



scanist

Analysis Date	Wednesday - October 24, 2007
Type of Analysis	Technical Report
Scan Date(s)	Monday - September 10, 2007
Technical Attention Priority	18%
Security Threats Discovered	136 (Low risk and greater)
Severe Threats Discovered	45
Scanned By	EXTERNAL (140.99.20.85, 140.99.20.86)

Target Description

1.2.3.1, 1.2.3.4, 1.2.3.8, 1.2.3.14, 1.2.3.19, 1.2.3.24-1.2.3.26, 1.2.3.34, 1.2.3.44, 1.2.3.56, 1.2.3.59, 1.2.3.63, 1.2.3.67, 1.2.3.75, 1.2.3.112, 1.2.3.137, 1.2.3.139, 1.2.3.169, 1.2.3.177, 1.2.3.189, 1.2.3.192, 1.2.3.215, 1.2.3.234, 1.2.3.237, 1.2.3.247, 1.2.3.249

Executive Summary

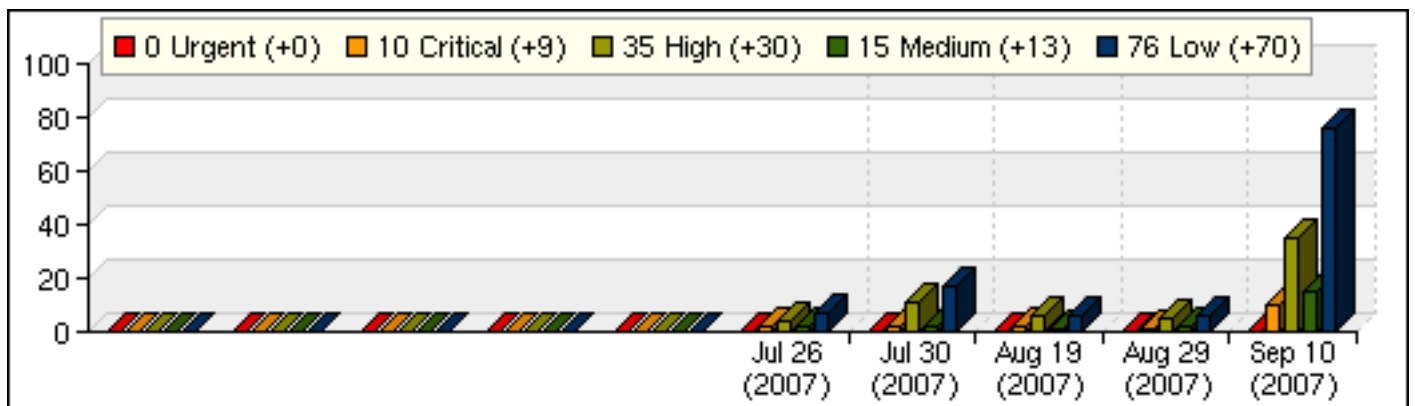
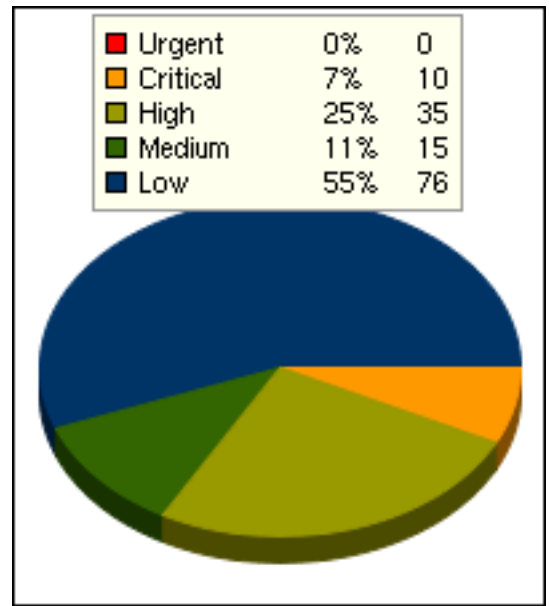
This document provides the results of the vulnerability assessment performed by Scanist. The information contained within this document is considered extremely confidential and should be treated as such.

The graph below represents the seriousness of the security threats found during the assessment. The higher the percentage, the higher the priority should be for resolving the discovered security threats.

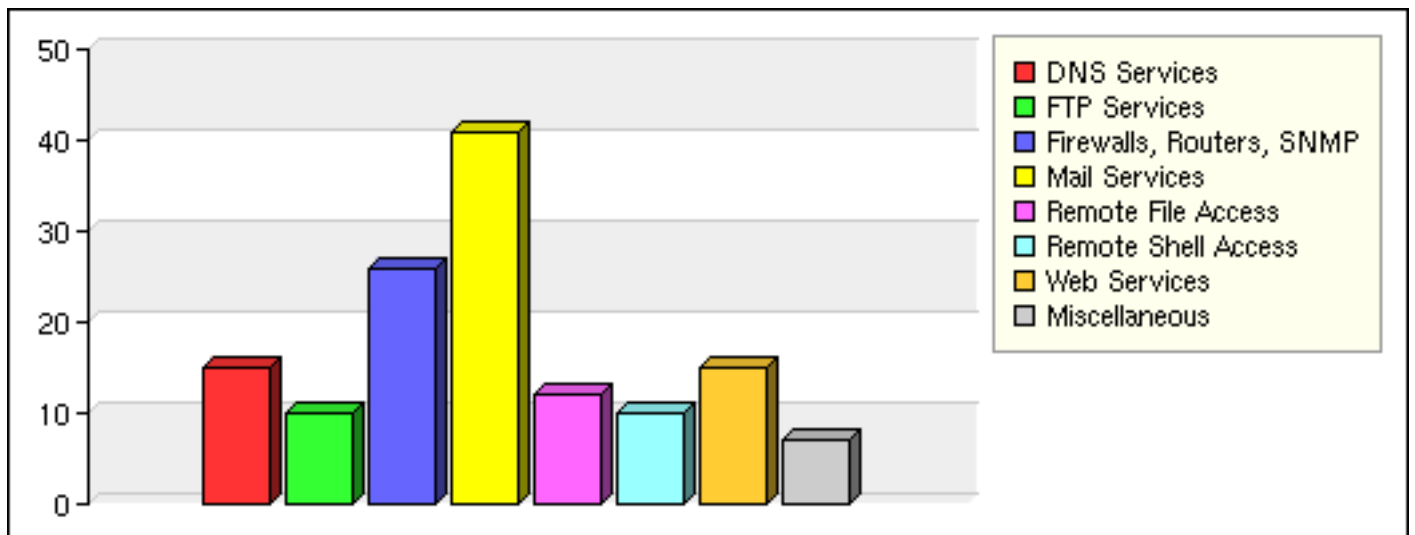


The scope of this analysis was to remotely audit and analyze the system and/or resources of each host in this assessment. This provides a "hacker's eye view" of the system to discover its security vulnerabilities and weaknesses to possible hacker penetration or attack. This assessment tested for 16810 different potential security vulnerabilities.

The graph below gives a historical perspective of the number of known security threats discovered for these hosts. Drastic changes indicate that something has impacted the security posture of these hosts and should be looked into immediately.



The chart below shows how the potential security threats are spread across different families of threat classifications. A large diversification of families (> 4) is cause for concern because these types of systems make for a more desirable target for potential attackers. A relatively minor threat in one service could help an attacker exploit a more difficult and significant threat in another service.



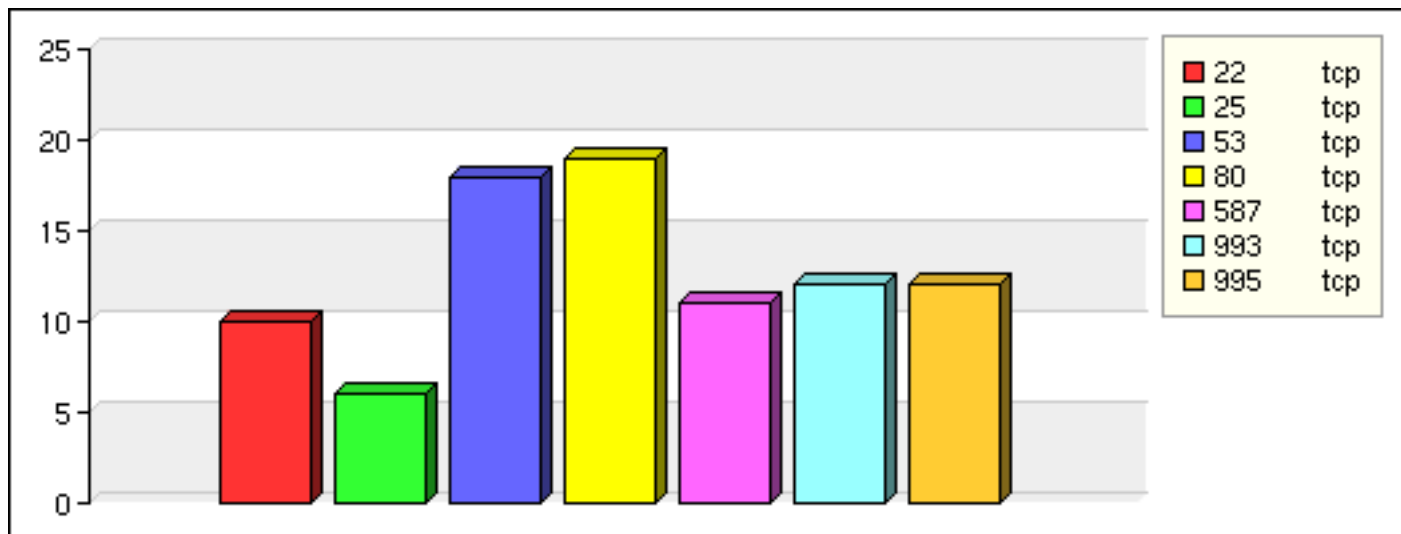
Vulnerable Hosts

This Scanist analysis scanned 27 total IP addresses. Of those, 27 hosts were found active with outstanding vulnerabilities or open ports. The following table provides a brief summary about each of these active hosts and their analysis data.

Scanner: EXTERNAL							
Host	Ports	Urgent	Critical	High	Medium	Low	Threats
1.2.3.215	5	0	1	3	1	5	10
1.2.3.24	5	0	1	2	1	5	9
1.2.3.177	5	0	1	2	1	5	9
1.2.3.14	3	0	1	2	1	3	7
1.2.3.137	3	0	1	2	1	2	6
1.2.3.44	3	0	1	2	0	3	6
1.2.3.34	5	0	1	1	1	3	6
1.2.3.4	4	0	1	1	1	4	7
1.2.3.247	3	0	1	1	1	3	6
1.2.3.139	2	0	0	3	1	0	4
1.2.3.169	6	0	1	0	0	5	6
1.2.3.234	5	0	0	2	1	4	7
1.2.3.249	6	0	0	1	1	4	6
1.2.3.237	6	0	0	1	0	6	7
1.2.3.56	2	0	0	2	0	2	4
1.2.3.192	4	0	0	1	1	4	6
1.2.3.1	1	0	0	2	0	0	2
1.2.3.189	1	0	0	2	0	0	2
1.2.3.26	2	0	0	1	1	1	3
1.2.3.19	2	0	0	1	0	2	3
1.2.3.25	2	0	0	1	0	2	3
1.2.3.63	2	0	0	1	0	2	3
1.2.3.75	2	0	0	1	0	2	3
1.2.3.59	3	0	0	0	1	3	4
1.2.3.8	3	0	0	0	1	2	3
1.2.3.112	2	0	0	0	0	3	3
1.2.3.67	1	0	0	0	0	1	1

Discovered Open Ports (Nmap)

This assessment discovered a total of 88 distinct open network ports on the hosts in this report. This does not mean each open port is a security threat, but it does show some possible points of entry to your network that an attacker could potentially leverage. It is generally considered good practice to keep the number of open ports to a minimum. Sometimes hackers will target computers with a large number of open network ports because they may be more susceptible to attack. Minimizing the number of open network ports will help to minimize this risk and make your network less "attractive" to hackers and attacks.



Number of Hosts vs. Open Ports

The following table shows a cross-reference of all discovered security threats by port number and risk factor. This analysis will help to determine which port represents the greatest overall risk to the target system. The most vulnerable port has been highlighted.

Host: 1.2.3.1 - ip-1.2.3.1.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
tcp	---	0	0	1	0	0	1
53 tcp	ISC BIND NONE	0	0	1	0	0	1

Host: 1.2.3.4 - ip-1.2.3.4.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
icmp	---	0	0	0	0	1	1
22 tcp	OPENSSSH 3.8.1P1 (PROTOCOL 2.0)	0	0	0	0	1	1
25 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
53 tcp	ISC BIND NONE	0	0	1	0	0	1
53 udp	---	0	1	0	0	0	1
80 tcp	APACHE HTTPD	0	0	0	1	1	2

Host: 1.2.3.8 - ip-1.2.3.8.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
80 tcp	APACHE HTTPD	0	0	0	1	0	1
587 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
995 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.14 - ip-1.2.3.14.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
icmp	---	0	0	0	0	1	1
tcp	---	0	0	1	0	0	1
53 tcp	ISC BIND NONE	0	0	1	0	0	1
53 udp	---	0	1	0	0	0	1
80 tcp	APACHE HTTPD	0	0	0	1	1	2
587 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1

Host: 1.2.3.19 - ip-1.2.3.19.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
tcp	---	0	0	1	0	0	1
25 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
993 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.24 - ip-1.2.3.24.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
icmp	---	0	0	0	0	1	1
tcp	---	0	0	2	0	0	2
53 tcp	ISC BIND NONE	0	0	0	0	0	0
53 udp	---	0	1	0	0	0	1
80 tcp	APACHE HTTPD	0	0	0	1	1	2
587 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
993 tcp	UW IMAPD 2003.339	0	0	0	0	1	1
995 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.25 - ip-1.2.3.25.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
tcp	---	0	0	1	0	0	1
80 tcp	APACHE HTTPD	0	0	0	0	1	1
995 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.26 - ip-1.2.3.26.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
tcp	---	0	0	1	0	0	1
80 tcp	APACHE HTTPD	0	0	0	1	0	1
995 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.34 - ip-1.2.3.34.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
22 tcp	OPENSSH 3.8.1P1 (PROTOCOL 2.0)	0	0	0	0	1	1
25 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
53 tcp	ISC BIND NONE	0	0	1	0	0	1
53 udp	---	0	1	0	0	0	1
80 tcp	APACHE HTTPD	0	0	0	1	0	1
995 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.44 - ip-1.2.3.44.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
icmp	---	0	0	0	0	1	1
tcp	---	0	0	1	0	0	1
22 tcp	OPENSSH 3.8.1P1 (PROTOCOL 2.0)	0	0	0	0	1	1
53 tcp	ISC BIND NONE	0	0	1	0	0	1
53 udp	---	0	1	0	0	0	1
993 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.56 - ip-1.2.3.56.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
icmp	---	0	0	0	0	1	1
tcp	---	0	0	1	0	0	1
53 tcp	ISC BIND NONE	0	0	1	0	0	1

587 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
---------	---------------------------------	---	---	---	---	---	---

Host: 1.2.3.59 - ip-1.2.3.59.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
icmp	---	0	0	0	0	1	1
80 tcp	APACHE HTTPD	0	0	0	1	0	1
587 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
995 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.63 - ip-1.2.3.63.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
icmp	---	0	0	0	0	1	1
53 tcp	ISC BIND NONE	0	0	1	0	0	1
80 tcp	APACHE HTTPD	0	0	0	0	1	1

Host: 1.2.3.67 - ip-1.2.3.67.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
993 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.75 - ip-1.2.3.75.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
tcp	---	0	0	1	0	0	1
22 tcp	OPENSSSH 3.8.1P1 (PROTOCOL 2.0)	0	0	0	0	1	1
993 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.112 - ip-1.2.3.112.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
icmp	---	0	0	0	0	1	1
587 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
993 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.137 - ip-1.2.3.137.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
------	--------------------------	--------	----------	------	--------	-----	-------

tcp	---	0	0	1	0	0	1
22 tcp	OPENSSSH 3.8.1P1 (PROTOCOL 2.0)	0	0	0	0	1	1
53 tcp	ISC BIND NONE	0	0	1	0	0	1
53 udp	---	0	1	0	0	0	1
80 tcp	APACHE HTTPD	0	0	0	1	1	2

Host: 1.2.3.139 - ip-1.2.3.139.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
tcp	---	0	0	2	0	0	2
53 tcp	ISC BIND NONE	0	0	1	0	0	1
80 tcp	APACHE HTTPD	0	0	0	1	0	1

Host: 1.2.3.169 - ip-1.2.3.169.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
22 tcp	OPENSSSH 3.8.1P1 (PROTOCOL 2.0)	0	0	0	0	1	1
53 tcp	ISC BIND NONE	0	0	0	0	0	0
53 udp	---	0	1	0	0	0	1
80 tcp	APACHE HTTPD	0	0	0	0	1	1
587 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
993 tcp	UW IMAPD 2003.339	0	0	0	0	1	1
995 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.177 - ip-1.2.3.177.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
icmp	---	0	0	0	0	1	1
tcp	---	0	0	1	0	0	1
53 tcp	ISC BIND NONE	0	0	1	0	0	1
53 udp	---	0	1	0	0	0	1
80 tcp	APACHE HTTPD	0	0	0	1	1	2
587 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
993 tcp	UW IMAPD 2003.339	0	0	0	0	1	1
995 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.189 - ip-1.2.3.189.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
tcp	---	0	0	1	0	0	1
53 tcp	ISC BIND NONE	0	0	1	0	0	1

Host: 1.2.3.192 - ip-1.2.3.192.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
tcp	---	0	0	1	0	0	1
22 tcp	OPENSSSH 3.8.1P1 (PROTOCOL 2.0)	0	0	0	0	1	1
80 tcp	APACHE HTTPD	0	0	0	1	1	2
587 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
995 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.215 - ip-1.2.3.215.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
icmp	---	0	0	0	0	1	1
tcp	---	0	0	2	0	0	2
22 tcp	OPENSSSH 3.8.1P1 (PROTOCOL 2.0)	0	0	0	0	1	1
53 tcp	ISC BIND NONE	0	0	1	0	0	1
53 udp	---	0	1	0	0	0	1
80 tcp	APACHE HTTPD	0	0	0	1	1	2
587 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
993 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.234 - ip-1.2.3.234.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
icmp	---	0	0	0	0	1	1
tcp	---	0	0	1	0	0	1
25 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
53 tcp	ISC BIND NONE	0	0	1	0	0	1
80 tcp	APACHE HTTPD	0	0	0	1	0	1
993 tcp	UW IMAPD 2003.339	0	0	0	0	1	1
995 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.237 - ip-1.2.3.237.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
icmp	---	0	0	0	0	1	1
22 tcp	OPENSSSH 3.8.1P1 (PROTOCOL 2.0)	0	0	0	0	1	1
25 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
53 tcp	ISC BIND NONE	0	0	1	0	0	1
80 tcp	APACHE HTTPD	0	0	0	0	1	1
993 tcp	UW IMAPD 2003.339	0	0	0	0	1	1
995 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Host: 1.2.3.247 - ip-1.2.3.247.www.scanist.com

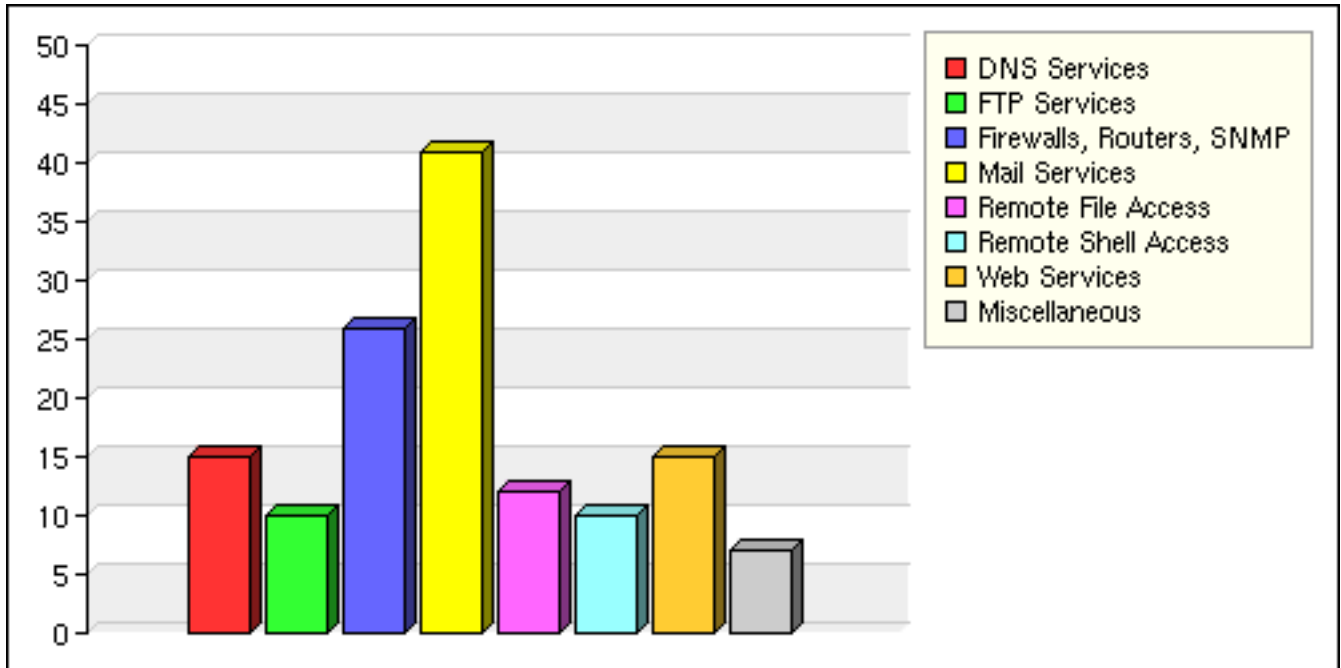
Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
icmp	---	0	0	0	0	1	1
tcp	---	0	0	1	0	0	1
25 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
53 tcp	ISC BIND NONE	0	0	0	0	0	0
53 udp	---	0	1	0	0	0	1
80 tcp	APACHE HTTPD	0	0	0	1	1	2

Host: 1.2.3.249 - ip-1.2.3.249.www.scanist.com

Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
22 tcp	OPENSSSH 3.8.1P1 (PROTOCOL 2.0)	0	0	0	0	1	1
53 tcp	ISC BIND NONE	0	0	1	0	0	1
80 tcp	APACHE HTTPD	0	0	0	1	0	1
587 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
993 tcp	UW IMAPD 2003.339	0	0	0	0	1	1
995 tcp	UW IMAPD 2003.339	0	0	0	0	1	1

Vulnerable Threat Families

The 136 total discovered vulnerabilities are spread across 8 families of threat classifications. The graph below shows the most frequently occurring threat families discovered on this network. Also, a complete list of every threat classification along with the number of vulnerabilities discovered is in the table below. The most vulnerable family has been highlighted.



Number of Discovered Threats vs. Family Classifications

Family	Urgent	Critical	High	Medium	Low	Total
DNS Services	0	0	15	0	0	15
FTP Services	0	10	0	0	0	10
Firewalls, Routers, SNMP	0	0	13	0	13	26
Mail Services	0	0	0	0	41	41
Miscellaneous	0	0	7	0	0	7
Remote File Access	0	0	0	0	12	12
Remote Shell Access	0	0	0	0	10	10
Web Services	0	0	0	15	0	15

Discovered Security Threat Summaries

This section provides a simple one-line summary of each discovered potential security threat on each host in this network. These summaries are grouped by host and sorted by risk factor. The full analysis report for each host is linked to the IP address.

Host: 1.2.3.1 - ip-1.2.3.1.www.scanist.com

Risk	Port	Protocol	ID	Summary
High	---	tcp	12213	TCP sequence number approximation
High	53	tcp	10595	DNS AXFR

Host: 1.2.3.4 - ip-1.2.3.4.www.scanist.com

Risk	Port	Protocol	ID	Summary
Critical	53	udp	11573	SmallFTP traversal
High	53	tcp	10595	DNS AXFR
Medium	80	tcp	11213	HTTP TRACE / TRACK Methods
Low	---	icmp	10114	icmp timestamp request
Low	22	tcp	10881	SSH protocol versions supported
Low	25	tcp	11421	smtpscan
Low	80	tcp	11419	Office files list

Host: 1.2.3.8 - ip-1.2.3.8.www.scanist.com

Risk	Port	Protocol	ID	Summary
Medium	80	tcp	11213	HTTP TRACE / TRACK Methods
Low	587	tcp	11421	smtpscan
Low	995	tcp	10185	POP Server Detection

Host: 1.2.3.14 - ip-1.2.3.14.www.scanist.com

Risk	Port	Protocol	ID	Summary
------	------	----------	----	---------

Critical	53	udp	11573	SmallFTP traversal
High	---	tcp	12213	TCP sequence number approximation
High	53	tcp	10595	DNS AXFR
Medium	80	tcp	11213	HTTP TRACE / TRACK Methods
Low	---	icmp	10114	icmp timestamp request
Low	80	tcp	11419	Office files list
Low	587	tcp	11421	smtpscan

Host: 1.2.3.19 - ip-1.2.3.19.www.scanist.com

Risk	Port	Protocol	ID	Summary
High	---	tcp	11618	Remote host replies to SYN+FIN
Low	25	tcp	11421	smtpscan
Low	993	tcp	11414	Get the IMAP Banner

Host: 1.2.3.24 - ip-1.2.3.24.www.scanist.com

Risk	Port	Protocol	ID	Summary
Critical	53	udp	11573	SmallFTP traversal
High	---	tcp	11618	Remote host replies to SYN+FIN
High	---	tcp	12213	TCP sequence number approximation
Medium	80	tcp	11213	HTTP TRACE / TRACK Methods
Low	---	icmp	10114	icmp timestamp request
Low	80	tcp	11419	Office files list
Low	587	tcp	11421	smtpscan
Low	993	tcp	11414	Get the IMAP Banner
Low	995	tcp	10185	POP Server Detection

Host: 1.2.3.25 - ip-1.2.3.25.www.scanist.com

Risk	Port	Protocol	ID	Summary
High	---	tcp	11618	Remote host replies to SYN+FIN
Low	80	tcp	11419	Office files list
Low	995	tcp	10185	POP Server Detection

Host: 1.2.3.26 - ip-1.2.3.26.www.scanist.com

Risk	Port	Protocol	ID	Summary
High	---	tcp	11618	Remote host replies to SYN+FIN
Medium	80	tcp	11213	HTTP TRACE / TRACK Methods
Low	995	tcp	10185	POP Server Detection

Host: 1.2.3.34 - ip-1.2.3.34.www.scanist.com

Risk	Port	Protocol	ID	Summary
Critical	53	udp	11573	SmallFTP traversal
High	53	tcp	10595	DNS AXFR
Medium	80	tcp	11213	HTTP TRACE / TRACK Methods
Low	22	tcp	10881	SSH protocol versions supported
Low	25	tcp	11421	smtpscan
Low	995	tcp	10185	POP Server Detection

Host: 1.2.3.44 - ip-1.2.3.44.www.scanist.com

Risk	Port	Protocol	ID	Summary
Critical	53	udp	11573	SmallFTP traversal
High	---	tcp	11618	Remote host replies to SYN+FIN
High	53	tcp	10595	DNS AXFR

Low	---	icmp	10114	icmp timestamp request
Low	22	tcp	10881	SSH protocol versions supported
Low	993	tcp	11414	Get the IMAP Banner

Host: 1.2.3.56 - ip-1.2.3.56.www.scanist.com

Risk	Port	Protocol	ID	Summary
High	---	tcp	11618	Remote host replies to SYN+FIN
High	53	tcp	10595	DNS AXFR
Low	---	icmp	10114	icmp timestamp request
Low	587	tcp	11421	smtpscan

Host: 1.2.3.59 - ip-1.2.3.59.www.scanist.com

Risk	Port	Protocol	ID	Summary
Medium	80	tcp	11213	HTTP TRACE / TRACK Methods
Low	---	icmp	10114	icmp timestamp request
Low	587	tcp	11421	smtpscan
Low	995	tcp	10185	POP Server Detection

Host: 1.2.3.63 - ip-1.2.3.63.www.scanist.com

Risk	Port	Protocol	ID	Summary
High	53	tcp	10595	DNS AXFR
Low	---	icmp	10114	icmp timestamp request
Low	80	tcp	11419	Office files list

Host: 1.2.3.67 - ip-1.2.3.67.www.scanist.com

Risk	Port	Protocol	ID	Summary
Low	993	tcp	11414	Get the IMAP Banner

Host: 1.2.3.75 - ip-1.2.3.75.www.scanist.com

Risk	Port	Protocol	ID	Summary
High	---	tcp	12213	TCP sequence number approximation
Low	22	tcp	10881	SSH protocol versions supported
Low	993	tcp	11414	Get the IMAP Banner

Host: 1.2.3.112 - ip-1.2.3.112.www.scanist.com

Risk	Port	Protocol	ID	Summary
Low	---	icmp	10114	icmp timestamp request
Low	587	tcp	11421	smtpscan
Low	993	tcp	11414	Get the IMAP Banner

Host: 1.2.3.137 - ip-1.2.3.137.www.scanist.com

Risk	Port	Protocol	ID	Summary
Critical	53	udp	11573	SmallFTP traversal
High	---	tcp	12213	TCP sequence number approximation
High	53	tcp	10595	DNS AXFR
Medium	80	tcp	11213	HTTP TRACE / TRACK Methods
Low	22	tcp	10881	SSH protocol versions supported
Low	80	tcp	11419	Office files list

Host: 1.2.3.139 - ip-1.2.3.139.www.scanist.com

Risk	Port	Protocol	ID	Summary
High	---	tcp	12213	TCP sequence number approximation
High	---	tcp	11618	Remote host replies to SYN+FIN
High	53	tcp	10595	DNS AXFR

Medium 80 tcp 11213 HTTP TRACE / TRACK Methods

Host: 1.2.3.169 - ip-1.2.3.169.www.scanist.com

Risk	Port	Protocol	ID	Summary
Critical	53	udp	11573	SmallFTP traversal
Low	22	tcp	10881	SSH protocol versions supported
Low	80	tcp	11419	Office files list
Low	587	tcp	11421	smtpscan
Low	993	tcp	11414	Get the IMAP Banner
Low	995	tcp	10185	POP Server Detection

Host: 1.2.3.177 - ip-1.2.3.177.www.scanist.com

Risk	Port	Protocol	ID	Summary
Critical	53	udp	11573	SmallFTP traversal
High	---	tcp	11618	Remote host replies to SYN+FIN
High	53	tcp	10595	DNS AXFR
Medium	80	tcp	11213	HTTP TRACE / TRACK Methods
Low	---	icmp	10114	icmp timestamp request
Low	80	tcp	11419	Office files list
Low	587	tcp	11421	smtpscan
Low	993	tcp	11414	Get the IMAP Banner
Low	995	tcp	10185	POP Server Detection

Host: 1.2.3.189 - ip-1.2.3.189.www.scanist.com

Risk	Port	Protocol	ID	Summary
High	---	tcp	11618	Remote host replies to SYN+FIN

High 53 tcp 10595 DNS AXFR

Host: 1.2.3.192 - ip-1.2.3.192.www.scanist.com

Risk	Port	Protocol	ID	Summary
High	---	tcp	11618	Remote host replies to SYN+FIN
Medium	80	tcp	11213	HTTP TRACE / TRACK Methods
Low	22	tcp	10881	SSH protocol versions supported
Low	80	tcp	11419	Office files list
Low	587	tcp	11421	smtpscan
Low	995	tcp	10185	POP Server Detection

Host: 1.2.3.215 - ip-1.2.3.215.www.scanist.com

Risk	Port	Protocol	ID	Summary
Critical	53	udp	11573	SmallFTP traversal
High	---	tcp	12213	TCP sequence number approximation
High	---	tcp	11618	Remote host replies to SYN+FIN
High	53	tcp	10595	DNS AXFR
Medium	80	tcp	11213	HTTP TRACE / TRACK Methods
Low	---	icmp	10114	icmp timestamp request
Low	22	tcp	10881	SSH protocol versions supported
Low	80	tcp	11419	Office files list
Low	587	tcp	11421	smtpscan
Low	993	tcp	11414	Get the IMAP Banner

Host: 1.2.3.234 - ip-1.2.3.234.www.scanist.com

Risk	Port	Protocol	ID	Summary
------	------	----------	----	---------

High	---	tcp	11618	Remote host replies to SYN+FIN
High	53	tcp	10595	DNS AXFR
Medium	80	tcp	11213	HTTP TRACE / TRACK Methods
Low	---	icmp	10114	icmp timestamp request
Low	25	tcp	11421	smtpscan
Low	993	tcp	11414	Get the IMAP Banner
Low	995	tcp	10185	POP Server Detection

Host: 1.2.3.237 - ip-1.2.3.237.www.scanist.com

Risk	Port	Protocol	ID	Summary
High	53	tcp	10595	DNS AXFR
Low	---	icmp	10114	icmp timestamp request
Low	22	tcp	10881	SSH protocol versions supported
Low	25	tcp	11421	smtpscan
Low	80	tcp	11419	Office files list
Low	993	tcp	11414	Get the IMAP Banner
Low	995	tcp	10185	POP Server Detection

Host: 1.2.3.247 - ip-1.2.3.247.www.scanist.com

Risk	Port	Protocol	ID	Summary
Critical	53	udp	11573	SmallFTP traversal
High	---	tcp	11618	Remote host replies to SYN+FIN
Medium	80	tcp	11213	HTTP TRACE / TRACK Methods
Low	---	icmp	10114	icmp timestamp request
Low	25	tcp	11421	smtpscan

Low 80 tcp 11419 Office files list

Host: 1.2.3.249 - ip-1.2.3.249.www.scanist.com

Risk	Port	Protocol	ID	Summary
High	53	tcp	10595	DNS AXFR
Medium	80	tcp	11213	HTTP TRACE / TRACK Methods
Low	22	tcp	10881	SSH protocol versions supported
Low	587	tcp	11421	smtpscan
Low	993	tcp	11414	Get the IMAP Banner
Low	995	tcp	10185	POP Server Detection

TCP/ICMP Echo (ping) Response

Although ping is sometimes considered a valuable network diagnostic tool, it can also sometimes be used for certain denial of service (DoS) attacks. You should consider the possible impact this may, or may not, have on your network resources.

The table below lists the packet loss and round-trip times (ms) for each host in this assessment. Non-zero packet loss is a sign of too much network traffic. A significant amount of packet loss may skew the results of the entire assessment. Please note, however, that hosts rejecting ICMP Echo and no ports are open packets will report 100% packet loss.

Host	Packet Loss	Min	Avg	Max
1.2.3.1 - ip-1.2.3.1.www.scanist.com	0%	118.3	122.2	126.0
1.2.3.4 - ip-1.2.3.4.www.scanist.com	0%	174.1	180.4	186.7
1.2.3.8 - ip-1.2.3.8.www.scanist.com	0%	50.4	97.6	144.8
1.2.3.14 - ip-1.2.3.14.www.scanist.com	100%	227.1	237.3	247.5
1.2.3.19 - ip-1.2.3.19.www.scanist.com	100%	249.8	258.0	266.2
1.2.3.24 - ip-1.2.3.24.www.scanist.com	0%	117.6	132.7	147.9
1.2.3.25 - ip-1.2.3.25.www.scanist.com	30%	131.6	175.0	218.4
1.2.3.26 - ip-1.2.3.26.www.scanist.com	0%	136.4	151.1	165.7
1.2.3.34 - ip-1.2.3.34.www.scanist.com	0%	185.7	211.4	237.2
1.2.3.44 - ip-1.2.3.44.www.scanist.com	0%	83.9	130.1	176.2
1.2.3.56 - ip-1.2.3.56.www.scanist.com	30%	98.6	104.2	109.8
1.2.3.59 - ip-1.2.3.59.www.scanist.com	0%	234.4	280.6	326.8
1.2.3.63 - ip-1.2.3.63.www.scanist.com	0%	69.3	114.8	160.4
1.2.3.67 - ip-1.2.3.67.www.scanist.com	0%	236.4	270.5	304.6
1.2.3.75 - ip-1.2.3.75.www.scanist.com	0%	242.6	273.1	303.6
1.2.3.112 - ip-1.2.3.112.www.scanist.com	0%	29.6	60.6	91.6
1.2.3.137 - ip-1.2.3.137.www.scanist.com	100%	177.8	204.1	230.4
1.2.3.139 - ip-1.2.3.139.www.scanist.com	0%	130.7	175.0	219.2
1.2.3.169 - ip-1.2.3.169.www.scanist.com	30%	102.2	110.4	118.6
1.2.3.177 - ip-1.2.3.177.www.scanist.com	0%	201.6	206.7	211.9
1.2.3.189 - ip-1.2.3.189.www.scanist.com	0%	152.8	154.9	157.0
1.2.3.192 - ip-1.2.3.192.www.scanist.com	0%	193.6	237.2	280.7
1.2.3.215 - ip-1.2.3.215.www.scanist.com	0%	118.7	145.2	171.7
1.2.3.234 - ip-1.2.3.234.www.scanist.com	0%	34.6	59.5	84.4
1.2.3.237 - ip-1.2.3.237.www.scanist.com	0%	148.2	150.6	153.0
1.2.3.247 - ip-1.2.3.247.www.scanist.com	0%	235.8	283.7	331.7
1.2.3.249 - ip-1.2.3.249.www.scanist.com	0%	28.5	68.1	107.8

Reverse DNS Information

Reverse DNS records are necessary for some network protocols and/or applications to function correctly. It is always a good idea to give an IP address a valid reverse DNS record, even if it is just a generic name within your domain. The results from attempting to resolve each host in this assessment are shown below.

IP Address	Reverse DNS	Resolved By	Authoritative Server
1.2.3.1	ip-1.2.3.1.www.scanist.com		ns1.isp.net.
1.2.3.4	ip-1.2.3.4.www.scanist.com		ns1.isp.net.
1.2.3.8	ip-1.2.3.8.www.scanist.com		ns1.isp.net.
1.2.3.14	ip-1.2.3.14.www.scanist.com		ns1.isp.net.
1.2.3.19	ip-1.2.3.19.www.scanist.com		ns1.isp.net.
1.2.3.24	ip-1.2.3.24.www.scanist.com		ns1.isp.net.
1.2.3.25	ip-1.2.3.25.www.scanist.com		ns1.isp.net.
1.2.3.26	ip-1.2.3.26.www.scanist.com		ns1.isp.net.
1.2.3.34	ip-1.2.3.34.www.scanist.com		ns1.isp.net.
1.2.3.44	ip-1.2.3.44.www.scanist.com		ns1.isp.net.
1.2.3.56	ip-1.2.3.56.www.scanist.com		ns1.isp.net.
1.2.3.59	ip-1.2.3.59.www.scanist.com		ns1.isp.net.
1.2.3.63	ip-1.2.3.63.www.scanist.com		ns1.isp.net.
1.2.3.67	ip-1.2.3.67.www.scanist.com		ns1.isp.net.
1.2.3.75	ip-1.2.3.75.www.scanist.com		ns1.isp.net.
1.2.3.112	ip-1.2.3.112.www.scanist.com		ns1.isp.net.
1.2.3.137	ip-1.2.3.137.www.scanist.com		ns1.isp.net.
1.2.3.139	ip-1.2.3.139.www.scanist.com		ns1.isp.net.
1.2.3.169	ip-1.2.3.169.www.scanist.com		ns1.isp.net.
1.2.3.177	ip-1.2.3.177.www.scanist.com		ns1.isp.net.
1.2.3.189	ip-1.2.3.189.www.scanist.com		ns1.isp.net.
1.2.3.192	ip-1.2.3.192.www.scanist.com		ns1.isp.net.
1.2.3.215	ip-1.2.3.215.www.scanist.com		ns1.isp.net.
1.2.3.234	ip-1.2.3.234.www.scanist.com		ns1.isp.net.
1.2.3.237	ip-1.2.3.237.www.scanist.com		ns1.isp.net.
1.2.3.247	ip-1.2.3.247.www.scanist.com		ns1.isp.net.
1.2.3.249	ip-1.2.3.249.www.scanist.com		ns1.isp.net.

Traceroute Response

The information below shows the round-trip times for each responsive hop between the scanner and target host in this assessment. This traceroute was performed using a maximum TTL value of 30, one UDP query per TTL, and a starting TTL of 5.

Host: 1.2.3.1 - ip-1.2.3.1.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	33.1
6	1.2.20.1	gw.phx1.puregig.net	6.0
7	1.2.11.100	gw3-4-56.phx1.puregig.net	13.6
8			5.2
9	1.2.3.1	gw-1.2.3.puregig.net	5.2
10	1.2.3.1	ip-1.2.3.1.www.scanist.com	92.5

Host: 1.2.3.4 - ip-1.2.3.4.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	24.8
6	1.2.20.1	gw.phx1.puregig.net	49.4
7	1.2.11.100	gw3-4-56.phx1.puregig.net	53.6
8			22.4
9	1.2.3.1	gw-1.2.3.puregig.net	89.7
10	1.2.3.4	ip-1.2.3.4.www.scanist.com	8.8

Host: 1.2.3.8 - ip-1.2.3.8.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	49.3
6	1.2.20.1	gw.phx1.puregig.net	2.4
7	1.2.11.100	gw3-4-56.phx1.puregig.net	51.0
8			27.3
9	1.2.3.1	gw-1.2.3.puregig.net	88.9
10	1.2.3.8	ip-1.2.3.8.www.scanist.com	72.1

Host: 1.2.3.14 - ip-1.2.3.14.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	20.4
6	1.2.20.1	gw.phx1.puregig.net	22.8
7	1.2.11.100	gw3-4-56.phx1.puregig.net	7.2
8			31.7
9	1.2.3.1	gw-1.2.3.puregig.net	76.7
10	1.2.3.14	ip-1.2.3.14.www.scanist.com	68.5

Host: 1.2.3.19 - ip-1.2.3.19.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	12.7
6	1.2.20.1	gw.phx1.puregig.net	36.4
7	1.2.11.100	gw3-4-56.phx1.puregig.net	16.5
8			38.2
9	1.2.3.1	gw-1.2.3.puregig.net	0.5
10	1.2.3.19	ip-1.2.3.19.www.scanist.com	74.7

Host: 1.2.3.24 - ip-1.2.3.24.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	0.7
6	1.2.20.1	gw.phx1.puregig.net	10.6
7	1.2.11.100	gw3-4-56.phx1.puregig.net	68.3
8			76.4
9	1.2.3.1	gw-1.2.3.puregig.net	5.1
10	1.2.3.24	ip-1.2.3.24.www.scanist.com	66.3

Host: 1.2.3.25 - ip-1.2.3.25.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	3.7
6	1.2.20.1	gw.phx1.puregig.net	56.4
7	1.2.11.100	gw3-4-56.phx1.puregig.net	61.6
8			13.9
9	1.2.3.1	gw-1.2.3.puregig.net	50.2
10	1.2.3.25	ip-1.2.3.25.www.scanist.com	61.9

Host: 1.2.3.26 - ip-1.2.3.26.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	19.2
6	1.2.20.1	gw.phx1.puregig.net	10.5
7	1.2.11.100	gw3-4-56.phx1.puregig.net	64.4
8			7.1
9	1.2.3.1	gw-1.2.3.puregig.net	65.5
10	1.2.3.26	ip-1.2.3.26.www.scanist.com	36.0

Host: 1.2.3.34 - ip-1.2.3.34.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	26.4
6	1.2.20.1	gw.phx1.puregig.net	48.8
7	1.2.11.100	gw3-4-56.phx1.puregig.net	18.3
8			28.3
9	1.2.3.1	gw-1.2.3.puregig.net	82.6
10	1.2.3.34	ip-1.2.3.34.www.scanist.com	68.4

Host: 1.2.3.44 - ip-1.2.3.44.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	4.0
6	1.2.20.1	gw.phx1.puregig.net	29.0
7	1.2.11.100	gw3-4-56.phx1.puregig.net	14.0
8			4.7
9	1.2.3.1	gw-1.2.3.puregig.net	59.7
10	1.2.3.44	ip-1.2.3.44.www.scanist.com	26.5

Host: 1.2.3.56 - ip-1.2.3.56.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	28.0
6	1.2.20.1	gw.phx1.puregig.net	20.5
7	1.2.11.100	gw3-4-56.phx1.puregig.net	43.6
8			38.9
9	1.2.3.1	gw-1.2.3.puregig.net	79.6
10	1.2.3.56	ip-1.2.3.56.www.scanist.com	45.2

Host: 1.2.3.59 - ip-1.2.3.59.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	3.9
6	1.2.20.1	gw.phx1.puregig.net	35.7
7	1.2.11.100	gw3-4-56.phx1.puregig.net	61.5
8			31.6
9	1.2.3.1	gw-1.2.3.puregig.net	84.3
10	1.2.3.59	ip-1.2.3.59.www.scanist.com	7.4

Host: 1.2.3.63 - ip-1.2.3.63.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	24.0
6	1.2.20.1	gw.phx1.puregig.net	37.1
7	1.2.11.100	gw3-4-56.phx1.puregig.net	40.9
8			73.6
9	1.2.3.1	gw-1.2.3.puregig.net	50.3
10	1.2.3.63	ip-1.2.3.63.www.scanist.com	59.4

Host: 1.2.3.67 - ip-1.2.3.67.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	44.4
6	1.2.20.1	gw.phx1.puregig.net	59.4
7	1.2.11.100	gw3-4-56.phx1.puregig.net	61.3
8			45.5
9	1.2.3.1	gw-1.2.3.puregig.net	34.4

Host: 1.2.3.75 - ip-1.2.3.75.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	7.2
6	1.2.20.1	gw.phx1.puregig.net	21.0
7	1.2.11.100	gw3-4-56.phx1.puregig.net	9.5
8			65.2
9	1.2.3.1	gw-1.2.3.puregig.net	43.2
10	1.2.3.75	ip-1.2.3.75.www.scanist.com	13.6

Host: 1.2.3.112 - ip-1.2.3.112.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	25.8
6	1.2.20.1	gw.phx1.puregig.net	57.6
7	1.2.11.100	gw3-4-56.phx1.puregig.net	4.5
8			51.2
9	1.2.3.1	gw-1.2.3.puregig.net	34.0
10	1.2.3.112	ip-1.2.3.112.www.scanist.com	54.5

Host: 1.2.3.137 - ip-1.2.3.137.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	9.9
6	1.2.20.1	gw.phx1.puregig.net	1.9
7	1.2.11.100	gw3-4-56.phx1.puregig.net	32.8
8			48.8
9	1.2.3.1	gw-1.2.3.puregig.net	9.5
10	1.2.3.137	ip-1.2.3.137.www.scanist.com	38.4

Host: 1.2.3.139 - ip-1.2.3.139.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	9.2
6	1.2.20.1	gw.phx1.puregig.net	3.5
7	1.2.11.100	gw3-4-56.phx1.puregig.net	51.2
8			76.8
9	1.2.3.1	gw-1.2.3.puregig.net	15.3
10	1.2.3.139	ip-1.2.3.139.www.scanist.com	76.2

Host: 1.2.3.169 - ip-1.2.3.169.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	4.3
6	1.2.20.1	gw.phx1.puregig.net	2.1

7	1.2.11.100	gw3-4-56.phx1.puregig.net	30.0
8			15.8
9	1.2.3.1	gw-1.2.3.puregig.net	60.3
10	1.2.3.169	ip-1.2.3.169.www.scanist.com	40.0

Host: 1.2.3.177 - ip-1.2.3.177.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	4.5
6	1.2.20.1	gw.phx1.puregig.net	50.2
7	1.2.11.100	gw3-4-56.phx1.puregig.net	52.5
8			20.9
9	1.2.3.1	gw-1.2.3.puregig.net	42.4
10	1.2.3.177	ip-1.2.3.177.www.scanist.com	11.6

Host: 1.2.3.189 - ip-1.2.3.189.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	16.3
6	1.2.20.1	gw.phx1.puregig.net	44.0
7	1.2.11.100	gw3-4-56.phx1.puregig.net	57.7
8			28.2
9	1.2.3.1	gw-1.2.3.puregig.net	28.7
10	1.2.3.189	ip-1.2.3.189.www.scanist.com	23.7

Host: 1.2.3.192 - ip-1.2.3.192.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	48.8
6	1.2.20.1	gw.phx1.puregig.net	17.7
7	1.2.11.100	gw3-4-56.phx1.puregig.net	7.7
8			50.0
9	1.2.3.1	gw-1.2.3.puregig.net	30.4
10	1.2.3.192	ip-1.2.3.192.www.scanist.com	30.1

Host: 1.2.3.215 - ip-1.2.3.215.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	15.0
6	1.2.20.1	gw.phx1.puregig.net	20.8
7	1.2.11.100	gw3-4-56.phx1.puregig.net	52.9
8			65.0
9	1.2.3.1	gw-1.2.3.puregig.net	88.3
10	1.2.3.215	ip-1.2.3.215.www.scanist.com	45.6

Host: 1.2.3.234 - ip-1.2.3.234.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
-----	------------	----------	-----------

5	1.2.20.110	gw2-7-100.phx1.puregig.net	28.9
6	1.2.20.1	gw.phx1.puregig.net	58.3
7	1.2.11.100	gw3-4-56.phx1.puregig.net	9.9
8			57.0
9	1.2.3.1	gw-1.2.3.puregig.net	57.1
10	1.2.3.234	ip-1.2.3.234.www.scanist.com	31.1

Host: 1.2.3.237 - ip-1.2.3.237.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	44.0
6	1.2.20.1	gw.phx1.puregig.net	36.7
7	1.2.11.100	gw3-4-56.phx1.puregig.net	16.6
8			4.6
9	1.2.3.1	gw-1.2.3.puregig.net	17.1
10	1.2.3.237	ip-1.2.3.237.www.scanist.com	10.4

Host: 1.2.3.247 - ip-1.2.3.247.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	18.5
6	1.2.20.1	gw.phx1.puregig.net	32.1
7	1.2.11.100	gw3-4-56.phx1.puregig.net	27.1
8			44.0
9	1.2.3.1	gw-1.2.3.puregig.net	52.0
10	1.2.3.247	ip-1.2.3.247.www.scanist.com	45.9

Host: 1.2.3.249 - ip-1.2.3.249.www.scanist.com

Hop	IP Address	Hostname	Time (ms)
5	1.2.20.110	gw2-7-100.phx1.puregig.net	9.7
6	1.2.20.1	gw.phx1.puregig.net	3.5
7	1.2.11.100	gw3-4-56.phx1.puregig.net	15.6
8			28.4
9	1.2.3.1	gw-1.2.3.puregig.net	60.3
10	1.2.3.249	ip-1.2.3.249.www.scanist.com	30.4

Discovered Security Threats Details

This section provides all the details about each discovered potential security threat for all of the hosts in this assessment. These details are grouped by host and ordered by risk factor.

Host: 1.2.3.1 - ip-1.2.3.1.www.scanist.com

TCP sequence number approximation

Risk	Port	Protocol	ID
High	---	tcp	12213

Family: Miscellaneous

Check for TCP approximations on the remote host

Security Warning|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.

This may cause problems for some dedicated services (BGP, a VPN over TCP, etc..).

Solution: See <http://www.securityfocus.com/bid/10183/solution/>

CVE: [CAN-2004-0230](#)

BugTraq ID: [10183](#)

Other references : OSVDB:4030, IAVA:2004-A-0007

DNS AXFR

Risk	Port	Protocol	ID
High	53	tcp	10595

Family: DNS Services

Determines if the remote name server allows zone transfers

Security Warning|The remote name server allows DNS zone transfers to be performed. A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

Host: 1.2.3.4 - ip-1.2.3.4.www.scanist.com

SmallFTP traversal

Risk	Port	Protocol	ID
------	------	----------	----

Family: FTP Services

Critical

53 udp

11573

Attempts to break out of the FTP root

The remote DNS server answers to queries for third party domains which do not have the recursion bit set.

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.

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...

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

DNS AXFR

Risk

Port Protocol

ID

Family: DNS Services

High

53 tcp

10595

Determines if the remote name server allows zone transfers

Security Warning|The remote name server allows DNS zone transfers to be performed.

A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

HTTP TRACE / TRACK Methods

Risk

Port Protocol

ID

Family: Web Services

Medium

80 tcp

11213

Test for TRACE / TRACK Methods

Security Warning|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>

icmp timestamp request

Risk	Port	Protocol	ID
Low	---	icmp	10114

Family: Firewalls, Routers, SNMP

Performs an ICMP timestamp request

Security Warning|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).

CVE: [CAN-1999-0524](#)

SSH protocol versions supported

Risk	Port	Protocol	ID
------	------	----------	----

Family: Remote Shell Access **Low** 22 tcp 10881
Negotiate SSHd connections

The remote SSH daemon supports the following versions of the SSH protocol :

- . 1.99
- . 2.0

SSHv2 host key fingerprint : 76:b8:68:fc:75:85:48:ba:56:f3:70:8c:af:da:ae:51

smtpscan	Risk	Port Protocol	ID
Family: Mail Services	Low	25 tcp	11421
SMTP server fingerprinting			

This server could be fingerprinted as being Sendmail 8.12.2

Office files list	Risk	Port Protocol	ID
Family: Remote File Access	Low	80 tcp	11419
Displays office files			

The following PDF files (.pdf) are available on the remote server :

- /Jay_Bio.pdf
- /Jay_Resume.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 to 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.

Host: 1.2.3.8 - ip-1.2.3.8.www.scanist.com

HTTP TRACE / TRACK Methods	Risk	Port Protocol	ID
Family: Web Services	Medium	80 tcp	11213
Test for TRACE / TRACK Methods			

Security Warning|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>

smtpscan	Risk	Port	Protocol	ID
Family: Mail Services SMTP server fingerprinting	Low	587	tcp	11421

This server could be fingerprinted as being Sendmail 8.12.2

POP Server Detection	Risk	Port	Protocol	ID
Family: Mail Services POP Server Detection	Low	995	tcp	10185

The remote POP3 server leaks information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy.

Versions and types should be omitted where possible.

The version of the remote POP3 server is :
+OK sample.report.com v2003.83 server ready

Solution: Change the login banner to something generic.

Host: 1.2.3.14 - ip-1.2.3.14.www.scanist.com

SmallFTP traversal

Family: FTP Services

Attempts to break out of the FTP root

Risk

Critical

Port Protocol

53 udp

ID

11573

The remote DNS server answers to queries for third party domains which do not have the recursion bit set.

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.

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...

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](http://community.sidestep.pt/~luis/DNS-Cache-Snooping/DNS%20Cache%20Snooping%201.1.pdf)

TCP sequence number approximation

Family: Miscellaneous

Check for TCP approximations on the remote host

Risk

High

Port Protocol

--- tcp

ID

12213

Security Warning|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.

This may cause problems for some dedicated services (BGP, a VPN over TCP, etc...).

Solution: See <http://www.securityfocus.com/bid/10183/solution/>

CVE: [CAN-2004-0230](#)

BugTraq ID: [10183](#)

Other references : OSVDB:4030, IAVA:2004-A-0007

DNS AXFR

Family: DNS Services

Determines if the remote name server allows zone transfers

Risk

High

Port Protocol

53 tcp

ID

10595

Security Warning|The remote name server allows DNS zone transfers to be performed. A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

HTTP TRACE / TRACK Methods

Family: Web Services

Test for TRACE / TRACK Methods

Risk

Medium

Port Protocol

80 tcp

ID

11213

Security Warning|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>

icmp timestamp request	Risk	Port	Protocol	ID
Family: Firewalls, Routers, SNMP	Low	---	icmp	10114
Performs an ICMP timestamp request				

Security Warning|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).

CVE: [CAN-1999-0524](#)

Office files list	Risk	Port	Protocol	ID
Family: Remote File Access	Low	80	tcp	11419
Displays office files				

The following PDF files (.pdf) are available on the remote server :

/Jay_Bio.pdf

/Jay_Resume.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 to 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.

smtpscan	Risk	Port	Protocol	ID
-----------------	-------------	-------------	-----------------	-----------

Family: Mail Services **Low** 587 tcp 11421
SMTP server fingerprinting

This server could be fingerprinted as being Sendmail 8.12.2

Host: 1.2.3.19 - ip-1.2.3.19.www.scanist.com

Remote host replies to SYN+FIN **Risk** **Port Protocol** **ID**
Family: Firewalls, Routers, SNMP **High** --- tcp 11618
Sends a SYN+FIN packet and expects a SYN+ACK

Security Warning|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

BugTraq ID: [7487](#)

smtpscan **Risk** **Port Protocol** **ID**
Family: Mail Services **Low** 25 tcp 11421
SMTP server fingerprinting

This server could be fingerprinted as being Sendmail 8.12.2

Get the IMAP Banner **Risk** **Port Protocol** **ID**
Family: Mail Services **Low** 993 tcp 11414
Grab and display the IMAP banner

The remote IMAP server banner is :

* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] sample.report.com IMAP4rev1 2003.339 at Sat, 16 Oct 2004 14:27:15 -0700 (MST)

Versions and types should be omitted where possible.

Change the imap banner to something generic.

Host: 1.2.3.24 - ip-1.2.3.24.www.scanist.com

SmallFTP traversal **Risk** **Port Protocol** **ID**

Family: FTP Services

Critical

53 udp

11573

Attempts to break out of the FTP root

The remote DNS server answers to queries for third party domains which do not have the recursion bit set.

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.

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...

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

Remote host replies to SYN+FIN

Risk

Port Protocol

ID

Family: Firewalls, Routers, SNMP

High

--- tcp

11618

Sends a SYN+FIN packet and expects a SYN+ACK

Security Warning|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

BugTraq ID: [7487](#)

TCP sequence number approximation

Risk

Port Protocol

ID

Family: Miscellaneous

High

--- tcp

12213

Check for TCP approximations on the remote host

Security Warning|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.

This may cause problems for some dedicated services (BGP, a VPN over TCP, etc...).

Solution: See <http://www.securityfocus.com/bid/10183/solution/>

CVE: [CAN-2004-0230](#)

BugTraq ID: [10183](#)

Other references : OSVDB:4030, IAVA:2004-A-0007

HTTP TRACE / TRACK Methods	Risk	Port Protocol	ID
Family: Web Services Test for TRACE / TRACK Methods	Medium	80 tcp	11213

Security Warning|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>

icmp timestamp request	Risk	Port	Protocol	ID
Family: Firewalls, Routers, SNMP Performs an ICMP timestamp request	Low	---	icmp	10114

Security Warning|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).

CVE: [CAN-1999-0524](#)

Office files list	Risk	Port	Protocol	ID
Family: Remote File Access Displays office files	Low	80	tcp	11419

The following PDF files (.pdf) are available on the remote server :

/Jay_Bio.pdf
/Jay_Resume.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 to 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.

smtpscan	Risk	Port	Protocol	ID
Family: Mail Services SMTP server fingerprinting	Low	587	tcp	11421

This server could be fingerprinted as being Sendmail 8.12.2

Get the IMAP Banner	Risk	Port	Protocol	ID
Family: Mail Services Grab and display the IMAP banner	Low	993	tcp	11414

The remote IMAP server banner is :

```
* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] sample.report.com IMAP4rev1
2003.339 at Sat, 16 Oct 2004 14:27:15 -0700 (MST)
```

Versions and types should be omitted where possible.

Change the imap banner to something generic.

POP Server Detection	Risk	Port	Protocol	ID
Family: Mail Services POP Server Detection	Low	995	tcp	10185

The remote POP3 server leaks information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy.

Versions and types should be omitted where possible.

The version of the remote POP3 server is :
+OK sample.report.com v2003.83 server ready

Solution: Change the login banner to something generic.

Host: 1.2.3.25 - ip-1.2.3.25.www.scanist.com

Remote host replies to SYN+FIN	Risk	Port	Protocol	ID
Family: Firewalls, Routers, SNMP Sends a SYN+FIN packet and expects a SYN+ACK	High	---	tcp	11618

Security Warning|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

BugTraq ID: [7487](#)

Office files list	Risk	Port	Protocol	ID
Family: Remote File Access Displays office files	Low	80	tcp	11419

The following PDF files (.pdf) are available on the remote server :
/Jay_Bio.pdf
/Jay_Resume.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 to 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.

POP Server Detection	Risk	Port	Protocol	ID
Family: Mail Services POP Server Detection	Low	995	tcp	10185

The remote POP3 server leaks information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy.

Versions and types should be omitted where possible.

The version of the remote POP3 server is :
+OK sample.report.com v2003.83 server ready

Solution: Change the login banner to something generic.

Host: 1.2.3.26 - ip-1.2.3.26.www.scanist.com

Remote host replies to SYN+FIN	Risk	Port	Protocol	ID
Family: Firewalls, Routers, SNMP Sends a SYN+FIN packet and expects a SYN+ACK	High	---	tcp	11618

Security Warning|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

BugTraq ID: [7487](#)

HTTP TRACE / TRACK Methods	Risk	Port	Protocol	ID
Family: Web Services Test for TRACE / TRACK Methods	Medium	80	tcp	11213

Security Warning|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>

POP Server Detection

Family: Mail Services
POP Server Detection

Risk	Port	Protocol	ID
Low	995	tcp	10185

The remote POP3 server leaks information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy.

Versions and types should be omitted where possible.

The version of the remote POP3 server is :

+OK sample.report.com v2003.83 server ready

Solution: Change the login banner to something generic.

Host: 1.2.3.34 - ip-1.2.3.34.www.scanist.com

SmallFTP traversal

Family: FTP Services

Attempts to break out of the FTP root

Risk	Port	Protocol	ID
Critical	53	udp	11573

The remote DNS server answers to queries for third party domains which do not have the recursion bit set.

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.

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...

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

DNS AXFR

Family: DNS Services

Determines if the remote name server allows zone transfers

Risk	Port	Protocol	ID
High	53	tcp	10595

Security Warning|The remote name server allows DNS zone transfers to be performed. A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

HTTP TRACE / TRACK Methods

Risk	Port	Protocol	ID
------	------	----------	----

Test for TRACE / TRACK Methods

Security Warning|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>

SSH protocol versions supported

Family: Remote Shell Access

Negotiate SSHd connections

Risk

Low

Port Protocol

22 tcp

ID

10881

The remote SSH daemon supports the following versions of the SSH protocol :

. 1.99
. 2.0

SSHv2 host key fingerprint : 76:b8:68:fc:75:85:48:ba:56:f3:70:8c:af:da:ae:51

smtpscan	Risk	Port	Protocol	ID
Family: Mail Services SMTP server fingerprinting	Low	25	tcp	11421

This server could be fingerprinted as being Sendmail 8.12.2

POP Server Detection	Risk	Port	Protocol	ID
Family: Mail Services POP Server Detection	Low	995	tcp	10185

The remote POP3 server leaks information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy.

Versions and types should be omitted where possible.

The version of the remote POP3 server is :
+OK sample.report.com v2003.83 server ready

Solution: Change the login banner to something generic.

Host: 1.2.3.44 - ip-1.2.3.44.www.scanist.com

SmallFTP traversal	Risk	Port	Protocol	ID
Family: FTP Services Attempts to break out of the FTP root	Critical	53	udp	11573

The remote DNS server answers to queries for third party domains which do not have the recursion bit set.

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.

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...

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

Remote host replies to SYN+FIN

Risk	Port	Protocol	ID
High	---	tcp	11618

Family: Firewalls, Routers, SNMP

Sends a SYN+FIN packet and expects a SYN+ACK

Security Warning|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

BugTraq ID: [7487](#)

DNS AXFR

Risk	Port	Protocol	ID
High	53	tcp	10595

Family: DNS Services

Determines if the remote name server allows zone transfers

Security Warning|The remote name server allows DNS zone transfers to be performed. A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

icmp timestamp request

Risk	Port	Protocol	ID
Low	---	icmp	10114

Family: Firewalls, Routers, SNMP

Performs an ICMP timestamp request

Security Warning|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).

CVE: [CAN-1999-0524](#)

SSH protocol versions supported	Risk	Port	Protocol	ID
Family: Remote Shell Access Negotiate SSHd connections	Low	22	tcp	10881

The remote SSH daemon supports the following versions of the SSH protocol :

- . 1.99
- . 2.0

SShv2 host key fingerprint : 76:b8:68:fc:75:85:48:ba:56:f3:70:8c:af:da:ae:51

Get the IMAP Banner	Risk	Port	Protocol	ID
Family: Mail Services Grab and display the IMAP banner	Low	993	tcp	11414

The remote IMAP server banner is :

```
* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] sample.report.com IMAP4rev1
2003.339 at Sat, 16 Oct 2004 14:27:15 -0700 (MST)
Versions and types should be omitted where possible.
```

Change the imap banner to something generic.

Host: 1.2.3.56 - ip-1.2.3.56.www.scanist.com

Remote host replies to SYN+FIN	Risk	Port	Protocol	ID
Family: Firewalls, Routers, SNMP Sends a SYN+FIN packet and expects a SYN+ACK	High	---	tcp	11618

Security Warning|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

BugTraq ID: [7487](#)

DNS AXFR**Family:** DNS Services

Determines if the remote name server allows zone transfers

Risk	Port	Protocol	ID
High	53	tcp	10595

Security Warning|The remote name server allows DNS zone transfers to be performed.

A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

icmp timestamp request**Family:** Firewalls, Routers, SNMP

Performs an ICMP timestamp request

Risk	Port	Protocol	ID
Low	---	icmp	10114

Security Warning|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).

CVE: [CAN-1999-0524](#)

smtpscan**Family:** Mail Services

SMTP server fingerprinting

Risk	Port	Protocol	ID
Low	587	tcp	11421

This server could be fingerprinted as being Sendmail 8.12.2

Host: 1.2.3.59 - ip-1.2.3.59.www.scanist.com

HTTP TRACE / TRACK Methods**Family:** Web Services

Test for TRACE / TRACK Methods

Risk	Port	Protocol	ID
Medium	80	tcp	11213

Security Warning|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>

icmp timestamp request

Family: Firewalls, Routers, SNMP
Performs an ICMP timestamp request

Risk	Port	Protocol	ID
Low	---	icmp	10114

Security Warning|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).

CVE: [CAN-1999-0524](#)

smtpscan	Risk	Port	Protocol	ID
Family: Mail Services SMTP server fingerprinting	Low	587	tcp	11421

This server could be fingerprinted as being Sendmail 8.12.2

POP Server Detection	Risk	Port	Protocol	ID
Family: Mail Services POP Server Detection	Low	995	tcp	10185

The remote POP3 server leaks information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy.

Versions and types should be omitted where possible.

The version of the remote POP3 server is :
+OK sample.report.com v2003.83 server ready

Solution: Change the login banner to something generic.

Host: 1.2.3.63 - ip-1.2.3.63.www.scanist.com

DNS AXFR	Risk	Port	Protocol	ID
Family: DNS Services Determines if the remote name server allows zone transfers	High	53	tcp	10595

Security Warning|The remote name server allows DNS zone transfers to be performed. A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

icmp timestamp request	Risk	Port	Protocol	ID
-------------------------------	-------------	-------------	-----------------	-----------

Family: Firewalls, Routers, SNMP
Performs an ICMP timestamp request

Low --- icmp 10114

Security Warning|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).

CVE: [CAN-1999-0524](#)

Office files list

Family: Remote File Access
Displays office files

Risk	Port	Protocol	ID
Low	80	tcp	11419

The following PDF files (.pdf) are available on the remote server :

/Jay_Bio.pdf
/Jay_Resume.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 to 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.

Host: 1.2.3.67 - ip-1.2.3.67.www.scanist.com

Get the IMAP Banner

Family: Mail Services
Grab and display the IMAP banner

Risk	Port	Protocol	ID
Low	993	tcp	11414

The remote IMAP server banner is :

```
* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] sample.report.com IMAP4rev1
2003.339 at Sat, 16 Oct 2004 14:27:15 -0700 (MST)
Versions and types should be omitted where possible.
```

Change the imap banner to something generic.

Host: 1.2.3.75 - ip-1.2.3.75.www.scanist.com

TCP sequence number approximation

Risk	Port	Protocol	ID
------	------	----------	----

Family: Miscellaneous

High

--- tcp

12213

Check for TCP approximations on the remote host

Security Warning|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.

This may cause problems for some dedicated services (BGP, a VPN over TCP, etc...).

Solution: See <http://www.securityfocus.com/bid/10183/solution/>

CVE: [CAN-2004-0230](#)

BugTraq ID: [10183](#)

Other references : OSVDB:4030, IAVA:2004-A-0007

SSH protocol versions supported

Family: Remote Shell Access

Negotiate SSHd connections

Risk

Low

Port Protocol

22 tcp

ID

10881

The remote SSH daemon supports the following versions of the SSH protocol :

- . 1.99
- . 2.0

SSHv2 host key fingerprint : 76:b8:68:fc:75:85:48:ba:56:f3:70:8c:af:da:ae:51

Get the IMAP Banner

Family: Mail Services

Grab and display the IMAP banner

Risk

Low

Port Protocol

993 tcp

ID

11414

The remote IMAP server banner is :

* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] sample.report.com IMAP4rev1 2003.339 at Sat, 16 Oct 2004 14:27:15 -0700 (MST)

Versions and types should be omitted where possible.

Change the imap banner to something generic.

Host: 1.2.3.112 - ip-1.2.3.112.www.scanist.com

icmp timestamp request

Family: Firewalls, Routers, SNMP

Performs an ICMP timestamp request

Risk

Low

Port Protocol

--- icmp

ID

10114

Security Warning|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).

CVE: [CAN-1999-0524](#)

smtpscan	Risk	Port	Protocol	ID
Family: Mail Services SMTP server fingerprinting	Low	587	tcp	11421

This server could be fingerprinted as being Sendmail 8.12.2

Get the IMAP Banner	Risk	Port	Protocol	ID
Family: Mail Services Grab and display the IMAP banner	Low	993	tcp	11414

The remote IMAP server banner is :

```
* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] sample.report.com IMAP4rev1 2003.339 at Sat, 16 Oct 2004 14:27:15 -0700 (MST)
```

Versions and types should be omitted where possible.

Change the imap banner to something generic.

Host: 1.2.3.137 - ip-1.2.3.137.www.scanist.com

SmallFTP traversal	Risk	Port	Protocol	ID
Family: FTP Services Attempts to break out of the FTP root	Critical	53	udp	11573

The remote DNS server answers to queries for third party domains which do not have the recursion bit set.

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.

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...

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](http://community.sidestep.pt/~luis/DNS-Cache-Snooping/DNS%20Cache%20Snooping%201.1.pdf)

TCP sequence number approximation

Risk	Port	Protocol	ID
High	---	tcp	12213

Family: Miscellaneous

Check for TCP approximations on the remote host

Security Warning|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.

This may cause problems for some dedicated services (BGP, a VPN over TCP, etc...).

Solution: See <http://www.securityfocus.com/bid/10183/solution/>

CVE: [CAN-2004-0230](#)

BugTraq ID: [10183](#)

Other references : OSVDB:4030, IAVA:2004-A-0007

DNS AXFR

Risk	Port	Protocol	ID
High	53	tcp	10595

Family: DNS Services

Determines if the remote name server allows zone transfers

Security Warning|The remote name server allows DNS zone transfers to be performed. A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

HTTP TRACE / TRACK Methods

Risk	Port	Protocol	ID
Medium	80	tcp	11213

Family: Web Services

Test for TRACE / TRACK Methods

Security Warning|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>

SSH protocol versions supported

Family: Remote Shell Access
Negotiate SSHd connections

Risk	Port	Protocol	ID
Low	22	tcp	10881

The remote SSH daemon supports the following versions of the SSH protocol :

- . 1.99
- . 2.0

SSHv2 host key fingerprint : 76:b8:68:fc:75:85:48:ba:56:f3:70:8c:af:da:ae:51

Office files list

Risk	Port	Protocol	ID
------	------	----------	----

Family: Remote File Access

Low

80 tcp

11419

Displays office files

The following PDF files (.pdf) are available on the remote server :

/Jay_Bio.pdf

/Jay_Resume.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 to 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.

Host: 1.2.3.139 - ip-1.2.3.139.www.scanist.com

TCP sequence number approximation

Risk

Port Protocol

ID

Family: Miscellaneous

High

--- tcp

12213

Check for TCP approximations on the remote host

Security Warning|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.

This may cause problems for some dedicated services (BGP, a VPN over TCP, etc..).

Solution: See <http://www.securityfocus.com/bid/10183/solution/>

CVE: [CAN-2004-0230](#)

BugTraq ID: [10183](#)

Other references : OSVDB:4030, IAVA:2004-A-0007

Remote host replies to SYN+FIN

Risk

Port Protocol

ID

Family: Firewalls, Routers, SNMP

High

--- tcp

11618

Sends a SYN+FIN packet and expects a SYN+ACK

Security Warning|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

BugTraq ID: [7487](#)

DNS AXFR	Risk	Port	Protocol	ID
Family: DNS Services	High	53	tcp	10595

Determines if the remote name server allows zone transfers

Security Warning|The remote name server allows DNS zone transfers to be performed. A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

HTTP TRACE / TRACK Methods	Risk	Port	Protocol	ID
Family: Web Services	Medium	80	tcp	11213

Test for TRACE / TRACK Methods

Security Warning|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>

Host: 1.2.3.169 - ip-1.2.3.169.www.scanist.com

SmallFTP traversal	Risk	Port	Protocol	ID
Family: FTP Services Attempts to break out of the FTP root	Critical	53	udp	11573

The remote DNS server answers to queries for third party domains which do not have the recursion bit set.

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.

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...

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

SSH protocol versions supported	Risk	Port	Protocol	ID
--	-------------	-------------	-----------------	-----------

Family: Remote Shell Access **Risk** Low **Port** 22 **Protocol** tcp **ID** 10881
Negotiate SSHd connections

The remote SSH daemon supports the following versions of the SSH protocol :

- . 1.99
- . 2.0

SSHv2 host key fingerprint : 76:b8:68:fc:75:85:48:ba:56:f3:70:8c:af:da:ae:51

Office files list **Risk** **Port** **Protocol** **ID**
Family: Remote File Access **Low** 80 tcp 11419
Displays office files

The following PDF files (.pdf) are available on the remote server :

- /Jay_Bio.pdf
- /Jay_Resume.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 to 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.

smtpscan **Risk** **Port** **Protocol** **ID**
Family: Mail Services **Low** 587 tcp 11421
SMTP server fingerprinting

This server could be fingerprinted as being Sendmail 8.12.2

Get the IMAP Banner **Risk** **Port** **Protocol** **ID**
Family: Mail Services **Low** 993 tcp 11414
Grab and display the IMAP banner

The remote IMAP server banner is :

* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] sample.report.com IMAP4rev1
2003.339 at Sat, 16 Oct 2004 14:27:15 -0700 (MST)
Versions and types should be omitted where possible.

Change the imap banner to something generic.

POP Server Detection **Risk** **Port** **Protocol** **ID**

Family: Mail Services
POP Server Detection

Low

995 tcp

10185

The remote POP3 server leaks information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy.

Versions and types should be omitted where possible.

The version of the remote POP3 server is :
+OK sample.report.com v2003.83 server ready

Solution: Change the login banner to something generic.

Host: 1.2.3.177 - ip-1.2.3.177.www.scanist.com

SmallFTP traversal

Family: FTP Services

Attempts to break out of the FTP root

Risk

Critical

Port Protocol

53 udp

ID

11573

The remote DNS server answers to queries for third party domains which do not have the recursion bit set.

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.

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...

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

Remote host replies to SYN+FIN

Family: Firewalls, Routers, SNMP

Sends a SYN+FIN packet and expects a SYN+ACK

Risk

High

Port Protocol

--- tcp

ID

11618

Security Warning|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

BugTraq ID: [7487](#)

DNS AXFR

	Risk	Port	Protocol	ID
Family: DNS Services	High	53	tcp	10595

Determines if the remote name server allows zone transfers

Security Warning|The remote name server allows DNS zone transfers to be performed. A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

HTTP TRACE / TRACK Methods

	Risk	Port	Protocol	ID
Family: Web Services	Medium	80	tcp	11213

Test for TRACE / TRACK Methods

Security Warning|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>

icmp timestamp request

Family: Firewalls, Routers, SNMP
Performs an ICMP timestamp request

Risk	Port	Protocol	ID
Low	---	icmp	10114

Security Warning|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).

CVE: [CAN-1999-0524](#)

Office files list

Family: Remote File Access
Displays office files

Risk	Port	Protocol	ID
Low	80	tcp	11419

The following PDF files (.pdf) are available on the remote server :

/Jay_Bio.pdf

/Jay_Resume.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 to 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.

smtpscan

Family: Mail Services
SMTP server fingerprinting

Risk	Port	Protocol	ID
Low	587	tcp	11421

This server could be fingerprinted as being Sendmail 8.12.2

Get the IMAP Banner

Family: Mail Services
Grab and display the IMAP banner

Risk	Port	Protocol	ID
Low	993	tcp	11414

The remote IMAP server banner is :

```
* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] sample.report.com IMAP4rev1 2003.339 at Sat, 16 Oct 2004 14:27:15 -0700 (MST)
```

Versions and types should be omitted where possible.

Change the imap banner to something generic.

POP Server Detection

Family: Mail Services
POP Server Detection

Risk	Port	Protocol	ID
Low	995	tcp	10185

The remote POP3 server leaks information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy.

Versions and types should be omitted where possible.

The version of the remote POP3 server is :

```
+OK sample.report.com v2003.83 server ready
```

Solution: Change the login banner to something generic.

Host: 1.2.3.189 - ip-1.2.3.189.www.scanist.com

Remote host replies to SYN+FIN

Family: Firewalls, Routers, SNMP
Sends a SYN+FIN packet and expects a SYN+ACK

Risk	Port	Protocol	ID
High	---	tcp	11618

Security Warning|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/bugtrag/2002-10/0266.html>

<http://www.kb.cert.org/vuls/id/464113>

Solution: Contact your vendor for a patch

BugTraq ID: [7487](#)

DNS AXFR	Risk	Port	Protocol	ID
Family: DNS Services Determines if the remote name server allows zone transfers	High	53	tcp	10595

Security Warning|The remote name server allows DNS zone transfers to be performed. A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

Host: 1.2.3.192 - ip-1.2.3.192.www.scanist.com

Remote host replies to SYN+FIN	Risk	Port	Protocol	ID
Family: Firewalls, Routers, SNMP Sends a SYN+FIN packet and expects a SYN+ACK	High	---	tcp	11618

Security Warning|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

BugTraq ID: [7487](#)

HTTP TRACE / TRACK Methods	Risk	Port	Protocol	ID
----------------------------	------	------	----------	----

Test for TRACE / TRACK Methods

Security Warning|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>

SSH protocol versions supported

Family: Remote Shell Access

Negotiate SSHd connections

Risk

Low

Port Protocol

22 tcp

ID

10881

The remote SSH daemon supports the following versions of the SSH protocol :

. 1.99
. 2.0

SSHv2 host key fingerprint : 76:b8:68:fc:75:85:48:ba:56:f3:70:8c:af:da:ae:51

Office files list	Risk	Port	Protocol	ID
Family: Remote File Access Displays office files	Low	80	tcp	11419

The following PDF files (.pdf) are available on the remote server :

/Jay_Bio.pdf
/Jay_Resume.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 to 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.

smtpscan	Risk	Port	Protocol	ID
Family: Mail Services SMTP server fingerprinting	Low	587	tcp	11421

This server could be fingerprinted as being Sendmail 8.12.2

POP Server Detection	Risk	Port	Protocol	ID
Family: Mail Services POP Server Detection	Low	995	tcp	10185

The remote POP3 server leaks information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy.

Versions and types should be omitted where possible.

The version of the remote POP3 server is :
+OK sample.report.com v2003.83 server ready

Solution: Change the login banner to something generic.

Host: 1.2.3.215 - ip-1.2.3.215.www.scanist.com

SmallFTP traversal	Risk	Port	Protocol	ID
<p>Family: FTP Services</p> <p>Attempts to break out of the FTP root</p> <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>	Critical	53	udp	11573

TCP sequence number approximation	Risk	Port	Protocol	ID
<p>Family: Miscellaneous</p> <p>Check for TCP approximations on the remote host</p> <p>Security Warning 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/</p> <p>CVE: CAN-2004-0230</p> <p>BugTraq ID: 10183</p> <p>Other references : OSVDB:4030, IAVA:2004-A-0007</p>	High	---	tcp	12213

Remote host replies to SYN+FIN	Risk	Port	Protocol	ID
<p>Family: Firewalls, Routers, SNMP</p> <p>Sends a SYN+FIN packet and expects a SYN+ACK</p> <p>Security Warning 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</p>	High	---	tcp	11618

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

BugTraq ID: [7487](#)

DNS AXFR

	Risk	Port	Protocol	ID
Family: DNS Services	High	53	tcp	10595
Determines if the remote name server allows zone transfers				

Security Warning|The remote name server allows DNS zone transfers to be performed. A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

HTTP TRACE / TRACK Methods

	Risk	Port	Protocol	ID
Family: Web Services	Medium	80	tcp	11213
Test for TRACE / TRACK Methods				

Security Warning|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>

icmp timestamp request

Family: Firewalls, Routers, SNMP

Performs an ICMP timestamp request

Risk	Port	Protocol	ID
Low	---	icmp	10114

Security Warning|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).

CVE: [CAN-1999-0524](#)

SSH protocol versions supported

Family: Remote Shell Access

Negotiate SSHd connections

Risk	Port	Protocol	ID
Low	22	tcp	10881

The remote SSH daemon supports the following versions of the SSH protocol :

. 1.99

. 2.0

SShv2 host key fingerprint : 76:b8:68:fc:75:85:48:ba:56:f3:70:8c:af:da:ae:51

Office files list

Family: Remote File Access
Displays office files

Risk	Port	Protocol	ID
Low	80	tcp	11419

The following PDF files (.pdf) are available on the remote server :
/Jay_Bio.pdf
/Jay_Resume.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 to 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.

smtpscan

Family: Mail Services
SMTP server fingerprinting

Risk	Port	Protocol	ID
Low	587	tcp	11421

This server could be fingerprinted as being Sendmail 8.12.2

Get the IMAP Banner

Family: Mail Services
Grab and display the IMAP banner

Risk	Port	Protocol	ID
Low	993	tcp	11414

The remote IMAP server banner is :

```
* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] sample.report.com IMAP4rev1
2003.339 at Sat, 16 Oct 2004 14:27:15 -0700 (MST)
Versions and types should be omitted where possible.
```

Change the imap banner to something generic.

Host: 1.2.3.234 - ip-1.2.3.234.www.scanist.com

Remote host replies to SYN+FIN

Family: Firewalls, Routers, SNMP
Sends a SYN+FIN packet and expects a SYN+ACK

Risk	Port	Protocol	ID
High	---	tcp	11618

Security Warning|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

BugTraq ID: [7487](#)

DNS AXFR	Risk	Port	Protocol	ID
Family: DNS Services	High	53	tcp	10595

Determines if the remote name server allows zone transfers

Security Warning|The remote name server allows DNS zone transfers to be performed. A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

HTTP TRACE / TRACK Methods	Risk	Port	Protocol	ID
Family: Web Services	Medium	80	tcp	11213

Test for TRACE / TRACK Methods

Security Warning|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>

icmp timestamp request

Family: Firewalls, Routers, SNMP
Performs an ICMP timestamp request

Risk	Port	Protocol	ID
Low	---	icmp	10114

Security Warning|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).

CVE: [CAN-1999-0524](#)

smtpscan

Family: Mail Services
SMTP server fingerprinting

Risk	Port	Protocol	ID
Low	25	tcp	11421

This server could be fingerprinted as being Sendmail 8.12.2

Get the IMAP Banner

Family: Mail Services
Grab and display the IMAP banner

Risk	Port	Protocol	ID
Low	993	tcp	11414

The remote IMAP server banner is :

```
* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] sample.report.com IMAP4rev1
2003.339 at Sat, 16 Oct 2004 14:27:15 -0700 (MST)
```

Versions and types should be omitted where possible.

Change the imap banner to something generic.

POP Server Detection

	Risk	Port	Protocol	ID
Family: Mail Services	Low	995	tcp	10185
POP Server Detection				

The remote POP3 server leaks information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy.

Versions and types should be omitted where possible.

The version of the remote POP3 server is :
+OK sample.report.com v2003.83 server ready

Solution: Change the login banner to something generic.

Host: 1.2.3.237 - ip-1.2.3.237.www.scanist.com

DNS AXFR

	Risk	Port	Protocol	ID
Family: DNS Services	High	53	tcp	10595
Determines if the remote name server allows zone transfers				

Security Warning|The remote name server allows DNS zone transfers to be performed.

A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

icmp timestamp request

	Risk	Port	Protocol	ID
Family: Firewalls, Routers, SNMP	Low	---	icmp	10114
Performs an ICMP timestamp request				

Security Warning|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).

CVE: [CAN-1999-0524](#)

SSH protocol versions supported	Risk	Port	Protocol	ID
Family: Remote Shell Access Negotiate SSHd connections	Low	22	tcp	10881

The remote SSH daemon supports the following versions of the SSH protocol :

- . 1.99
- . 2.0

SSHv2 host key fingerprint : 76:b8:68:fc:75:85:48:ba:56:f3:70:8c:af:da:ae:51

smtpscan	Risk	Port	Protocol	ID
Family: Mail Services SMTP server fingerprinting	Low	25	tcp	11421

This server could be fingerprinted as being Sendmail 8.12.2

Office files list	Risk	Port	Protocol	ID
Family: Remote File Access Displays office files	Low	80	tcp	11419

The following PDF files (.pdf) are available on the remote server :

- /Jay_Bio.pdf
- /Jay_Resume.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 to 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.

Get the IMAP Banner	Risk	Port	Protocol	ID
Family: Mail Services Grab and display the IMAP banner	Low	993	tcp	11414

The remote IMAP server banner is :

* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] sample.report.com IMAP4rev1

2003.339 at Sat, 16 Oct 2004 14:27:15 -0700 (MST)
Versions and types should be omitted where possible.

Change the imap banner to something generic.

POP Server Detection	Risk	Port	Protocol	ID
Family: Mail Services POP Server Detection	Low	995	tcp	10185

The remote POP3 server leaks information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy.

Versions and types should be omitted where possible.

The version of the remote POP3 server is :
+OK sample.report.com v2003.83 server ready

Solution: Change the login banner to something generic.

Host: 1.2.3.247 - ip-1.2.3.247.www.scanist.com

SmallFTP traversal	Risk	Port	Protocol	ID
Family: FTP Services Attempts to break out of the FTP root	Critical	53	udp	11573

The remote DNS server answers to queries for third party domains which do not have the recursion bit set.

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.

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...

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

Remote host replies to SYN+FIN	Risk	Port	Protocol	ID
Family: Firewalls, Routers, SNMP Sends a SYN+FIN packet and expects a SYN+ACK	High	---	tcp	11618

Security Warning|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

BugTraq ID: [7487](#)

HTTP TRACE / TRACK Methods

	Risk	Port	Protocol	ID
Family: Web Services	Medium	80	tcp	11213
Test for TRACE / TRACK Methods				

Security Warning|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>

icmp timestamp request

Family: Firewalls, Routers, SNMP

Performs an ICMP timestamp request

Risk	Port	Protocol	ID
Low	---	icmp	10114

Security Warning|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).

CVE: [CAN-1999-0524](#)

smtpscan

Family: Mail Services

SMTP server fingerprinting

Risk	Port	Protocol	ID
Low	25	tcp	11421

This server could be fingerprinted as being Sendmail 8.12.2

Office files list

Family: Remote File Access

Displays office files

Risk	Port	Protocol	ID
Low	80	tcp	11419

The following PDF files (.pdf) are available on the remote server :

/Jay_Bio.pdf

/Jay_Resume.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 to 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.

DNS AXFR

	Risk	Port	Protocol	ID
Family: DNS Services	High	53	tcp	10595
Determines if the remote name server allows zone transfers				

Security Warning|The remote name server allows DNS zone transfers to be performed. A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

CVE: [CAN-1999-0532](#)

HTTP TRACE / TRACK Methods

	Risk	Port	Protocol	ID
Family: Web Services	Medium	80	tcp	11213
Test for TRACE / TRACK Methods				

Security Warning|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>

SSH protocol versions supported

Family: Remote Shell Access
Negotiate SSHd connections

Risk	Port	Protocol	ID
Low	22	tcp	10881

The remote SSH daemon supports the following versions of the SSH protocol :

- . 1.99
- . 2.0

SSHv2 host key fingerprint : 76:b8:68:fc:75:85:48:ba:56:f3:70:8c:af:da:ae:51

smtpscan

Family: Mail Services
SMTP server fingerprinting

Risk	Port	Protocol	ID
Low	587	tcp	11421

This server could be fingerprinted as being Sendmail 8.12.2

Get the IMAP Banner

Family: Mail Services
Grab and display the IMAP banner

Risk	Port	Protocol	ID
Low	993	tcp	11414

The remote IMAP server banner is :

* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] sample.report.com IMAP4rev1 2003.339 at Sat, 16 Oct 2004 14:27:15 -0700 (MST)

Versions and types should be omitted where possible.

Change the imap banner to something generic.

POP Server Detection

Family: Mail Services
POP Server Detection

Risk	Port	Protocol	ID
Low	995	tcp	10185

The remote POP3 server leaks information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy.

Versions and types should be omitted where possible.

The version of the remote POP3 server is :
+OK sample.report.com v2003.83 server ready

Solution: Change the login banner to something generic.

Web Vulnerability Scanner (Nikto)

Each host in this assessment was tested for additional web server vulnerabilities using the Nikto scanner. Any additional vulnerabilities discovered by Nikto are listed below. Hosts with no additional web server vulnerabilities are not listed.

Host: 1.2.3.4 - ip-1.2.3.4.www.scanist.com

Path:/index.php?SqlQuery=test%20

This might be interesting... has been seen in web logs from an unknown scanner. (GET)

Nikto

Port:80

Host: 1.2.3.8 - ip-1.2.3.8.www.scanist.com

Path:/index.php?module=My_eGallery

My_eGallery prior to 3.1.1.g are vulnerable to a remote execution bug via SQL command injection. (GET)

Nikto

Port:80

Host: 1.2.3.14 - ip-1.2.3.14.www.scanist.com

Path:/index.php?module=My_eGallery

My_eGallery prior to 3.1.1.g are vulnerable to a remote execution bug via SQL command injection. (GET)

Nikto

Port:80

Host: 1.2.3.24 - ip-1.2.3.24.www.scanist.com

Path:/icons/

Directory indexing is enabled, it should only be enabled for specific directories (if required). If indexing is not used all, the /icons directory should be removed. (GET)

Nikto

Port:80

Host: 1.2.3.25 - ip-1.2.3.25.www.scanist.com

Path:/index.php?module=My_eGallery

My_eGallery prior to 3.1.1.g are vulnerable to a remote execution bug via SQL command injection. (GET)

Nikto

Port:80

Host: 1.2.3.26 - ip-1.2.3.26.www.scanist.com

Path: /index.php?module=My_eGallery	Nikto
My_eGallery prior to 3.1.1.g are vulnerable to a remote execution bug via SQL command injection. (GET)	Port:80

Host: 1.2.3.34 - ip-1.2.3.34.www.scanist.com

Path: /icons/	Nikto
Directory indexing is enabled, it should only be enabled for specific directories (if required). If indexing is not used all, the /icons directory should be removed. (GET)	Port:80

Host: 1.2.3.59 - ip-1.2.3.59.www.scanist.com

Path: /index.php?SqlQuery=test%20	Nikto
This might be interesting... has been seen in web logs from an unknown scanner. (GET)	Port:80

Host: 1.2.3.63 - ip-1.2.3.63.www.scanist.com

Path: /index.php?SqlQuery=test%20	Nikto
This might be interesting... has been seen in web logs from an unknown scanner. (GET)	Port:80

Host: 1.2.3.137 - ip-1.2.3.137.www.scanist.com

Path: /icons/	Nikto
Directory indexing is enabled, it should only be enabled for specific directories (if required). If indexing is not used all, the /icons directory should be removed. (GET)	Port:80

Host: 1.2.3.139 - ip-1.2.3.139.www.scanist.com

Path: /index.php?module=My_eGallery	Nikto
My_eGallery prior to 3.1.1.g are vulnerable to a remote execution bug via SQL command injection. (GET)	Port:80

Host: 1.2.3.169 - ip-1.2.3.169.www.scanist.com

Path: /icons/	Nikto
Directory indexing is enabled, it should only be enabled for specific directories (if required). If indexing is not used all, the /icons directory should be removed. (GET)	Port: 80

Host: 1.2.3.177 - ip-1.2.3.177.www.scanist.com

Path: /index.php?SqlQuery=test%20	Nikto
This might be interesting... has been seen in web logs from an unknown scanner. (GET)	Port: 80

Host: 1.2.3.192 - ip-1.2.3.192.www.scanist.com

Path: /icons/	Nikto
Directory indexing is enabled, it should only be enabled for specific directories (if required). If indexing is not used all, the /icons directory should be removed. (GET)	Port: 80

Host: 1.2.3.215 - ip-1.2.3.215.www.scanist.com

Path: /icons/	Nikto
Directory indexing is enabled, it should only be enabled for specific directories (if required). If indexing is not used all, the /icons directory should be removed. (GET)	Port: 80

Host: 1.2.3.234 - ip-1.2.3.234.www.scanist.com

Path: /icons/	Nikto
Directory indexing is enabled, it should only be enabled for specific directories (if required). If indexing is not used all, the /icons directory should be removed. (GET)	Port: 80

Host: 1.2.3.237 - ip-1.2.3.237.www.scanist.com

Path: /icons/	Nikto
Directory indexing is enabled, it should only be enabled for specific directories (if required). If indexing is not used all, the /icons directory should be removed. (GET)	Port: 80

Host: 1.2.3.247 - ip-1.2.3.247.www.scanist.com

Path: /index.php?module=My_eGallery My_eGallery prior to 3.1.1.g are vulnerable to a remote execution bug via SQL command injection. (GET)	Nikto Port: 80
--	---------------------------------

Host: 1.2.3.249 - ip-1.2.3.249.www.scanist.com

Path: /index.php?SqlQuery=test%20 This might be interesting... has been seen in web logs from an unknown scanner. (GET)	Nikto Port: 80
---	---------------------------------

External Advisories

Some of the security threats discovered have external advisory sources for additional cross-reference information. To view the external advisory information, click on the reference number in the table below.

ID	Risk	Description and References
11573	Critical	SmallFTP traversal BID-7472 , BID-7473 , BID-7474
10595	High	DNS AXFR CVE-1999-0532 , OSVDB-492
11618	High	Remote host replies to SYN+FIN BID-7487 , OSVDB-2118
12213	High	TCP sequence number approximation CVE-2004-0230 , BID-10183 , OSVDB-4030 , IAVA-2004-A-0007
11213	Medium	HTTP TRACE / TRACK Methods CVE-2004-2320 , BID-9506 , BID-9561 , BID-11604 , OSVDB-877 , OSVDB-3726
10114	Low	icmp timestamp request CVE-1999-0524