html

## Mailman Detection

**Family:** Web Services

**Risk**

**Low**

**Port/Protocol**

443/tcp

**ID**

16338

### Synopsis:

The remote web server contains a mailing list management application written in Python.

### Description:

The remote host is running Mailman, an open-source, Python-based mailing list management package.

Mailman 2.1.9 was detected on the remote host under the path /mailman.

### Cross-References:

<http://www.list.org/>

## HTTP Server type and version

**Family:** Web Services

**Risk**

**Low**

**Port/Protocol**

443/tcp

**ID**

10107

### 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.

The remote web server type is :

Apache/2.2.3 (CentOS)

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

## Supported SSL Ciphers Suites

Family: Miscellaneous

Risk

Port/Protocol

ID

Low

443/tcp

21643

### Synopsis:

The remote service encrypts communications using SSL.

### Description:

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

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-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-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

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) Mac=SHA1

EXP1024-DES-CBC-SHA Kx=RSA(1024) Au=RSA Enc=DES(56) Mac=SHA1 export

EXP1024-RC4-SHA Kx=RSA(1024) Au=RSA Enc=RC4(56) Mac=SHA1 export

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

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

##### SSLv2

DES-CBC3-MD5 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5

RC2-CBC-MD5 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5

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

##### SSLv3

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

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

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

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

##### TLSv1

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

DHE-RSA-AES128-SHA Kx=DH Au=RSA Enc=AES(128) Mac=SHA1

DHE-RSA-AES256-SHA Kx=DH Au=RSA Enc=AES(256) Mac=SHA1

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

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

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

The fields above are :

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

**Cross-References:**

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

## SSL Certificate

**Family:** Service Detection

Risk	Port/Protocol	ID
Low	443/tcp	10863

### Description:

Here is the SSLv2 server certificate:

Certificate:

Data:

Version: 1 (0x0)

Serial Number: 1209771934 (0x481ba79e)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=US, ST=Virginia, L=Herndon, O=SWsoft, Inc., OU=Plesk, CN=plesk/emailAddress=info@plesk.com

Validity

Not Before: May 2 23:45:34 2008 GMT

Not After : May 2 23:45:34 2009 GMT

Subject: C=US, ST=Virginia, L=Herndon, O=SWsoft, Inc., OU=Plesk, CN=plesk/emailAddress=info@plesk.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (2048 bit)

Modulus (2048 bit):

00:c9:86:9f:2f:5d:c2:77:e0:6b:29:39:1b:c8:40:  
85:da:de:f1:31:c8:97:3f:58:ee:8e:3c:84:9e:59:  
c2:70:90:9e:4e:08:7a:2d:84:0a:aa:42:66:1a:55:  
9c:b9:d2:82:19:14:10:1f:a7:d1:fa:34:8c:b0:b9:  
d9:28:7e:9e:a7:34:a3:9c:d8:ab:97:67:ad:e5:cc:  
97:7f:c6:e8:ee:82:c6:7c:44:de:65:85:59:ae:f1:  
25:06:35:8d:01:e6:cc:90:49:b2:20:5f:ff:33:eb:  
73:5e:13:4c:1d:09:4a:3f:da:dc:a7:f7:a3:5a:d0:  
7b:42:4d:94:2c:7f:c0:48:b2:96:e4:ae:86:98:92:  
6b:61:cf:69:9b:29:5b:b7:ec:e9:49:1f:27:ca:4f:  
d1:43:46:38:3d:75:14:42:c7:f5:28:67:6f:56:c5:  
40:6e:88:11:40:8d:d4:02:98:20:98:6b:61:c9:ef:  
e4:b6:56:7f:4a:28:81:36:82:5f:5d:b5:03:75:c3:  
f8:01:b7:f7:54:7a:77:99:40:6c:40:68:7c:32:e5:  
92:39:2d:ca:d8:7e:e3:93:17:05:40:d8:fa:8e:27:  
a5:eb:ad:d0:db:2c:e7:b5:91:c2:57:a6:1d:de:a9:  
a4:25:9c:71:f4:e1:5a:07:9f:7a:2a:f6:24:b7:4c:  
44:43

Exponent: 65537 (0x10001)

Signature Algorithm: sha1WithRSAEncryption

31:31:63:ba:0d:ef:38:63:88:94:f9:93:a2:3a:a3:7e:05:59:  
34:3d:ed:61:d0:23:03:bc:70:3d:a4:be:67:7b:d3:48:3a:f9:  
be:81:bf:a4:b8:62:c1:07:9b:1c:45:56:f8:7a:0b:c8:0d:ab:  
2f:5d:29:a3:d2:14:89:29:5e:6b:b8:1d:e5:9e:ce:d7:cb:15:  
65:24:bb:d0:c2:c3:56:de:d8:9b:d4:a5:8d:eb:ff:c4:9e:d7:  
2a:0e:13:da:17:a3:bb:28:7d:ce:bb:a6:5e:2e:49:ac:25:44:  
cf:0a:f3:30:1c:2f:a6:10:62:98:d1:7f:29:7d:c6:9b:86:0e:  
fe:ab:e1:c1:39:3a:8c:ec:e5:fe:92:43:37:66:63:4e:c7:b6:  
30:1d:6a:fb:ff:d4:23:46:71:6c:ce:71:a7:89:98:23:64:94:  
c8:bd:8f:9b:85:43:c7:fb:83:1d:01:00:b3:f6:c2:08:45:ec:  
73:31:71:4c:9c:b7:8c:43:c0:14:52:85:3c:71:6c:bc:6e:a7:  
28:32:05:0c:e1:bc:bf:f4:de:b4:db:2c:bf:fe:6e:d6:0b:a1:  
e2:0a:cb:e7:64:1a:c9:70:3e:70:b0:bd:48:0b:ff:05:bd:4b:  
23:bb:dd:ac:a7:cb:46:55:94:94:bb:b7:66:14:ae:17:e3:32:  
0d:6f:14:b5

This SSLv2 server also accepts SSLv3 connections.

This SSLv2 server also accepts TLSv1 connections.

## RPC Services Enumeration

**Family:** Service Detection

Risk	Port/Protocol	ID
Low	771/udp	11111

### 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.

The following RPC services are available on UDP port 771 :

- program: 100024 (status), version: 1

## RPC Services Enumeration

**Family:** Service Detection

Risk	Port/Protocol	ID
Low	774/tcp	11111

### 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.

The following RPC services are available on TCP port 774 :

- program: 100024 (status), version: 1

**VMware ESX/GSX Server detection**

Risk

Port/Protocol

ID

**Family:** Service Detection**Low**

904/tcp

20301

**Synopsis:**

The remote host appears to be running VMware Server, ESX Server, or GSX Server.

**Description:**

According to its banner, the remote host appears to be running a VMware server authentication daemon, which likely indicates the remote host is running VMware Server, ESX Server, or GSX Server.

**Cross-References:**

<http://www.vmware.com/>

## Supported SSL Ciphers Suites

**Family:** Miscellaneous

**Risk**

**Low**

**Port/Protocol**

993/tcp

**ID**

21643

### Synopsis:

The remote service encrypts communications using SSL.

### Description:

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

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

High Strength Ciphers ( >= 112-bit key)

SSLv3

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

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

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

TLSv1

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

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

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

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

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

The fields above are :

{OpenSSL ciphername}

Kx={key exchange}

Au={authentication}

Enc={symmetric encryption method}

Mac={message authentication code}

{export flag}

### Cross-References:

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

## Get the IMAP Banner

**Family:** Mail Services

**Risk**

**Low**

**Port/Protocol**

993/tcp

**ID**

11414

### Synopsis:

An IMAP server is running on the remote host.

### Description:

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

The remote imap server banner is :

```
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT  
THREAD=REFERENCES SORT QUOTA IDLE AUTH=PLAIN ACL ACL2=UNION] Courier-IMAP ready. Copyright  
1998-2004 Double Precision, Inc. See COPYING for distribution information.
```

## SSL Certificate

**Family:** Service Detection

Risk	Port/Protocol	ID
Low	993/tcp	10863

### Description:

Here is the SSLv3 server certificate:

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

d6:0a:58:14:72:c8:5f:cd

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=US, ST=NY, L=New York, O=Courier Mail Server, OU=Automatically-generated IMAP SSL key, CN=localhost/emailAddress=postmaster@example.com

Validity

Not Before: May 2 23:44:29 2008 GMT

Not After : May 2 23:44:29 2009 GMT

Subject: C=US, ST=NY, L=New York, O=Courier Mail Server, OU=Automatically-generated IMAP SSL key, CN=localhost/emailAddress=postmaster@example.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:d8:5a:e7:d5:80:f2:74:b4:7d:89:19:38:6a:41:

d0:b5:34:c8:06:e1:34:c2:71:01:ce:01:a9:c2:dc:

d9:dc:0b:3b:e0:be:5d:55:69:d5:c2:d8:11:fe:09:

c0:11:57:6e:79:30:ec:26:d8:b0:82:92:72:58:03:

1c:4d:f0:cb:f8:07:0c:e5:e1:93:e4:9b:2d:a6:ad:

6a:69:5a:3d:13:58:7f:c1:9d:97:f0:91:3b:02:ce:

37:4e:9b:12:0f:9a:17:d3:ed:1f:b1:57:e4:85:93:

11:87:7c:b3:00:e4:98:8a:61:92:6d:3e:20:d1:dc:

df:9e:57:ad:df:ec:33:5a:55

Exponent: 65537 (0x10001)

X509v3 extensions:

Netscape Cert Type:

SSL Server

Signature Algorithm: sha1WithRSAEncryption

51:43:25:a2:37:68:d8:1e:17:54:9c:a2:92:5a:7b:1e:30:7b:

53:a6:4a:4f:a7:c0:77:27:05:23:8c:f5:09:d8:6d:82:06:79:

85:91:57:66:d9:30:20:44:a7:3f:26:e9:37:c3:74:1d:4c:94:

5c:63:a4:e7:8d:bb:0f:95:8c:7d:6a:01:7d:dc:3f:8a:0a:c2:

79:b4:fe:02:df:be:3e:3d:e7:39:2f:1d:d9:a3:46:fc:55:e5:

33:f7:3f:c5:8c:6c:96:df:a0:c9:90:a8:6d:bc:aa:a8:6a:5f:

4b:65:13:e0:06:55:50:60:7b:55:5a:53:21:97:ac:ab:82:f9:

a6:14

This TLSv1 server does not accept SSLv2 connections.

This TLSv1 server also accepts SSLv3 connections.

## POP Server Detection

**Family:** Mail Services

**Risk**

**Low**

**Port/Protocol**

995/tcp

**ID**

10185

### Synopsis:

A POP server is listening on the remote port

### Solution:

Disable this service if you do not use it.

### Description:

The remote host is running a POP server.

Remote POP server banner :

```
+OK Hello there. <28018.1217426140@localhost.localdomain >
```

## Supported SSL Ciphers Suites

**Family:** Miscellaneous

**Risk**

**Low**

**Port/Protocol**

995/tcp

**ID**

21643

### Synopsis:

The remote service encrypts communications using SSL.

### Description:

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

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

High Strength Ciphers ( >= 112-bit key)

SSLv3

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

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

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

TLSv1

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

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

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

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

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

The fields above are :

{OpenSSL ciphername}

Kx={key exchange}

Au={authentication}

Enc={symmetric encryption method}

Mac={message authentication code}

{export flag}

### Cross-References:

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

## SSL Certificate

**Family:** Service Detection

**Risk**

**Port/Protocol**

**ID**

**Low**

995/tcp

10863

### Description:

Here is the SSLv3 server certificate:

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

fd:e5:10:a2:58:42:fa:44

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=US, ST=NY, L=New York, O=Courier Mail Server, OU=Automatically-generated POP3 SSL key, CN=localhost/emailAddress=postmaster@example.com

Validity

Not Before: May 2 23:44:29 2008 GMT

Not After : May 2 23:44:29 2009 GMT

Subject: C=US, ST=NY, L=New York, O=Courier Mail Server, OU=Automatically-generated POP3 SSL key, CN=localhost/emailAddress=postmaster@example.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:ac:9a:66:73:f9:ee:a2:57:0d:dc:c6:19:fe:25:

1d:36:89:de:dd:d0:2f:c6:7a:4f:5b:32:a6:2d:66:

5d:1b:eb:27:0d:ec:13:61:b3:fd:05:1a:3f:f9:76:

39:7d:59:25:d5:3a:53:70:08:00:54:14:fa:95:e0:

13:60:72:79:e5:94:ed:31:44:3e:e2:9b:45:56:f4:

e9:f8:4d:e2:66:e2:d9:36:8c:43:44:80:37:50:55:

7c:05:16:47:e7:5d:47:65:a8:ed:87:45:f5:73:fa:

75:49:72:3f:ff:c7:47:4b:a8:29:62:0a:f8:fe:bd:

42:43:9c:34:dc:b7:df:c5:e5

Exponent: 65537 (0x10001)

X509v3 extensions:

Netscape Cert Type:

SSL Server

Signature Algorithm: sha1WithRSAEncryption

5e:15:90:5e:18:3b:27:48:72:86:d3:15:a8:05:ec:2d:04:36:

a3:ef:35:41:66:ed:76:ac:33:62:f6:8d:e9:c3:fc:b5:f1:3e:

49:94:f1:87:ff:9f:d3:c9:12:d5:98:c7:cd:c0:e3:4f:d3:32:

6b:c1:53:fd:75:32:31:a3:11:e7:36:aa:a6:f1:09:64:40:49:

1f:93:f5:5d:04:a5:97:d2:9f:89:22:22:58:ff:2e:99:4f:e8:

bb:51:b4:2b:2d:8e:01:de:71:3f:91:ed:cd:8c:19:de:94:ed:

33:5e:b9:9b:56:f2:8d:66:22:47:33:0f:8d:f1:3f:bb:96:d6:

85:cc

This TLSv1 server does not accept SSLv2 connections.

This TLSv1 server also accepts SSLv3 connections.

## MySQL Server detection

**Family:** Database Services

Risk	Port/Protocol	ID
Low	3306/tcp	10719

### Synopsis:

A database server is listening on the remote port.

### Solution:

Restrict access to the database to allowed IPs only.

### Description:

The remote host is running MySQL, an open-source database server. It is possible to extract the version number of the remote installation from the server greeting.

The remote MySQL version is 5.0.45

## Service Identification (2nd pass)

**Family:** Service Detection

Risk	Port/Protocol	ID
Low	3306/tcp	11153

### Description:

A MySQL server is running on this port

## mDNS Detection

**Family:** DNS Services

**Risk**

**Low**

**Port/Protocol**

5353/udp

**ID**

12218

### Synopsis:

It is possible to obtain information about the remote host.

### Solution:

filter incoming traffic to UDP port 5353

### Description:

The remote host is running the Bonjour (also known as ZeroConf or mDNS) protocol.

This protocol allows anyone to dig information from the remote host, such as its operating system type and exact version, its hostname, and the list of services it is running.

An attacker may use this information to perform a more accurate attack.

We could extract the following information :

Computer name : plesk.local.

Ethernet addr : 00:30:48:8e:0b:c4

Computer Type : I686

Operating System : LINUX

## Apache Remote Username Enumeration Vulnerability

**Family:** Web Services

Risk	Port/Protocol	ID
Low	8443/tcp	10766

### Synopsis:

The remote Apache server can be used to guess the presence of a given user name on the remote host.

### Solution:

In httpd.conf, set the 'UserDir' to 'disabled'.

### Description:

When configured with the 'UserDir' option, requests to URLs containing a tilde followed by a username will redirect the user to a given subdirectory in the user home.

For instance, by default, requesting `/~root/` displays the HTML contents from `/root/public_html/`.

If the username requested does not exist, then Apache will reply with a different error code. Therefore, an attacker may exploit this vulnerability to guess the presence of a given user name on the remote host.

### Cross-References:

[CVE-CVE-2001-1013](#), [BID-3335](#), [OSVDB-637](#)

### CVSS(2) Base Score:

5.0

### CVSS(2) Base Vector:

AV:N/AC:L/Au:N/C:P/I:N/A:N

## HyperText Transfer Protocol Information

**Family:** Web Services

Risk	Port/Protocol	ID
Low	8443/tcp	24260

### Synopsis:

Some information about the remote HTTP configuration can be extracted.

### Solution:

None.

### 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

Protocol version : HTTP/1.1

SSL : yes

Pipelining : yes

Keep-Alive : yes

Options allowed : GET, HEAD, OPTIONS, TRACE

Headers :

Date: Wed, 30 Jul 2008 14:06:28 GMT

Server: Apache

X-Powered-By: PHP/5.2.3

Expires: Fri, 28 May 1999 00:00:00 GMT

Last-Modified: Wed, 30 Jul 2008 14:06:28 GMT

Cache-Control: no-store, no-cache, must-revalidate

Cache-Control: post-check=0, pre-check=0

Pragma: no-cache

P3P: CP="NON COR CURa ADMa OUR NOR UNI COM NAV STA"

Keep-Alive: timeout=15, max=50

Connection: Keep-Alive

Transfer-Encoding: chunked

Content-Type: text/html

## HTTP Server type and version

**Family:** Web Services

**Risk**

**Low**

**Port/Protocol**

8443/tcp

**ID**

10107

### **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.

The remote web server type is :

Apache

and the 'ServerTokens' directive is ProductOnly

Apache does not offer a way to hide the server type.

## Supported SSL Ciphers Suites

**Family:** Miscellaneous

Risk	Port/Protocol	ID
Low	8443/tcp	21643

### Synopsis:

The remote service encrypts communications using SSL.

### Description:

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

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

High Strength Ciphers ( >= 112-bit key)

SSLv3

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

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

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

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

TLSv1

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

DHE-RSA-AES128-SHA Kx=DH Au=RSA Enc=AES(128) Mac=SHA1

DHE-RSA-AES256-SHA Kx=DH Au=RSA Enc=AES(256) Mac=SHA1

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

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

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

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

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

The fields above are :

{OpenSSL ciphername}

Kx={key exchange}

Au={authentication}

Enc={symmetric encryption method}

Mac={message authentication code}

{export flag}

### Cross-References:

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

## SSL Certificate

Family: Service Detection

Risk	Port/Protocol	ID
Low	8443/tcp	10863

### Description:

Here is the SSLv3 server certificate:

Certificate:

Data:

Version: 1 (0x0)

Serial Number: 1209771934 (0x481ba79e)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=US, ST=Virginia, L=Herndon, O=SWsoft, Inc., OU=Plesk, CN=plesk/emailAddress=info@plesk.com

Validity

Not Before: May 2 23:45:34 2008 GMT

Not After : May 2 23:45:34 2009 GMT

Subject: C=US, ST=Virginia, L=Herndon, O=SWsoft, Inc., OU=Plesk, CN=plesk/emailAddress=info@plesk.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (2048 bit)

Modulus (2048 bit):

00:c9:86:9f:2f:5d:c2:77:e0:6b:29:39:1b:c8:40:  
85:da:de:f1:31:c8:97:3f:58:ee:8e:3c:84:9e:59:  
c2:70:90:9e:4e:08:7a:2d:84:0a:aa:42:66:1a:55:  
9c:b9:d2:82:19:14:10:1f:a7:d1:fa:34:8c:b0:b9:  
d9:28:7e:9e:a7:34:a3:9c:d8:ab:97:67:ad:e5:cc:  
97:7f:c6:e8:ee:82:c6:7c:44:de:65:85:59:ae:f1:  
25:06:35:8d:01:e6:cc:90:49:b2:20:5f:ff:33:eb:  
73:5e:13:4c:1d:09:4a:3f:da:dc:a7:f7:a3:5a:d0:  
7b:42:4d:94:2c:7f:c0:48:b2:96:e4:ae:86:98:92:  
6b:61:cf:69:9b:29:5b:b7:ec:e9:49:1f:27:ca:4f:  
d1:43:46:38:3d:75:14:42:c7:f5:28:67:6f:56:c5:  
40:6e:88:11:40:8d:d4:02:98:20:98:6b:61:c9:ef:  
e4:b6:56:7f:4a:28:81:36:82:5f:5d:b5:03:75:c3:  
f8:01:b7:f7:54:7a:77:99:40:6c:40:68:7c:32:e5:  
92:39:2d:ca:d8:7e:e3:93:17:05:40:d8:fa:8e:27:  
a5:eb:ad:d0:db:2c:e7:b5:91:c2:57:a6:1d:de:a9:  
a4:25:9c:71:f4:e1:5a:07:9f:7a:2a:f6:24:b7:4c:  
44:43

Exponent: 65537 (0x10001)

Signature Algorithm: sha1WithRSAEncryption

31:31:63:ba:0d:ef:38:63:88:94:f9:93:a2:3a:a3:7e:05:59:  
34:3d:ed:61:d0:23:03:bc:70:3d:a4:be:67:7b:d3:48:3a:f9:  
be:81:bf:a4:b8:62:c1:07:9b:1c:45:56:f8:7a:0b:c8:0d:ab:  
2f:5d:29:a3:d2:14:89:29:5e:6b:b8:1d:e5:9e:ce:d7:cb:15:  
65:24:bb:d0:c2:c3:56:de:d8:9b:d4:a5:8d:eb:ff:c4:9e:d7:  
2a:0e:13:da:17:a3:bb:28:7d:ce:bb:a6:5e:2e:49:ac:25:44:  
cf:0a:f3:30:1c:2f:a6:10:62:98:d1:7f:29:7d:c6:9b:86:0e:  
fe:ab:e1:c1:39:3a:8c:ec:e5:fe:92:43:37:66:63:4e:c7:b6:  
30:1d:6a:fb:ff:d4:23:46:71:6c:ce:71:a7:89:98:23:64:94:  
c8:bd:8f:9b:85:43:c7:fb:83:1d:01:00:b3:f6:c2:08:45:ec:  
73:31:71:4c:9c:b7:8c:43:c0:14:52:85:3c:71:6c:bc:6e:a7:  
28:32:05:0c:e1:bc:bf:f4:de:b4:db:2c:bf:fe:6e:d6:0b:a1:  
e2:0a:cb:e7:64:1a:c9:70:3e:70:b0:bd:48:0b:ff:05:bd:4b:  
23:bb:dd:ac:a7:cb:46:55:94:94:bb:b7:66:14:ae:17:e3:32:  
0d:6f:14:b5

This TLSv1 server does not accept SSLv2 connections.

This TLSv1 server also accepts SSLv3 connections.

## Apache Remote Username Enumeration Vulnerability

**Family:** Web Services

**Risk**

**Low**

**Port/Protocol**

8880/tcp

**ID**

10766

### Synopsis:

The remote Apache server can be used to guess the presence of a given user name on the remote host.

### Solution:

In httpd.conf, set the 'UserDir' to 'disabled'.

### Description:

When configured with the 'UserDir' option, requests to URLs containing a tilde followed by a username will redirect the user to a given subdirectory in the user home.

For instance, by default, requesting `/~root/` displays the HTML contents from `/root/public_html/`.

If the username requested does not exist, then Apache will reply with a different error code. Therefore, an attacker may exploit this vulnerability to guess the presence of a given user name on the remote host.

### Cross-References:

[CVE-CVE-2001-1013](#), [BID-3335](#), [OSVDB-637](#)

### CVSS(2) Base Score:

5.0

### CVSS(2) Base Vector:

AV:N/AC:L/Au:N/C:P/I:N/A:N

## HyperText Transfer Protocol Information

**Family:** Web Services

Risk	Port/Protocol	ID
Low	8880/tcp	24260

### Synopsis:

Some information about the remote HTTP configuration can be extracted.

### Solution:

None.

### 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

Protocol version : HTTP/1.1

SSL : no

Pipelining : yes

Keep-Alive : yes

Options allowed : GET, HEAD, OPTIONS, TRACE

Headers :

Date: Wed, 30 Jul 2008 14:06:28 GMT

Server: Apache

X-Powered-By: PHP/5.2.3

Expires: Fri, 28 May 1999 00:00:00 GMT

Last-Modified: Wed, 30 Jul 2008 14:06:28 GMT

Cache-Control: no-store, no-cache, must-revalidate

Cache-Control: post-check=0, pre-check=0

Pragma: no-cache

P3P: CP="NON COR CURa ADMa OUR NOR UNI COM NAV STA"

Keep-Alive: timeout=15, max=50

Connection: Keep-Alive

Transfer-Encoding: chunked

Content-Type: text/html

## HTTP Server type and version

Risk	Port/Protocol	ID
Low	8880/tcp	10107

**Family:** Web Services

### 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.

The remote web server type is :

Apache

and the 'ServerTokens' directive is ProductOnly

Apache does not offer a way to hide the server type.

## HyperText Transfer Protocol Information

Risk	Port/Protocol	ID
Low	51235/tcp	24260

**Family:** Web Services

### Synopsis:

Some information about the remote HTTP configuration can be extracted.

### Solution:

None.

### 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

Protocol version : HTTP/1.0

SSL : no

Pipelining : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Server: BaseHTTP/0.3 Python/2.4.3

Date: Wed, 30 Jul 2008 14:06:26 GMT

Content-Type: text/html

Connection: close

## HTTP Server type and version

**Family:** Web Services

Risk	Port/Protocol	ID
Low	51235/tcp	10107

### 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.

The remote web server type is :

BaseHTTP/0.3 Python/2.4.3