



For

Demo Site

**Vulnerability Assessment
SecureScout**

Report Generation Date:
Generated on 2006-04-19 11:04:57 GMT-04.00

Powered by

SecureScout

Table of Contents

Introduction	3
Nondisclosure	4
Report Summary	5
General Information	5
Security Risk Classifications	5
Hosts at Risk	6
Hosts Tested	7
Network Information	8
Trace route	8
Operating Systems	8
Open Ports and Services	10
Vulnerabilities	12
High risk vulnerabilities	14
Medium risk vulnerabilities	15
Low risk vulnerabilities	18

Introduction

The CougarScan Online service utilizes the most comprehensive database of vulnerabilities in the market. The proprietary CougarScan assessment tool is updated more frequently than other commercial and open source tools, providing you with the most reliable results available. This report consolidates the data obtained from the CougarScan Online assessment. Vulnerabilities are detected on the basis of direct detection, system fingerprinting, and a variety of other pass/ fail criteria. The CougarScan Assessment cannot always determine with 100% certainty that the detected vulnerability is present on the target system. In general terms these vulnerabilities may be classified as "False Positives". All "False positives" must be investigated further in order to determine if they are present on the host system. CougarSecurity's Security Engineers and Research and Development Team continue to add intelligence to CougarScan that helps classify "possible risks" according to the true threat they pose to organizations. Although CougarScan makes every effort to minimize false positives, it errs on the side of caution when reporting vulnerabilities. This provides systems administrators the most reliable foundation for investigating and fixing vulnerabilities to assure digital assets are safe.

Nondisclosure







Nondisclosure statement

This report is the sole property of the customer. All information obtained during a CougarScan assessment about the customer's operations and assets including, but not limited to, its procedures and systems, is deemed privileged information and not for public dissemination. The Business Partner and CougarSecurity.com jointly and severally pledge their commitment that this information will remain strictly confidential. It will not be discussed or disclosed to any third party without the express written consent of the customer. CougarSecurity.com strives to maintain the highest level of ethical standards in its business practice. Nondisclosure agreement The Business Partner has accepted that CougarSecurity Inc. can perform a security audit using the CougarScan service. The acceptance was given for a limited number of IP addresses as stated in the report summary section of this report. All product names referenced herein are trademarks of their respective companies. The information in this document is subject to change without notice and should not be construed as a commitment by the manufacturer or supplier. CougarSecurity takes no responsibility for errors that may appear in this document. Neither the supplier nor the manufacturer of CougarScan, can be held liable if performance of the customer's IT systems are degraded during or after the CougarScan audit. The CougarScan audit was carried out and delivered in accordance with the CougarScan general business terms.

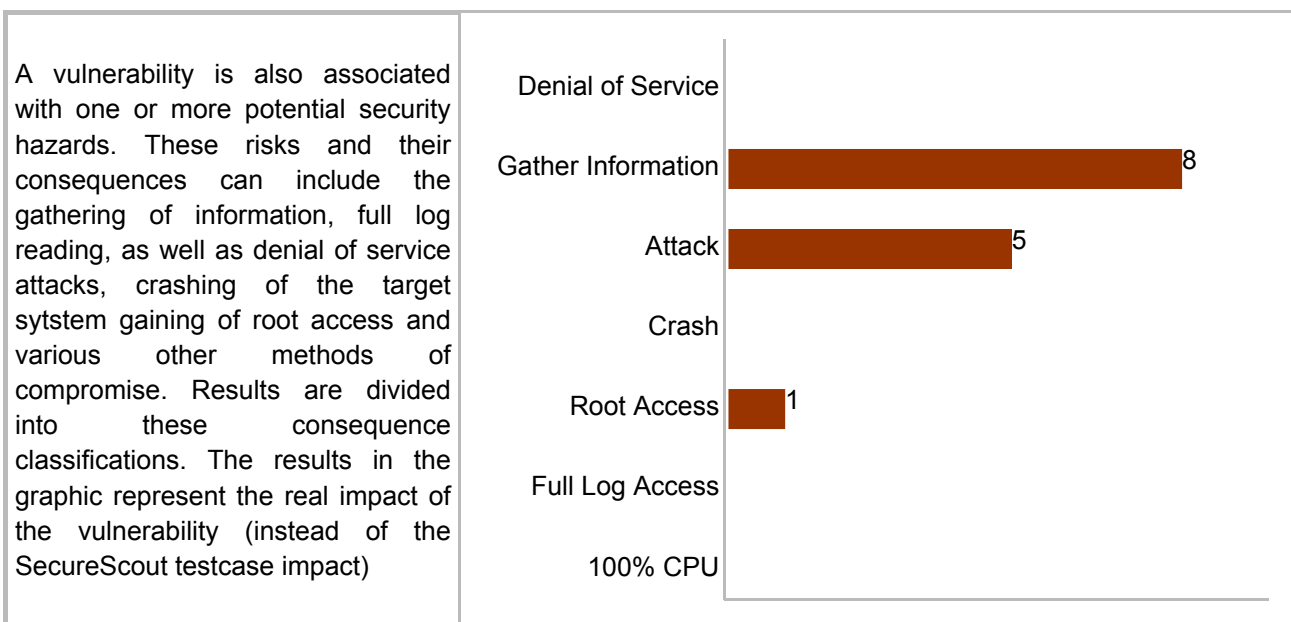
Report Summary

User Name: Site Admin
 Company: Demo Site
 Session ID: 10537
 Session Name: Session for TJID:14661
 TJID: 14661
 Job Type: VulnScan
 Job Start Date: 2006-04-19 10:34:51 GMT-04.00
 Job End Date: 2006-04-19 10:47:14 GMT-04.00
 SecureScout NX version: 2.6.203.0
 Policy: Safe Scan

General Information

Vulnerabilities			Total Found : 14
	High risk vulnerabilities	1	
	Medium risk vulnerabilities	7	
	Low risk vulnerabilities	6	

Security Risk Classifications

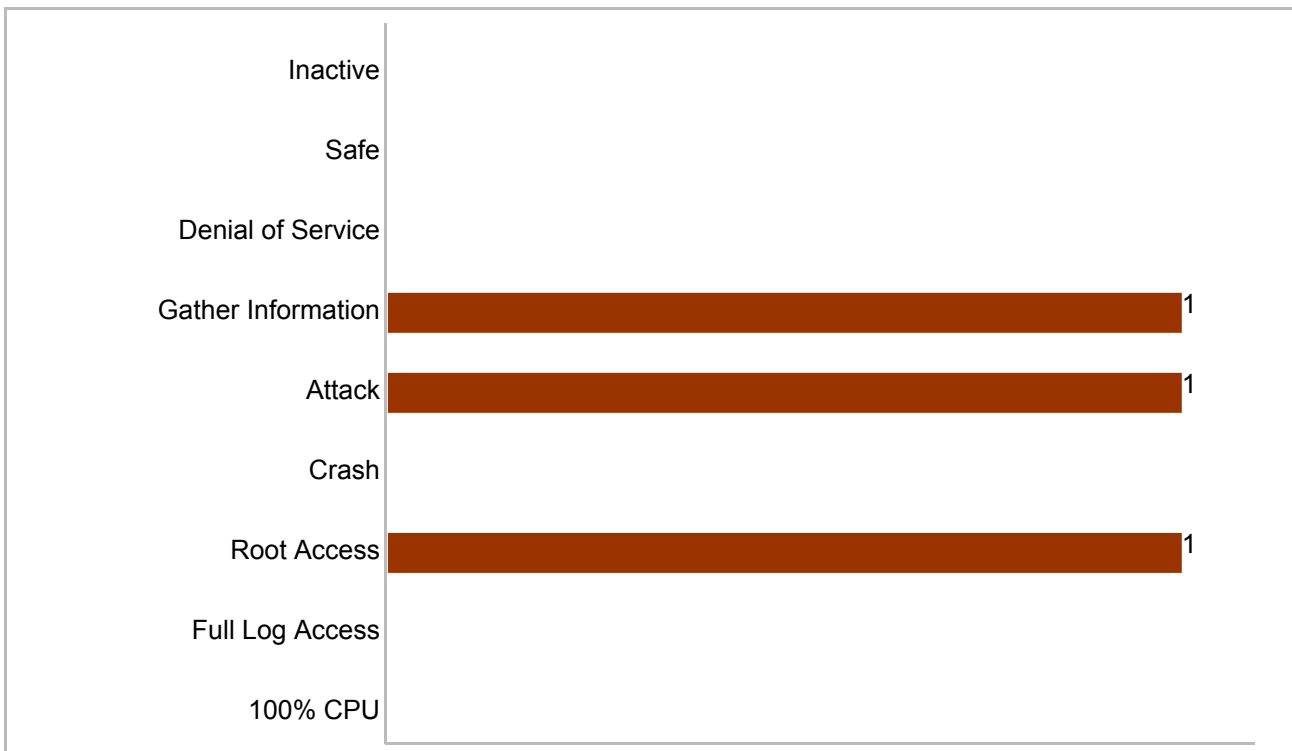


Hosts at Risk

Among the 1 host(s) tested, SecureScout found 1 host(s) vulnerable and 0 host(s) inactive. The following graph counts the hosts according to their highest vulnerability risk.

Hosts at High Risk	1
Hosts at Medium Risk	0
Hosts at Low Risk	0
Safe Hosts	0
Inactive Hosts	0

The following graph counts the hosts vulnerable to each of the security classification based on the real impact of the vulnerabilities (instead of the SecureScout testcase impact) .



Hosts Tested

Sorted by IP address, hosts are presented with their name (if available), their risk level, and the total number of vulnerabilities that they tested positive for as well as the medium used in their testing (console or agent).

Hosts IP	Name	Max Risk	Nb Vuln	Assessed from
24.47.44.82	24.47.44.82		14	Console

Network Information

The SecureScout testing was configured and executed against the following IP address(es):
24.47.44.82

Ports Tested :

TCP	1-1023
UDP	NULL

Trace route

Trace routing a target can provide potentially sensitive information about the relationships between systems and software. A determined cracker can infer enough from a trace route to use Web servers as a launching pad for penetrating internal systems. Disclosing such data about Internet-connected systems that reside inside the router should be avoided to prevent crackers from mapping your resources.

If the system was able to trace the path packets traversed while being delivered to the target system, the route information is listed here:


Hosts IP	Trace route
24.47.44.82	Traceroute to host 24.47.44.82: > 208.151.248.241 208.151.248.241 > 206.103.54.187 206.103.54.187 > ge1-0-0.cis025cor02.bea1.easy.easystreet.com 10.57.2.2 > fe3-0.cis001bdr01.bea1.easy.easystreet.com 209.162.220.65 > sl-gw7-sea-6-0-0.sprintlink.net 144.228.98.17 > sl-bb20-sea-5-6.sprintlink.net 144.232.6.73 > so-3-0-0.gar1.Seattle1.Level3.net 209.0.227.133 > ae-31-55.ebr1.Seattle1.Level3.net 4.68.105.158 > ae-1.ebr2.Seattle1.Level3.net 4.69.132.18 > ae-2.ebr2.Denver1.Level3.net 4.69.132.54 > ae-3.ebr1.Chicago1.Level3.net 4.69.132.62 > ae-2.ebr2.NewYork1.Level3.net 4.69.132.66 > ge-5-0-0-54.gar1.NewYork1.Level3.net 4.68.97.98 > * * * > * * * > * * * > dstswr2-ge3-16.rh.stjmny.cv.net 167.206.39.134 > ubr203-ge1-0-0.cmts.stjmny.cv.net 167.206.39.174 > ool-182f2c52.dyn.optonline.net 24.47.44.82

Operating Systems and Ping

Vulnerabilities can be classified by operating system. Identifying operating system information is valuable to potential intruders because it allows them to better focus and refine their attacks. SecureScout tries to detect the operating system running on the target system. Indicating that automated operating system detection is not always possible based upon the information retrieved from the target system. This may then be

considered as an advantage for the general security level on the target system. Ping can be used to monitor the presence of the system; response to ping is not obligatory for the vast majority of targetted systems. SecureScout tries to reach the target system by making a ping and/or a TCP ping request. If the system replies, it is listed in the table below.

Discovered OS

Operating Systems	%	
Undefined	100 %	

Note: Operating systems representing less than 5% of the total are included in the "others" category

Ping

Ping can be used to monitor the presence of a system. Response to a ping is not obligatory for the vast majority of systems. SecureScout tried to reach the target system by making a ping and/or a TCP ping request. If the system replied, it is listed in the table below.

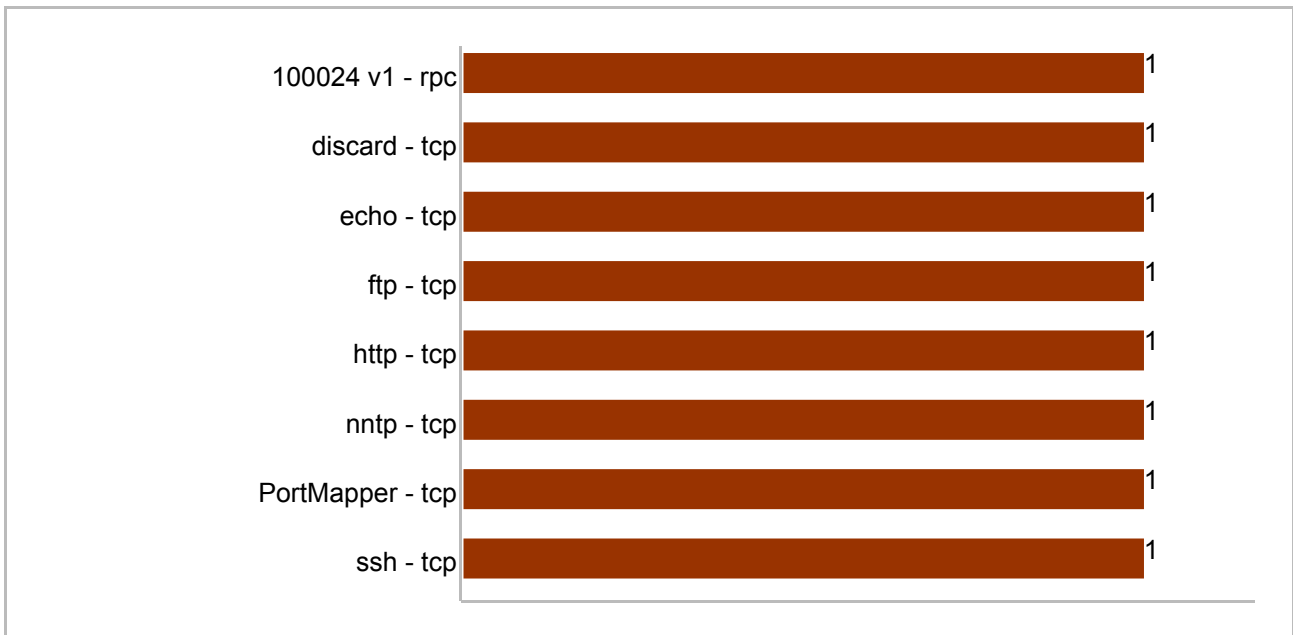
IP	Operating Systems	Pingable
24.47.44.82	UNDEFINED	No

Open Ports and Services

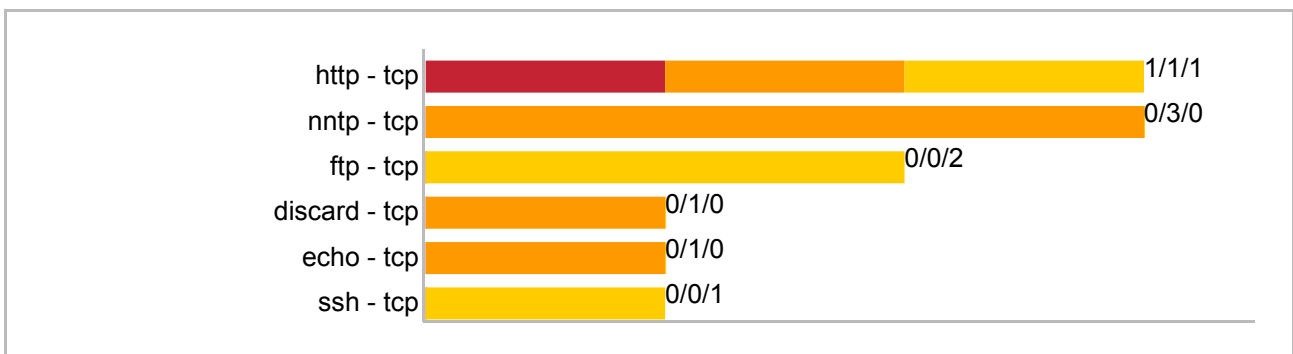
A port is the interface to a service on the target system. An optional security configuration provides that the number of open ports is kept as low as possible while still enabling the system to function are required.

Certain Test cases might find additional open ports.

Top ten list of services



Vulnerabilities and Services



Open Ports List

This is a list of the open ports found on the tested IP range. The services mentioned are the services identified by SecureScout.

24.47.44.82		
(TCP/UDP/RPC)	Port/RPC program	Identified service
TCP	9	discard
TCP	7	echo
TCP	21	ftp
TCP	443	http
TCP	119	nntp
TCP	111	PortMapper
TCP	22	ssh
UDP	7	echo
RPC	100024 version: 1	
RPC	100000 version: 2	PortMapper

Vulnerabilities

This section contains the vulnerabilities found in the assessment. The vulnerabilities are classified in 3 categories: high, medium and low risk.



High risk vulnerabilities classification

SecureScout classifies a high-risk vulnerability as any vulnerability that can unilaterally and directly (not combined with any other vulnerability) lead to compromise the host. Some examples of such compromises are vulnerabilities that allow theft, alteration or deletion of data, control over the host (such as but not limited to hacking into other machines or planting back doors), or execution of arbitrary code.



Medium risk vulnerabilities classification

SecureScout classifies a medium risk vulnerability as any vulnerability that can lead to the compromise of the host, but not by itself (see High Risk Vulnerability above for examples of how hosts are compromised). However, a medium risk vulnerability can be combined with at least one other medium vulnerability to compromise a host. Moreover, a medium risk vulnerability in conjunction with information gathered from several low risk vulnerabilities can lead to compromise a host. SecureScout regards denial of service attacks as medium risk vulnerabilities.



Low risk vulnerabilities classification

Low Risk Vulnerabilities make a host more susceptible to further compromise. (See High Risk Vulnerability above for examples of how hosts are compromised.) A typical low risk vulnerability is the provision of excessive information regarding the host or its environment. It is recommended that all vulnerabilities reported are checked, and at least all high and medium risk vulnerabilities should be corrected.

High risk vulnerabilities list

Name	Vulnerable Host
Microsoft IIS worms root.exe backdoor detected (CodeRed II)	24.47.44.82

Medium risk vulnerabilities list

Name	Vulnerable Host
discard/tcp Service is Running	24.47.44.82
echo/tcp Service is Running	24.47.44.82
echo/udp Service is running	24.47.44.82
HTTP Directory Listing	24.47.44.82
NNTP Available Banner Vulnerability	24.47.44.82
NNTP Reading is Possible Vulnerability	24.47.44.82
NNTP Unauthenticated Posting Allowed Vulnerability	24.47.44.82


Low risk vulnerabilities list


Name	Vulnerable Host
<u>Anonymous FTP Allowed</u>	24.47.44.82
<u>FTP Banner Exposure</u>	24.47.44.82
<u>HTTP Banner Exposure</u>	24.47.44.82
<u>SSH Information Obtained</u>	24.47.44.82
<u>TCP/IP Flag Combination Inconsistence Vulnerability</u>	24.47.44.82
<u>Traceroute Is Possible</u>	24.47.44.82


High risk vulnerabilities

	Microsoft IIS worms root.exe backdoor detected (CodeRed II)	CVE id	<u>GENERIC-MAP-NOMATCH</u>
		SecureScout id	<u>14212</u>
Description	<p>This worm uses the same mechanism as the original Code Red worm to infect vulnerable computers. That is, the worm looks for systems running IIS that have not patched the unchecked buffer vulnerability in idq.dll or removed the ISAPI script mappings. The worm exploits the vulnerability to inject itself into a system.</p> <p>Note that ANY system running Microsoft Windows 2000 (any version including Professional) may have a vulnerable IIS server installed.</p> <p>Code Red II is more dangerous because it opens backdoors on infected servers that allow any follow-on remote attacker to execute arbitrary commands. Several IIS worms place a copy of cmd.exe renamed root.exe in known executable directories like /scripts or /msadc.</p>		
Reference	<p>http://www.securityfocus.com/archive/75/201885 http://www.cert.org/advisories/CA-2001-11.html http://www.eeye.com/html/Research/Advisories/AL20010804.html</p>		
Solution	<p>The presence of this type of software indicates that the system was at some point fully compromised. In addition to removing the tool itself, you should seriously consider re-installing the system from scratch.</p>		
<p>Found on: 24.47.44.82 - Port: 443</p>			
<p>HTTP Server response for /scripts/root.exe?/c+dir+c:\ file contents: Directory of c: 01/27/2006 10:59p <DIR> agent 01/11/2006 01:10p <DIR> Documents and Settings 01/29/2006 06:17p 65 HPJIPP.dat 04/19/2006 07:16a <DIR> Inetpub 04/18/2006 06:56p <DIR> Microsoft UAM Volume 01/12/2006 07:01p 2,403 odbccconf.log 01/26/2006 08:16p <DIR> php 01/26/2006 07:34p 29,013 php.ini 03/23/2006 09:52a <DIR> Program Files 01/28/2006 08:21p <DIR> Python22 03/27/2006 09:41a 380 r.txt 01/28/2006 08:26p <DIR> rebrand 01/29/2006 06:17p <DIR> temp 04/18/2006 06:48a <DIR> WINNT 4 File(s) 31,861 bytes 10 Dir(s) 125,788,160 bytes free</p>			

Medium risk vulnerabilities

	discard/tcp Service is Running	CVE id	CAN-1999-0636
		SecureScout id	15040
Description	Discard/TCP was designed to debug TCP/IP. When a discard/TCP server (port 9) receives a packet, it just throws it away. No answer is returned. An attacker can use this service to waste the network bandwidth.		
Reference	Detailed description at http://www.cert.org/advisories/CA-1996-01.html on the CERT Web site For information about the discard service, see RFC 863 at http://www.ietf.org/rfc/rfc0863.txt on the IETF Web site		
Solution	UNIX systems: disable service in inetd. Windows NT: Microsoft recommends that you install Windows NT 4.0 Service Pack 4 (SP4) to correct this problem. However, if you don't use Simple TCP/IP Services (Chargen, echo, daytime, etc.), you can disable them: from the Start Menu, select Settings>Control Panel>Services, open Simple TCP/IP Services and choose Stop. Block port 9 on TCP protocol at the firewall.		
Found on: 24.47.44.82 - Port: 9			

	echo/tcp Service is Running	CVE id	CAN-1999-0635
			CVE-1999-0103
		SecureScout id	15036
Description	When an echo/TCP server (port 7) receives data segments, it sends back the content to the original sender. An attacker can use troubleshooting tools that send a flow of echo/TCP datagrams with spoofed and broadcast addresses. This can generate a storm on the network. And can also be used in Denial of Service attacks.		
Reference	For information about the echo service, see RFC 862 at http://www.ietf.org/rfc/rfc0862.txt on IETF Web site		
Solution	UNIX systems: disable service in inetd. Windows NT: Microsoft recommends that you install Windows NT 4.0 Service Pack 4 (SP4) to correct this problem. However, if you don't use Simple TCP/IP Services (Chargen, echo, daytime, etc.), you can disable them: from the Start Menu, select Settings>Control Panel>Services, open Simple TCP/IP Services and choose Stop. Block port 7 on TCP protocol at firewall.		
Found on: 24.47.44.82 - Port: 7			


	echo/udp Service is running	CVE id	CVE-1999-0103
			CAN-1999-0635
		SecureScout id	15030
Description	When an echo/UDP server (port 7) receives datagrams, it sends back the content to the original sender. An attacker can use troubleshooting tools that send a flow of echo/UDP datagrams with spoofed and broadcast addresses. This can generate a storm on the network. Can also be used in Denial of Service attacks.		
Reference	Detailed description at http://www.cert.org/advisories/CA-1996-01.html on the CERT		


	echo/udp Service is running	CVE id	CVE-1999-0103
			CAN-1999-0635
		SecureScout id	15030
	<p>Web site</p> <p>For information about this attack against Microsoft Windows NT, see the Q154460 article at http://support.microsoft.com/support/kb/articles/q154/4/60.asp on the Microsoft Web site</p> <p>For information about the echo service, see RFC 862 at http://www.ietf.org/rfc/rfc0862.txt on IETF Web site</p>		
Solution	<p>UNIX systems: disable service in inetd.</p> <p>Windows NT: Microsoft recommends that you install Windows NT4.0 Service Pack 4 (SP4) to correct this problem. However, if you don't use Simple TCP/IP Services (Chargen, echo, daytime, etc.), you can disable them: from the Start Menu, select Settings>Control Panel>Services, open Simple TCP/IP Services and choose Stop. Block port 7 on UDP protocol at firewall.</p>		
Found on: 24.47.44.82 - Port: 7			

	HTTP Directory Listing	CVE id	GENERIC-MAP-NOMATCH
			15013
		SecureScout id	15013
Description	<p>HTTP servers have a common feature: unless it is forbidden by explicit configuration, the server will return a directory listing when no default index file is present. This can give away valuable information to a potential intruder.</p>		
Reference	<p>See the section "Running a Secure Server" in the document "The World Wide Web Security FAQ" at http://www.w3.org/Security/faq/wwwsf2.html on the W3C Web site.</p>		
Solution	<p>Either install an index file such as index.html in every directory, or set up the Web server so that it is not in automatic directory listing mode.</p>		
Found on: 24.47.44.82 - Port: 443			
/_vti_bin directory is listable			
/images directory is listable			


	NNTP Available Banner Vulnerability	CVE id	CAN-1999-0655
			CAN-1999-0644
		SecureScout id	11205
Description	<p>An NNTP server is enabled on the target system.</p> <p>It is possible to retrieve useful information in its banner, that could be used for further attacks.</p>		
Reference	<p>The NNTP protocol is defined in RFC 977 http://www.ietf.org/rfc/rfc0977.txt</p>		
Solution	<p>Change the NNTP banner to avoid disclosure of sensitive information.</p>		
Found on: 24.47.44.82 - Port: 119			
200 NNTP Service 5.00.0984 Version: 5.0.2195.7034 Posting Allowed			


	NNTP Reading is Possible Vulnerability	CVE id	GENERIC-MAP-NOMATCH
			11206
		SecureScout id	11206
Description	<p>A NNTP server with read access is enabled on the target system.</p> <p>Private company information may be obtained and used by unauthorized users.</p>		


	NNTP Reading is Possible Vulnerability	CVE id	<u>GENERIC-MAP-NOMATCH</u>
		SecureScout id	<u>11206</u>
Reference	The NNTP protocol is defined in RFC 977 http://www.ietf.org/rfc/rfc0977.txt See also: http://www.mibsoftware.com/userkt/userkt.html		
Solution	Add an authentication mechanism (e.g. AUTHINFO command of the NNTP protocol). Add a wrapper to enforce authorized sources.		
Found on: 24.47.44.82 - Port: 119			


	NNTP Unauthenticated Posting Allowed Vulnerability	CVE id	<u>GENERIC-MAP-NOMATCH</u>
		SecureScout id	<u>11201</u>
Description	A NNTP server is enabled on the target system. It is used for Usenet News storing or any Intranet news hierarchy activity. It has been found that this NNTP allows posting from unauthenticated sources.		
Reference	The NNTP protocol is defined in RFC 977 http://www.ietf.org/rfc/rfc0977.txt See also: http://www.mibsoftware.com/userkt/userkt.html		
Solution	Add an authentication mechanism (e.g. AUTHINFO command of the NNTP protocol). Add a wrapper to enforce authorized sources.		
Found on: 24.47.44.82 - Port: 119			


Low risk vulnerabilities


	Anonymous FTP Allowed	CVE id	CAN-1999-0497
		SecureScout id	15006
Description	The target host accepts anonymous FTP connections, which allows unauthenticated users to retrieve files. This may be legitimate according to your security policy.		
Reference	CERT advisory: http://www.cert.org/advisories/CA-1993-10.html		
Solution	Disable anonymous FTP access if not required. Follow guidelines supplied by CERT.		
Found on: 24.47.44.82 - Port: 21			


	FTP Banner Exposure	CVE id	CAN-1999-0655
		SecureScout id	15019
Description	By opening an FTP connection to the target host, it is possible to retrieve information on the system that is running, and infer potential vulnerabilities.		
Reference	Some FTPD versions such as WU-FTPD have this feature; more at http://www.landfield.com/wu-ftp/newvirt/newvirt.html		
Solution	Change the FTP banner to a less informative message if possible.		
Found on: 24.47.44.82 - Port: 21			
220 sp-teacher Microsoft FTP Service (Version 5.0).			


	HTTP Banner Exposure	CVE id	CAN-1999-0655
		SecureScout id	15025
Description	The target host reveals an accurate Web server version. This may be used by attackers trying to exploit known vulnerabilities.		
Reference	Read section 10.14 of RFC 1945 http://www.ietf.org/rfc/rfc1945.txt		
Solution	Change (whenever possible) the Server: field returned in the HTTP header. RFC 1945 suggests it should be configurable.		
Found on: 24.47.44.82 - Port: 443			
HTTP server version: Microsoft-IIS/5.0			

	SSH Information Obtained	CVE id	GENERIC-MAP-NOMATCH
		SecureScout id	13078
Description	By connecting to the server and processing the received buffer, SSH Server's type and version are detected. This information could be used to mount an attack on the network.		
Reference	No reference		
Solution	Change the login banner to show less information.		
Found on: 24.47.44.82 - Port: 22			
SSH-2.0-OPENSSH_4.0			

	TCP/IP Flag Combination Inconsistence Vulnerability	CVE id	GENERIC-MAP-NOMATCH
		SecureScout id	12083
Description	The normal way to establish a TCP/IP connection to a server is to make three-way		

	TCP/IP Flag Combination Inconsistence Vulnerability	CVE id SecureScout id	<u>GENERIC-MAP-NOMATCH</u> <u>12083</u>
	handshake. First the client sends a SYN packet. The server answers with a SYN-ACK packet and the client finishes the connection establishment by sending an ACK. Some TCP/IP implementations are too liberal in the flags they accept during this packet exchange and they allow the handshake to complete even if other flags are also set. This can be used by attackers to bypass packet filtering and establish unauthorized connections.		
Reference	Initial advisory: http://www.securityfocus.com/archive/1/296122 TCP/IP implementations handle unusual flag combinations inconsistently: http://www.kb.cert.org/vuls/id/464113 TCP/IP RFC: http://www.ietf.org/rfc/rfc793.txt BID: http://www.securityfocus.com/bid/7487		
Solution	Upgrade your TCP/IP stack. A list of vulnerable products can be read at http://www.kb.cert.org/vuls/id/464113 . You should also consider using your firewall to filter out illegal packets.		
Found on: 24.47.44.82			
Vulnerable flag combinations: SYN/FIN , SYN/PSH , SYN/URG			

	Traceroute Is Possible	CVE id SecureScout id	<u>CAN-1999-0525</u> <u>11100</u>
Description	The traceroute application maps the route to the host. It releases information about the routing path, including names of intermediate routers and the internal IP addressing scheme.		
Reference	See detailed information in the Network administration services part in the book Building Internet Firewalls, Chapman - Zwicky, O'Reilly & Associates Inc.		
Solution	Traceroute must be available for machines exposed on the Internet. For machines on the internal network, filter all unused UDP ports from outside and traceroute replies from inside at the firewall. traceroute requests use UDP with port numbers generally >32768. traceroute replies can be TTL exceeded -type 11- messages on ICMP protocol, and Service unavailable -type 3- messages on ICMP protocol).		

	Traceroute Is Possible	CVE id	CAN-1999-0525
Found on: 24.47.44.82		SecureScout id	11100
<p>Traceroute to host 24.47.44.82:</p> <ul style="list-style-type: none">> 208.151.248.241 208.151.248.241> 206.103.54.187 206.103.54.187> ge1-0-0.cis025cor02.bea1.easy.easystreet.com 10.57.2.2> fe3-0.cis001bdr01.bea1.easy.easystreet.com 209.162.220.65> sl-gw7-sea-6-0-0.sprintlink.net 144.228.98.17> sl-bb20-sea-5-6.sprintlink.net 144.232.6.73> so-3-0-0.gar1.Seattle1.Level3.net 209.0.227.133> ae-31-55.ebr1.Seattle1.Level3.net 4.68.105.158> ae-1.ebr2.Seattle1.Level3.net 4.69.132.18> ae-2.ebr2.Denver1.Level3.net 4.69.132.54> ae-3.ebr1.Chicago1.Level3.net 4.69.132.62> ae-2.ebr2.NewYork1.Level3.net 4.69.132.66> ge-5-0-0-54.gar1.NewYork1.Level3.net 4.68.97.98> * * *> * * *> * * *> dstswr2-ge3-16.rh.stjmny.cv.net 167.206.39.134> ubr203-ge1-0-0.cmts.stjmny.cv.net 167.206.39.174> ool-182f2c52.dyn.optonline.net 24.47.44.82			