Network Vulnerability Assessment Report

Session name: 192.168.3.0_LiveHosts
Sorted by host names

Start Time: 15.08.2004 08:50:27
Finish Time: 16.08.2004 09:40:27
Elapsed: 20063 second(s) 65533:65533:65521

Total records generated:	129
high severity:	16
low severity:	86
informational:	27

Summary of scanned hosts

Host	Holes	Warnings	Open ports	State
192.168.3.201	2	13	4	Finished
192.168.3.22	0	0	0	Aborted
192.168.3.152	0	10	2	Aborted
192.168.3.240	13	57	20	Finished
192.168.3.254	1	6	1	Aborted

192.168.3.152

Service	Severity	Description
ssh (22/tcp)	Info	Port is open
isakmp (500/tcp)	Info	Port is open
general/tcp	Low	The remote host does not discard TCP SYN packets which have the FIN flag set. Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules. See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113 Solution : Contact your vendor for a patch Risk factor : Medium BID : 7487
isakmp (500/tcp)	Low	A SSLv2 server answered on this port
general/icmp	Low	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols. Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

		Risk factor : Low CVE : CAN-1999-0524
isakmp (500/tcp)	**Low**	The remote web server type is : MiniServ/0.01 Solution : We recommend that you configure (if possible) your web server to return a bogus Server header in order to not leak information.
isakmp (500/tcp)	**Low**	A web server is running on this port through SSL
general/tcp	**Low**	PTR was not able to reliably identify the remote operating system. It might be: IBM OS/400 Netilla Service Platform 4.0 The fingerprint differs from these known signatures on 5 points. If you know what operating system this host is running, please send this signature to os-signatures@PTR.org : :1:1:0:64:1:64:1:0:64:1:0:64:1:>64:64:0:1:1:2:1:1:1:1:0:64:5792:MSTNW:0:1:1
ssh (22/tcp)	**Low**	Remote SSH version : SSH-2.0-OpenSSH_3.4p1 Debian 1:3.4p1-1.woody.3
general/udp	**Low**	For your information, here is the traceroute to 192.168.3.152 : 192.168.3.22 192.168.3.152
isakmp (500/tcp)	**Low**	Here is the SSLv2 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 4 (0x4) Signature Algorithm: md5WithRSAEncryption Issuer: C=DE, ST=Baden-Wuerttemberg, L=Stuttgart, O=Wapsol GmbH, OU=Wireless Security, CN=Wapsol GmbH/emailAddress=wpa@wapsol.de Validity Not Before: Apr 29 14:25:52 2004 GMT Not After : Oct 26 14:25:52 2004 GMT Subject: C=DE, ST=Baden-Wuerttemberg, L=Stuttgart, O=Wapsol GmbH, OU=Wireless Security, CN=Wapsol Secure-AP (WPA) 051/emailAddress=wpa@wapsol.de Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:a7:5b:9b:bb:21:05:1c:50:b2:5b:37:dc:b9:0d: 7a:e6:af:83:5d:12:a2:c4:4b:ab:6f:b8:be:ec:e2: 44:58:b8:81:43:67:6a:f3:e2:e3:ee:4c:ab:7a:fc: e2:bb:a8:dc:fb:e9:a1:ec:02:96:26:3a:60:fb:f8: 1e:5b:5e:f5:37:2a:75:ad:5c:9d:53:32:7b:0e:38: 55:3c:65:0e:c6:d1:8e:08:56:df:4f:d7:b6:8c:f2: 52:29:b6:25:e3:af:a9:6a:7c:ee:eb:f3:ec:96:e8: bd:3d:90:06:70:1b:75:fd:ee:69:5f:2d:c1:d3:e4: 7a:c4:a7:23:02:c0:27:0d:47 Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Extended Key Usage: TLS Web Server Authentication Signature Algorithm: md5WithRSAEncryption 15:a1:f0:35:8a:cf:2c:eb:3c:b5:91:25:7b:44:9d:f9:e8:fb: a9:61:f6:20:a4:10:36:35:8e:a7:a8:62:a5:b7:bf:3a:b7:f4:

		55:3f:fa:7e:46:20:cb:4b:97:8e:4d:91:b2:76:80:12:c3:80: 70:b9:47:a0:34:a4:9d:f3:89:2d:5b:60:94:49:47:0a:23:f1: ff:0d:68:44:7a:63:1f:af:55:86:c1:3c:72:1f:95:db:fa:33: 31:f6:35:f5:c4:6e:eb:a9:88:a4:d1:15:85:e6:31:20:00:3b: a9:55:da:db:52:25:62:b3:aa:b9:f9:e5:81:99:31:e5:65:65: 0c:da Here is the list of available SSLv2 ciphers: RC4-MD5 EXP-RC4-MD5 RC2-CBC-MD5 EXP-RC2-CBC-MD5 DES-CBC-MD5 DES-CBC3-MD5 RC4-64-MD5 The SSLv2 server offers 5 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack Solution: disable those ciphers and upgrade your client software if necessary. See http://support.microsoft.com/default.aspx?scid=kb en-us 216482 or http://httpd.apache.org/docs-2.0/mod/mod_ssl.html#sslciphersuite This SSLv2 server also accepts SSLv3 connections. This SSLv2 server also accepts TLSv1 connections.
ssh (22/tcp)	**Low**	An ssh server is running on this port

192.168.3.201

Service	Severity	Description
ssh (22/tcp)	**Info**	Port is open
sunrpc (111/udp)	**Info**	Port is open
sunrpc (111/tcp)	**Info**	Port is open
mysql (3306/tcp)	**Info**	Port is open
ssh (22/tcp)	**High**	You are running a version of OpenSSH which is older than 3.7.1 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. An exploit for this issue is rumored to exist. Note that several distribution patched this hole without changing the version number of OpenSSH. Since PTR solely relied on the banner of the remote SSH server to perform this check, this might be a false positive. If you are running a RedHat host, make sure that the command : rpm -q openssh-server Returns :

		openssh-server-3.1p1-13 (RedHat 7.x) openssh-server-3.4p1-7 (RedHat 8.0) openssh-server-3.5p1-11 (RedHat 9) Solution : Upgrade to OpenSSH 3.7.1 See also : http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375452423794&w=2 http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375456923804&w=2 Risk factor : High CVE : CAN-2003-0682, CAN-2003-0693, CAN-2003-0695 BID : 8628 Other references : RHSA:RHSA-2003:279, SuSE:SUSE-SA:2003:039
general/icmp	**High**	The remote host is vulnerable to an 'Etherleak' - the remote ethernet driver seems to leak bits of the content of the memory of the remote operating system. Note that an attacker may take advantage of this flaw only when its target is on the same physical subnet. See also : http://www.atstake.com/research/advisories/2003/a010603-1.txt Solution : Contact your vendor for a fix Risk factor : High CVE : CAN-2003-0001 BID : 6535
general/tcp	**Low**	The remote host does not discard TCP SYN packets which have the FIN flag set. Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules. See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113 Solution : Contact your vendor for a patch Risk factor : Medium BID : 7487
ssh (22/tcp)	**Low**	An ssh server is running on this port
general/icmp	**Low**	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols. Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). Risk factor : Low CVE : CAN-1999-0524
sunrpc (111/udp)	**Low**	RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port
ssh (22/tcp)	**Low**	The remote SSH daemon supports the following versions of the SSH protocol : . 1.33 . 1.5

		. 1.99 . 2.0 SSHv1 host key fingerprint : 0e:60:6d:52:36:10:3e:29:f1:df:f6:54:c3:6f:6a:b8 SSHv2 host key fingerprint : 52:5b:97:07:c0:68:f2:c7:21:92:63:c2:39:9b:04:c6
ssh (22/tcp)	**Low**	You are running OpenSSH-portable 3.6.1 or older. There is a flaw in this version which may allow an attacker to bypass the access controls set by the administrator of this server. 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). 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. Solution : Upgrade to OpenSSH 3.6.2 when it comes out Risk factor : Low CVE : CAN-2003-0386 BID : 7831
ssh (22/tcp)	**Low**	Remote SSH version : SSH-1.99-OpenSSH_3.4p1
mysql (3306/tcp)	**Low**	An unknown service is running on this port. It is usually reserved for MySQL
general/udp	**Low**	For your information, here is the traceroute to 192.168.3.201 : 192.168.3.22 192.168.3.201
ssh (22/tcp)	**Low**	The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol. These protocols are not completely cryptographically safe so they should not be used. Solution : If you use OpenSSH, set the option 'Protocol' to '2' If you use SSH.com's set the option 'Ssh1Compatibility' to 'no' Risk factor : Low
sunrpc (111/tcp)	**Low**	RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port
sunrpc (111/tcp)	**Low**	The RPC portmapper is running on this port. An attacker may use it to enumerate your list of RPC services. We recommend you filter traffic going to this port. Risk factor : Low

		CVE : CAN-1999-0632, CVE-1999-0189 BID : 205
ssh (22/tcp)	**Low**	You are running OpenSSH-portable 3.6.1p1 or older. If PAM support is enabled, an attacker may use a flaw in this version to determine the existence or a given login name by comparing the times the remote sshd daemon takes to refuse a bad password for a non-existent login compared to the time it takes to refuse a bad password for a valid login. An attacker may use this flaw to set up a brute force attack against the remote host. *** PTR did not check whether the remote SSH daemon is actually *** using PAM or not, so this might be a false positive Solution : Upgrade to OpenSSH-portable 3.6.1p2 or newer Risk factor : Low CVE : CAN-2003-0190 BID : 7342, 7467, 7482 Other references : RHSA:RHSA-2003:222-01

192.168.3.240

Service	Severity	Description
unknown (1024/udp)	**Info**	Port is open
sunrpc (111/udp)	**Info**	Port is open
unknown (20012/tcp)	**Info**	Port is open
snet-sensor-mgmt (10000/tcp)	**Info**	Port is open
kdm (1024/tcp)	**Info**	Port is open
netbios-ns (137/udp)	**Info**	Port is open
time (37/tcp)	**Info**	Port is open
sunrpc (111/tcp)	**Info**	Port is open
netbios-ssn (139/tcp)	**Info**	Port is open
https (443/tcp)	**Info**	Port is open
exec (512/tcp)	**Info**	Port is open
login (513/tcp)	**Info**	Port is open
discard (9/tcp)	**Info**	Port is open
shell (514/tcp)	**Info**	Port is open
printer (515/tcp)	**Info**	Port is open
ipp (631/tcp)	**Info**	Port is open
tftp (69/udp)	**Info**	Port is open
daytime (13/tcp)	**Info**	Port is open
ssh (22/tcp)	**Info**	Port is open
smtp (25/tcp)	**Info**	Port is open

https (443/tcp)	**High**	The remote host appears to be running a version of Apache which is older than 1.3.29 There are several flaws in this version, which may allow an attacker to possibly execute arbitrary code through mod_alias and mod_rewrite. You should upgrade to 1.3.29 or newer. *** Note that PTR solely relied on the version number *** of the remote server to issue this warning. This might *** be a false positive Solution : Upgrade to version 1.3.29 See also : http://www.apache.org/dist/httpd/Announcement.html Risk factor : High CVE : CAN-2003-0542
snet-sensor-mgmt (10000/tcp)	**High**	The remote host seems to be using a version of OpenSSL which is older than 0.9.6e or 0.9.7-beta3 This version is vulnerable to a buffer overflow which, may allow an attacker to obtain a shell on this host. *** Note that since safe checks are enabled, this check *** might be fooled by non-openssl implementations and *** produce a false positive. *** In doubt, re-execute the scan without the safe checks Solution : Upgrade to version 0.9.6e (0.9.7beta3) or newer Risk factor : High CVE : CAN-2002-0656, CAN-2002-0655, CAN-2002-0657, CAN-2002-0659, CVE-2001-1141 BID : 3004, 4316, 5363 Other references : IAVA:2002-A-0009, SuSE:SUSE-SA:2002:033
unknown (1024/udp)	**High**	The remote statd service may be vulnerable to a format string attack. This means that an attacker may execute arbitrary code thanks to a bug in this daemon. Only older versions of statd under Linux are affected by this problem. *** PTR reports this vulnerability using only information that was gathered. *** Use caution when testing without safe checks enabled. Solution : upgrade to the latest version of rpc.statd Risk factor : High CVE : CVE-2000-0666, CAN-2000-0800 BID : 1480
https (443/tcp)	**High**	The remote host seems to be using a version of OpenSSL which is older than 0.9.6e or 0.9.7-beta3 This version is vulnerable to a buffer overflow which, may allow an attacker to obtain a shell on this host.

		*** Note that since safe checks are enabled, this check *** might be fooled by non-openssl implementations and *** produce a false positive. *** In doubt, re-execute the scan without the safe checks Solution : Upgrade to version 0.9.6e (0.9.7beta3) or newer Risk factor : High CVE : CAN-2002-0656, CAN-2002-0655, CAN-2002-0657, CAN-2002-0659, CVE-2001-1141 BID : 3004, 4316, 5363 Other references : IAVA:2002-A-0009, SuSE:SUSE-SA:2002:033
https (443/tcp)	**High**	The remote host seem to be running a version of OpenSSL which is older than 0.9.6k or 0.9.7c. There is a heap corruption bug in this version which might be exploited by an attacker to gain a shell on this host. Solution : If you are running OpenSSL, Upgrade to version 0.9.6k or 0.9.7c or newer Risk factor : High CVE : CAN-2003-0543, CAN-2003-0544, CAN-2003-0545 BID : 8732 Other references : IAVA:2003-A-0015, RHSA:RHSA-2003:291-01, SuSE:SUSE-SA:2003:043
netbios-ssn (139/tcp)	**High**	The remote Samba server, according to its version number, may be vulnerable to a remote buffer overflow when receiving specially crafted SMB fragment packets. An attacker needs to be able to access at least one share to exploit this flaw. Solution : upgrade to Samba 2.2.8 Risk factor : High CVE : CAN-2003-0085, CAN-2003-0086 BID : 7106, 7107 Other references : RHSA:RHSA-2003:095-03, SuSE:SUSE-SA:2003:016
https (443/tcp)	**High**	The target is running an Apache web server that may not properly handle access controls. In effect, on big-endian 64-bit platforms, Apache fails to match allow or deny rules containing an IP address but not a netmask. ***** PTR has determined the vulnerability exists only by looking at ***** the Server header returned by the web server running on the target. ***** If the target is not a big-endian 64-bit platform, consider this a ***** false positive. Additional information on the vulnerability can be found at : - http://www.apacheweek.com/features/security-13 - http://marc.theaimsgroup.com/?l=apache-cvs&m=107869603013722 - http://nagoya.apache.org/bugzilla/show_bug.cgi?id=23850 Solution : Upgrade to Apache version 1.3.31 or newer. Risk factor : Medium CVE : CAN-2003-0993 BID : 9829 Other references : GLSA:GLSA 200405-22, MDKSA:MDKSA-2004:046, OpenPKG-SA:OpenPKG-SA-2004.021, SSA:SSA:2004-133-01, TSLSA:TSLSA-2004-0027

netbios-ssn (139/tcp)	**High**	The following shares can be accessed using a NULL session : - IPC$ - (readable?, writeable?) Solution : To restrict their access under WindowsNT, open the explorer, do a right click on each, go to the 'sharing' tab, and click on 'permissions' Risk factor : High CVE : CAN-1999-0519, CAN-1999-0520 BID : 8026
general/icmp	**High**	The remote host is vulnerable to an 'Etherleak' - the remote ethernet driver seems to leak bits of the content of the memory of the remote operating system. Note that an attacker may take advantage of this flaw only when its target is on the same physical subnet. See also : http://www.atstake.com/research/advisories/2003/a010603-1.txt Solution : Contact your vendor for a fix Risk factor : High CVE : CAN-2003-0001 BID : 6535
https (443/tcp)	**High**	The remote host is running a version of PHP which is older than 5.0.2. The remote version of this software is vulnerable to a memory disclosure vulnerability in PHP_Variables. An attacker may exploit this flaw to remotely read portions of the memory of the httpd process on the remote host. See also : http://www.php.net/ChangeLog-5.php#5.0.2 Solution : Upgrade to PHP 5.0.2 Risk factor : High BID : 11334
https (443/tcp)	**High**	The remote host appears to be running a version of Apache which is older than 1.3.32. There is a local buffer overflow in htpasswd command in this version, which may allow a local user to gain the privileges of the httpd process. *** Note that PTR solely relied on the version number *** of the remote server to issue this warning. This might *** be a false positive See also : http://xforce.iss.net/xforce/xfdb/17413 Solution : Upgrade to Apache 1.3.32 when available Risk factor : High
https (443/tcp)	**High**	The remote host is running a version of ApacheSSL which is older than 1.3.29/1.53. This version is vulnerable to a flaw which may allow an attacker to make the remote server to forge a client certificate. Solution : Upgrade to version ApacheSSL 1.3.29/1.53 or newer See also : http://www.apache-ssl.org Risk factor : High BID : 9590

https (443/tcp)	**High**	The remote host is running a version of PHP which is older than 4.3.9 or 5.0.2. The remote version of this software is affected by an unspecified file upload vulnerability which may allow an attacker to upload arbitrary files to the remote server. See also : http://viewcvs.php.net/viewcvs.cgi/php-src/NEWS.diff?r1=1.1247.2.724&r2=1.1247.2.726 Solution : Upgrade to PHP 4.3.9 or 5.0.2 when available Risk factor : Medium BID : 11190
ipp (631/tcp)	**Low**	The remote web server type is : CUPS/1.1 Solution : We recommend that you configure (if possible) your web server to return a bogus Server header in order to not leak information.
time (37/tcp)	**Low**	A time server seems to be running on this port
netbios-ssn (139/tcp)	**Low**	Here is the list of the SMB shares of this host : ashant - hjhunger - company - IPC$ - ADMIN$ - lp - This is potentially dangerous as this may help the attack of a potential hacker. Solution : filter incoming traffic to this port Risk factor : Medium
netbios-ssn (139/tcp)	**Low**	Here is the browse list of the remote host : BUDAPEST - 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 Risk factor : Low
ssh (22/tcp)	**Low**	Remote SSH version : SSH-2.0-OpenSSH_3.4p1 Debian 1:3.4p1-1.woody.3
snet-sensor-mgmt (10000/tcp)	**Low**	Here is the SSLv2 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 0 (0x0) Signature Algorithm: md5WithRSAEncryption Issuer: O=Webmin Webserver on budapest, CN=*/emailAddress=root@budapest Validity Not Before: Sep 12 16:32:53 2004 GMT

		Not After : Sep 11 16:32:53 2009 GMT Subject: O=Webmin Webserver on budapest, CN=*/emailAddress=root@budapest Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (512 bit) Modulus (512 bit): 00:f4:c5:66:af:18:fc:c4:75:c5:0f:be:1a:e5:32: d1:d5:ae:12:87:5c:12:39:7c:f9:2e:ee:d8:b3:43: bd:13:41:d1:27:a2:c2:56:59:ef:14:79:83:fc:67: 55:05:3d:7c:9f:95:32:c9:50:c0:8e:ed:d8:cf:45: 0e:71:c7:2c:3f Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Subject Key Identifier: 1A:17:D6:82:30:81:82:37:57:6D:39:FD:36:12:3B:21:81:03:B9:6F X509v3 Authority Key Identifier: keyid:1A:17:D6:82:30:81:82:37:57:6D:39:FD:36:12:3B:21:81:03:B9:6F DirName:/O=Webmin Webserver on budapest/CN=*/emailAddress=root@budapest serial:00 X509v3 Basic Constraints: CA:TRUE Signature Algorithm: md5WithRSAEncryption 1a:c3:89:05:79:1a:d4:4a:4b:4e:54:18:e8:87:13:31:7b:b9: 6b:13:e7:b2:f5:3b:9a:61:d6:4a:8c:dc:1c:d7:ce:8b:c7:78: 96:86:d2:b3:7d:54:9f:c3:4f:52:16:01:85:51:eb:fb:b5:b9: bc:dc:91:3f:d8:7a:94:f8:b0:05 Here is the list of available SSLv2 ciphers: RC4-MD5 EXP-RC4-MD5 RC2-CBC-MD5 EXP-RC2-CBC-MD5 DES-CBC-MD5 DES-CBC3-MD5 RC4-64-MD5 The SSLv2 server offers 5 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack Solution: disable those ciphers and upgrade your client software if necessary. See http://support.microsoft.com/default.aspx?scid=kb en-us 216482 or http://httpd.apache.org/docs-2.0/mod/mod_ssl.html#sslciphersuite This SSLv2 server also accepts SSLv3 connections. This SSLv2 server also accepts TLSv1 connections.
https (443/tcp)	**Low**	The remote host appears to be running a version of Apache which is older than 1.3.27 There are several flaws in this version, you should upgrade to 1.3.27 or newer. *** Note that PTR solely relied on the version number *** of the remote server to issue this warning. This might *** be a false positive

		Solution : Upgrade to version 1.3.27 See also : http://www.apache.org/dist/httpd/Announcement.html Risk factor : Medium CVE : CAN-2002-0839, CAN-2002-0840, CAN-2002-0843 BID : 5847, 5884, 5887, 5995, 5996
https (443/tcp)	**Low**	The remote host is running a version of PHP earlier than 4.2.2. The mail() function does not properly sanitize user input. This allows users to forge email to make it look like it is coming from a different source other than the server. Users can exploit this even if SAFE_MODE is enabled. Solution : Contact your vendor for the latest PHP release. Risk factor : Medium CVE : CAN-2002-0985 BID : 5562
https (443/tcp)	**Low**	The remote web server type is : Apache/1.3.26 Ben-SSL/1.48 (Unix) Debian GNU/Linux PHP/4.1.2 Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
general/tcp	**Low**	PTR was not able to reliably identify the remote operating system. It might be: Allot NetEnforcer Linux Kernel 2.4 The fingerprint differs from these known signatures on 3 points. If you know what operating system this host is running, please send this signature to os-signatures@PTR.org : :1:1:0:255:1:255:1:0:255:1:0:255:1:>64:255:0:1:1:2:1:1:1:1:0:64:5792:MSTNW:0:1:1
https (443/tcp)	**Low**	The remote web server appears to be running a version of Apache that is less that 2.0.49 or 1.3.31. These versions are vulnerable to a denial of service attack where a remote attacker can block new connections to the server by connecting to a listening socket on a rarely accessed port. Solution: Upgrade to Apache 2.0.49 or 1.3.31. CVE : CAN-2004-0174 BID : 9921
netbios-ssn (139/tcp)	**Low**	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/PTR-0204/50/1.html All the smb tests will be done as ''/'whatever' in domain KET CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222, CAN-1999-0505, CAN-2002-1117

		BID : 494, 990, 11199
general/udp	**Low**	For your information, here is the traceroute to 192.168.3.240 : 192.168.3.22 192.168.3.240
ipp (631/tcp)	**Low**	The remote host is running CUPS (Common Unix Printing System). An attacker may connect to this port and browse /printers to obtain the list of printers this host can access. This is particulary useful as some attacks require an attacker to provide a valid printer name. The following list of printers has been obtained : . HP Color Laser 2500 The remote host default printer is {default_name} Solution : Filter incoming traffic to this port Risk factor : Low
smtp (25/tcp)	**Low**	An SMTP server is running on this port Here is its banner : 220 budapest ESMTP Postfix (Debian/GNU)
smtp (25/tcp)	**Low**	This server could be fingerprinted as being Postfix
https (443/tcp)	**Low**	Here is the SSLv2 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 0 (0x0) Signature Algorithm: md5WithRSAEncryption Issuer: C=DE, ST=BW, L=Stuttgart, O=Wapsol GmbH, OU=Wireless Security, CN=budapest.intra.wapsol.de/emailAddress=info@wapsol.de Validity Not Before: Jun 27 08:18:29 2004 GMT Not After : Jul 27 08:18:29 2004 GMT Subject: C=DE, ST=BW, L=Stuttgart, O=Wapsol GmbH, OU=Wireless Security, CN=budapest.intra.wapsol.de/emailAddress=info@wapsol.de Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:c3:88:c0:7f:09:e4:b9:31:2e:c1:f2:68:4d:29: 53:cc:d3:bd:c5:cc:1e:af:ea:67:fd:d2:7a:7d:58: b9:23:33:ed:48:44:62:2a:de:a4:a5:16:d4:89:d5: f7:1c:c8:15:0a:0f:f6:51:75:d9:6c:2d:55:fc:9f: 57:d5:7f:4e:58:f9:d1:0b:10:c7:25:44:bd:12:dd: 70:57:6b:29:1f:13:39:7d:f3:10:fc:a4:12:4a:a0: 5c:c7:c3:7c:48:87:b5:b9:b6:9a:65:3a:4b:42:65: 96:2e:2c:9b:09:e4:5e:ef:2e:9a:bb:d6:8c:8e:a5: 6e:51:79:7a:e1:c6:7c:7e:07 Exponent: 65537 (0x10001) Signature Algorithm: md5WithRSAEncryption bb:cd:72:af:10:02:70:d7:4a:f3:bb:05:55:1b:2b:5c:73:b8: 62:33:7c:c3:74:e4:32:d5:b3:3c:62:ef:2a:6a:53:1d:cf:73: b7:14:c9:92:46:37:fb:71:46:3b:0c:1f:4c:c2:3e:2f:c2:65: ed:8f:a4:3b:1f:0f:87:5f:30:dc:18:13:bf:8d:e4:56:a8:6c:

		a3:98:b5:68:ab:5e:32:85:07:db:77:b1:9c:63:f1:76:8d:e2: 6f:56:67:5e:5c:eb:07:c9:b0:7f:cb:b5:5f:63:54:6d:c7:a2: 7c:8a:8a:d2:ff:e4:48:9a:8f:a7:ce:fe:c0:76:69:9c:8c:0e: 09:5b Here is the list of available SSLv2 ciphers: RC4-MD5 EXP-RC4-MD5 RC2-CBC-MD5 EXP-RC2-CBC-MD5 DES-CBC-MD5 DES-CBC3-MD5 RC4-64-MD5 The SSLv2 server offers 5 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack Solution: disable those ciphers and upgrade your client software if necessary. See http://support.microsoft.com/default.aspx?scid=kb en-us 216482 or http://httpd.apache.org/docs-2.0/mod/mod_ssl.html#sslciphersuite This SSLv2 server also accepts SSLv3 connections. This SSLv2 server also accepts TLSv1 connections.
https (443/tcp)	**Low**	The remote host is running a version of PHP which is older than 4.3.2 There is a flaw in this version which may allow an attacker who has the ability to inject an arbitrary argument to the function socket_iovec_alloc() to crash the remote service and possibly to execute arbitrary code. For this attack to work, PHP has to be compiled with the option --enable-sockets (which is disabled by default), and an attacker needs to be able to pass arbitrary values to socket_iovec_alloc(). Other functions are vulnerable to such flaws : openlog(), socket_recv(), socket_recvfrom() and emalloc() Solution : Upgrade to PHP 4.3.2 Risk factor : Low CVE : CAN-2003-0172 BID : 7187, 7197, 7198, 7199, 7210, 7256, 7259
daytime (13/tcp)	**Low**	The remote host is running a 'daytime' service. This service is designed to give the local time of the day of this host to whoever connects to this port. The date format issued by this service may sometimes help an attacker to guess the operating system type of this host, or to set up timed authentication attacks against the remote host. In addition to that, the UDP version of daytime is running, an attacker may link it to the echo port of a third party host using spoofing, thus creating a possible denial of service condition between this host and a third party.

		Solution : - Under Unix systems, comment out the 'daytime' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry keys to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service. Risk factor : Low CVE : CVE-1999-0103
ipp (631/tcp)	**Low**	The following CGI have been discovered : Syntax : cginame (arguments [default value]) /admin/ (printer_name [HP_Laserjet_2500] op [add-class]) /jobs (which_jobs [completed])
ipp (631/tcp)	**Low**	The following Acrobat files (.pdf) are available on the remote server : /ssr.pdf /svd.pdf /sps.pdf /sdd.pdf /idd.pdf /ipp.pdf /cmp.pdf /spm.pdf /sam.pdf /sum.pdf /overview.pdf You should make sure that none of these files contain confidential or otherwise sensitive information. An attacker may use these files to gain a more intimate knowledge of your organization and eventually use them do perform social engineering attacks (abusing the trust of the personnel of your company). Solution : sensitive files should not be accessible by everyone, but only by authenticated users.
ipp (631/tcp)	**Low**	It seems that your web server tries to hide its version or name, which is a good thing. However, using a special crafted request, PTR was able to determine that is is running : CUPS/1.1 Risk factor : None Solution : Fix your configuration.
unknown (1024/udp)	**Low**	The statd RPC service is running. This service has a long history of

		security holes, so you should really know what you are doing if you decide to let it run. *** No security hole regarding this program have been tested, so *** this might be a false positive. Solution : We suggest that you disable this service. Risk factor : High CVE : CVE-1999-0018, CVE-1999-0019, CVE-1999-0493 BID : 127, 450, 6831
login (513/tcp)	**Low**	The remote host is running the 'rlogin' service, a remote login daemon which allows people to log in this host and obtain an interactive shell. This service is dangerous in the sense thatit is not ciphered - that is, everyone can sniff the data that passes between the rlogin client and the rlogin server, which includes logins and passwords as well as the commands executed by the remote host. You should disable this service and use openssh instead (www.openssh.com) Solution : Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Risk factor : Low CVE : CAN-1999-0651
tftp (69/udp)	**Low**	The remote host is running a tftpd server. Solution : If you do not use this service, you should disable it. Risk factor : Low
smtp (25/tcp)	**Low**	A SMTP server is running on this port
discard (9/tcp)	**Low**	The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives. This service is unused these days, so it is advised that you disable it. Solution : - Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry key to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service. Risk factor : Low

		CVE : CAN-1999-0636
ipp (631/tcp)	**Low**	It seems that the PUT method is enabled on your web server Although we could not exploit this, you'd better disable it Solution : disable this method Risk factor : High
netbios-ssn (139/tcp)	**Low**	The host Security Identifier (SID) can be obtained remotely. Its value is : BUDAPEST : 5-21--1891759134--2072753058-772255953 An attacker can use it to obtain the list of the local users of this host Solution : filter the ports 137-139 and 445 Risk factor : Low CVE : CVE-2000-1200 BID : 959
netbios-ssn (139/tcp)	**Low**	The remote native lan manager is : Samba 2.2.3a-13 for Debian The remote Operating System is : Unix The remote SMB Domain Name is : KWEST
https (443/tcp)	**Low**	The target is running an Apache web server which allows for the injection of arbitrary escape sequences into its error logs. An attacker might use this vulnerability in an attempt to exploit similar vulnerabilities in terminal emulators. ***** PTR has determined the vulnerability exists only by looking at ***** the Server header returned by the web server running on the target. Solution : Upgrade to Apache version 1.3.31 or 2.0.49 or newer. Risk factor : Low CVE : CAN-2003-0020 BID : 9930 Other references : APPLE-SA:APPLE-SA-2004-05-03, CLSA:CLSA-2004:839, HPSB:HPSBUX01022, RHSA:RHSA-2003:139-07, RHSA:RHSA-2003:243-07, MDKSA:MDKSA-2003:050, OpenPKG-SA:OpenPKG-SA-2004.021-apache, SSA:SSA:2004-133-01, SuSE-SA:SuSE-SA:2004:009, TLSA:TLSA-2004-11, TSLSA:TSLSA-2004-0017
exec (512/tcp)	**Low**	An unknown server is running on this port. If you know what it is, please send this banner to the PTR team: 00: 01 57 68 65 72 65 20 61 72 65 20 79 6f 75 3f 0a .Where are you?. 10:
smtp (25/tcp)	**Low**	Remote SMTP server banner : 220 budapest ESMTP Postfix (Debian/GNU) This is probably: Postfix
https (443/tcp)	**Low**	The following directories were discovered: /cgi-bin, /icons 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
unknown	**Low**	A SMTP server is running on this port

(20012/tcp)		
netbios-ns (137/udp)	**Low**	The following 7 NetBIOS names have been gathered : BUDAPEST = This is the computer name registered for workstation services by a WINS client. BUDAPEST = This is the current logged in user registered for this workstation. BUDAPEST = Computer name __MSBROWSE__ KWEST = Workgroup / Domain name KWEST KWEST = Workgroup / Domain name (part of the Browser elections) . 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 If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. Risk factor : Medium CVE : CAN-1999-0621
netbios-ssn (139/tcp)	**Low**	An SMB server is running on this port
general/tcp	**Low**	The remote host does not discard TCP SYN packets which have the FIN flag set. Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules. See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113 Solution : Contact your vendor for a patch Risk factor : Medium BID : 7487
general/icmp	**Low**	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols. Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). Risk factor : Low CVE : CAN-1999-0524
https (443/tcp)	**Low**	A web server is running on this port through SSL
unknown (1024/udp)	**Low**	RPC program #100024 version 1 'status' is running on this port
sunrpc (111/udp)	**Low**	RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port
kdm (1024/tcp)	**Low**	RPC program #100024 version 1 'status' is running on this port
https (443/tcp)	**Low**	A SSLv2 server answered on this port
https (443/tcp)	**Low**	

		The remote web server appears to be running a version of Apache that is older than version 1.3.33. This version is vulnerable to a local buffer overflow in the get_tag() function of the module 'mod_include' when a specially crafted document with malformed server-side includes is requested though an HTTP session. Successful exploitation can lead to execution of arbitrary code with escalated privileges, but requires that server-side includes (SSI) is enabled. Solution: Disable SSI or upgrade to a newer version when available. Risk factor: Medium CVE : CAN-2004-0940 BID : 11471
sunrpc (111/tcp)	**Low**	RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port
ssh (22/tcp)	**Low**	An ssh server is running on this port
ssh (22/tcp)	**Low**	The remote SSH daemon supports the following versions of the SSH protocol : . 1.99 . 2.0 SSHv2 host key fingerprint : 22:7f:90:41:24:64:20:95:19:56:50:07:87:79:2b:12
printer (515/tcp)	**Low**	A LPD server seems to be running on this port
ipp (631/tcp)	**Low**	A web server is running on this port
snet-sensor-mgmt (10000/tcp)	**Low**	A SSLv2 server answered on this port
exec (512/tcp)	**Low**	The rexecd service is open. This service is design to allow users of a network to execute commands remotely. However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third party host. Solution : comment out the 'exec' line in /etc/inetd.conf and restart the inetd process Risk factor : Medium CVE : CAN-1999-0618
sunrpc (111/tcp)	**Low**	The RPC portmapper is running on this port. An attacker may use it to enumerate your list of RPC services. We recommend you filter traffic going to this port. Risk factor : Low CVE : CAN-1999-0632, CVE-1999-0189 BID : 205
https (443/tcp)	**Low**	The remote web server appears to be running a version of Apache that is older than version 1.3.32.

		This version is vulnerable to a heap based buffer overflow in proxy_util.c for mod_proxy. This issue may lead remote attackers to cause a denial of service and possibly execute arbitrary code on the server. Solution: Don't use mod_proxy or upgrade to a newer version. Risk factor: Medium CVE : CAN-2004-0492 BID : 10508
https (443/tcp)	**Low**	Your webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this 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. If you are using Apache, add the following lines for each virtual host in your configuration file : RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F] If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. If you are using Sun ONE Web Server releases 6.0 SP2 and later, add the following to the default object section in obj.conf: <Client method="TRACE"> AuthTrans fn="set-variable" remove-headers="transfer-encoding" set-headers="content-length: -1" error="501" </Client> If you are using Sun ONE Web Server releases 6.0 SP2 or below, compile the NSAPI plugin located at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603 See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603 http://www.kb.cert.org/vuls/id/867593 Risk factor : Medium
shell (514/tcp)	**Low**	The rsh service is running. This service is dangerous in the sense that it is not ciphered - that is, o everyone can sniff the data that passes between the rsh client and the rsh server. This includes logins and passwords.

		Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files. It is a built-in backdoor into a system that an attacker will make easy use of. You should disable this service and use ssh instead. Solution : Comment out the 'rsh' line in /etc/inetd.conf. Risk factor : Low CVE : CAN-1999-0651
https (443/tcp)	Low	The following CGI have been discovered : Syntax : cginame (arguments [default value]) . (D [A] M [A] N [D] S [A]) /libapache-mod-auth-mysql/ (D [A] M [A] N [D] D=D [] S [A]) Directory index found at / Directory index found at /libapache-mod-auth-mysql/

192.168.3.254

Service	Severity	Description
cadlock (1000/tcp)	Info	Port is open
cadlock (1000/tcp)	High	The remote host seems to be using a version of OpenSSL which is older than 0.9.6e or 0.9.7-beta3 This version is vulnerable to a buffer overflow which, may allow an attacker to obtain a shell on this host. *** Note that since safe checks are enabled, this check *** might be fooled by non-openssl implementations and *** produce a false positive. *** In doubt, re-execute the scan without the safe checks Solution : Upgrade to version 0.9.6e (0.9.7beta3) or newer Risk factor : High CVE : CAN-2002-0656, CAN-2002-0655, CAN-2002-0657, CAN-2002-0659, CVE-2001-1141 BID : 3004, 4316, 5363 Other references : IAVA:2002-A-0009, SuSE:SUSE-SA:2002:033
cadlock (1000/tcp)	Low	A web server is running on this port through SSL
general/icmp	Low	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.

		Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). Risk factor : Low CVE : CAN-1999-0524
cadlock (1000/tcp)	**Low**	Here is the SSLv2 server certificate: Certificate: Data: Version: 1 (0x0) Serial Number: 0 (0x0) Signature Algorithm: md5WithRSAEncryption Issuer: O=m0n0wall Validity Not Before: Sep 8 17:03:46 2003 GMT Not After : Sep 7 17:03:46 2004 GMT Subject: O=m0n0wall Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:c0:4a:1b:33:84:5c:fe:a3:c9:6c:31:64:c6:81: 3c:6c:4c:c3:d1:fa:fe:3e:a8:be:63:5c:3c:98:f7: b3:0b:4c:61:4a:ed:aa:90:3a:da:48:41:cf:93:71: 37:38:8e:49:60:39:59:47:a1:1e:e8:05:7a:ec:8b: c6:2b:6c:27:7e:f3:72:cf:42:64:28:48:f0:b4:56: a8:5f:53:7b:98:7f:73:73:c6:22:bc:af:de:da:3c: 2b:26:5a:0c:13:da:94:3a:4d:c1:12:4e:6e:ac:17: b9:cb:a6:b3:9f:ff:31:4f:0b:88:c4:d9:fb:e3:91: bc:f2:56:89:4f:cb:00:6e:7b Exponent: 65537 (0x10001) Signature Algorithm: md5WithRSAEncryption ad:83:f0:da:90:4a:55:2c:a4:50:9e:e4:9f:6e:7b:52:eb:8d: f1:87:1f:2e:07:13:dc:c0:f5:ab:e0:af:3d:d0:8e:ef:b5:24: eb:21:13:0c:bf:d4:12:63:67:dd:ed:41:46:e2:45:2e:d1:c2: f0:ce:e1:ca:c6:1b:82:1e:8e:38:45:73:3c:c0:d8:22:17:de: b7:76:ad:83:36:a0:6a:68:8c:a8:26:e5:8b:ae:85:5e:65:60: fc:00:1d:43:8b:6c:16:8b:39:5a:a5:2e:1c:f0:56:a8:c3:ed: 1d:83:91:75:08:7e:12:79:65:e9:2a:2b:96:70:ce:a2:57:b5: af:14 Here is the list of available SSLv2 ciphers: RC4-MD5 EXP-RC4-MD5 RC2-CBC-MD5 EXP-RC2-CBC-MD5 DES-CBC-MD5 DES-CBC3-MD5 RC4-64-MD5 The SSLv2 server offers 5 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack Solution: disable those ciphers and upgrade your client software if necessary. See http://support.microsoft.com/default.aspx?scid=kb en-us 216482 or http://httpd.apache.org/docs-2.0/mod/mod_ssl.html#sslciphersuite This SSLv2 server also accepts SSLv3 connections.

		This SSLv2 server also accepts TLSv1 connections.
general/tcp	**Low**	PTR was not able to reliably identify the remote operating system. It might be: FreeBSD 4.9 FreeBSD 4.7 FreeBSD 4.8 The fingerprint differs from these known signatures on 1 points. If you know what operating system this host is running, please send this signature to os-signatures@PTR.org : :1:1:1:64:1:64:1:0:64:1:0:64:1:8:64:1:1:0:2:1:1:1:1:1:64:57344:MNWNNT:0:1:1
general/udp	**Low**	For your information, here is the traceroute to 192.168.3.254 : 192.168.3.22 192.168.3.254
cadlock (1000/tcp)	**Low**	A SSLv2 server answered on this port