



# Security Scan Report

private & confidential

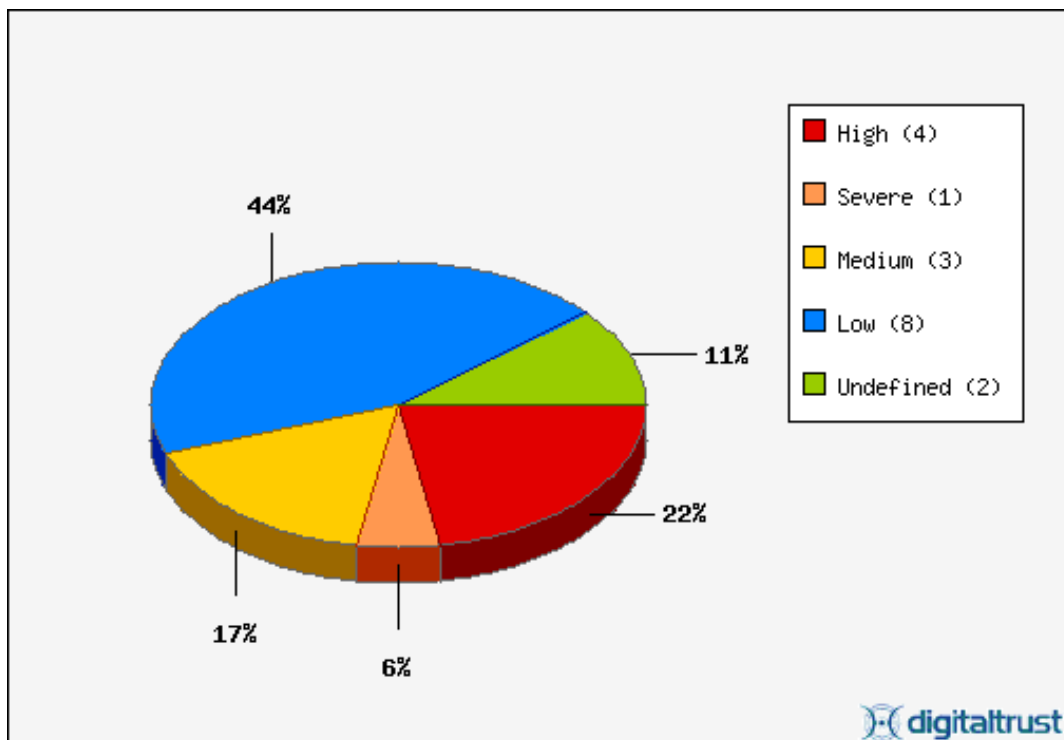
27.01.2003

Ogni materiale, rapporto, soluzione, suggerimento o informazione di qualsiasi natura fornito da Digitaltrust SpA, compreso il servizio software "Digitaltrust Sonar" o "Sonar", è fornito sulla base "così com'è". Digitaltrust SpA non offre garanzie di alcun tipo, né espresse né implicite, relativamente ad alcun elemento della fornitura, come, ma non solo, garanzie di rispondenza ad uno specifico obiettivo, di commerciabilità, di esclusività o di efficacia per il conseguimento di risultati grazie all'uso del materiale. Digitaltrust SpA non garantisce altresì l'inesistenza di brevetti, marchi commerciali di terzi, o di eventuali violazioni di copyright.

**INFORMAZIONI SULLA SCANSIONE:**

**Numero:** 3  
**Inizio:** 24.01.2003 22:00:37  
**Fine:** 27.01.2003 16:56:49  
**Target:** 192.168.1.251  
**Sistema Operativo:** Linux 2.4.7 (X86)  
**Esecutore:** Luca La Ferla  
**Azienda:** Digitaltrust

## RISCHI DI SICUREZZA:



HOST	High	Severe	Medium	Low	Undefined	Total
192.168.1.251	4 (2.3%)	1 (0.6%)	3 (1.7%)	8 (4.6%)	2 (1.1%)	18 (10.3%)
<b>NETWORK</b>	<b>27 (15.5%)</b>	<b>6 (3.4%)</b>	<b>37 (21.3%)</b>	<b>78 (44.8%)</b>	<b>26 (14.9%)</b>	<b>174 (100%)</b>

FAMILY	High	Severe	Medium	Low	Undefined
Windows	0	0	2	3	0
FTP	4	0	0	1	0
Misc.	0	0	1	2	0
General	0	1	0	1	0
Backdoors	0	0	0	0	0
<b>NETWORK</b>	<b>4</b>	<b>1</b>	<b>3</b>	<b>7</b>	<b>0</b>

**High**

Name	ftp
Proto	tcp
Port	21
Plugin	10508
Risk	High
Severity	Security Hole

Name	ftp
Proto	tcp
Port	21
Plugin	11160
Risk	High
Severity	Security Hole

Name	ftp
Proto	tcp
Port	21
Plugin	10305
Risk	High
Severity	Security Hole

Name	ftp
Proto	tcp
Port	21
Plugin	10080
Risk	High
Severity	Security Hole

**Severe**

Name	domain
Proto	tcp
Port	53
Plugin	10539
Risk	Severe
Severity	Security Warning

**Medium**

Name	netbios-ssn
Proto	tcp
Port	139
Plugin	10395
Risk	Medium
Severity	Security Warning

Name	www
------	-----

Proto	tcp
Port	80
Plugin	11137
Risk	Medium
Severity	Security Warning

Name	netbios-ns
Proto	udp
Port	137
Plugin	10150
Risk	Medium
Severity	Security Warning

### Low

Name	netbios-ssn
Proto	tcp
Port	139
Plugin	10397
Risk	Low
Severity	Security Warning

Name	general
Proto	tcp
Port	general
Plugin	10201
Risk	Low
Severity	Security Warning

Name	netbios-ssn
Proto	tcp
Port	139
Plugin	10859
Risk	Low
Severity	Security Warning

Name	ftp
Proto	tcp
Port	21
Plugin	10079
Risk	Low
Severity	Security Warning

Name	netbios-ssn
Proto	tcp
Port	139
Plugin	10398
Risk	Low

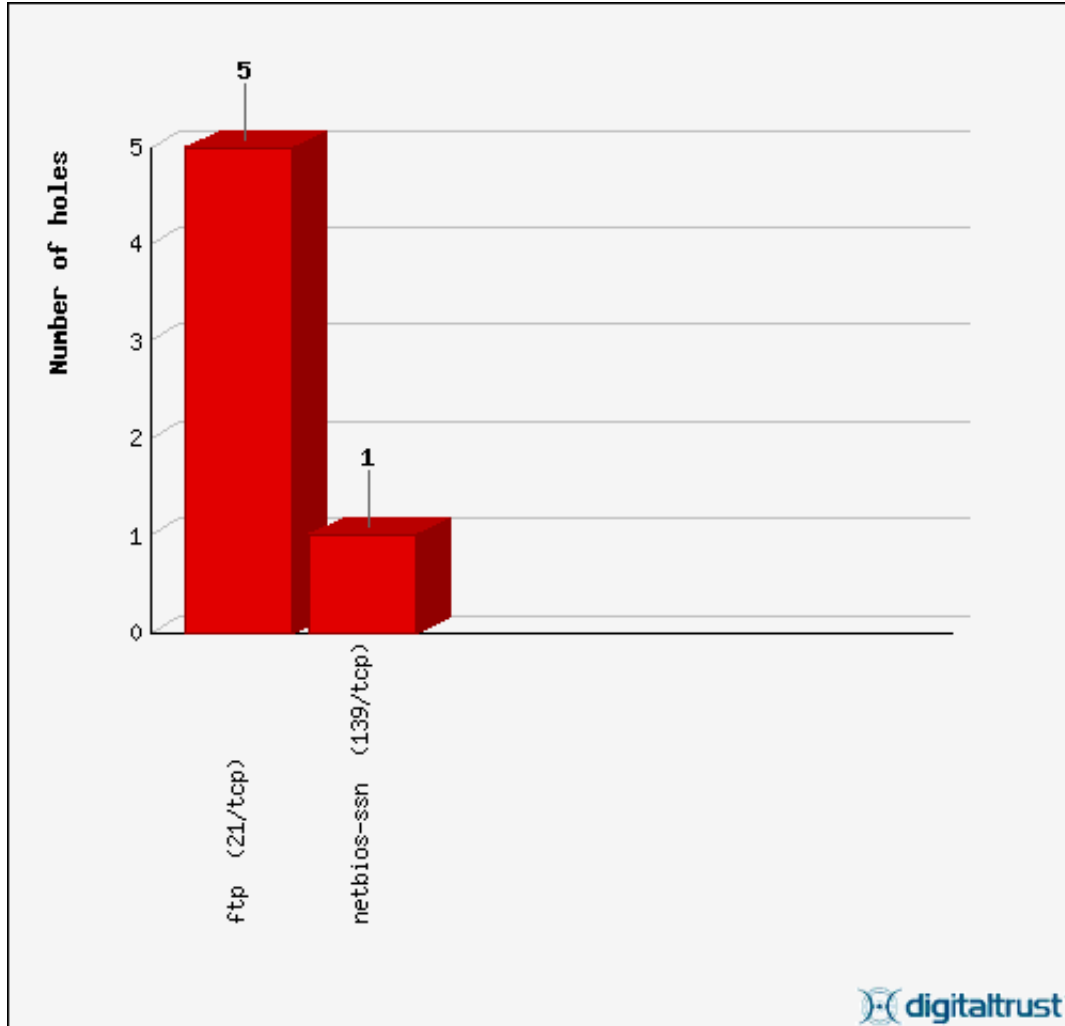
Severity	Security Warning
----------	------------------

Name	www
Proto	tcp
Port	80
Plugin	10678
Risk	Low
Severity	Security Warning

Name	www
Proto	tcp
Port	80
Plugin	10677
Risk	Low
Severity	Security Warning

### Undefined

Name	ftp
Proto	tcp
Port	21
Plugin	10990
Risk	None
Severity	Security Hole

**SERVIZI DI RETE ALTAMENTE PERICOLOSI:**

**SERVIZI PRESENTI**

Ftp (21/tcp)	8
Www (80/tcp)	7
Netbios-ssn (139/tcp)	6
Unknown (8987/tcp)	3
Ssh (22/tcp)	3
Domain (53/tcp)	2
General (general/tcp)	2
Amanda (10080/udp)	1
Netbios-ns (137/udp)	1
Kamanda (10081/udp)	1
General (general/udp)	1

**LISTA VULNERABILITA':****Amanda (10080/udp)**

<b>Name:</b>	amanda
<b>Port:</b>	10080
<b>Proto:</b>	udp
<b>Plugin:</b>	10462
<b>Risk:</b>	
<b>Severity:</b>	Security Note
<b>CVE:</b>	
<b>Data:</b>	Amanda version: Amanda 2.4

**Domain (53/tcp)**

<b>Name:</b>	domain
<b>Port:</b>	53
<b>Proto:</b>	tcp
<b>Plugin:</b>	10539
<b>Risk:</b>	Severe
<b>Severity:</b>	Security Warning
<b>CVE:</b>	CVE-1999-0024
<b>Data:</b>	<p>The remote name server allows recursive queries to be performed by the host running nessesd.</p> <p>If this is your internal nameserver, then forget this warning.</p> <p>If you are probing a remote nameserver, then it allows anyone to use it to resolve third parties names (such as <a href="http://www.nessus.org">www.nessus.org</a>). This allows hackers to do cache poisoning attacks against this nameserver.</p> <p>See also : <a href="http://www.cert.org/advisories/CA-1997-22.html">http://www.cert.org/advisories/CA-1997-22.html</a></p> <p>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</p> <p>If you are using another name server, consult its documentation.</p>

<b>Name:</b>	domain
<b>Port:</b>	53
<b>Proto:</b>	tcp
<b>Plugin:</b>	10028
<b>Risk:</b>	
<b>Severity:</b>	Security Note

<b>CVE:</b>	
<b>Data:</b>	The remote bind version is : 9.2.1

### Ftp (21/tcp)

<b>Name:</b>	ftp
<b>Port:</b>	21
<b>Proto:</b>	tcp
<b>Plugin:</b>	10092
<b>Risk:</b>	
<b>Severity:</b>	Security Note
<b>CVE:</b>	
<b>Data:</b>	Remote FTP server banner : 220-=(*)=-:.. (( Welcome to PureFTPd 1.0.12 )) ..-=(*)=-@r

<b>Name:</b>	ftp
<b>Port:</b>	21
<b>Proto:</b>	tcp
<b>Plugin:</b>	10080
<b>Risk:</b>	High
<b>Severity:</b>	Security Hole
<b>CVE:</b>	CAN-1999-0452
<b>Data:</b>	There is a backdoor in the old ftp daemons of Linux, which allows remote users to log in as 'NULL', with password 'NULL', and to get root privileges over FTP.  Solution : Update your FTP server to the latest version available.

<b>Name:</b>	ftp
<b>Port:</b>	21
<b>Proto:</b>	tcp
<b>Plugin:</b>	10330
<b>Risk:</b>	
<b>Severity:</b>	Security Note
<b>CVE:</b>	
<b>Data:</b>	An FTP server is running on this port. Here is its banner : 220-=(*)=-:.. (( Welcome to PureFTPd 1.0.12 )) ..-=(*)=-@r

<b>Name:</b>	ftp
<b>Port:</b>	21
<b>Proto:</b>	tcp
<b>Plugin:</b>	10990
<b>Risk:</b>	None
<b>Severity:</b>	Security Hole
<b>CVE:</b>	
<b>Data:</b>	The FTP service can be accessed using any username and password. Many other plugins may trigger falsely because of this, although

they can be fixed by setting this plugin as a dependency and excluding the ftp/AnyUser KB key item.

Solution: None

<b>Name:</b>	ftp
<b>Port:</b>	21
<b>Proto:</b>	tcp
<b>Plugin:</b>	10305
<b>Risk:</b>	High
<b>Severity:</b>	Security Hole
<b>CVE:</b>	CAN-1999-0200
<b>Data:</b>	<p>This FTP server accepts any login/password combination. This is a real threat, since anyone can browse the FTP section of your disk without your consent.</p> <p>Solution : upgrade WFTP.</p>

<b>Name:</b>	ftp
<b>Port:</b>	21
<b>Proto:</b>	tcp
<b>Plugin:</b>	10079
<b>Risk:</b>	Low
<b>Severity:</b>	Security Warning
<b>CVE:</b>	CAN-1999-0497
<b>Data:</b>	<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>Under most Unix system, doing :</p> <pre>echo ftp -- /etc/ftpusers</pre> <p>will correct this.</p>

<b>Name:</b>	ftp
<b>Port:</b>	21
<b>Proto:</b>	tcp
<b>Plugin:</b>	10508
<b>Risk:</b>	High
<b>Severity:</b>	Security Hole
<b>CVE:</b>	
<b>Data:</b>	<p>It is possible to log into the remote FTP server as ' '.</p> <p>If the remote server is PFTP, then anyone can use this account to read arbitrary files on the remote host.</p>

Solution : upgrade PFTP to version 2.9g

<b>Name:</b>	ftp
<b>Port:</b>	21
<b>Proto:</b>	tcp
<b>Plugin:</b>	11160
<b>Risk:</b>	High
<b>Severity:</b>	Security Hole
<b>CVE:</b>	
<b>Data:</b>	The remote server is incorrectly configured with a NULL password for the user 'Administrator' and has FTP enabled.  Solution : Change the Administrator password on this host.

### General (general/udp)

<b>Name:</b>	general
<b>Port:</b>	general
<b>Proto:</b>	udp
<b>Plugin:</b>	10287
<b>Risk:</b>	
<b>Severity:</b>	Security Note
<b>CVE:</b>	
<b>Data:</b>	For your information, here is the traceroute to 192.168.1.251 : 192.168.1.251

### General (general/tcp)

<b>Name:</b>	general
<b>Port:</b>	general
<b>Proto:</b>	tcp
<b>Plugin:</b>	10336
<b>Risk:</b>	
<b>Severity:</b>	Security Note
<b>CVE:</b>	
<b>Data:</b>	Nmap found that this host is running Linux 2.4.7 (X86)

<b>Name:</b>	general
<b>Port:</b>	general
<b>Proto:</b>	tcp
<b>Plugin:</b>	10201
<b>Risk:</b>	Low
<b>Severity:</b>	Security Warning
<b>CVE:</b>	
<b>Data:</b>	The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.

An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things.

Solution : Contact your vendor for a patch

### Kamanda (10081/udp)

Name:	kamanda
Port:	10081
Proto:	udp
Plugin:	10462
Risk:	
Severity:	Security Note
CVE:	
Data:	Amanda version: Amanda 2.4

### Netbios-ns (137/udp)

Name:	netbios-ns
Port:	137
Proto:	udp
Plugin:	10150
Risk:	Medium
Severity:	Security Warning
CVE:	
Data:	<p>. The following 5 NetBIOS names have been gathered :</p> <ul style="list-style-type: none"><li>DIGITALTRUST</li><li>DIGITALTRUST</li><li>DIGITALTRUST</li><li>ICE2K</li><li>ICE2K</li></ul> <p>. This SMB server seems to be a SAMBA server (this is not a security risk, this is for your information). This can be told because this server claims to have a null MAC address</p> <p>If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port.</p>

### Netbios-ssn (139/tcp)

Name:	netbios-ssn
Port:	139
Proto:	tcp
Plugin:	10397
Risk:	Low
Severity:	Security Warning
CVE:	
Data:	Here is the browse list of the remote host :

DIGITALTRUST -  
SUPERLORENZO -

This is potentially dangerous as this may help the attack of a potential hacker by giving him extra targets to check for

Solution : filter incoming traffic to this port

<b>Name:</b>	netbios-ssn
<b>Port:</b>	139
<b>Proto:</b>	tcp
<b>Plugin:</b>	10398
<b>Risk:</b>	Low
<b>Severity:</b>	Security Warning
<b>CVE:</b>	CVE-2000-1200
<b>Data:</b>	The domain SID can be obtained remotely. Its value is :  ICE2K : 5-21-1897569073-1503127143-3341040036  An attacker can use it to obtain the list of the local users of this host Solution : filter the ports 137 to 139 and 445

<b>Name:</b>	netbios-ssn
<b>Port:</b>	139
<b>Proto:</b>	tcp
<b>Plugin:</b>	10785
<b>Risk:</b>	
<b>Severity:</b>	Security Note
<b>CVE:</b>	
<b>Data:</b>	The remote native lan manager is : Samba 2.2.7 The remote Operating System is : Unix The remote SMB Domain Name is : ICE2K

<b>Name:</b>	netbios-ssn
<b>Port:</b>	139
<b>Proto:</b>	tcp
<b>Plugin:</b>	10394
<b>Risk:</b>	
<b>Severity:</b>	Security Hole
<b>CVE:</b>	CVE-2000-0222
<b>Data:</b>	. It was possible to log into the remote host using a NULL session. The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access  To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261 (Windows 2000).

Note that this won't completely disable null sessions, but will prevent them from connecting to IPC\$  
Please see <http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html>

. All the smb tests will be done as ''/whatever' in domain

<b>Name:</b>	netbios-ssn
<b>Port:</b>	139
<b>Proto:</b>	tcp
<b>Plugin:</b>	10859
<b>Risk:</b>	Low
<b>Severity:</b>	Security Warning
<b>CVE:</b>	CVE-2000-1200
<b>Data:</b>	The host SID can be obtained remotely. Its value is :  DIGITALTRUST : 5-21-3716969939-3938956257-2006975788  An attacker can use it to obtain the list of the local users of this host Solution : filter the ports 137 to 139 and 445

<b>Name:</b>	netbios-ssn
<b>Port:</b>	139
<b>Proto:</b>	tcp
<b>Plugin:</b>	10395
<b>Risk:</b>	Medium
<b>Severity:</b>	Security Warning
<b>CVE:</b>	
<b>Data:</b>	Here is the list of the SMB shares of this host :  _daniela - digit_biz - digit_it - digitmpbiz - digitmp - digit_old - www_icenet_it - wanapoli.it - vitruvius.lu - signncrypt - demarc - secure - italianohomes - IPC\$ - ADMIN\$ -  This is potentially dangerous as this may help the attack

of a potential hacker.

Solution : filter incoming traffic to this port

### Ssh (22/tcp)

Name:	ssh
Port:	22
Proto:	tcp
Plugin:	10267
Risk:	
Severity:	Security Note
CVE:	
Data:	Remote SSH version : SSH-2.0-OpenSSH_3.4p1

Name:	ssh
Port:	22
Proto:	tcp
Plugin:	10330
Risk:	
Severity:	Security Note
CVE:	
Data:	An ssh server is running on this port

Name:	ssh
Port:	22
Proto:	tcp
Plugin:	10881
Risk:	
Severity:	Security Note
CVE:	
Data:	The remote SSH daemon supports the following versions of the SSH protocol :  . 1.99 . 2.0

### Unknown (8987/tcp)

Name:	unknown
Port:	8987
Proto:	tcp
Plugin:	10386
Risk:	
Severity:	Security Note
CVE:	
Data:	The remote web servers is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning

a site map or search page instead.

Nessus enabled some counter measures for that, however they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate

<b>Name:</b>	unknown
<b>Port:</b>	8987
<b>Proto:</b>	tcp
<b>Plugin:</b>	10919
<b>Risk:</b>	
<b>Severity:</b>	Security Note
<b>CVE:</b>	
<b>Data:</b>	This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by some information gathering plugin

<b>Name:</b>	unknown
<b>Port:</b>	8987
<b>Proto:</b>	tcp
<b>Plugin:</b>	10330
<b>Risk:</b>	
<b>Severity:</b>	Security Note
<b>CVE:</b>	
<b>Data:</b>	A web server is running on this port

### **Www (80/tcp)**

<b>Name:</b>	www
<b>Port:</b>	80
<b>Proto:</b>	tcp
<b>Plugin:</b>	10330
<b>Risk:</b>	
<b>Severity:</b>	Security Note
<b>CVE:</b>	
<b>Data:</b>	A web server is running on this port

<b>Name:</b>	www
<b>Port:</b>	80
<b>Proto:</b>	tcp
<b>Plugin:</b>	10107
<b>Risk:</b>	
<b>Severity:</b>	Security Note
<b>CVE:</b>	
<b>Data:</b>	The remote web server type is :  Apache/1.3.26 (Unix) mod_perl/1.26 PHP/4.2.3@r  Solution : You can set the directive 'ServerTokens Prod' to limit

the information emanating from the server in its response headers.

<b>Name:</b>	www
<b>Port:</b>	80
<b>Proto:</b>	tcp
<b>Plugin:</b>	10766
<b>Risk:</b>	Low
<b>Severity:</b>	Security Note
<b>CVE:</b>	CAN-2001-1013
<b>Data:</b>	<p>An information leak occurs on Apache based web servers whenever the UserDir module is enabled. The vulnerability allows an external attacker to enumerate existing accounts by requesting access to their home directory and monitoring the response.</p> <p>Solution:</p> <p>1) Disable this feature by changing 'UserDir public_html' (or whatever) to 'UserDir disabled'.</p> <p>Or</p> <p>2) Use a RedirectMatch rewrite rule under Apache -- this works even if there is no such entry in the password file, e.g.:</p> <pre>RedirectMatch ^~(.*\$ http://my-target-webserver.somewhere.org/\$1</pre> <p>Or</p> <p>3) Add into httpd.conf:</p> <pre>ErrorDocument 404 http://localhost/sample.html ErrorDocument 403 http://localhost/sample.html</pre> <p>(NOTE: You need to use a FQDN inside the URL for it to work properly).</p> <p>Additional Information:</p> <p><a href="http://www.securiteam.com/unixfocus/5WP0C1F5FI.html">http://www.securiteam.com/unixfocus/5WP0C1F5FI.html</a></p>

<b>Name:</b>	www
<b>Port:</b>	80
<b>Proto:</b>	tcp
<b>Plugin:</b>	11032
<b>Risk:</b>	
<b>Severity:</b>	Security Note
<b>CVE:</b>	
<b>Data:</b>	<p>The following directories were discovered:</p> <p>, /admin, /cgi-bin, /dm, /download, /downloads, /icons, /img, /info, /links, /linux, /logs, /register, /server-info, /server-status, /tools</p>

<b>Name:</b>	www
<b>Port:</b>	80
<b>Proto:</b>	tcp
<b>Plugin:</b>	10678
<b>Risk:</b>	Low
<b>Severity:</b>	Security Warning
<b>CVE:</b>	
<b>Data:</b>	<p>Requesting the URI /server-info gives information about your Apache configuration.</p> <p>Solution :</p> <p>If you don't use this feature, comment the appropriate section in your httpd.conf file. If you really need it, limit its access to the administrator's machine.</p>

<b>Name:</b>	www
<b>Port:</b>	80
<b>Proto:</b>	tcp
<b>Plugin:</b>	10677
<b>Risk:</b>	Low
<b>Severity:</b>	Security Warning
<b>CVE:</b>	
<b>Data:</b>	<p>Requesting the URI /server-status gives information about the currently running Apache.</p> <p>Solution :</p> <p>If you don't use this feature, comment the appropriate section in your httpd.conf file. If you really need it, limit its access to the administrator's machine.</p>

<b>Name:</b>	www
<b>Port:</b>	80
<b>Proto:</b>	tcp
<b>Plugin:</b>	11137
<b>Risk:</b>	Medium
<b>Severity:</b>	Security Warning
<b>CVE:</b>	CAN-2002-0840
<b>Data:</b>	<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>

Solution : Upgrade to version 1.3.27

See also : <http://www.apache.org/dist/httpd/Announcement.html>

**PLUGINS UTILIZZATI**

Backdoors	41
CGI abuses	345
CISCO	23
Denial of Service	12
FTP	48
Finger abuses	10
Firewalls	17
Gain a shell remotely	33
Gain root remotely	82
General	72
Misc.	55
NIS	2
Netware	2
Port scanners	4
RPC	42
Remote file access	40
SMTP problems	33
SNMP	10
Settings	6
Untested	4
Useless services	20
Windows	86
Windows : User management	24

## **PLUGIN PREFERENCES**

**Brute force login (Hydra)**

**Default accounts**

**FTP bounce scan**

**HTTP NIDS evasion**

**Libwhisker options**

**Login configurations**

**Misc information on News server**

**NIDS evasion**

**Nmap**

**Ping the remote host**

**RedHat 6.2 inetd**

**SMB Scope**

**SMB use domain SID to enumerate users**

**SMB use host SID to enumerate local users**

**SMTP settings**

**Services**

**Test HTTP dangerous methods**

**Web mirroring**

## Ftp writeable directories