Summary

This report gives details on hosts that were tested and issues that were found.Please follow the recommended steps and procedures to eradicate these threats.

Scan started at: Sat Sep 10 18:43:13 2005
Scan finished at: Sat Sep 10 18:45:16 2005

Host	Possible Issues	Holes	Warnings	Notes
localhost	Security warning(s) found	0	6	15
Total: 1		0	6	15

Reports per Host

localhost

Scan of this host started at: Sat Sep 10 18:43:14 2005
Scan of this host finished at: Sat Sep 10 18:45:16 2005

Service (Port)	Issue regarding port
smtp (25/tcp)	Security notes found
pop3 (110/tcp)	Security warning(s) found
ipp (631/tcp)	Security warning(s) found
netinfo (1033/tcp)	Security warning(s) found
nessus (1241/tcp)	Security warning(s) found
rendezvous (3689/tcp)	Security notes found
ntp (123/udp)	Security notes found
general/tcp	Security notes found

[return to summary]

Security Issues and Fixes − Host localhost

localhost − smtp (25/tcp)

Informational:
An SMTP server is running on this port Here is its banner : 220 myth.us.nessus.org ESMTP Postfix Nessus ID : 10330
Informational:
Remote SMTP server banner : 220 myth.us.nessus.org ESMTP Postfix   This is probably: Postfix

Nessus ID : 10263

[return to localhost]

localhost − pop3 (110/tcp)

Warning:
The remote server appears to be running a version of QPopper that is older than 4.0.6. Versions older than 4.0.6 are vulnerable to a bug where remote attackers can enumerate valid usernames based on server responses during the authentication process. Solution : None at this time Risk factor : Low BID : 7110 Nessus ID : 12279
Informational:
A pop3 server is running on this port Nessus ID : 10330
Informational:
The remote POP3 servers leak information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy. Versions and types should be omitted where possible. The version of the remote POP3 server is : +OK Qpopper (version 4.0.5) at myth.local starting. Solution : Change the login banner to something generic. Risk factor : Low Nessus ID : 10185

[return to localhost]

localhost − ipp (631/tcp)

Warning:
It seems that your web server tries to hide its version or name, which is a good thing. However, using a special crafted request, Nessus was able to determine that is is running : CUPS/1.1 Risk factor : None Solution : Fix your configuration. Nessus ID : 11239

Warning:
It seems that the PUT method is enabled on your web server Although we could not exploit this, you'd better disable it Solution : disable this method Risk factor : High BID : 12141 Other references : OWASP:OWASP−CM−001 Nessus ID : 10498
Informational:
A web server is running on this port Nessus ID : 10330
Informational:
The following CGI have been discovered : Syntax : cginame (arguments [default value]) /jobs (which_jobs [completed]) /admin/ (op [add−class]) Nessus ID : 10662
Informational:
The remote web server type is : CUPS/1.1 Nessus ID : 10107
Informational:
The following Acrobat files (.pdf) are available on the remote server : /overview.pdf /sum.pdf /sam.pdf /spm.pdf /cmp.pdf /ipp.pdf /idd.pdf /sdd.pdf /sps.pdf /ssr.pdf /translation.pdf /stp.pdf /svd.pdf You should make sure that none of these files contain confidential or otherwise sensitive information. An attacker may use these files to gain a more intimate knowledge of your organization and eventually use them do perform social engineering attacks (abusing the trust of the personnel of your company). Solution : sensitive files should not be accessible by everyone, but only by authenticated users.

Nessus ID : 11419

Informational:

Some Web Servers use a file called /robot(s).txt to make search engines and
any other indexing tools visit their WebPages more frequently and
more efficiently.

By connecting to the server and requesting the /robot(s).txt file, an
attacker may gain additional information about the system they are
attacking.

Such information as, restricted directories, hidden directories, cgi script
directories and etc. Take special care not to tell the robots not to index
sensitive directories, since this tells attackers exactly which of your
directories are sensitive.

Risk factor : None/Low

The file 'robots.txt' contains the following:
#
"$Id: robots.txt,v 1.1.1.5 2005/01/04 19:15:19 jlovell Exp $"
#
This file tells search engines not to index your CUPS server.
#
Copyright 1993−2005 by Easy Software Products.
#
These coded instructions, statements, and computer programs are the
property of Easy Software Products and are protected by Federal
copyright law. Distribution and use rights are outlined in the file
"LICENSE.txt" which should have been included with this file. If this
file is missing or damaged please contact Easy Software Products
at:
#
Attn: CUPS Licensing Information
Easy Software Products
44141 Airport View Drive, Suite 204
Hollywood, Maryland 20636 USA
#
Voice: (301) 373−9600
EMail: cups−info@cups.org
WWW: http://www.cups.org
#

User−agent: *
Disallow: /

#
End of "$Id: robots.txt,v 1.1.1.5 2005/01/04 19:15:19 jlovell Exp $".
#

Nessus ID : 10302

[return to localhost]

localhost − netinfo (1033/tcp)

Warning:

A 'NetInfo' daemon is running on this port. NetInfo is in charge of maintaining databases (or 'maps') regarding the system. Such databases include the list of users, the password file, and more. This service should not be reachable directly from the network.

Solution : Filter incoming traffic to this port
Risk factor : Medium
Nessus ID : 11897

Warning:

Using NetInfo, it was possible to obtain the password file of the remote host by querying it directly. The content of this file is :

. In domain 'unknown_on_port_1033' :

nobody:*:−2:−2:Unprivileged User:/dev/null:/dev/null
daemon:*:1:1:System Services:/var/root:/dev/null
unknown:*:99:99:Unknown User:/dev/null:/dev/null
smmsp:*:25:25:Sendmail User:/private/etc/mail:/dev/null
www:*:70:70:World Wide Web Server:/Library/WebServer:/dev/null
mysql:*:74:74:MySQL Server:/dev/null:/dev/null
sshd:*:75:75:sshd Privilege separation:/var/empty:/dev/null
renaud:********:501:20:Renaud:/Users/renaud:/bin/bash
postfix:*:502:6:Postfix Server:/dev/null:/dev/null
uucp:*:66:66:UUCP daemon:/opt/local/var/spool/uucp:/bin/bash
cyrusimap:*:77:6:Cyrus IMAP User:/var/imap:/usr/bin/false
qtss:*:76:76:QuickTime streaming Server:/var/empty:/usr/bin/false
eppc:*:71:71:Apple Events User:/var/empty:/usr/bin/false
lp:*:26:26:Printing Services:/var/spool/cups:/usr/bin/false
mailman:*:78:78:Mailman user:/var/empty:/usr/bin/false
amavisd:*:83:83:Amavisd User:/var/virusmails:/bin/tcsh
appowner:*:87:87:Application Owner:/var/empty:/usr/bin/false
appserver:*:79:79:Application Server:/var/empty:/usr/bin/false
clamav:*:82:82:Clamav User:/var/virusmails:/bin/tcsh
jabber:*:84:84:jabber:/var/empty:/usr/bin/false
securityagent:*:92:92:SecurityAgent:/var/empty:/usr/bin/false
tokend:*:91:91:Token Daemon:/var/empty:/usr/bin/false
windowserver:*:88:88:WindowServer:/var/empty:/usr/bin/false
xgridagent:*:86:86:Xgrid Agent:/var/xgrid/agent:/usr/bin/false
xgridcontroller:*:85:85:Xgrid Controller:/var/xgrid/controller:/usr/bin/false

An attacker may use it to set up a brute force attack against the remote account names.
BID : 2953
Nessus ID : 11898

[return to localhost]

localhost − nessus (1241/tcp)

Warning:
A Nessus Daemon is listening on this port. Nessus ID : 10147

[return to localhost]

localhost − rendezvous (3689/tcp)

Informational:
A web server is running on this port Nessus ID : 10330
Informational:
This web server is [mis]configured in that it does not return '404 Not Found' error codes when a non−existent file is requested, perhaps returning a site map, search page or authentication page instead. Nessus enabled some counter measures for that, however they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate Nessus ID : 10386

[return to localhost]

localhost − ntp (123/udp)

Informational:
It is possible to determine a lot of information about the remote host by querying the NTP (Network Time Protocol) variables − these include OS descriptor, and time settings. It was possible to gather the following information from the remote NTP host : version='ntpd 4.1.1@1.786 Sun Mar 20 15:40:56 PST 2005 (1)', processor='Power Macintosh', system='Darwin8.2.0', leap=0, stratum=16, precision=−17, rootdelay=346.162, rootdispersion=470.032, peer=0, refid=17.254.0.28, reftime=0xc6cd532a.fa57d9db, poll=4, clock=0xc6cd8bd3.f70fcf80, state=2, offset=0.000, frequency=−61.869, jitter=148.884, stability=19.266 Quickfix: Set NTP to restrict default access to ignore all info packets: restrict default ignore Risk factor : Low Nessus ID : 10884

[return to localhost]

localhost − general/tcp

Informational:
127.0.0.1 resolves as localhost. Nessus ID : 12053
Informational:
The remote host is running Mac OS X 10.4.2 Nessus ID : 11936
Informational:
Information about this scan : Nessus version : 2.9.99 Scanner IP : 127.0.0.1 Port scanner(s) : nessus_tcp_scanner Port range : default Scan Start Date : 2005/9/10 18:43 Scan duration : 122 sec Nessus ID : 19506

[return to localhost]

This file was generated by Nessus, the free security scanner.