

Network Vulnerability Assessment Report

Sorted by host names

Session name: ACME LAN

Start time: 00.00.0000 00:00:00

Finish time: 00.00.0000 00:00:00

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

Total records generated: 59

high severity: 9

low severity: 18

informational: 32

Summary of scanned hosts

Host	Holes	Warnings	Open ports	State
192.168.0.12	3	12	2	Finished
192.168.0.1	4	3	1	Finished
192.168.0.50	2	3	2	Finished

192.168.0.1

Service	Severity	Description
http (80/tcp)	Info	Port is open
domain (53/tcp)	High	<p>The remote BIND server, according to its version number, is vulnerable to the SIG cached RR overflow vulnerability.</p> <p>An attacker may use this flaw to gain a shell on this system.</p> <p>Solution : upgrade to bind 8.2.7, 8.3.4 or 4.9.11</p> <p>Workaround : Disable recursion on this server if it's not used as a recursive name server.</p> <p>Risk factor : High CVE : CAN-2002-1219 BID : 6160 Other references : IAVA:2002-A-0011, SuSE:SUSE-SA:2002:044</p>
general/tcp	High	<p>The remote host has predictable TCP sequence numbers.</p> <p>An attacker may use this flaw to establish spoofed TCP connections to this host.</p> <p>Solution : Contact your vendor for a patch Risk factor : High CVE : CVE-1999-0077 BID : 107, 10881, 670</p>
domain (53/tcp)	High	<p>This is associated with three different vulnerabilities.</p> <p>1) The remote BIND server, based on its version number, if running</p>

		<p>recursive DNS functionality, is vulnerable to a buffer overflow.</p> <p>2) The remote BIND server is vulnerable to a denial of service (crash) via SIG RR elements with invalid expiry times.</p> <p>3) The remote BIND server is vulnerable to a denial of service. When a DNS lookup is requested on a non-existent sub-domain of a valid domain and an OPT resource record with a large UDP payload is attached, the server may fail.</p> <p>Solution : upgrade to at least bind 8.3.4 Risk factor : High CVE : CAN-2002-1221, CAN-2002-1219, CAN-2002-1220 BID : 6159, 6160, 6161 Other references : IAVA:2002-A-0011, SuSE:SUSE-SA:2002:044</p>
domain (53/tcp)	High	<p>The remote BIND server, according to its version number, is vulnerable to the negative cache poison bug that may allow an attacker to disable this service remotely.</p> <p>Solution : upgrade to bind 8.3.7 or 8.4.3 Risk factor : High CVE : CAN-2003-0914 BID : 9114 Other references : SuSE:SUSE-SA:2003:047</p>
general/tcp	Low	<p>The remote host accepts loose source routed IP packets. The feature was designed for testing purpose. An attacker may use it to circumvent poorly designed IP filtering and exploit another flaw. However, it is not dangerous by itself.</p> <p>Solution : drop source routed packets on this host or on other ingress routers or firewalls.</p> <p>Risk factor : Low</p>
general/tcp	Low	<p>The remote host does not discard TCP SYN packets which have the FIN flag set.</p> <p>Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.</p> <p>See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113</p> <p>Solution : Contact your vendor for a patch Risk factor : Medium BID : 7487</p>
domain (53/udp)	Low	<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 www.nessus.org). This allows hackers to do cache poisoning attacks against this nameserver.</p>

		<p>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.</p> <p>See also : http://www.cert.org/advisories/CA-1997-22.html</p> <p>Solution : Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it).</p> <p>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 bind 9, you can define a grouping of internal addresses using the 'acl' command</p> <p>Then, within the options block, you can explicitly state: 'allow-recursion { hosts_defined_in_acl }'</p> <p>For more info on Bind 9 administration (to include recursion), see: http://www.nominum.com/content/documents/bind9arm.pdf</p> <p>If you are using another name server, consult its documentation.</p> <p>Risk factor : High CVE : CVE-1999-0024 BID : 136, 678</p>
unknown (520/udp)	Info	<p>A RIP-2 agent is running on this port. The following routes are advertised: 0.0.0.0/0.0.0.0 at 1 hop 207.227.112.96/255.255.255.224 at 1 hop This information on your network topology may help an attacker</p> <p>Risk factor : Low</p>
domain (53/udp)	Info	<p>The remote DNS server answers to queries for third party domains which do not have the recursion bit set.</p> <p>This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.</p> <p>For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of aforementioned financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more...</p> <p>For a much more detailed discussion of the potential risks of allowing DNS cache information to be queried anonymously, please see: http://community.sidestep.pt/~luis/DNS-Cache-Snooping/DNS_Cache_Snooping_1.1.pdf</p> <p>Risk factor : Low</p>
general/udp	Info	<p>For your information, here is the traceroute to 192.168.0.1 :</p>

		192.168.0.50 192.168.0.1
domain (53/udp)	Info	<p>BIND 'NAMED' is an open-source DNS server from ISC.org. Many proprietary DNS servers are based on BIND source code.</p> <p>The BIND based NAMED servers (or DNS servers) allow remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind', will typically prompt the server to send the information back to the querying source.</p> <p>The remote bind version is : 8.2.5-REL</p> <p>Solution : Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts.</p>
http (80/tcp)	Info	A web server is running on this port
bootps (67/udp)	Info	<p>Here is the information we could gather from the remote DHCP server. This allows an attacker on your local network to gain information about it easily :</p> <p>Master DHCP server of this network : 0.0.0.0 IP address the DHCP server would attribute us : 192.168.0.15 DHCP server(s) identifier = 192.168.0.1 netmask = 255.255.255.0 router = 192.168.0.1 domain name server(s) = 206.54.254.3 , 206.54.254.15</p> <p>Solution : remove the options that are not in use in your DHCP server Risk factor : Low</p>
domain (53/udp)	Info	<p>A DNS server is running on this port. If you do not use it, disable it.</p> <p>Risk factor : Low</p>
domain (53/udp)	Info	<p>The remote name server could be fingerprinted as being one of the following :</p> <p>ISC BIND 8.3 ISC BIND 8.4</p>
http (80/tcp)	Info	<p>The remote web server type is :</p> <p>Embedded HTTPD v1.00, 1999(c) Delta Networks Inc.r</p> <p>Solution : We recommend that you configure (if possible) your web server to return a bogus Server header in order to not leak information.</p>

192.168.0.12

Service	Severity	Description
netbios-ssn (139/tcp)	Info	Port is open
microsoft-ds (445/tcp)	Info	Port is open
general/tcp	High	<p>There is a flaw in the Task Scheduler application which could allow a remote attacker to execute code remotely. There are many attack vectors for this flaw. An attacker, exploiting this flaw, would need to either have the ability to connect to the target machine or be able to coerce a local user to either install a .job file or browse to a malicious website.</p> <p>See also :</p>

		<p>http://www.microsoft.com/technet/security/bulletin/ms04-022.msp</p> <p>Risk factor : High CVE : CAN-2004-0212 BID : 10708</p>
general/icmp	High	<p>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.</p> <p>Note that an attacker may take advantage of this flaw only when its target is on the same physical subnet.</p> <p>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</p>
unknown (135/udp)	High	<p>A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. Disabling the Messenger Service will prevent the possibility of attack.</p> <p>This plugin actually checked for the presence of this flaw.</p> <p>Solution : see http://www.microsoft.com/technet/security/bulletin/ms03-043.msp</p> <p>Risk factor : High CVE : CAN-2003-0717 BID : 8826 Other references : IAVA:2003-A-0028</p>
netbios-ns (137/udp)	Low	<p>The following 8 NetBIOS names have been gathered :</p> <p>ENGINEER2 = This is the computer name registered for workstation services by a WINS client. CYBERLYNK = Workgroup / Domain name ENGINEER2 = This is the current logged in user registered for this workstation. ENGINEER2 = Computer name CYBERLYNK = Workgroup / Domain name (part of the Browser elections) JSMITH = This is the current logged in user registered for this workstation. CYBERLYNK</p> <p><u>MSBROWSE</u></p> <p>The remote host has the following MAC address on its adapter :</p> <p>00:02:8a:5c:73:45</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> <p>Risk factor : Medium CVE : CAN-1999-0621</p>

unknown (135/tcp)	Low	<p>Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.</p> <p>An attacker may use this fact to gain more knowledge about the remote host.</p> <p>Solution : filter incoming traffic to this port. Risk factor : Low</p>
microsoft-ds (445/tcp)	Low	<p>Here is the browse list of the remote host :</p> <p>ENGINEER2 -</p> <p>This is potentially dangerous as this may help the attack of a potential hacker by giving him extra targets to check for</p> <p>Solution : filter incoming traffic to this port Risk factor : Low</p>
general/icmp	Low	<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 : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).</p> <p>Risk factor : Low CVE : CAN-1999-0524</p>
microsoft-ds (445/tcp)	Low	<p>The host Security Identifier (SID) can be obtained remotely. Its value is :</p> <p>ENGINEER2 : 5-21-2025429265-1993962763-1343024091</p> <p>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</p> <p>CVE : CVE-2000-1200 BID : 959</p>
general/tcp	Low	<p>The remote host accepts loose source routed IP packets. The feature was designed for testing purpose. An attacker may use it to circumvent poorly designed IP filtering and exploit another flaw. However, it is not dangerous by itself.</p> <p>Solution : drop source routed packets on this host or on other ingress routers or firewalls.</p> <p>Risk factor : Low</p>
general/tcp	Low	<p>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.</p> <p>An attacker may use this feature to determine traffic patterns within your network. A few examples (not at all exhaustive) are:</p> <ol style="list-style-type: none"> 1. A remote attacker can determine if the remote host sent a packet

		<p>in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another network.</p> <p>2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines.</p> <p>3. A remote attacker can roughly estimate the number of requests that a web server processes over a period of time.</p> <p>Solution : Contact your vendor for a patch Risk factor : Low</p>
general/tcp	Low	<p>The remote host does not discard TCP SYN packets which have the FIN flag set.</p> <p>Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.</p> <p>See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113</p> <p>Solution : Contact your vendor for a patch Risk factor : Medium BID : 7487</p>
unknown (5000/tcp)	Low	<p>The remote host is running Microsoft UPnP TCP helper.</p> <p>If the tested network is not a home network, you should disable this service.</p> <p>Solution : Set the following registry key :</p> <p>Location : HKLM\SYSTEM\CurrentControlSet\Services\SSDPSRV Key : Start Value : 0x04</p> <p>Risk factor : Low CVE : CVE-2001-0876 BID : 3723</p>
general/tcp	Low	<p>The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections.</p> <p>This may cause problems for some dedicated services (BGP, a VPN over TCP, etc...).</p> <p>Solution : See http://www.securityfocus.com/bid/10183/solution/ Risk factor : Medium CVE : CAN-2004-0230</p>

		BID : 10183 Other references : OSVDB:4030, IAVA:2004-A-0007
netbios-ns (137/udp)	Low	<p>The remote host is running a version of the NetBT name service which suffers from a memory disclosure problem.</p> <p>An attacker may send a special packet to the remote NetBT name service, and the reply will contain random arbitrary data from the remote host memory. This arbitrary data may be a fragment from the web page the remote user is viewing, or something more serious like a POP password or anything else.</p> <p>An attacker may use this flaw to continuously 'poll' the content of the memory of the remote host and might be able to obtain sensitive information.</p> <p>Solution : See http://www.microsoft.com/technet/security/bulletin/ms03-034.msp Risk factor : Medium CVE : CAN-2003-0661 BID : 8532</p>
isakmp (500/udp)	Low	<p>The remote host seems to be enabled to do Internet Key Exchange. This is typically indicative of a VPN server. VPN servers are used to connect remote hosts into internal resources. In addition, The remote host seems to be configured to force all communications across port 500 for both the source and destination port. That is, we sent the machine a packet from a random port greater than 1024. The machine sent the reply back to port 500.</p> <p>NOTE: This sort of behavior has been observed on Microsoft machines.</p> <p>Solution: You should ensure that:</p> <ol style="list-style-type: none"> 1) The VPN is authorized for your Companies computing environment 2) The VPN utilizes strong encryption 3) The VPN utilizes strong authentication <p>Risk factor : Low</p>
microsoft-ds (445/tcp)	Info	<p>The remote native lan manager is : Windows 2000 LAN Manager The remote Operating System is : Windows 5.1 The remote SMB Domain Name is : CYBERLYNK</p>
general/udp	Info	<p>For your information, here is the traceroute to 192.168.0.12 :</p> <pre>192.168.0.50 192.168.0.12</pre>
microsoft-ds (445/tcp)	Info	<p>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</p> <p>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</p> <p>All the smb tests will be done as "/" in domain CYBERLYNK CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222,</p>

		CAN-1999-0505, CAN-2002-1117 BID : 494, 990, 11199
unknown (1026/udp)	Info	<p>Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.</p> <p>An attacker may use this fact to gain more knowledge about the remote host.</p> <p>Here is the list of DCE services running on this port:</p> <p>UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1</p> <p>Endpoint: ncadg_ip_udp:192.168.0.12[1026]</p> <p>Annotation: Messenger Service</p> <p>Named pipe : ntsvcs</p> <p>Win32 service or process : messenger</p> <p>Description : Messenger service</p> <p>Solution : filter incoming traffic to this port. Risk factor : Low</p>
netbios-ssn (139/tcp)	Info	An SMB server is running on this port
unknown (1025/tcp)	Info	<p>Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.</p> <p>An attacker may use this fact to gain more knowledge about the remote host.</p> <p>Here is the list of DCE services running on this port:</p> <p>UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.12[1025]</p> <p>Named pipe : atsvc</p> <p>Win32 service or process : mstask.exe</p> <p>Description : Scheduler service</p> <p>UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.12[1025]</p> <p>UUID: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1</p>

		<p>Endpoint: ncacn_ip_tcp:192.168.0.12[1025]</p> <p>UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.12[1025]</p> <p>Annotation: Messenger Service</p> <p>Named pipe : ntsvcs</p> <p>Win32 service or process : messenger</p> <p>Description : Messenger service</p> <p>Solution : filter incoming traffic to this port.</p> <p>Risk factor : Low</p>
ntp (123/udp)	Info	<p>A NTP (Network Time Protocol) server is listening on this port.</p> <p>Risk factor : Low</p>
general/tcp	Info	The remote host is running Windows XP
microsoft-ds (445/tcp)	Info	A CIFS server is running on this port

192.168.0.50

Service	Severity	Description
sunrpc (111/tcp)	Info	Port is open
ssh (22/tcp)	Info	Port is open
ssh (22/tcp)	High	<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 :</p> <pre>rpm -q openssh-server</pre> <p>Returns :</p> <pre>openssh-server-3.1p1-13 (RedHat 7.x) openssh-server-3.4p1-7 (RedHat 8.0) openssh-server-3.5p1-11 (RedHat 9)</pre> <p>Solution : Upgrade to OpenSSH 3.7.1</p> <p>See also :</p> <p>http://marc.theaimsgroup.com/?l=openbsd-misc&m=1063754524237</p>

		<p>94&w=2</p> <p>http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375456923804&w=2</p> <p>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</p>
unknown (32768/udp)	High	<p>The remote statd service may be vulnerable to a format string attack.</p> <p>This means that an attacker may execute arbitrary code thanks to a bug in this daemon.</p> <p>Only older versions of statd under Linux are affected by this problem.</p> <p>*** Nessus reports this vulnerability using only information that was gathered. *** Use caution when testing without safe checks enabled.</p> <p>Solution : upgrade to the latest version of rpc.statd Risk factor : High CVE : CVE-2000-0666, CAN-2000-0800 BID : 1480</p>
unknown (32775/tcp)	Low	<p>The fam RPC service is running.</p> <p>Several versions of this service have a well-known buffer overflow condition that allows intruders to execute arbitrary commands as root on this system.</p> <p>Solution : disable this service in /etc/inetd.conf See also : http://www.nai.com/nai_labs/asp_set/advisory/16_fam_adv.asp Risk factor : High CVE : CVE-1999-0059 BID : 353</p>
unknown (32768/udp)	Low	<p>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.</p> <p>*** No security hole regarding this program have been tested, so *** this might be a false positive.</p> <p>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</p>
ssh (22/tcp)	Low	<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 : If you use OpenSSH, set the option 'Protocol' to '2' If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'</p> <p>Risk factor : Low</p>
sunrpc (111/tcp)	Info	<p>The RPC portmapper is running on this port.</p>

		<p>An attacker may use it to enumerate your list of RPC services. We recommend you filter traffic going to this port.</p> <p>Risk factor : Low CVE : CAN-1999-0632, CVE-1999-0189 BID : 205</p>
unknown (32774/tcp)	Info	RPC program #100024 version 1 'status' is running on this port
sunrpc (111/udp)	Info	RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port
sunrpc (111/tcp)	Info	RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port
unknown (32775/tcp)	Info	RPC program #391002 version 2 'sgi_fam' (fam) is running on this port
ssh (22/tcp)	Info	An ssh server is running on this port
unknown (32768/udp)	Info	RPC program #100024 version 1 'status' is running on this port
ssh (22/tcp)	Info	Remote SSH version : SSH-1.99-OpenSSH_3.6.1p2
ssh (22/tcp)	Info	<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 : 8e:1e:25:56:a1:20:ea:08:13:5e:2c:58:e5:88:fa:98 SSHv2 host key fingerprint : bc:55:53:22:73:37:4d:25:55:0f:d0:28:8c:93:2a:7b</p>