

Network Vulnerability Assessment Report

Sorted by host names

Session name: quasar.net

Start time: 06.07.2002 13:25:33

Finish time: 06.07.2002 14:18:52

Elapsed: 0 day(s) 00:53:19

Total records generated: 45

high severity: 3

low severity: 31

informational: 11

Summary of scanned hosts

Host	Holes	Warnings	Open ports	State
199.166.31.3	3	31	11	Finished

199.166.31.3

Service	Severity	Description
rtsserv (2500/tcp)	Info	Port is open
ssh (22/tcp)	Info	Port is open
smtp (25/tcp)	Info	Port is open
whois (43/tcp)	Info	Port is open
domain (53/tcp)	Info	Port is open
http (80/tcp)	Info	Port is open
pop-3 (110/tcp)	Info	Port is open
auth (113/tcp)	Info	Port is open
imap2 (143/tcp)	Info	Port is open
https (443/tcp)	Info	Port is open
ftp (21/tcp)	Info	Port is open
imap2 (143/tcp)	High	<p>The remote UW-IMAP server seems to be vulnerable to various buffer overflow which allow an authenticated user to gain a shell on this host.</p> <p>An attacker may use this flaw to escalate his privileges.</p> <p>*** Nessus solely relied on the server banner to *** issue this warning.</p> <p>Solution : Upgrade to the latest version of UW-IMAP Risk factor : High CVE : CAN-1999-1224</p>
imap2 (143/tcp)	High	<p>There is a buffer overflow in the remote imap server which allows an authenticated user to obtain a remote shell.</p> <p>By supplying an overly long tag the the BODY command, an attacker may gain a shell on this host.</p>

		Solution : Upgrade to imap-2001a Risk factor : Serious CVE : CAN-2002-0379
http (80/tcp)	High	'cgiwrap' is installed. This CGI has a well known security flaw that lets anyone execute arbitrary commands with the privileges of the http daemon (root or nobody). *** Note that all versions of cgiwrap are not affected *** by this problem ! Consult your vendor. Solution : remove it from /cgi-bin. Risk factor : Serious CVE : CVE-1999-1530
smtp (25/tcp)	Low	a SMTP server is running on this port Here is its banner : 220 blackhole.quasar.net ESMTP Sendmail 8.12.1/8.12.1/Debian -2 Sat, 6 Jul 2002 14:02:00 -0400 (No UCE/UBE) logging access from: ip68-99-108-41.hr.hr.cox.net(OK)-ip68-99-108-41.hr.hr.cox.net [68.99.108.41]
ssh (22/tcp)	Low	a ssh server is running on this port
imap2 (143/tcp)	Low	an IMAP server is running on this port
https (443/tcp)	Low	A TLSv1 server answered on this port
rtsserv (2500/tcp)	Low	a SMTP server is running on this port Here is its banner : 220 blackhole.quasar.net ESMTP Sendmail 8.12.1/8.12.1/Debian -2 Sat, 6 Jul 2002 14:03:01 -0400 (No UCE/UBE) logging access from: ip68-99-108-41.hr.hr.cox.net(OK)-ip68-99-108-41.hr.hr.cox.net [68.99.108.41]
ftp (21/tcp)	Low	a FTP server is running on this port. Here is its banner : 220 ProFTPD 1.2.4 Server ready.
http (80/tcp)	Low	a web server is running on this port
general/tcp	Low	Nmap did not do a UDP scan, I guess.
pop-3 (110/tcp)	Low	a pop3 server is running on this port
domain (53/tcp)	Low	The remote bind version is : 8.3.1-REL-NOESW
ssh (22/tcp)	Low	Remote SSH version : SSH-2.0-OpenSSH_3.4p1 Debian 1:3.4p1-0.0potato1
smtp (25/tcp)	Low	Remote SMTP server banner : blackhole.quasar.net ESMTP Sendmail 8.12.1/8.12.1/Debian -2 Sat, 6 Jul 2002 14:05:22 -0400 (No UCE/UBE) logging access from: ip68-99-108-41.hr.hr.cox.net(OK)-ip68-99-108-41.hr.hr.cox.net [68.99.108.41] 502 5.3.0 Sendmail 8.12.1 -- HELP not implemented
general/tcp	Low	QueSO has found out that the remote host OS is * Standard: Solaris 2.x, Linux 2.1.???, Linux 2.2, MacOS CVE : CAN-1999-0454
rtsserv (2500/tcp)	Low	Remote SMTP server banner : blackhole.quasar.net ESMTP Sendmail 8.12.1/8.12.1/Debian -2 Sat, 6 Jul 2002 14:05:24 -0400 (No UCE/UBE) logging access from: ip68-99-108-41.hr.hr.cox.net(OK)-ip68-99-108-41.hr.hr.cox.net

		[68.99.108.41] 502 5.3.0 Sendmail 8.12.1 -- HELP not implemented
ssh (22/tcp)	Low	The remote SSH daemon supports the following versions of the SSH protocol : . 1.99 . 2.0
general/tcp	Low	The plugin PC_anywhere_tcp.nasl was too slow to finish - the server killed it
auth (113/tcp)	Low	The 'ident' service provides sensitive information to potential attackers. It mainly says which accounts are running which services. This helps attackers to focus on valuable services [those owned by root]. If you don't use this service, disable it. Risk factor : Low Solution : comment out the 'auth' or 'ident' line in /etc/inetd.conf CVE : CAN-1999-0629
domain (53/tcp)	Low	The remote name server allows recursive queries to be performed by the host running nssusd. If this is your internal nameserver, then forget this warning. 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. 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 another name server, consult its documentation. Risk factor : Serious CVE : CVE-1999-0024
ftp (21/tcp)	Low	Remote FTP server banner : ProFTPD 1.2.4 Server ready.
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
pop-3 (110/tcp)	Low	The remote POP server banner is : +OK Cubic Circle's v1.31 1998/05/13 POP3 ready <552100000533273d@blackhole>
general/udp	Low	For your information, here is the traceroute to 199.166.31.3 : 10.0.224.1 68.10.9.33 68.10.8.49

		68.10.14.5 68.1.0.24 68.1.0.8 209.246.169.5 64.159.3.5 64.159.1.110 209.247.10.110 209.245.240.138 199.166.31.3
https (443/tcp)	Low	Here is the SSLv2 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 1 (0x1) Signature Algorithm: md5WithRSAEncryption Issuer: C=US, ST=Florida, L=Orlando, O=@quasar Internet Solutions, OU=SSL Certification, CN=@quasar Internet Solutions/Email=ssl-cert@quasar.net Validity Not Before: Mar 6 00:00:45 2000 GMT Not After : Mar 6 00:00:45 2001 GMT Subject: C=US, ST=Florida, L=Orlando, O=@quasar Internet Solutions, OU=Webhosting, CN=secure.quasar.net/Email=ssl-cert@quasar.net Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:df:4a:ff:a4:a5:f7:4b:44:5b:a8:db:32:d3:90: e0:b9:a4:14:49:21:69:21:e0:a8:fc:e3:04:5d:40: 4c:f8:8d:ad:42:e8:95:1b:d3:65:e2:85:3c:03:d7: 2e:f8:c8:8b:39:60:ee:6c:af:84:d8:95:26:f5:88: 16:f2:df:04:36:1b:60:58:eb:ab:85:14:45:fc:69: a9:18:61:d2:85:61:8d:15:d3:c7:6d:10:6b:87:4a: f0:0f:60:62:87:38:7d:a7:46:54:c1:23:c2:43:eb: 2a:65:16:3c:9e:93:df:28:69:06:79:0f:b6:e7:6e: 34:03:c1:d1:70:ca:06:cc:dd Exponent: 65537 (0x10001)

		<p>X509v3 extensions:</p> <p>Netscape CA Revocation Url:</p> <p>http://www.cryptsoft.com/ca-crl.pem</p> <p>Netscape Comment:</p> <p>This is a comment</p> <p>Netscape Cert Type:</p> <p>SSL Server</p> <p>Signature Algorithm: md5WithRSAEncryption</p> <p>31:ee:09:b2:c9:2f:7d:53:c1:9e:78:44:0c:6c:b1:3b:09:6b: 96:76:f8:f1:b4:65:34:38:3d:a2:97:31:92:fe:f7:de:2c:fd: d9:c0:26:66:61:c4:f9:03:ab:72:63:23:6e:ce:af:31:91:9f: 28:ff:be:35:36:74:6d:be:b2:15:e9:a5:5e:1a:4a:f8:54:0c: 57:80:4f:f9:11:98:77:7a:87:46:1a:6c:18:7a:e7:c2:45:53: f9:eb:b8:db:49:55:c5:da:c9:22:0c:9b:6c:f1:dc:07:74:bb: 51:2a:cd:db:74:8b:c4:4e:9b:e4:0a:fc:85:a5:14:52:67:49: 68:1d</p>
https (443/tcp)	Low	<p>Here is the list of available SSLv2 ciphers:</p> <p>DES-CBC3-MD5 SSLv2 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5</p> <p>RC2-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5</p> <p>RC4-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5</p> <p>RC4-64-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC4(64) Mac=MD5</p> <p>DES-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5</p> <p>EXP-RC2-CBC-MD5 SSLv2 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export</p> <p>EXP-RC4-MD5 SSLv2 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export</p>
https (443/tcp)	Low	<p>The SSLv2 server offers 3 strong ciphers, but also 2 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</p> <p>Solution: disable those ciphers and upgrade your client software if necessary</p>
https (443/tcp)	Low	<p>Here is the list of available SSLv3 ciphers:</p> <p>EDH-RSA-DES-CBC3-SHA SSLv3 Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1</p> <p>EDH-DSS-DES-CBC3-SHA SSLv3 Kx=DH Au=DSS Enc=3DES(168) Mac=SHA1</p> <p>DES-CBC3-SHA SSLv3 Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1</p> <p>DHE-DSS-RC4-SHA SSLv3 Kx=DH Au=DSS</p>

		<p>Enc=RC4(128) Mac=SHA1 RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1 RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5 EXP1024-DHE-DSS-RC4-SHA SSLv3 Kx=DH(1024) Au=DSS Enc=RC4(56) Mac=SHA1 export EXP1024-RC4-SHA SSLv3 Kx=RSA(1024) Au=RSA Enc=RC4(56) Mac=SHA1 export EXP1024-DHE-DSS-DES-CBC-SHA SSLv3 Kx=DH(1024) Au=DSS Enc=DES(56) Mac=SHA1 export EXP1024-DES-CBC-SHA SSLv3 Kx=RSA(1024) Au=RSA Enc=DES(56) Mac=SHA1 export EXP1024-RC2-CBC-MD5 SSLv3 Kx=RSA(1024) Au=RSA Enc=RC2(56) Mac=MD5 export EXP1024-RC4-MD5 SSLv3 Kx=RSA(1024) Au=RSA Enc=RC4(56) Mac=MD5 export EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH Au=RSA Enc=DES(56) Mac=SHA1 EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH Au=DSS Enc=DES(56) Mac=SHA1 DES-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1 EXP-EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export EXP-EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH(512) Au=DSS Enc=DES(40) Mac=SHA1 export EXP-DES-CBC-SHA SSLv3 Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export EXP-RC2-CBC-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export EXP-RC4-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export</p>
smtp (25/tcp)	Low	<p>The remote SMTP server answers to the EXPN and/or VRFY commands.</p> <p>The EXPN command can be used to find the delivery address of mail aliases, or even the full name of the recipients, and the VRFY command may be used to check the validity of an account.</p> <p>Your mailer should not allow remote users to use any of these commands, because it gives them too much information.</p> <p>Solution : if you are using Sendmail, add the option O PrivacyOptions=goaway in /etc/sendmail.cf.</p> <p>Risk factor : Low CVE : CAN-1999-0531</p>
smtp (25/tcp)	Low	The EICAR test string was sent 2 times. Check your mailbox!
rtsserv (2500/tcp)	Low	The EICAR test string was sent 2 times. Check your mailbox!
http (80/tcp)	Low	<p>The remote web server type is :</p> <p>Apache/1.3.26 (Unix) Debian GNU/Linux mod_perl/1.26</p>

		We recommend that you configure your web server to return bogus versions in order to not leak information
ntp (123/udp)	Low	<p>An NTP server is running on the remote host. Make sure that you are running the latest version of your NTP server, has some versions have been found out to be vulnerable to buffer overflows.</p> <p>*** Nessus reports this vulnerability using only *** information that was gathered. Use caution *** when testing without safe checks enabled.</p> <p>If you happen to be vulnerable : upgrade Solution : Upgrade Risk factor : High CVE : CVE-2001-0414</p>