



scanist

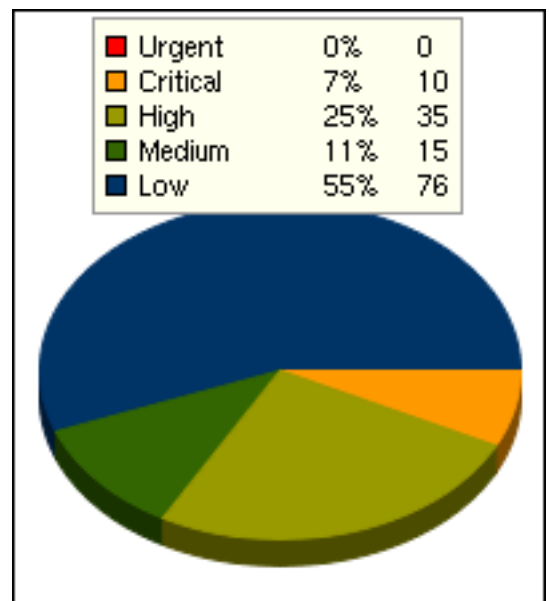
Analysis Date	Wednesday - October 24, 2007
Type of Analysis	Network Overview
Scan Date(s)	Monday - September 10, 2007
Technical Attention Priority	18%
Security Threats Discovered	136 (Low risk and greater)
Severe Threats Discovered	45
Scanned By	EXTERNAL (140.99.20.86, 140.99.20.85)

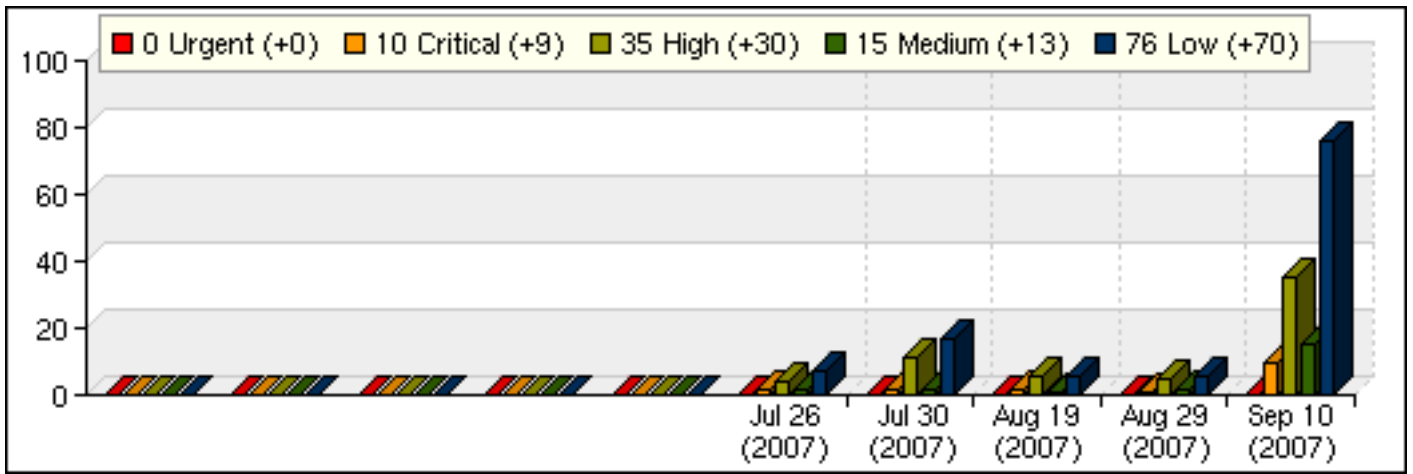
Target Description

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

Overview

This Scanist assessment was performed against a total of 27 hosts. The chart on the right provides details on the number of threats discovered for each risk classification. The number of threats found for up to the last 10 scans of all the hosts in this network are shown below. Drastic changes indicate that something has impacted the security posture of these hosts and should be looked into immediately.





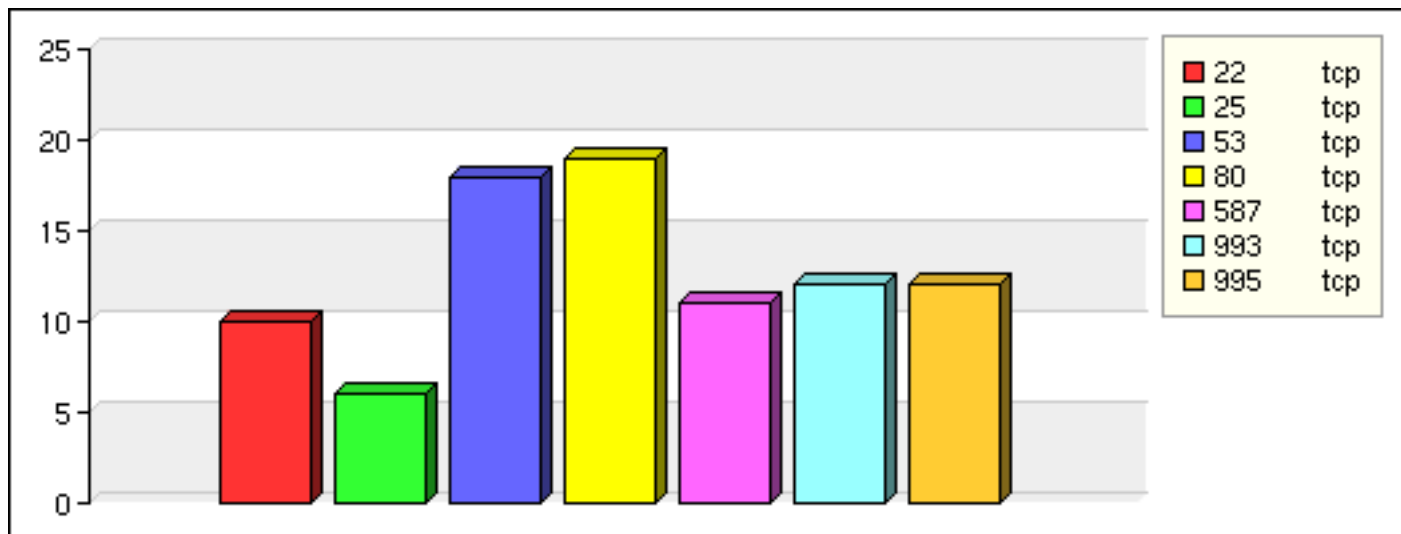
Vulnerable Hosts

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	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	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	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
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

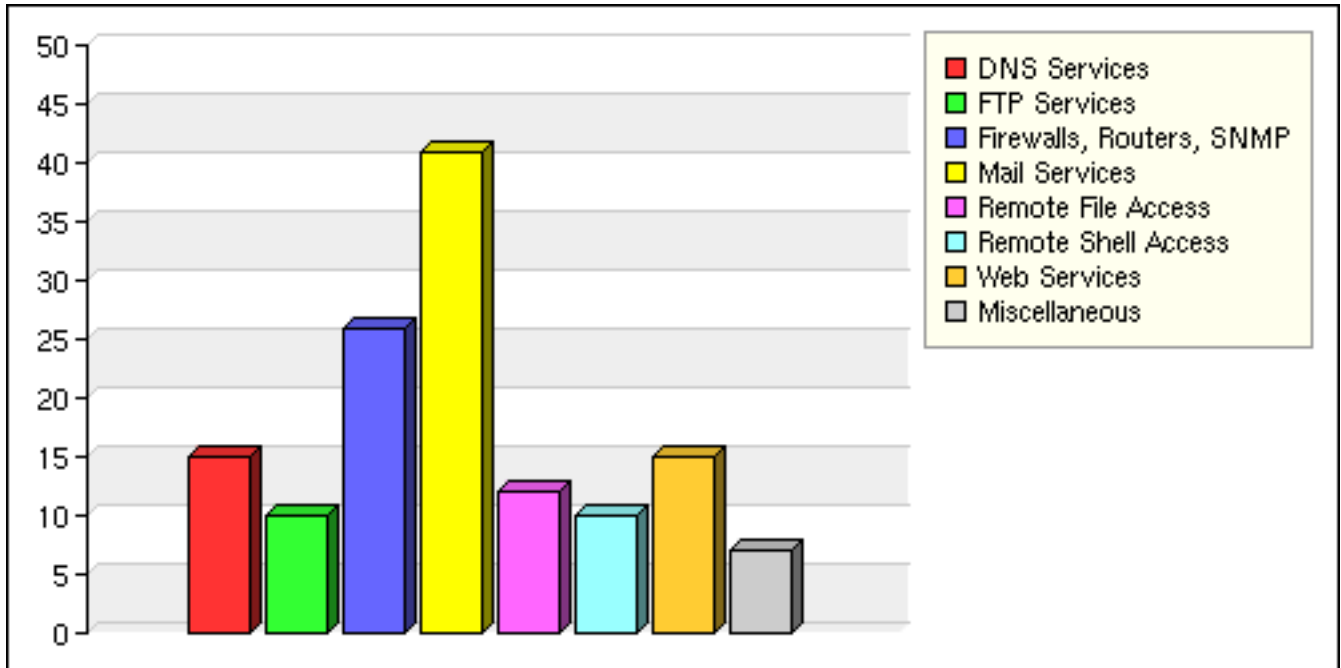
Port	Service Type (estimated)	Urgent	Critical	High	Medium	Low	Total
icmp	---	0	0	0	0	1	1
tcp	---	0	0	1	0	0	1
25 tcp	SENDMAIL 8.13.2/8.13.2/DEBIAN-1	0	0	0	0	1	1
53 tcp	ISC BIND NONE	0	0	0	0	0	0
53 udp	---	0	1	0	0	0	1
80 tcp	APACHE HTTPD	0	0	0	1	1	2

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