



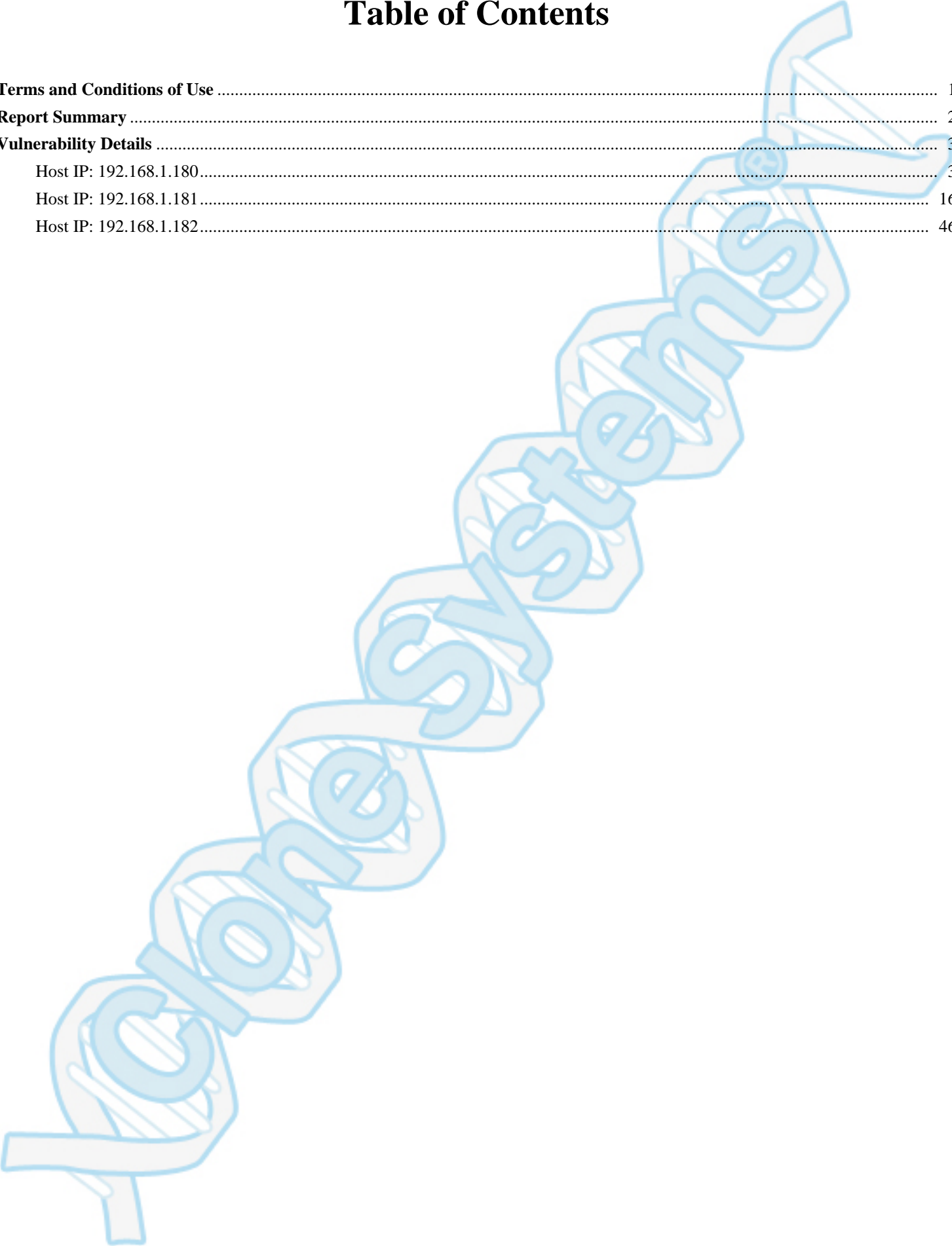
Clone Systems[®]
On-Demand VScan Report

Prepared for: admin

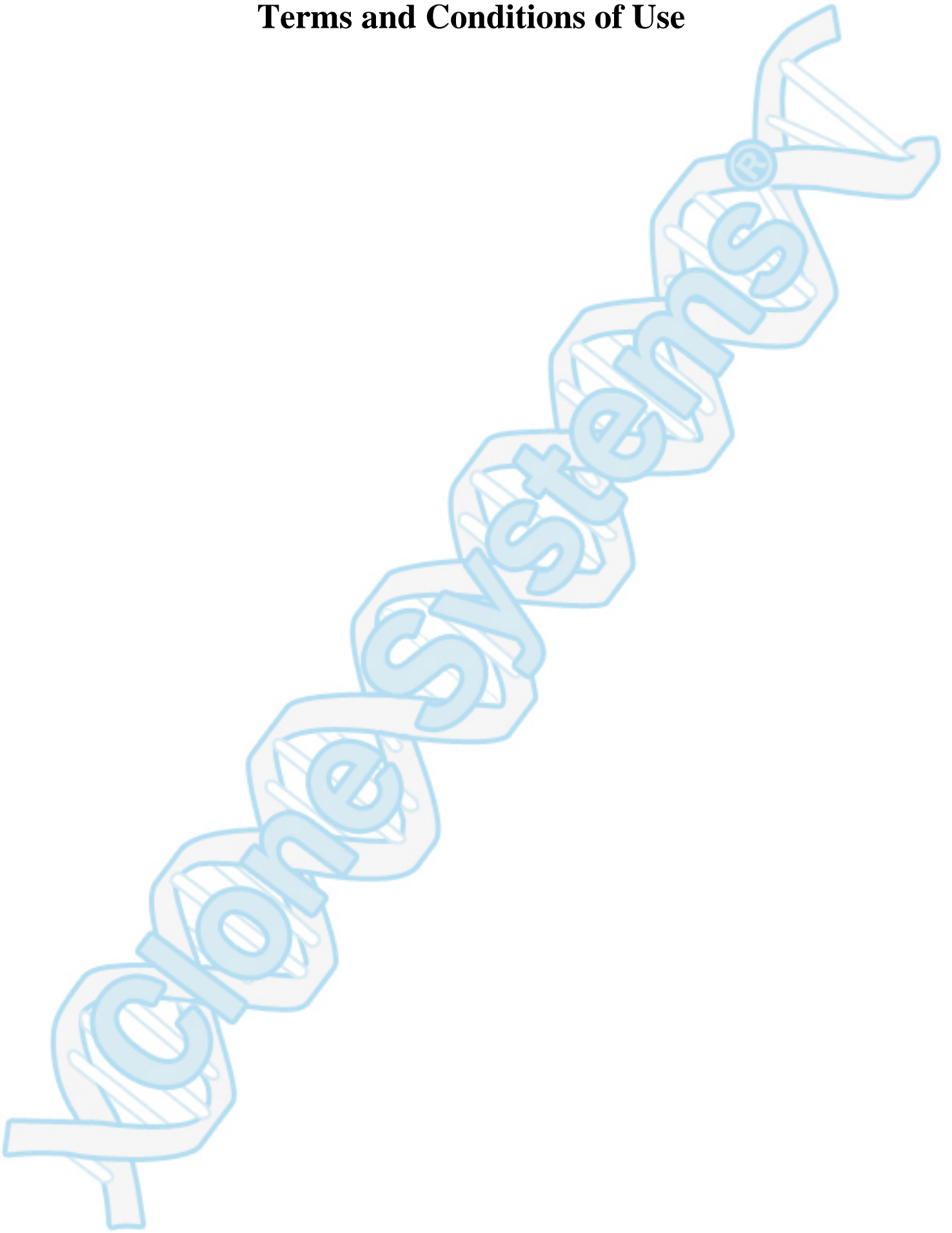
Scanned: 01/17/2008 13:10:20

Table of Contents

Terms and Conditions of Use	1
Report Summary	2
Vulnerability Details	3
Host IP: 192.168.1.180.....	3
Host IP: 192.168.1.181.....	16
Host IP: 192.168.1.182.....	46



Terms and Conditions of Use



Report Summary

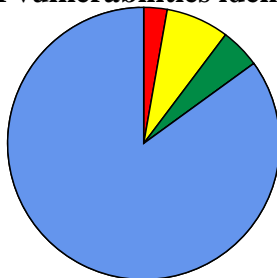
Profile: Profile-for-test-user -

Schedule: Scan Linux Servers2

Owner: admin

Total number of vulnerabilities identified on 3 system(s)

High : 9
Medium : 24
Low : 15
Info : 266



High
Medium
Low
Info

Total number of vulnerabilities identified per system

Host	Serious	High	Medium	Med/Low	Low/Med	Low	Info
192.168.1.180 -	--	7	4	--	--	4	41
192.168.1.181 -	--	1	12	--	--	6	131
192.168.1.182 -	--	1	8	--	--	5	94



Open Port	Open Port
ssh (22/tcp)	filenet-tms (32768/tcp)
sunrpc (111/tcp)	http (80/tcp)
vnc-http-1 (5801/tcp)	vnc-1 (5901/tcp)
smux (199/tcp)	X11:1 (6001/tcp)
ssh (22/tcp)	http (80/tcp)
sunrpc (111/tcp)	smux (199/tcp)
vnc-http-1 (5801/tcp)	vnc-1 (5901/tcp)
X11:1 (6001/tcp)	filenet-tms (32768/tcp)

Service	Risk	PluginID	Description
ssh (22/tcp)	High	10823	<p>You are running a version of OpenSSH which is older than 3.0.2.</p> <p>Versions prior than 3.0.2 are vulnerable to an environment variables export that can allow a local user to execute command with root privileges. This problem affect only versions prior than 3.0.2, and when the UseLogin feature is enabled (usually disabled by default)</p> <p>Solution : Upgrade to OpenSSH 3.0.2 or apply the patch for prior versions. (Available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH)</p> <p>Risk factor : High (If UseLogin is enabled, and locally)</p> <p>CVE : CVE-2001-0872</p> <p>BID : 3614</p> <p>Other references : IAVA:2001-t-0017, OSVDB:688</p>
ssh (22/tcp)	High	10883	<p>You are running a version of OpenSSH which is older than 3.1.</p> <p>Versions prior than 3.1 are vulnerable to an off by one error that allows local users to gain root access, and it may be possible for remote users to similarly compromise the daemon for remote access.</p> <p>In addition, a vulnerable SSH client may be compromised by connecting to a malicious SSH daemon that exploits this vulnerability in the client code, thus compromising the client system.</p> <p>Solution : Upgrade to OpenSSH 3.1 or apply the patch for prior versions. (See: http://www.openssh.org)</p> <p>CVE : CVE-2002-0083</p> <p>BID : 4241</p> <p>Other references : OSVDB:730</p>
ssh (22/tcp)	High	10954	<p>You are running a version of OpenSSH older than OpenSSH 3.2.1</p> <p>A buffer overflow exists in the daemon if AFS is enabled on</p>

			<p>your system, or if the options KerberosTgtPassing or AFSTokenPassing are enabled. Even in this scenario, the vulnerability may be avoided by enabling UsePrivilegeSeparation.</p> <p>Versions prior to 2.9.9 are vulnerable to a remote root exploit. Versions prior to 3.2.1 are vulnerable to a local root exploit.</p> <p>Solution : Upgrade to the latest version of OpenSSH</p> <p>CVE : CVE-2002-0575 BID : 4560 Other references : IAVA:2002-t-0011, OSVDB:781</p>
ssh (22/tcp)	High	11837	<p>You are running a version of OpenSSH which is older than 3.7.1</p> <p>Versions older than 3.7.1 are vulnerable to a flaw in the buffer management functions which might allow an attacker to execute arbitrary commands on this host.</p> <p>An exploit for this issue is rumored to exist.</p> <p>Note that several distribution patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.</p> <p>If you are running a RedHat host, make sure that the command : <code>rpm -q openssh-server</code></p> <p>Returns : openssh-server-3.1p1-13 (RedHat 7.x) openssh-server-3.4p1-7 (RedHat 8.0) openssh-server-3.5p1-11 (RedHat 9)</p> <p>Solution : Upgrade to OpenSSH 3.7.1 See also : http://marc.info/?l=openbsd-misc&m=106375452423794&w=2 http://marc.info/?l=openbsd-misc&m=106375456923804&w=2 CVE : CVE-2003-0682, CVE-2003-0693, CVE-2003-0695 BID : 8628 Other references : IAVA:2003-t-0020, OSVDB:2557, OSVDB:3456, RHTSA:RHTSA-2003:279, SuSE:SUSE-SA:2003:039</p>
ssh (22/tcp)	High	11031	<p>You are running a version of OpenSSH which is older than 3.4</p> <p>There is a flaw in this version that can be exploited remotely to give an attacker a shell on this host.</p> <p>Note that several distribution patched this hole without changing</p>

			<p>the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.</p> <p>If you are running a RedHat host, make sure that the command :</p> <pre>rpm -q openssh-server</pre> <p>Returns :</p> <pre>openssh-server-3.1p1-6</pre> <p>Solution : Upgrade to OpenSSH 3.4 or contact your vendor for a patch CVE : CVE-2002-0639, CVE-2002-0640 BID : 5093 Other references : IAVA:2002-t-0011, OSVDB:839, OSVDB:6245</p>
http (80/tcp)	High	11915	<p>The remote host appears to be running a version of Apache which is older than 1.3.29</p> <p>There are several flaws in this version, which may allow an attacker to possibly execute arbitrary code through mod_alias and mod_rewrite.</p> <p>You should upgrade to 1.3.29 or newer.</p> <p>*** Note that Nessus solely relied on the version number *** of the remote server to issue this warning. This might *** be a false positive</p> <p>Solution : Upgrade to version 1.3.29 See also : http://www.apache.org/dist/httpd/Announcement.html CVE : CVE-2003-0542 BID : 8911 Other references : OSVDB:2733, OSVDB:7611</p>
http (80/tcp)	High	11030	<p>The remote host appears to be vulnerable to the Apache Web Server Chunk Handling Vulnerability.</p> <p>An attacker may exploit this flaw to execute arbitrary code on the remote host with the privileges of the httpd process.</p> <p>Solution : Upgrade to version 1.3.26 or 2.0.39 or newer See also : http://httpd.apache.org/info/security_bulletin_20020617.txt http://httpd.apache.org/info/security_bulletin_20020620.txt CVE : CVE-2002-0392 BID : 5033 Other references : IAVA:2002-a-0003, OSVDB:838</p>
vnc-http-1 (5801/tcp)	Medium	10758	<p>The remote server is running VNC.</p> <p>VNC permits a console to be displayed remotely.</p> <p>Solution: Disable VNC access from the network by using a firewall, or stop VNC service if not needed.</p>
http (80/tcp)	Medium	10766	<p>Synopsis :</p>

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

Description :

When configured with the `Options 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.

Solution :

In `httpd.conf`, set the `Options UserDir` to `Options Disabled`.

CVSS Base Score : 5.0

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

CVE : CVE-2001-1013

BID : 3335

Other references : OSVDB:637

http (80/tcp)

Medium

11213

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

In addition, it has been shown that servers supporting the TRACE method are subject to cross-site scripting attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution :

Disable these methods.

See also :

			<p>http://www.kb.cert.org/vuls/id/867593</p> <p>CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)</p> <p>Solution :</p> <p>Add the following lines for each virtual host in your configuration file :</p> <pre>RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE</pre>
http (80/tcp)	Medium	11137	<p>The remote host appears to be running a version of Apache which is older than 1.3.27</p> <p>There are several flaws in this version, you should upgrade to 1.3.27 or newer.</p> <p>*** Note that Nessus solely relied on the version number *** of the remote server to issue this warning. This might *** be a false positive</p> <p>Solution : Upgrade to version 1.3.27</p> <p>See also : http://www.apache.org/dist/httpd/Announcement.html</p> <p>CVE : CVE-2002-0839, CVE-2002-0840, CVE-2002-0843</p> <p>BID : 5847, 5884, 5887, 5995, 5996</p> <p>Other references : OSVDB:862, OSVDB:4552</p>
X11:1 (6001/tcp)	Low	10407	<p>Synopsis :</p> <p>An X11 server is listening on the remote host</p> <p>Description :</p> <p>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.</p> <p>Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.</p> <p>Solution :</p> <p>Restrict access to this port. If the X11 client/server facility is not used, disable TCP entirely.</p> <p>CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)</p> <p>Plugin output :</p> <p>X11 Version : 11.0</p>

ssh (22/tcp)	Low	11712	<p>You are running OpenSSH-portable 3.6.1 or older.</p> <p>There is a flaw in this version which may allow an attacker to bypass the access controls set by the administrator of this server.</p> <p>OpenSSH features a mechanism which can restrict the list of hosts a given user can log from by specifying a pattern in the user key file (ie: *.mynetwork.com would let a user connect only from the local network).</p> <p>However there is a flaw in the way OpenSSH does reverse DNS lookups. If an attacker configures his DNS server to send a numeric IP address when a reverse lookup is performed, he may be able to circumvent this mechanism.</p> <p>Solution : Upgrade to OpenSSH 3.6.2 when it comes out CVE : CVE-2003-0386 BID : 7831 Other references : OSVDB:2112</p>
ssh (22/tcp)	Low	10882	<p>Synopsis :</p> <p>The remote service offers an insecure cryptographic protocol</p> <p>Description :</p> <p>The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.</p> <p>These protocols are not completely cryptographically safe so they should not be used.</p> <p>Solution :</p> <p>Disable compatibility with version 1 of the protocol.</p> <p>CVSS Base Score : 3 (AV:R/AC:H/Au:NR/C:P/A:N/I:N/B:C) CVE : CVE-2001-0361 BID : 2344 Other references : OSVDB:2116</p>
ssh (22/tcp)	Low	10802	<p>You are running a version of OpenSSH which is older than 3.0.1.</p> <p>Versions older than 3.0.1 are vulnerable to a flaw in which an attacker may authenticate, provided that Kerberos V support has been enabled (which is not the case by default).</p> <p>It is also vulnerable as an excessive memory clearing bug, believed to be unexploitable.</p> <p>*** You may ignore this warning if this host is not using</p>

			<p>*** Kerberos V</p> <p>Solution : Upgrade to OpenSSH 3.0.1</p> <p>Risk factor : Low (if you are not using Kerberos) / High (if kerberos is enabled)</p> <p>CVE : CVE-2001-1507</p> <p>BID : 3560</p>
general/icmp	Info	10114	<p>Synopsis :</p> <p>It is possible to determine the exact time set on the remote host.</p> <p>Description :</p> <p>The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.</p> <p>This may help him to defeat all your time based authentication protocols.</p> <p>Solution :</p> <p>Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).</p> <p>Plugin output :</p> <p>The difference between the local and remote clocks is -1593 seconds</p> <p>CVE : CVE-1999-0524</p>
general/tcp	Info	25220	<p>Synopsis :</p> <p>The remote service implements TCP timestamps.</p> <p>Description :</p> <p>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.</p> <p>See also :</p> <p>http://www.ietf.org/rfc/rfc1323.txt</p>
sunrpc (111/tcp)	Info	10223	<p>Synopsis :</p> <p>An ONC RPC portmapper is running on the remote host.</p> <p>Description :</p> <p>The RPC portmapper is running on this port.</p>

			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.
general/udp	Info	10287	For your information, here is the traceroute from 192.168.1.25 to 192.168.1.180 : 192.168.1.25 192.168.1.180
smux (199/tcp)	Info	10330	An SNMP Multiplexer (smux) seems to be running on this port
sunrpc (111/tcp)	Info	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. Plugin output : The following RPC services are available on TCP port 111 : - program: 100000 (portmapper), version: 2
filenet-tms (32768/tcp)	Info	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. Plugin output : The following RPC services are available on TCP port 32768 : - program: 100024 (status), version: 1
filenet-rpc (32769/tcp)	Info	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

			<p>each service by sending an RPC request to the remote port.</p> <p>Plugin output :</p> <p>The following RPC services are available on TCP port 32769 :</p> <p>- program: 391002 (sgi_fam), version: 2</p>
sunrpc (111/udp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p> <p>Description :</p> <p>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.</p> <p>Plugin output :</p> <p>The following RPC services are available on UDP port 111 :</p> <p>- program: 100000 (portmapper), version: 2</p>
filenet-tms (32768/udp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p> <p>Description :</p> <p>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.</p> <p>Plugin output :</p> <p>The following RPC services are available on UDP port 32768 :</p> <p>- program: 100024 (status), version: 1</p>
ssh (22/tcp)	Info	10330	An ssh server is running on this port
http (80/tcp)	Info	10330	A web server is running on this port
vnc-http-1 (5801/tcp)	Info	10330	A web server is running on this port
http (80/tcp)	Info	11422	<p>Synopsis :</p> <p>The remote web server is not configured at all or is not properly configured.</p> <p>Description :</p>

			<p>The remote web server seems to have its default welcome page set. It probably means that this server is not used at all.</p> <p>Solution :</p> <p>Disable this service, as you do not use it.</p> <p>Other references : OSVDB:2117</p>
vnc-1 (5901/tcp)	Info	10342	<p>Synopsis :</p> <p>The remote host is running a remote display software (VNC).</p> <p>Description :</p> <p>The remote server is running VNC, a software which permits a console to be displayed remotely. This allows users to control the host remotely.</p> <p>Solution :</p> <p>Make sure the use of this software is done in accordance with your corporate security policy and filter incoming traffic to this port.</p> <p>Plugin output :</p> <p>The version of the VNC protocol is : RFB 003.003</p>
general/tcp	Info	20094	<p>Synopsis :</p> <p>The remote host seems to be a VMware virtual machine.</p> <p>Description :</p> <p>According to the MAC address of its network adapter, the remote host is a VMware virtual machine running.</p> <p>Since it is physically accessible through the network, you should ensure that its configuration matches the one of your corporate security policy.</p>
vnc-1 (5901/tcp)	Info	19288	<p>Synopsis :</p> <p>A VNC server is running on the remote host.</p> <p>Description :</p> <p>This script checks the remote VNC server protocol version and the available security types.</p> <p>Plugin output :</p>

			The remote VNC server chose security type #2 (VNC authentication)
ssh (22/tcp)	Info	10267	<p>Synopsis :</p> <p>An SSH server is listening on this port.</p> <p>Description :</p> <p>It is possible to obtain information about the remote SSH server by sending an empty authentication request.</p> <p>Plugin output :</p> <p>SSH version : SSH-1.99-OpenSSH_2.9p2 SSH supported authentication : publickey,password,keyboard-interactive</p>
http (80/tcp)	Info	11032	<p>Synopsis :</p> <p>It is possible to enumerate web directories.</p> <p>Description :</p> <p>This plugin attempts to determine the presence of various common dirs on the remote web server.</p> <p>Plugin output :</p> <p>The following directories were discovered: /cgi-bin, /icons, /manual, /usage</p> <p>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</p> <p>Other references : OWASP:OWASP-CM-006</p>
ssh (22/tcp)	Info	10881	<p>Synopsis :</p> <p>An SSH server is running on the remote host.</p> <p>Description :</p> <p>This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.</p> <p>Plugin output :</p> <p>The remote SSH daemon supports the following versions of the SSH protocol :</p> <ul style="list-style-type: none"> . 1.33 . 1.5

			<p>. 1.99</p> <p>. 2.0</p> <p>SSHv1 host key fingerprint : e8:38:72:51:a8:a8:67:f2:28:30:59:29:9f:c6:71:16</p> <p>SSHv2 host key fingerprint : e6:5d:e7:a5:37:b6:5a:13:1c:0c:a2:07:55:24:49:be</p>
http (80/tcp)	Info	10662	<p>Directory index found at /manual/</p> <p>Directory index found at /manual/mod/mod_perl/</p> <p>Directory index found at /manual/mod/</p>
http (80/tcp)	Info	10107	<p>Synopsis :</p> <p>A web server is running on the remote host.</p> <p>Description :</p> <p>This plugin attempts to determine the type and the version of the remote web server.</p> <p>Plugin output :</p> <p>The remote web server type is :</p> <p>Apache/1.3.20 (Unix) (Red-Hat/Linux)\r</p> <p>Solution : You can set the directive <code>ServerTokens Prod</code> to limit the information emanating from the server in its response headers.</p>
http (80/tcp)	Info	24260	<p>Synopsis :</p> <p>Some information about the remote HTTP configuration can be extracted.</p> <p>Description :</p> <p>This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...</p> <p>This test is informational only and does not denote any security problem</p> <p>Solution :</p> <p>None.</p> <p>Plugin output :</p> <p>Protocol version : HTTP/1.1</p> <p>SSL : no</p> <p>Pipelining : no</p>

			<p>Keep-Alive : no</p> <p>Options allowed : GET, HEAD, OPTIONS, TRACE</p> <p>Headers :</p> <p>Date: Thu, 17 Jan 2008 18:39:59 GMT\r</p> <p>Server: Apache/1.3.20 (Unix) (Red-Hat/Linux)\r</p> <p>Last-Modified: Thu, 06 Sep 2001 03:12:46 GMT\r</p> <p>ETag: "5b257-b4a-3b96e9ae"\r</p> <p>Accept-Ranges: bytes\r</p> <p>Content-Length: 2890\r</p> <p>Connection: close\r</p> <p>Content-Type: text/html\r</p>
general/tcp	Info	11936	<p>Remote operating system : Linux Kernel 2.4</p> <p>Confidence Level : 70</p> <p>Method : SinFP</p> <p>The remote host is running Linux Kernel 2.4</p>
general/tcp	Info	19506	<p>Information about this scan :</p> <p>Nessus version : 3.0.6</p> <p>Plugin feed version : 200801161235</p> <p>Type of plugin feed : Registered (7 days delay)</p> <p>Scanner IP : 192.168.1.25</p> <p>Port scanner(s) : nessus_tcp_scanner synscan</p> <p>Port range : default</p> <p>Thorough tests : no</p> <p>Experimental tests : no</p> <p>Paranoia level : 1</p> <p>Report Verbosity : 1</p> <p>Safe checks : yes</p> <p>Optimize the test : yes</p> <p>Max hosts : 40</p> <p>Max checks : 5</p> <p>Scan Start Date : 2008/1/17 13:11</p> <p>Scan duration : 203 sec</p>



Open Port	Open Port
domain (53/tcp)	ssh (22/tcp)
https (443/tcp)	pop3s (995/tcp)
pop3 (110/tcp)	finger (79/tcp)
telnet (23/tcp)	filenet-tms (32768/tcp)
imaps (993/tcp)	x11 (6000/tcp)
sunrpc (111/tcp)	http (80/tcp)
ftp (21/tcp)	smux (199/tcp)
time (37/tcp)	imap (143/tcp)
pop2 (109/tcp)	ftp (21/tcp)
ssh (22/tcp)	telnet (23/tcp)
time (37/tcp)	domain (53/tcp)
finger (79/tcp)	http (80/tcp)
pop2 (109/tcp)	pop3 (110/tcp)
sunrpc (111/tcp)	imap (143/tcp)
smux (199/tcp)	https (443/tcp)
ftp (21/tcp)	ssh (22/tcp)
telnet (23/tcp)	time (37/tcp)
domain (53/tcp)	finger (79/tcp)
http (80/tcp)	pop2 (109/tcp)
pop3 (110/tcp)	sunrpc (111/tcp)
imap (143/tcp)	smux (199/tcp)
imaps (993/tcp)	pop3s (995/tcp)
https (443/tcp)	imaps (993/tcp)
pop3s (995/tcp)	time (37/tcp)
finger (79/tcp)	http (80/tcp)
pop2 (109/tcp)	pop3 (110/tcp)
sunrpc (111/tcp)	imap (143/tcp)
ftp (21/tcp)	ssh (22/tcp)
telnet (23/tcp)	domain (53/tcp)
smux (199/tcp)	https (443/tcp)
imaps (993/tcp)	pop3s (995/tcp)
time (37/tcp)	finger (79/tcp)
http (80/tcp)	pop2 (109/tcp)
pop3 (110/tcp)	sunrpc (111/tcp)
imap (143/tcp)	ftp (21/tcp)
ssh (22/tcp)	telnet (23/tcp)
domain (53/tcp)	smux (199/tcp)
https (443/tcp)	imaps (993/tcp)
pop3s (995/tcp)	x11 (6000/tcp)
filenet-tms (32768/tcp)	



Service	Risk	PluginID	Description
domain (53/tcp)	High	11318	The remote BIND 9 DNS server, according to its version number, is vulnerable to a

			<p>buffer overflow which may allow an attacker to gain a shell on this host or to disable this server.</p> <p>Solution : upgrade to bind 9.2.2 or downgrade to the 8.x series</p> <p>See also : http://www.isc.org/products/BIND/bind9.html http://cert.uni-stuttgart.de/archive/bugtraq/2003/03/msg00075.html http://www.cert.org/advisories/CA-2002-19.html CVE : CVE-2002-0684 Other references : IAVA:2003-B-0001</p>
telnet (23/tcp)	Medium	10281	<p>Synopsis :</p> <p>A telnet server is listening on the remote port</p> <p>Description :</p> <p>The remote host is running a telnet server. Using telnet is not recommended as logins, passwords and commands are transferred in clear text.</p> <p>An attacker may eavesdrop on a telnet session and obtain the credentials of other users.</p> <p>Solution :</p> <p>Disable this service and use SSH instead</p> <p>CVSS Base Score : 4 (AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:C)</p> <p>Plugin output :</p> <p>Remote telnet banner: Red Hat Linux release 8.0 (Psyche)r Kernel 2.4.18-14 on an i686r login:</p>
pop3s (995/tcp)	Medium	20007	<p>Synopsis :</p> <p>The remote service encrypts traffic using a protocol with known weaknesses.</p> <p>Description :</p> <p>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.</p>

			<p>See also :</p> <p>http://www.schneier.com/paper-ssl.pdf</p> <p>Solution :</p> <p>Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.</p> <p>CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)</p>
https (443/tcp)	Medium	2007	<p>Synopsis :</p> <p>The remote service encrypts traffic using a protocol with known weaknesses.</p> <p>Description :</p> <p>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.</p> <p>See also :</p> <p>http://www.schneier.com/paper-ssl.pdf</p> <p>Solution :</p> <p>Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.</p> <p>CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)</p>
imaps (993/tcp)	Medium	2007	<p>Synopsis :</p> <p>The remote service encrypts traffic using a protocol with known weaknesses.</p> <p>Description :</p> <p>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.</p>

			<p>See also :</p> <p>http://www.schneier.com/paper-ssl.pdf</p> <p>Solution :</p> <p>Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.</p> <p>CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)</p>
finger (79/tcp)	Medium	10068	<p>Synopsis :</p> <p>It is possible to obtain information about the remote host.</p> <p>Description :</p> <p>The remote host is running the 'finger' service.</p> <p>The purpose of this service is to show who is currently logged into the remote system, and to give information about the users of the remote system.</p> <p>It provides useful information to attackers, since it allows them to gain usernames, determine how used a machine is, and see when each user logged in for the last time.</p> <p>Solution :</p> <p>Comment out the 'finger' line in /etc/inetd.conf and restart the inetd process</p> <p>CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)</p> <p>Plugin output :</p> <p>The 'finger' service provides useful information to attackers, since it allows them to gain usernames, check if a machine is being used, and so on...</p> <p>Here is the output we obtained for 'root' :</p> <pre> Login: root Name: root\r Directory: /root Shell: /bin/bash\r Never logged in.\r Mail last read Wed Jan 16 04:02 2008 (EST)\r No Plan.\r </pre>

CVE : CVE-1999-0612
Other references : OSVDB:11451

pop3s (995/tcp)

Medium

26928

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.

See also :

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

Solution :

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

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

Plugin output :

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-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-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

The fields above are :

{OpenSSL ciphername}

Kx={key exchange}

Au={authentication}

Enc={symmetric encryption method}

Mac={message authentication code}

{export flag}

https (443/tcp)

Medium

26928

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.

See also :

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

Solution :

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

CVSS Base Score : 5.0

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

Plugin output :

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-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

			<p>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</p> <p>The fields above are :</p> <p>{OpenSSL ciphername} Kx={key exchange} Au={authentication} Enc={symmetric encryption method} Mac={message authentication code} {export flag}</p>
imaps (993/tcp)	Medium	26928	<p>Synopsis :</p> <p>The remote service supports the use of weak SSL ciphers.</p> <p>Description :</p> <p>The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.</p> <p>See also :</p> <p>http://www.openssl.org/docs/apps/ciphers.html</p> <p>Solution :</p> <p>Reconfigure the affected application if possible to avoid use of weak ciphers.</p> <p>CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)</p> <p>Plugin output :</p> <p>Here is the list of weak SSL ciphers supported by the remote server :</p> <p>Low Strength Ciphers (< 56-bit key)</p> <p>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</p>

			<p>SSLv3</p> <p>EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export</p> <p>EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export</p> <p>EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export</p> <p>TLSv1</p> <p>EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export</p> <p>EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export</p> <p>EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export</p> <p>The fields above are :</p> <p>{OpenSSL ciphername} Kx={key exchange} Au={authentication} Enc={symmetric encryption method} Mac={message authentication code} {export flag}</p>
<p>http (80/tcp)</p>	<p>Medium</p>	<p>11909</p>	<p>Synopsis :</p> <p>The remote web server is affected by an information disclosure vulnerability.</p> <p>Description :</p> <p>It is possible to obtain the listing of the content of the remote web server root by sending the request <code>&#039;GET // HTTP/1.0&#039;</code> This vulnerability usually affects the default Apache configuration which is shipped with Red Hat Linux, although it might affect other Linux distributions or other web server.</p> <p>An attacker can exploit this flaw to browse the contents of the remote web server and possibly find hidden links.</p> <p>See also :</p> <p>http://www.securityfocus.com/archive/1/342578/30/0/threaded</p> <p>Solution :</p> <p>Create an index file for each directory instead of default welcome pages.</p> <p>CVSS Base Score : 5.0</p>

			(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) CVE : CVE-2003-1138 BID : 8898
https (443/tcp)	Medium	11909	<p>Synopsis :</p> <p>The remote web server is affected by an information disclosure vulnerability.</p> <p>Description :</p> <p>It is possible to obtain the listing of the content of the remote web server root by sending the request <code>&#039;GET // HTTP/1.0&#039;</code> This vulnerability usually affects the default Apache configuration which is shipped with Red Hat Linux, although it might affect other Linux distributions or other web server.</p> <p>An attacker can exploit this flaw to browse the contents of the remote web server and possibly find hidden links.</p> <p>See also :</p> <p>http://www.securityfocus.com/archive/1/342578/30/0/threaded</p> <p>Solution :</p> <p>Create an index file for each directory instead of default welcome pages.</p> <p>CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) CVE : CVE-2003-1138 BID : 8898</p>
http (80/tcp)	Medium	11213	<p>Synopsis :</p> <p>Debugging functions are enabled on the remote HTTP server.</p> <p>Description :</p> <p>The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.</p> <p>In addition, it has been shown that servers supporting the TRACE method are subject to cross-site scripting attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.</p> <p>Solution :</p>

			<p>Disable these methods.</p> <p>See also :</p> <p>http://www.kb.cert.org/vuls/id/867593</p> <p>CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)</p> <p>Solution :</p> <p>Add the following lines for each virtual host in your configuration file :</p> <p>RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE</p>
https (443/tcp)	Medium	11213	<p>Synopsis :</p> <p>Debugging functions are enabled on the remote HTTP server.</p> <p>Description :</p> <p>The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.</p> <p>In addition, it has been shown that servers supporting the TRACE method are subject to cross-site scripting attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.</p> <p>Solution :</p> <p>Disable these methods.</p> <p>See also :</p> <p>http://www.kb.cert.org/vuls/id/867593</p> <p>CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)</p> <p>Solution :</p> <p>Add the following lines for each virtual host in your configuration file :</p> <p>RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE</p>
domain (53/udp)	Low	11002	A DNS server is running on this port. If you do not use it, disable it.
domain (53/tcp)	Low	11002	A DNS server is running on this port. If you do not use it, disable it.

pop2 (109/tcp)	Low	15854	<p>The remote host is running a POP2 daemon that allows cleartext logins over unencrypted connections. An attacker can uncover login names and passwords by sniffing traffic to the POP2 daemon.</p> <p>Solution : Encrypt traffic with SSL / TLS using stunnel.</p> <p>Other references : OSVDB:3119</p>
ftp (21/tcp)	Low	10079	<p>Synopsis :</p> <p>Anonymous logins are allowed on the remote FTP server.</p> <p>Description :</p> <p>This FTP service allows anonymous logins. If you do not want to share data with anyone you do not know, then you should deactivate the anonymous account, since it can only cause troubles.</p> <p>CVSS Base Score : 2 (AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)</p> <p>Plugin output :</p> <p>The content of the remote FTP root is :</p> <pre>d--x--x--x 2 0 0 4096 Jan 15 15:40 bin\r d--x--x--x 2 0 0 4096 Jan 15 15:40 etc\r drwxr-xr-x 2 0 0 4096 Jan 15 15:40 lib\r drwxr-sr-x 2 0 50 4096 Jun 23 2002 pub\r</pre> <p>CVE : CVE-1999-0497</p>
x11 (6000/tcp)	Low	10407	<p>Synopsis :</p> <p>An X11 server is listening on the remote host</p> <p>Description :</p> <p>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.</p> <p>Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.</p> <p>Solution :</p> <p>Restrict access to this port. If the X11 client/server facility is not used, disable TCP entirely.</p> <p>CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)</p>

			<p>Plugin output :</p> <p>X11 Version : 11.0</p>
ssh (22/tcp)	Low	10882	<p>Synopsis :</p> <p>The remote service offers an insecure cryptographic protocol</p> <p>Description :</p> <p>The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.</p> <p>These protocols are not completely cryptographically safe so they should not be used.</p> <p>Solution :</p> <p>Disable compatibility with version 1 of the protocol.</p> <p>CVSS Base Score : 3 (AV:R/AC:H/Au:NR/C:P/A:N/I:N/B:C)</p> <p>CVE : CVE-2001-0361</p> <p>BID : 2344</p> <p>Other references : OSVDB:2116</p>
general/icmp	Info	10114	<p>Synopsis :</p> <p>It is possible to determine the exact time set on the remote host.</p> <p>Description :</p> <p>The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.</p> <p>This may help him to defeat all your time based authentication protocols.</p> <p>Solution :</p> <p>Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).</p> <p>Plugin output :</p> <p>The difference between the local and remote clocks is 870 seconds</p> <p>CVE : CVE-1999-0524</p>
general/tcp	Info	25220	<p>Synopsis :</p> <p>The remote service implements TCP timestamps.</p>

			<p>Description :</p> <p>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.</p> <p>See also :</p> <p>http://www.ietf.org/rfc/rfc1323.txt</p>
ntalk (518/udp)	Info	25201	<p>Synopsis :</p> <p>The remote service is a talk server (talkd)</p> <p>Description :</p> <p>The remote service answered to a ntalk request.</p> <p>talkd is a server which notifies a user that someone else wants to initiate a conversation. It works over UDP and is considered by many to be obsolete today.</p> <p>ntalk is implemented on UDP by the Unix command <code>&#039;talk&#039;</code>.</p> <p>See also :</p> <p>The protocol is defined in <code><protocols/talkd.h></code></p> <p>Solution :</p> <p>If you do not use this service, disable it.</p>
sunrpc (111/tcp)	Info	10223	<p>Synopsis :</p> <p>An ONC RPC portmapper is running on the remote host.</p> <p>Description :</p> <p>The RPC portmapper is running on this port.</p> <p>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.</p>
general/udp	Info	10287	<p>For your information, here is the traceroute from 192.168.1.25 to 192.168.1.181 :</p> <p>192.168.1.25</p> <p>192.168.1.181</p>
sunrpc (111/tcp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p>

			<p>Description :</p> <p>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.</p> <p>Plugin output :</p> <p>The following RPC services are available on TCP port 111 :</p> <p>- program: 100000 (portmapper), version: 2</p>
filenet-tms (32768/tcp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p> <p>Description :</p> <p>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.</p> <p>Plugin output :</p> <p>The following RPC services are available on TCP port 32768 :</p> <p>- program: 100024 (status), version: 1</p>
filenet-rpc (32769/tcp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p> <p>Description :</p> <p>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.</p> <p>Plugin output :</p> <p>The following RPC services are available on TCP port 32769 :</p> <p>- program: 391002 (sgi_fam), version: 2</p>
sunrpc (111/udp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p> <p>Description :</p>

			<p>By sending a DUMP request to the portmapper it was possible to enumerate the ONC RPC services running on the remote port.</p> <p>Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port.</p> <p>Plugin output :</p> <p>The following RPC services are available on UDP port 111 :</p> <p>- program: 100000 (portmapper), version: 2</p>
filenet-tms (32768/udp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p> <p>Description :</p> <p>By sending a DUMP request to the portmapper it was possible to enumerate the ONC RPC services running on the remote port.</p> <p>Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port.</p> <p>Plugin output :</p> <p>The following RPC services are available on UDP port 32768 :</p> <p>- program: 100024 (status), version: 1</p>
domain (53/tcp)	Info	10028	<p>Synopsis :</p> <p>It is possible to obtain the version number of the remote DNS server.</p> <p>Description :</p> <p>The remote host is running BIND, an open-source DNS server. It is possible to extract the version number of the remote installation by sending a special DNS request for the text <code>version.bind</code> in the domain <code>chaos</code>.</p> <p>Solution :</p> <p>It is possible to hide the version number of bind by using the <code>version</code> directive in the <code>options</code> section in <code>named.conf</code></p> <p>Plugin output:</p> <p>The version of the remote BIND server is : 9.2.1</p> <p>Other references : OSVDB:23</p>
pop3s (995/tcp)	Info	10330	A SSLv2 server answered on this port
pop3 (110/tcp)	Info	10330	A pop3 server is running on this port

time (37/tcp)	Info	10330	A time server seems to be running on this port
ssh (22/tcp)	Info	10330	An ssh server is running on this port
http (80/tcp)	Info	10330	A web server is running on this port
pop3s (995/tcp)	Info	10330	A pop3 server is running on this port
https (443/tcp)	Info	10330	A SSLv2 server answered on this port
pop2 (109/tcp)	Info	10330	a pop2 server is running on this port
https (443/tcp)	Info	10330	A web server is running on this port through SSL
telnet (23/tcp)	Info	10330	A telnet server seems to be running on this port
ftp (21/tcp)	Info	10330	An FTP server is running on this port. Here is its banner : 220 ready, dude (vsFTPd 1.1.0: beat me, break me)
finger (79/tcp)	Info	10330	A finger server seems to be running on this port
imaps (993/tcp)	Info	10330	A SSLv2 server answered on this port
imap (143/tcp)	Info	10330	An IMAP server is running on this port
imaps (993/tcp)	Info	10330	An IMAP server is running on this port through SSL
pop3s (995/tcp)	Info	10863	Here is the SSLv2 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 0 (0x0) Signature Algorithm: md5WithRSAEncryption Issuer: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit, CN=localhost.localdomain/emailAddress=root@localhost.localdomain Validity Not Before: Jan 15 15:54:22 2008 GMT Not After : Jan 14 15:54:22 2009 GMT Subject: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit, CN=localhost.localdomain/emailAddress=root@localhost.localdomain Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:b8:20:29:3f:db:50:a7:7b:01:97:b2:0c:dc:65: 2c:14:dd:8f:00:7c:a3:fe:19:05:bd:67:86:5e:ae: c0:c0:63:cb:b1:d3:77:e3:9c:23:e2:63:f5:53:a8: e5:c0:ed:cf:4a:09:77:14:3b:42:08:70:9d:df:20: bb:91:8d:92:22:1e:b5:73:ae:de:75:b0:89:dd:6a: 80:1a:a8:9b:fe:41:38:aa:c6:7e:33:70:2f:dd:82: e8:5b:e7:95:45:00:ea:2a:e6:f3:c1:53:eb:f3:2a: a2:51:45:a8:69:a2:c6:cd:df:17:6f:8b:f4:47:3b: 6a:d7:b1:d8:7b:6e:30:7b:13 Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Subject Key Identifier: 9D:B0:88:D2:79:6C:BD:4B:D5:8E:90:10:9B:88:A7:66:5C:DD:F3:A3 X509v3 Authority Key Identifier: keyid:9D:B0:88:D2:79:6C:BD:4B:D5:8E:90:10:9B:88:A7:66:5C:DD:F3:A3

DirName:/C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganization
 alUnit/CN=localhost.localdomain/emailAddress=root@localhost.localdomain
 serial:00

X509v3 Basic Constraints:
 CA:TRUE

Signature Algorithm: md5WithRSAEncryption
 77:6c:7a:88:70:87:17:7e:35:22:4a:f8:a1:4f:96:d1:d9:a8:
 93:9c:ea:98:72:c0:e3:8b:be:96:e2:37:df:24:62:45:9d:18:
 7c:f4:9f:07:a2:f3:76:ec:0d:9b:02:6a:d8:46:88:fa:d1:11:
 d7:1e:2e:9a:b6:da:ed:c1:f2:9f:31:62:f4:c1:36:1e:68:64:
 39:23:02:05:61:24:11:7c:59:a6:7b:9d:c5:6f:2c:8a:7c:8e:
 7f:61:da:de:ea:f1:ea:1d:78:03:1f:cf:32:a4:81:1a:9c:41:
 de:69:49:71:9a:bf:84:3e:07:f8:2f:2d:fd:57:ab:2e:02:2d:
 31:c8

This SSLv2 server also accepts SSLv3 connections.
 This SSLv2 server also accepts TLSv1 connections.

https (443/tcp)

Info

10863

Here is the SSLv2 server certificate:
 Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: 0 (0x0)
 Signature Algorithm: md5WithRSAEncryption
 Issuer: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization,
 OU=SomeOrganizationalUnit,
 CN=localhost.localdomain/emailAddress=root@localhost.localdomain

Validity
 Not Before: Jan 15 15:59:02 2008 GMT
 Not After : Jan 14 15:59:02 2009 GMT
 Subject: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization,
 OU=SomeOrganizationalUnit,
 CN=localhost.localdomain/emailAddress=root@localhost.localdomain

Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 RSA Public Key: (1024 bit)
 Modulus (1024 bit):
 00:d2:5a:d2:48:dd:69:33:b0:49:77:af:cd:9c:d6:
 9f:9d:d2:35:e8:5e:cb:a4:ec:db:40:b7:bc:de:a5:
 c6:e2:2e:1f:f8:37:6d:53:e0:eb:36:14:2e:18:f9:
 bb:f9:d5:c4:e6:c9:a0:73:71:eb:53:35:ba:af:08:
 fa:78:1e:a1:90:b0:5a:c8:3c:40:5f:4d:0d:2f:6f:
 0e:64:e2:17:a5:cf:8d:c0:f6:c0:17:21:0f:61:ee:
 50:39:2c:27:0b:88:16:ff:5b:e7:20:01:7f:54:fd:
 17:be:1f:9a:73:82:85:92:1b:ba:14:6c:f1:58:e2:
 83:d9:36:67:5d:3a:22:89:eb

Exponent: 65537 (0x10001)

X509v3 extensions:
 X509v3 Subject Key Identifier:

			<p>04:C6:15:B4:6B:A6:52:0E:06:04:5D:EE:12:F2:A7:1B:83:89:15:20 X509v3 Authority Key Identifier: keyid:04:C6:15:B4:6B:A6:52:0E:06:04:5D:EE:12:F2:A7:1B:83:89:15:20</p> <p>DirName:/C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganization alUnit/CN=localhost.localdomain/emailAddress=root@localhost.localdomain serial:00</p> <p>X509v3 Basic Constraints: CA:TRUE</p> <p>Signature Algorithm: md5WithRSAEncryption 3a:2c:19:77:39:e4:0c:06:56:20:8e:ae:9e:47:0f:dd:9e:76: 13:88:09:5c:dd:9b:2d:33:07:62:21:94:ed:bb:51:65:08:1e: d0:ca:41:60:5c:5f:ff:8c:84:e6:9b:bf:3f:3d:3b:34:1c:77: c2:53:d4:29:f7:b9:ef:e8:f9:23:f9:14:dd:69:e5:0d:b4:d2: 6e:ec:c9:5c:11:bc:f7:d8:67:b0:e4:dd:fc:8a:12:e8:db:42: 39:a5:3a:57:c2:b0:40:72:56:23:e4:15:09:6c:43:64:77:b1: 99:f8:d6:4e:c5:2d:51:91:07:3b:df:4d:13:b7:44:55:b1:0d: e7:f6</p> <p>This SSLv2 server also accepts SSLv3 connections. This SSLv2 server also accepts TLSv1 connections.</p>
imaps (993/tcp)	Info	10863	<p>Here is the SSLv2 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 0 (0x0) Signature Algorithm: md5WithRSAEncryption Issuer: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit, CN=localhost.localdomain/emailAddress=root@localhost.localdomain</p> <p>Validity Not Before: Jan 15 15:54:21 2008 GMT Not After : Jan 14 15:54:21 2009 GMT Subject: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit, CN=localhost.localdomain/emailAddress=root@localhost.localdomain</p> <p>Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:ae:65:af:0f:2f:e5:ba:dd:80:61:fa:0b:af:02: 60:4f:8b:3f:ee:c1:16:c8:39:58:77:8c:4d:ea:a8: 5d:35:9e:30:78:a5:d0:70:8a:f1:e8:a4:65:1b:ae: 57:04:42:98:11:9b:8a:05:03:a9:07:2e:c8:3b:43: 79:61:a4:77:05:d0:b9:32:3a:58:41:ad:b3:42:98: 47:9d:4c:32:d1:08:72:41:3c:5d:3d:78:1b:88:a2: ac:13:a2:3b:e6:74:d0:da:7f:34:c9:92:fe:9c:08: 06:44:49:a2:55:a8:6a:37:02:81:2b:b4:e7:30:58: 78:02:d4:7b:f4:01:50:88:73</p>

			<p>Exponent: 65537 (0x10001)</p> <p>X509v3 extensions:</p> <p>X509v3 Subject Key Identifier: 50:9A:CA:94:F7:E8:0D:DF:DD:BF:C0:72:00:DF:E2:42:49:5C:DD:42</p> <p>X509v3 Authority Key Identifier: keyid:50:9A:CA:94:F7:E8:0D:DF:DD:BF:C0:72:00:DF:E2:42:49:5C:DD:42</p> <p>DirName:/C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=localhost.localdomain/emailAddress=root@localhost.localdomain serial:00</p> <p>X509v3 Basic Constraints: CA:TRUE</p> <p>Signature Algorithm: md5WithRSAEncryption 97:bd:9c:91:b2:b2:ac:2b:f8:68:cd:11:4d:42:34:d6:f0:0f: 0a:b0:6d:a7:b4:e0:ee:a2:5e:cd:47:c5:3b:7b:16:a6:08:05: a9:5c:54:d8:4f:0f:96:65:1f:d5:75:1b:a0:79:db:89:64:8c: 9c:34:62:6d:e8:76:f4:19:1e:18:d8:c9:f9:d5:7a:91:77:7c: f8:ff:21:8f:0c:b9:a0:65:25:1e:02:da:ee:ab:79:84:2c:81: b6:9a:01:fa:9b:aa:da:23:e1:e4:3d:58:df:6c:f3:1a:9f:f8: ef:45:05:12:1f:35:2f:97:68:0f:d0:e2:76:eb:76:a5:cc:4f: 5a:8f</p> <p>This SSLv2 server also accepts SSLv3 connections. This SSLv2 server also accepts TLSv1 connections.</p>
ftp (21/tcp)	Info	10092	<p>Synopsis :</p> <p>An FTP server is listening on this port</p> <p>Description :</p> <p>It is possible to obtain the banner of the remote FTP server by connecting to the remote port.</p> <p>Plugin output :</p> <p>The remote FTP banner is : 220 ready, dude (vsFTPD 1.1.0: beat me, break me)</p>
pop3 (110/tcp)	Info	10185	<p>Synopsis :</p> <p>A POP server is listening on the remote port</p> <p>Description :</p> <p>The remote host is running a POP server.</p> <p>Solution :</p> <p>Disable this service if you do not use it.</p>

			<p>Plugin output :</p> <p>Remote POP server banner : +OK POP3 [192.168.1.181] v2001.78rh server ready</p>
pop3s (995/tcp)	Info	10185	<p>Synopsis :</p> <p>A POP server is listening on the remote port</p> <p>Description :</p> <p>The remote host is running a POP server.</p> <p>Solution :</p> <p>Disable this service if you do not use it.</p> <p>Plugin output :</p> <p>Remote POP server banner : +OK POP3 [192.168.1.181] v2001.78rh server ready</p>
http (80/tcp)	Info	11422	<p>Synopsis :</p> <p>The remote web server is not configured at all or is not properly configured.</p> <p>Description :</p> <p>The remote web server seems to have its default welcome page set. It probably means that this server is not used at all.</p> <p>Solution :</p> <p>Disable this service, as you do not use it.</p> <p>Other references : OSVDB:2117</p>
https (443/tcp)	Info	11422	<p>Synopsis :</p> <p>The remote web server is not configured at all or is not properly configured.</p> <p>Description :</p> <p>The remote web server seems to have its default welcome page set. It probably means that this server is not used at all.</p> <p>Solution :</p> <p>Disable this service, as you do not use it.</p>

			Other references : OSVDB:2117
http (80/tcp)	Info	11032	<p>Synopsis :</p> <p>It is possible to enumerate web directories.</p> <p>Description :</p> <p>This plugin attempts to determine the presence of various common dirs on the remote web server.</p> <p>Plugin output :</p> <p>The following directories were discovered: /cgi-bin, /error, /icons, /manual, /usage</p> <p>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</p> <p>Other references : OWASP:OWASP-CM-006</p>
imap (143/tcp)	Info	11414	<p>Synopsis :</p> <p>An IMAP server is running on the remote host.</p> <p>Description :</p> <p>An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.</p> <p>Plugin output :</p> <p>The remote imap server banner is : * OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS STARTTLS AUTH=LOGIN] [192.168.1.181] IMAP4rev1 2001.315rh at Thu, 17 Jan 2008 12:57:58 -0500 (EST)</p>
imaps (993/tcp)	Info	11414	<p>Synopsis :</p> <p>An IMAP server is running on the remote host.</p> <p>Description :</p> <p>An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.</p> <p>Plugin output :</p> <p>The remote imap server banner is : * OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] [192.168.1.181] IMAP4rev1 2001.315rh at Thu, 17 Jan 2008 12:58:01 -0500 (EST)</p>
general/tcp	Info	20094	<p>Synopsis :</p>

			<p>The remote host seems to be a VMware virtual machine.</p> <p>Description :</p> <p>According to the MAC address of its network adapter, the remote host is a VMware virtual machine running.</p> <p>Since it is physically accessible through the network, you should ensure that its configuration matches the one of your corporate security policy.</p>
ssh (22/tcp)	Info	10267	<p>Synopsis :</p> <p>An SSH server is listening on this port.</p> <p>Description :</p> <p>It is possible to obtain information about the remote SSH server by sending an empty authentication request.</p> <p>Plugin output :</p> <p>SSH version : SSH-1.99-OpenSSH_3.4p1 SSH supported authentication : publickey,password,keyboard-interactive</p>
ssh (22/tcp)	Info	10881	<p>Synopsis :</p> <p>An SSH server is running on the remote host.</p> <p>Description :</p> <p>This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.</p> <p>Plugin output :</p> <p>The remote SSH daemon supports the following versions of the SSH protocol :</p> <ul style="list-style-type: none"> . 1.33 . 1.5 . 1.99 . 2.0 <p>SSHv1 host key fingerprint : 52:f4:cc:91:dd:03:c4:f7:7a:87:ab:7d:df:04:5a:f4 SSHv2 host key fingerprint : 3e:da:7f:75:98:be:ad:1c:f2:4b:6f:a2:e7:07:b6:1b</p>
https (443/tcp)	Info	11032	<p>Synopsis :</p> <p>It is possible to enumerate web directories.</p>

Description :

This plugin attempts to determine the presence of various common dirs on the remote web server.

Plugin output :

The following directories were discovered:

/cgi-bin, /error, /icons, /manual, /usage

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

Other references : OWASP:OWASP-CM-006

pop3s (995/tcp)

Info

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.

See also :

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

Plugin output :

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-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-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)
 TLSv1
 EXP1024-DES-CBC-SHA Kx=RSA(1024) Au=RSA Enc=DES(56)
 Mac=SHA1 export
 EXP1024-RC2-CBC-MD5 Kx=RSA(1024) Au=RSA Enc=RC2(56)
 Mac=MD5 export
 EXP1024-RC4-MD5 Kx=RSA(1024) Au=RSA Enc=RC4(56) Mac=MD5
 export
 EXP1024-RC4-SHA Kx=RSA(1024) Au=RSA Enc=RC4(56) Mac=SHA1
 export
 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
 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
 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}

https (443/tcp)

Info

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.

See also :

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

Plugin output :

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

RC4-64-MD5 Kx=RSA Au=RSA Enc=RC4(64) 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

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

			<p>SSLv3</p> <p>EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES(168)</p> <p>Mac=SHA1</p> <p>DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1</p> <p>RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5</p> <p>RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1</p> <p>TLSv1</p> <p>EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES(168)</p> <p>Mac=SHA1</p> <p>DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1</p> <p>RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5</p> <p>RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1</p> <p>The fields above are :</p> <p>{OpenSSL ciphername}</p> <p>Kx={key exchange}</p> <p>Au={authentication}</p> <p>Enc={symmetric encryption method}</p> <p>Mac={message authentication code}</p> <p>{export flag}</p>
<p>imaps (993/tcp)</p>	<p>Info</p>	<p>21643</p>	<p>Synopsis :</p> <p>The remote service encrypts communications using SSL.</p> <p>Description :</p> <p>This script detects which SSL ciphers are supported by the remote service for encrypting communications.</p> <p>See also :</p> <p>http://www.openssl.org/docs/apps/ciphers.html</p> <p>Plugin output :</p> <p>Here is the list of SSL ciphers supported by the remote server :</p> <p>Low Strength Ciphers (< 56-bit key)</p> <p>SSLv2</p> <p>EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5</p> <p>export</p> <p>EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5</p> <p>export</p> <p>SSLv3</p> <p>EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1</p> <p>export</p> <p>EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5</p> <p>export</p>

EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5
 export
 TLSv1
 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)
 TLSv1
 EXP1024-DES-CBC-SHA Kx=RSA(1024) Au=RSA Enc=DES(56)
 Mac=SHA1 export
 EXP1024-RC2-CBC-MD5 Kx=RSA(1024) Au=RSA Enc=RC2(56)
 Mac=MD5 export
 EXP1024-RC4-MD5 Kx=RSA(1024) Au=RSA Enc=RC4(56) Mac=MD5
 export
 EXP1024-RC4-SHA Kx=RSA(1024) Au=RSA Enc=RC4(56) Mac=SHA1
 export

 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
 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
 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}

http (80/tcp)

Info

10662

The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/manual/howto/ (C [N] O [D])

/manual/images/ (C [N] O [D])

			<p>/usage/ (C [N] O [D])</p> <p>/manual/platform/ (C [N] O [D])</p> <p>Directory index found at /usage/</p> <p>Directory index found at /manual/images/</p> <p>Directory index found at /manual/platform/</p> <p>Directory index found at /manual/howto/</p>
http (80/tcp)	Info	10107	<p>Synopsis :</p> <p>A web server is running on the remote host.</p> <p>Description :</p> <p>This plugin attempts to determine the type and the version of the remote web server.</p> <p>Plugin output :</p> <p>The remote web server type is :</p> <p>Apache/2.0.40 (Red Hat Linux)\r</p> <p>Solution : You can set the directive <code>ServerTokens Prod</code> to limit the information emanating from the server in its response headers.</p>
https (443/tcp)	Info	10107	<p>Synopsis :</p> <p>A web server is running on the remote host.</p> <p>Description :</p> <p>This plugin attempts to determine the type and the version of the remote web server.</p> <p>Plugin output :</p> <p>The remote web server type is :</p> <p>Apache/2.0.40 (Red Hat Linux)\r</p> <p>Solution : You can set the directive <code>ServerTokens Prod</code> to limit the information emanating from the server in its response headers.</p>
http (80/tcp)	Info	24260	<p>Synopsis :</p> <p>Some information about the remote HTTP configuration can be extracted.</p> <p>Description :</p>

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 :

None.

Plugin output :

Protocol version : HTTP/1.1

SSL : no

Pipelining : no

Keep-Alive : no

Options allowed : GET,HEAD,POST,OPTIONS,TRACE

Headers :

Date: Thu, 17 Jan 2008 18:02:30 GMT\r

Server: Apache/2.0.40 (Red Hat Linux)\r

Accept-Ranges: bytes\r

Content-Length: 2898\r

Connection: close\r

Content-Type: text/html

charset=ISO-8859-1\r

https (443/tcp)

Info

24260

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 :

None.

Plugin output :

Protocol version : HTTP/1.1

SSL : yes

			Pipelining : no Keep-Alive : no Options allowed : GET,HEAD,POST,OPTIONS,TRACE Headers : Date: Thu, 17 Jan 2008 18:02:31 GMT\r Server: Apache/2.0.40 (Red Hat Linux)\r Accept-Ranges: bytes\r Content-Length: 2898\r Connection: close\r Content-Type: text/html charset=ISO-8859-1\r
general/tcp	Info	18261	Using the remote HTTP banner, it is possible to guess that the Linux distribution installed on the remote host is : - Red Hat Linux 8.0 or 9
general/tcp	Info	11936	Remote operating system : Linux Kernel 2.4 Confidence Level : 70 Method : SinFP The remote host is running Linux Kernel 2.4
general/tcp	Info	19506	Information about this scan : Nessus version : 3.0.6 Plugin feed version : 200801161235 Type of plugin feed : Registered (7 days delay) Scanner IP : 192.168.1.25 Port scanner(s) : nessus_tcp_scanner synscan Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : yes Optimize the test : yes Max hosts : 40 Max checks : 5 Scan Start Date : 2008/1/17 13:11 Scan duration : 694 sec



Open Port	Open Port
domain (53/tcp)	ssh (22/tcp)
https (443/tcp)	filenet-nch (32770/tcp)
pop3s (995/tcp)	echo (7/tcp)
pop3 (110/tcp)	finger (79/tcp)
telnet (23/tcp)	filenet-tms (32768/tcp)
imaps (993/tcp)	x11 (6000/tcp)
login (513/tcp)	sunrpc (111/tcp)
http (80/tcp)	ftp (21/tcp)
smux (199/tcp)	imap (143/tcp)
pop2 (109/tcp)	echo (7/tcp)
ftp (21/tcp)	ssh (22/tcp)
telnet (23/tcp)	domain (53/tcp)
finger (79/tcp)	http (80/tcp)
pop2 (109/tcp)	pop3 (110/tcp)
sunrpc (111/tcp)	imap (143/tcp)
smux (199/tcp)	https (443/tcp)
login (513/tcp)	imaps (993/tcp)
pop3s (995/tcp)	x11 (6000/tcp)
filenet-tms (32768/tcp)	filenet-nch (32770/tcp)

Service	Risk	PluginID	Description
domain (53/tcp)	High	11318	<p>The remote BIND 9 DNS server, according to its version number, is vulnerable to a buffer overflow which may allow an attacker to gain a shell on this host or to disable this server.</p> <p>Solution : upgrade to bind 9.2.2 or downgrade to the 8.x series</p> <p>See also : http://www.isc.org/products/BIND/bind9.html http://cert.uni-stuttgart.de/archive/bugtraq/2003/03/msg00075.html http://www.cert.org/advisories/CA-2002-19.html CVE : CVE-2002-0684 Other references : IAVA:2003-B-0001</p>
domain (53/tcp)	Medium	10539	<p>Synopsis :</p> <p>The remote name server allows recursive queries to be performed by the host running nessusd.</p> <p>Description :</p> <p>It is possible to query the remote name server for third party names.</p> <p>If this is your internal nameserver, then forget this warning.</p>

If you are probing a remote nameserver, then it allows anyone to use it to resolve third parties names (such as www.nessus.org). This allows hackers to do cache poisoning attacks against this nameserver.

If the host allows these recursive queries via UDP, then the host can be used to 'bounce' Denial of Service attacks against another network or system.

See also :

<http://www.cert.org/advisories/CA-1997-22.html>

Solution :

Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it).

If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf

If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command

Then, within the options block, you can explicitly state:
'allow-recursion { hosts_defined_in_acl }'

For more info on Bind 9 administration (to include recursion), see: <http://www.nominum.com/content/documents/bind9arm.pdf>

If you are using another name server, consult its documentation.

CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVE : CVE-1999-0024
BID : 136, 678

telnet (23/tcp)

Medium

10281

Synopsis :

A telnet server is listening on the remote port

Description :

The remote host is running a telnet server. Using telnet is not recommended as logins, passwords and commands are transferred in clear text.

An attacker may eavesdrop on a telnet session and obtain the credentials of other users.

			<p>Solution :</p> <p>Disable this service and use SSH instead</p> <p>CVSS Base Score : 4 (AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:C)</p> <p>Plugin output :</p> <p>Remote telnet banner: Red Hat Linux release 9 (Shrike)\r Kernel 2.4.20-8 on an i686\r login:</p>
https (443/tcp)	Medium	20007	<p>Synopsis :</p> <p>The remote service encrypts traffic using a protocol with known weaknesses.</p> <p>Description :</p> <p>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.</p> <p>See also :</p> <p>http://www.schneier.com/paper-ssl.pdf</p> <p>Solution :</p> <p>Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.</p> <p>CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)</p>
https (443/tcp)	Medium	26928	<p>Synopsis :</p> <p>The remote service supports the use of weak SSL ciphers.</p> <p>Description :</p> <p>The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.</p> <p>See also :</p> <p>http://www.openssl.org/docs/apps/ciphers.html</p>

Solution :

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

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

Plugin output :

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-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

The fields above are :

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

http (80/tcp)

Medium

11909

Synopsis :

The remote web server is affected by an information disclosure

		<p>vulnerability.</p> <p>Description :</p> <p>It is possible to obtain the listing of the content of the remote web server root by sending the request <code>&#039;GET // HTTP/1.0&#039;</code>; This vulnerability usually affects the default Apache configuration which is shipped with Red Hat Linux, although it might affect other Linux distributions or other web server.</p> <p>An attacker can exploit this flaw to browse the contents of the remote web server and possibly find hidden links.</p> <p>See also :</p> <p>http://www.securityfocus.com/archive/1/342578/30/0/threaded</p> <p>Solution :</p> <p>Create an index file for each directory instead of default welcome pages.</p> <p>CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)</p> <p>CVE : CVE-2003-1138 BID : 8898</p>
<p>https (443/tcp)</p>	<p>Medium</p>	<p>11909</p> <p>Synopsis :</p> <p>The remote web server is affected by an information disclosure vulnerability.</p> <p>Description :</p> <p>It is possible to obtain the listing of the content of the remote web server root by sending the request <code>&#039;GET // HTTP/1.0&#039;</code>; This vulnerability usually affects the default Apache configuration which is shipped with Red Hat Linux, although it might affect other Linux distributions or other web server.</p> <p>An attacker can exploit this flaw to browse the contents of the remote web server and possibly find hidden links.</p> <p>See also :</p> <p>http://www.securityfocus.com/archive/1/342578/30/0/threaded</p> <p>Solution :</p> <p>Create an index file for each directory instead of default welcome</p>

			<p>pages.</p> <p>CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)</p> <p>CVE : CVE-2003-1138</p> <p>BID : 8898</p>
http (80/tcp)	Medium	11213	<p>Synopsis :</p> <p>Debugging functions are enabled on the remote HTTP server.</p> <p>Description :</p> <p>The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.</p> <p>In addition, it has been shown that servers supporting the TRACE method are subject to cross-site scripting attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.</p> <p>Solution :</p> <p>Disable these methods.</p> <p>See also :</p> <p>http://www.kb.cert.org/vuls/id/867593</p> <p>CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)</p> <p>Solution :</p> <p>Add the following lines for each virtual host in your configuration file :</p> <pre>RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE</pre>
https (443/tcp)	Medium	11213	<p>Synopsis :</p> <p>Debugging functions are enabled on the remote HTTP server.</p> <p>Description :</p> <p>The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.</p> <p>In addition, it has been shown that servers supporting the TRACE</p>

			<p>method are subject to cross-site scripting attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.</p> <p>Solution :</p> <p>Disable these methods.</p> <p>See also :</p> <p>http://www.kb.cert.org/vuls/id/867593</p> <p>CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)</p> <p>Solution :</p> <p>Add the following lines for each virtual host in your configuration file :</p> <p>RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE</p>
domain (53/udp)	Low	11002	A DNS server is running on this port. If you do not use it, disable it.
domain (53/tcp)	Low	11002	A DNS server is running on this port. If you do not use it, disable it.
pop2 (109/tcp)	Low	15854	<p>The remote host is running a POP2 daemon that allows cleartext logins over unencrypted connections. An attacker can uncover login names and passwords by sniffing traffic to the POP2 daemon.</p> <p>Solution : Encrypt traffic with SSL / TLS using stunnel.</p> <p>Other references : OSVDB:3119</p>
x11 (6000/tcp)	Low	10407	<p>Synopsis :</p> <p>An X11 server is listening on the remote host</p> <p>Description :</p> <p>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.</p> <p>Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.</p> <p>Solution :</p> <p>Restrict access to this port. If the X11 client/server facility is not used, disable TCP entirely.</p> <p>CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)</p>

			<p>Plugin output :</p> <p>X11 Version : 11.0</p>
ssh (22/tcp)	Low	10882	<p>Synopsis :</p> <p>The remote service offers an insecure cryptographic protocol</p> <p>Description :</p> <p>The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.</p> <p>These protocols are not completely cryptographically safe so they should not be used.</p> <p>Solution :</p> <p>Disable compatibility with version 1 of the protocol.</p> <p>CVSS Base Score : 3 (AV:R/AC:H/Au:NR/C:P/A:N/I:N/B:C)</p> <p>CVE : CVE-2001-0361 BID : 2344 Other references : OSVDB:2116</p>
general/icmp	Info	10114	<p>Synopsis :</p> <p>It is possible to determine the exact time set on the remote host.</p> <p>Description :</p> <p>The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.</p> <p>This may help him to defeat all your time based authentication protocols.</p> <p>Solution :</p> <p>Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).</p> <p>Plugin output :</p> <p>The difference between the local and remote clocks is -1560 seconds</p> <p>CVE : CVE-1999-0524</p>
general/tcp	Info	25220	<p>Synopsis :</p>

			<p>The remote service implements TCP timestamps.</p> <p>Description :</p> <p>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.</p> <p>See also :</p> <p>http://www.ietf.org/rfc/rfc1323.txt</p>
ntalk (518/udp)	Info	25201	<p>Synopsis :</p> <p>The remote service is a talk server (talkd)</p> <p>Description :</p> <p>The remote service answered to a ntalk request.</p> <p>talkd is a server which notifies a user that someone else wants to initiate a conversation. It works over UDP and is considered by many to be obsolete today.</p> <p>ntalk is implemented on UDP by the Unix command <code>&#039;talk&#039;</code>.</p> <p>See also :</p> <p>The protocol is defined in <code><protocols/talkd.h></code></p> <p>Solution :</p> <p>If you do not use this service, disable it.</p>
sunrpc (111/tcp)	Info	10223	<p>Synopsis :</p> <p>An ONC RPC portmapper is running on the remote host.</p> <p>Description :</p> <p>The RPC portmapper is running on this port.</p> <p>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.</p>
finger (79/tcp)	Info	10330	<p>A finger server seems to be running on this port</p>
nfs (2049/tcp)	Info	10437	<p>You are running a superfluous NFS daemon. You should consider removing it</p> <p>CVE : CVE-1999-0554, CVE-1999-0548</p>
pop3s (995/tcp)	Info	10330	<p>A SSLv2 server answered on this port</p>

pop2 (109/tcp)	Info	10330	a pop2 server is running on this port
pop3s (995/tcp)	Info	10330	A pop3 server is running on this port
https (443/tcp)	Info	10330	A SSLv2 server answered on this port
http (80/tcp)	Info	10330	A web server is running on this port
https (443/tcp)	Info	10330	A web server is running on this port through SSL
general/udp	Info	10287	For your information, here is the traceroute from 192.168.1.25 to 192.168.1.182 : 192.168.1.25 ? 192.168.1.182
sunrpc (111/tcp)	Info	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. Plugin output : The following RPC services are available on TCP port 111 : - program: 100000 (portmapper), version: 2
unknown (895/tcp)	Info	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. Plugin output : The following RPC services are available on TCP port 895 : - program: 100011 (rquotad), version: 1 - program: 100011 (rquotad), version: 2
filenet-nch (32770/tcp)	Info	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

			<p>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.</p> <p>Plugin output :</p> <p>The following RPC services are available on TCP port 32770 :</p> <ul style="list-style-type: none"> - program: 100005 (mountd), version: 1 - program: 100005 (mountd), version: 2
filenet-tms (32768/tcp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p> <p>Description :</p> <p>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.</p> <p>Plugin output :</p> <p>The following RPC services are available on TCP port 32768 :</p> <ul style="list-style-type: none"> - program: 100024 (status), version: 1
filenet-rpc (32769/tcp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p> <p>Description :</p> <p>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.</p> <p>Plugin output :</p> <p>The following RPC services are available on TCP port 32769 :</p> <ul style="list-style-type: none"> - program: 391002 (sgi_fam), version: 2
nfs (2049/udp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p> <p>Description :</p> <p>By sending a DUMP request to the portmapper it was possible to</p>

			<p>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.</p> <p>Plugin output :</p> <p>The following RPC services are available on UDP port 2049 :</p> <ul style="list-style-type: none"> - program: 100003 (nfs), version: 2 - program: 100003 (nfs), version: 3
sunrpc (111/udp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p> <p>Description :</p> <p>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.</p> <p>Plugin output :</p> <p>The following RPC services are available on UDP port 111 :</p> <ul style="list-style-type: none"> - program: 100000 (portmapper), version: 2
unknown (892/udp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p> <p>Description :</p> <p>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.</p> <p>Plugin output :</p> <p>The following RPC services are available on UDP port 892 :</p> <ul style="list-style-type: none"> - program: 100011 (rquotad), version: 1 - program: 100011 (rquotad), version: 2
filenet-nch (32770/udp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p> <p>Description :</p>

			<p>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.</p> <p>Plugin output :</p> <p>The following RPC services are available on UDP port 32770 :</p> <ul style="list-style-type: none"> - program: 100021 (nlockmgr), version: 1 - program: 100021 (nlockmgr), version: 3 - program: 100021 (nlockmgr), version: 4
filenet-rmi (32771/udp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p> <p>Description :</p> <p>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.</p> <p>Plugin output :</p> <p>The following RPC services are available on UDP port 32771 :</p> <ul style="list-style-type: none"> - program: 100005 (mountd), version: 1 - program: 100005 (mountd), version: 2
filenet-tms (32768/udp)	Info	11111	<p>Synopsis :</p> <p>An ONC RPC service is running on the remote host.</p> <p>Description :</p> <p>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.</p> <p>Plugin output :</p> <p>The following RPC services are available on UDP port 32768 :</p> <ul style="list-style-type: none"> - program: 100024 (status), version: 1
echo (7/tcp)	Info	10330	An echo server is running on this port
domain (53/tcp)	Info	10028	<p>Synopsis :</p> <p>It is possible to obtain the version number of the remote DNS server.</p>

			<p>Description :</p> <p>The remote host is running BIND, an open-source DNS server. It is possible to extract the version number of the remote installation by sending a special DNS request for the text <code>&#039;version.bind&#039;</code> in the domain <code>&#039;chaos&#039;</code>.</p> <p>Solution :</p> <p>It is possible to hide the version number of bind by using the <code>&#039;version&#039;</code> directive in the <code>&#039;options&#039;</code> section in <code>named.conf</code></p> <p>Plugin output:</p> <p>The version of the remote BIND server is : 9.2.1</p> <p>Other references : OSVDB:23</p>
ssh (22/tcp)	Info	10330	An ssh server is running on this port
ftp (21/tcp)	Info	10330	An FTP server is running on this port. Here is its banner : 220 (vsFTPd 1.1.3)
imap (143/tcp)	Info	10330	An IMAP server is running on this port
telnet (23/tcp)	Info	10330	A telnet server seems to be running on this port
pop3 (110/tcp)	Info	10330	A pop3 server is running on this port
imaps (993/tcp)	Info	10330	A SSLv2 server answered on this port
imaps (993/tcp)	Info	10330	An IMAP server is running on this port through SSL
pop3s (995/tcp)	Info	10863	<p>Here is the SSLv2 server certificate:</p> <p>Certificate:</p> <p>Data:</p> <p>Version: 3 (0x2)</p> <p>Serial Number: 0 (0x0)</p> <p>Signature Algorithm: md5WithRSAEncryption</p> <p>Issuer: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit, CN=localhost.localdomain/emailAddress=root@localhost.localdomain</p> <p>Validity</p> <p>Not Before: Jan 15 21:41:45 2008 GMT</p> <p>Not After : Jan 14 21:41:45 2009 GMT</p> <p>Subject: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit, CN=localhost.localdomain/emailAddress=root@localhost.localdomain</p> <p>Subject Public Key Info:</p> <p>Public Key Algorithm: rsaEncryption</p> <p>RSA Public Key: (1024 bit)</p> <p>Modulus (1024 bit):</p> <p>00:b8:7b:31:bc:67:fb:f7:58:e6:b8:ec:b4:2a:60: 69:d0:ff:86:56:34:ac:31:ea:79:df:a2:e8:d1:f6: 95:0e:7a:b8:4f:5a:28:76:e1:26:07:d7:4c:1e:c7: 2f:1e:6a:d8:f9:46:79:10:c4:e3:63:96:51:81:46:</p>

da:d4:21:51:bd:98:3d:7b:14:c0:60:15:37:ed:e1:
95:8f:78:52:19:4f:47:c6:9d:6c:70:47:54:ed:a8:
55:31:e8:fe:45:06:ce:38:78:8a:82:80:1b:e1:f8:
1f:ad:37:cf:86:67:3b:cf:be:14:90:d8:47:4f:a2:
5a:ce:fc:d7:97:de:1e:c2:1d

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

E6:67:D6:E2:7D:4B:84:F5:80:71:8C:EA:4A:92:3D:F4:B9:32:BE:E2

X509v3 Authority Key Identifier:

keyid:E6:67:D6:E2:7D:4B:84:F5:80:71:8C:EA:4A:92:3D:F4:B9:32:BE:E2

DirName:/C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganization
alUnit/CN=localhost.localdomain/emailAddress=root@localhost.localdomain

serial:00

X509v3 Basic Constraints:

CA:TRUE

Signature Algorithm: md5WithRSAEncryption

46:c9:0f:a1:2a:a5:ec:af:8c:d0:9c:80:71:a0:c1:46:ed:a8:

47:6c:f4:e7:14:c1:9e:08:f5:94:7e:3e:71:e1:6f:a0:b2:b2:

90:6f:76:22:90:c0:dd:30:ad:cd:09:6c:77:57:d9:77:f6:bb:

09:06:5b:c0:e5:b7:e1:50:2a:fe:0c:c3:27:6f:b2:a7:f8:90:

79:e0:b3:95:ec:2c:b8:df:7e:6d:8f:b5:a7:f4:45:a9:bd:86:

fe:7a:37:99:90:0d:ff:9c:3a:63:3b:b1:3f:d8:4f:e8:99:90:

f3:37:db:05:7a:62:a0:bc:9c:0d:f3:17:ab:19:e7:25:ce:56:

08:79

This SSLv2 server also accepts SSLv3 connections.

This SSLv2 server also accepts TLSv1 connections.

https (443/tcp)

Info

10863

Here is the SSLv2 server certificate:

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization,

OU=SomeOrganizationalUnit,

CN=localhost.localdomain/emailAddress=root@localhost.localdomain

Validity

Not Before: Jan 15 21:07:01 2008 GMT

Not After : Jan 14 21:07:01 2009 GMT

Subject: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization,

OU=SomeOrganizationalUnit,

CN=localhost.localdomain/emailAddress=root@localhost.localdomain

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:c3:eb:b7:90:3d:ad:8b:02:f0:32:56:62:39:1b:

			<p>63:b8:e0:95:51:9d:ae:cb:5a:20:0e:67:d5:64:73: be:77:4c:7f:de:8f:44:d6:4a:db:73:69:6b:e2:18: b8:c6:88:a6:b1:48:d6:58:c4:18:72:b5:e1:d3:d1: 58:64:37:ea:61:b0:86:18:cc:b2:37:70:e7:00:63: 4a:91:8d:0b:c0:79:6e:60:64:ff:3d:49:a9:b5:5d: b7:29:c0:1d:b7:00:0d:d8:f5:10:65:19:66:b2:52: dd:19:e2:73:50:56:25:66:f9:81:c7:5e:e5:66:0c: 05:85:08:6c:9f:f5:fa:f4:95</p> <p>Exponent: 65537 (0x10001)</p> <p>X509v3 extensions:</p> <p>X509v3 Subject Key Identifier: A0:A4:87:52:1F:4D:AA:10:05:04:58:5A:5D:89:20:EE:38:19:1D:87</p> <p>X509v3 Authority Key Identifier: keyid:A0:A4:87:52:1F:4D:AA:10:05:04:58:5A:5D:89:20:EE:38:19:1D:87</p> <p>DirName:/C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganization alUnit/CN=localhost.localdomain/emailAddress=root@localhost.localdomain serial:00</p> <p>X509v3 Basic Constraints: CA:TRUE</p> <p>Signature Algorithm: md5WithRSAEncryption 34:7c:4b:50:9d:c3:f2:94:84:5f:60:c2:42:57:91:73:f5:63: 36:6e:48:6b:4e:76:fa:3e:e0:dd:01:2d:84:ee:ef:85:7d:31: ed:b9:27:5c:65:8a:1b:40:7f:1b:58:c3:5b:4c:e8:44:db:77: 5a:04:73:51:16:65:c3:b1:dd:b6:1d:6c:5d:08:50:6e:03:51: ac:1b:2c:46:39:a8:4a:b9:f6:2e:f4:90:95:45:c1:e5:36:8a: 3c:6e:aa:71:cc:ae:7b:67:2e:00:ce:39:2c:99:98:66:79:56: bf:57:8e:09:f7:e9:21:fa:01:c8:65:a1:f9:60:b4:55:0f:a9: 51:d7</p> <p>This SSLv2 server also accepts SSLv3 connections. This SSLv2 server also accepts TLSv1 connections.</p>
ftp (21/tcp)	Info	10092	<p>Synopsis :</p> <p>An FTP server is listening on this port</p> <p>Description :</p> <p>It is possible to obtain the banner of the remote FTP server by connecting to the remote port.</p> <p>Plugin output :</p> <p>The remote FTP banner is : 220 (vsFTPd 1.1.3)</p>
imaps (993/tcp)	Info	10863	<p>Here is the SSLv2 server certificate:</p> <p>Certificate:</p> <p>Data:</p> <p>Version: 3 (0x2)</p>

Serial Number: 0 (0x0)
 Signature Algorithm: md5WithRSAEncryption
 Issuer: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization,
 OU=SomeOrganizationalUnit,
 CN=localhost.localdomain/emailAddress=root@localhost.localdomain
 Validity
 Not Before: Jan 15 21:41:45 2008 GMT
 Not After : Jan 14 21:41:45 2009 GMT
 Subject: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization,
 OU=SomeOrganizationalUnit,
 CN=localhost.localdomain/emailAddress=root@localhost.localdomain
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 RSA Public Key: (1024 bit)
 Modulus (1024 bit):
 00:b4:5a:f6:49:6a:5e:fb:f5:dd:73:72:6c:67:8a:
 4c:bf:a6:6b:39:44:a8:46:87:11:90:10:e1:b7:9f:
 a8:6a:bc:42:3a:df:52:85:ac:1a:8c:ac:f5:70:3d:
 2c:f5:4a:3a:7b:46:ab:f0:d9:be:dd:c9:57:7e:4c:
 0b:61:3f:67:ee:2d:e9:68:1b:4c:a9:28:a8:da:3f:
 ca:56:65:7f:e1:98:06:e7:e2:74:4a:2b:58:b3:00:
 13:ab:85:37:f5:80:16:96:31:97:2b:c1:d2:5e:7e:
 00:aa:36:1e:44:b5:55:40:21:7f:f1:88:2e:5b:93:
 35:2c:0e:ea:87:28:a5:d4:b1
 Exponent: 65537 (0x10001)
 X509v3 extensions:
 X509v3 Subject Key Identifier:
 C5:CC:A5:B4:12:E1:77:D4:7A:12:33:11:3C:B3:43:1F:9A:9E:6D:2E
 X509v3 Authority Key Identifier:
 keyid:C5:CC:A5:B4:12:E1:77:D4:7A:12:33:11:3C:B3:43:1F:9A:9E:6D:2E
 DirName:/C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=localhost.localdomain/emailAddress=root@localhost.localdomain
 serial:00
 X509v3 Basic Constraints:
 CA:TRUE
 Signature Algorithm: md5WithRSAEncryption
 b4:25:7e:ae:6c:39:61:16:34:16:c1:4c:61:f3:8f:94:2c:8c:
 e3:fc:18:41:e0:16:1a:3c:fc:bb:e8:54:11:6d:18:e7:c5:0a:
 89:41:b5:0e:33:95:7b:0e:2f:5a:4a:c5:a9:a2:64:20:97:99:
 3d:ad:1b:c8:90:cf:08:82:65:18:f2:b6:43:8a:56:88:fe:f0:
 f8:7a:a4:a4:c1:56:62:d6:ae:62:71:61:48:3f:a3:ed:47:54:
 c9:53:65:47:d9:6d:e5:97:20:e9:db:98:55:41:8a:f1:2c:50:
 eb:39:c1:df:99:64:32:53:6b:f8:b5:8a:ec:05:cb:f4:a8:6e:
 b0:a7
 This SSLv2 server also accepts SSLv3 connections.
 This SSLv2 server also accepts TLSv1 connections.

http (80/tcp)

Info

11422

Synopsis :

			<p>The remote web server is not configured at all or is not properly configured.</p> <p>Description :</p> <p>The remote web server seems to have its default welcome page set. It probably means that this server is not used at all.</p> <p>Solution :</p> <p>Disable this service, as you do not use it.</p> <p>Other references : OSVDB:2117</p>
https (443/tcp)	Info	11422	<p>Synopsis :</p> <p>The remote web server is not configured at all or is not properly configured.</p> <p>Description :</p> <p>The remote web server seems to have its default welcome page set. It probably means that this server is not used at all.</p> <p>Solution :</p> <p>Disable this service, as you do not use it.</p> <p>Other references : OSVDB:2117</p>
http (80/tcp)	Info	11032	<p>Synopsis :</p> <p>It is possible to enumerate web directories.</p> <p>Description :</p> <p>This plugin attempts to determine the presence of various common dirs on the remote web server.</p> <p>Plugin output :</p> <p>The following directories were discovered: /cgi-bin, /error, /icons, /manual, /usage</p> <p>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</p> <p>Other references : OWASP:OWASP-CM-006</p>
imap (143/tcp)	Info	11414	<p>Synopsis :</p>

			<p>An IMAP server is running on the remote host.</p> <p>Description :</p> <p>An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.</p> <p>Plugin output :</p> <p>The remote imap server banner is :</p> <pre>* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS STARTTLS AUTH=LOGIN] [192.168.1.182] IMAP4rev1 2001.315rh at Thu, 17 Jan 2008 13:38:20 -0500 (EST)</pre>
imaps (993/tcp)	Info	11414	<p>Synopsis :</p> <p>An IMAP server is running on the remote host.</p> <p>Description :</p> <p>An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.</p> <p>Plugin output :</p> <p>The remote imap server banner is :</p> <pre>* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] [192.168.1.182] IMAP4rev1 2001.315rh at Thu, 17 Jan 2008 13:38:23 -0500 (EST)</pre>
pop3s (995/tcp)	Info	21643	<p>Synopsis :</p> <p>The remote service encrypts communications using SSL.</p> <p>Description :</p> <p>This script detects which SSL ciphers are supported by the remote service for encrypting communications.</p> <p>See also :</p> <p>http://www.openssl.org/docs/apps/ciphers.html</p> <p>Plugin output :</p> <p>Here is the list of SSL ciphers supported by the remote server :</p> <p>High Strength Ciphers (>= 112-bit key)</p> <pre>SSLv2 DES-CBC3-MD5 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5</pre> <p>The fields above are :</p>

			<p>{OpenSSL ciphername} Kx={key exchange} Au={authentication} Enc={symmetric encryption method} Mac={message authentication code} {export flag}</p>
https (443/tcp)	Info	21643	<p>Synopsis :</p> <p>The remote service encrypts communications using SSL.</p> <p>Description :</p> <p>This script detects which SSL ciphers are supported by the remote service for encrypting communications.</p> <p>See also :</p> <p>http://www.openssl.org/docs/apps/ciphers.html</p> <p>Plugin output :</p> <p>Here is the list of SSL ciphers supported by the remote server :</p> <p>Low Strength Ciphers (< 56-bit key)</p> <p>SSLv2</p> <p>EXP-RC2-CBC-MD5 export Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5</p> <p>EXP-RC4-MD5 export Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5</p> <p>SSLv3</p> <p>EXP-EDH-RSA-DES-CBC-SHA Mac=SHA1 export Kx=DH(512) Au=RSA Enc=DES(40)</p> <p>EXP-DES-CBC-SHA export Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1</p> <p>EXP-RC2-CBC-MD5 export Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5</p> <p>EXP-RC4-MD5 export Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5</p> <p>TLSv1</p> <p>EXP-EDH-RSA-DES-CBC-SHA Mac=SHA1 export Kx=DH(512) Au=RSA Enc=DES(40)</p> <p>EXP-DES-CBC-SHA export Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1</p> <p>EXP-RC2-CBC-MD5 export Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5</p> <p>EXP-RC4-MD5 export Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5</p>

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

SSLv2

DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5
 RC4-64-MD5 Kx=RSA Au=RSA Enc=RC4(64) 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

 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}

general/tcp

Info

20094

Synopsis :

The remote host seems to be a VMware virtual machine.

Description :

			<p>According to the MAC address of its network adapter, the remote host is a VMware virtual machine running.</p> <p>Since it is physically accessible through the network, you should ensure that its configuration matches the one of your corporate security policy.</p>
ssh (22/tcp)	Info	10267	<p>Synopsis :</p> <p>An SSH server is listening on this port.</p> <p>Description :</p> <p>It is possible to obtain information about the remote SSH server by sending an empty authentication request.</p> <p>Plugin output :</p> <p>SSH version : SSH-1.99-OpenSSH_3.5p1 SSH supported authentication : publickey,password,keyboard-interactive</p>
ssh (22/tcp)	Info	10881	<p>Synopsis :</p> <p>An SSH server is running on the remote host.</p> <p>Description :</p> <p>This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.</p> <p>Plugin output :</p> <p>The remote SSH daemon supports the following versions of the SSH protocol :</p> <ul style="list-style-type: none"> . 1.33 . 1.5 . 1.99 . 2.0 <p>SSHv1 host key fingerprint : 34:16:c8:e2:8a:e6:d3:75:c1:1b:8f:68:5b:e3:ba:3a SSHv2 host key fingerprint : 05:29:fa:cd:10:a8:1b:14:99:cb:b0:65:8e:43:ba:ad</p>
https (443/tcp)	Info	11032	<p>Synopsis :</p> <p>It is possible to enumerate web directories.</p> <p>Description :</p> <p>This plugin attempts to determine the presence of various common dirs on the remote web server.</p>

			<p>Plugin output :</p> <p>The following directories were discovered: /cgi-bin, /error, /icons, /manual, /usage</p> <p>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</p> <p>Other references : OWASP:OWASP-CM-006</p>
http (80/tcp)	Info	10662	<p>The following CGI have been discovered :</p> <p>Syntax : cginame (arguments [default value])</p> <p>/manual/howto/ (C [N] O [D]) /manual/images/ (C [N] O [D]) /usage/ (C [N] O [D]) /manual/platform/ (C [N] O [D])</p> <p>Directory index found at /usage/ Directory index found at /manual/images/ Directory index found at /manual/platform/ Directory index found at /manual/howto/</p>
http (80/tcp)	Info	10107	<p>Synopsis :</p> <p>A web server is running on the remote host.</p> <p>Description :</p> <p>This plugin attempts to determine the type and the version of the remote web server.</p> <p>Plugin output :</p> <p>The remote web server type is :</p> <p>Apache/2.0.40 (Red Hat Linux)\r</p> <p>Solution : You can set the directive <code>&#039;ServerTokens Prod&#039;</code> to limit the information emanating from the server in its response headers.</p>
https (443/tcp)	Info	10107	<p>Synopsis :</p> <p>A web server is running on the remote host.</p> <p>Description :</p>

			<p>This plugin attempts to determine the type and the version of the remote web server.</p> <p>Plugin output :</p> <p>The remote web server type is :</p> <p>Apache/2.0.40 (Red Hat Linux)\r</p> <p>Solution : You can set the directive <code>ServerTokens Prod</code>; to limit the information emanating from the server in its response headers.</p>
http (80/tcp)	Info	24260	<p>Synopsis :</p> <p>Some information about the remote HTTP configuration can be extracted.</p> <p>Description :</p> <p>This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...</p> <p>This test is informational only and does not denote any security problem</p> <p>Solution :</p> <p>None.</p> <p>Plugin output :</p> <p>Protocol version : HTTP/1.1 SSL : no Pipelining : no Keep-Alive : no Options allowed : GET,HEAD,POST,OPTIONS,TRACE Headers :</p> <p>Date: Thu, 17 Jan 2008 18:42:25 GMT\r Server: Apache/2.0.40 (Red Hat Linux)\r Accept-Ranges: bytes\r Content-Length: 2898\r Connection: close\r Content-Type: text/html charset=ISO-8859-1\r</p>
https (443/tcp)	Info	24260	<p>Synopsis :</p> <p>Some information about the remote HTTP configuration can be extracted.</p>

			<p>Description :</p> <p>This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...</p> <p>This test is informational only and does not denote any security problem</p> <p>Solution :</p> <p>None.</p> <p>Plugin output :</p> <p>Protocol version : HTTP/1.1 SSL : yes Pipelining : no Keep-Alive : no Options allowed : GET,HEAD,POST,OPTIONS,TRACE Headers :</p> <p>Date: Thu, 17 Jan 2008 18:42:25 GMT\r Server: Apache/2.0.40 (Red Hat Linux)\r Accept-Ranges: bytes\r Content-Length: 2898\r Connection: close\r Content-Type: text/html charset=ISO-8859-1\r</p>
general/tcp	Info	18261	<p>Using the remote HTTP banner, it is possible to guess that the Linux distribution installed on the remote host is :</p> <p>- Red Hat Linux 8.0 or 9</p>
general/tcp	Info	11936	<p>Remote operating system : Linux Kernel 2.4 Confidence Level : 70 Method : SinFP</p> <p>The remote host is running Linux Kernel 2.4</p>
general/tcp	Info	19506	<p>Information about this scan :</p> <p>Nessus version : 3.0.6 Plugin feed version : 200801161235 Type of plugin feed : Registered (7 days delay) Scanner IP : 192.168.1.25 Port scanner(s) : nessus_tcp_scanner synscan Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1</p>

		Report Verbosity : 1 Safe checks : yes Optimize the test : yes Max hosts : 40 Max checks : 5 Scan Start Date : 2008/1/17 13:11 Scan duration : 761 sec
--	--	--

