

## Vulnerability Assessment Report

<b>Analysis Date</b>	Thursday - April 26, 2007
<b>Type of Analysis</b>	Full Report
<b>Scan Date(s)</b>	Thursday - September 28, 2006
<b>Technical Attention Priority</b>	90%
<b>Security Threats Discovered</b>	26 (Low risk and greater)
<b>Severe Threats Discovered</b>	7

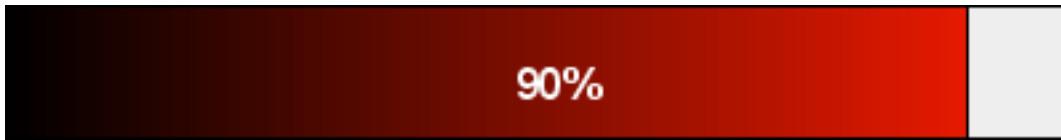
### Target Description

1.2.3.4

# Executive Summary

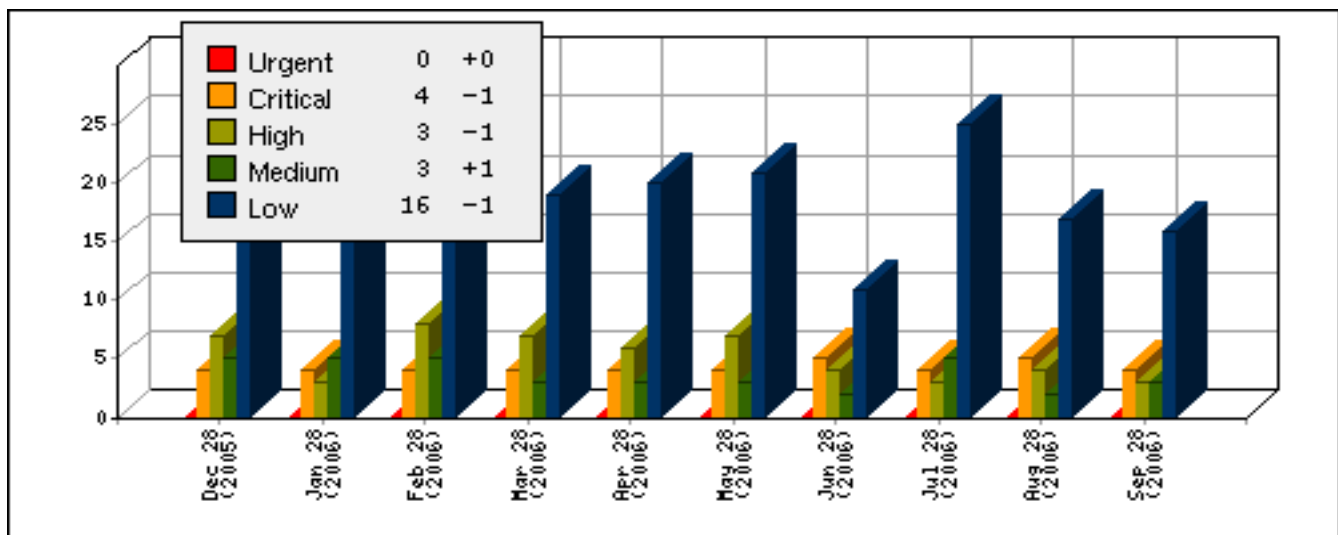
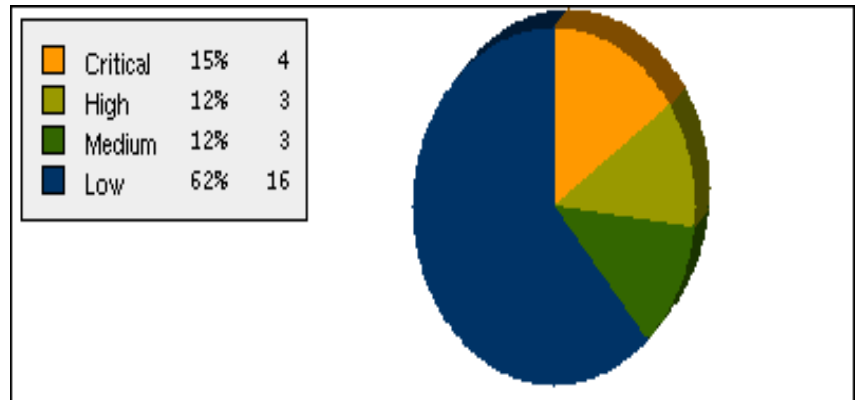
This document provides the results of the vulnerability assessment performed by Zenith Infotech. The information contained within this document is considered extremely confidential and should be treated as such.

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.

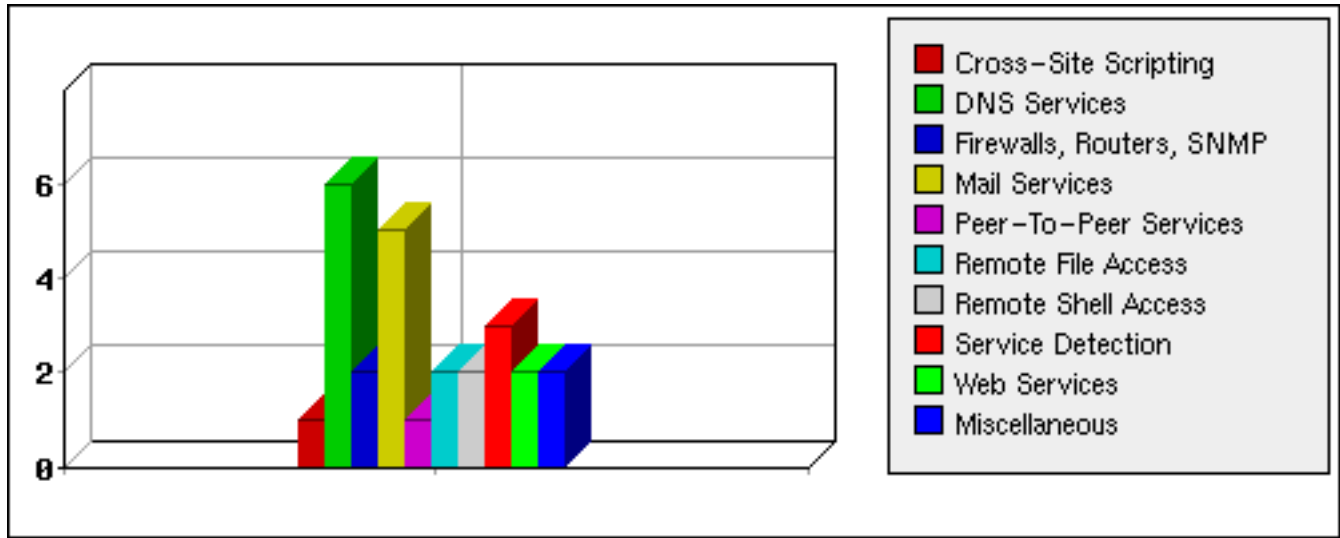


The scope of this analysis was to remotely audit and analyze the system and/or resources of each host in this assessment. This provides a "hacker's eye view" of the system to discover its security vulnerabilities and weaknesses to possible hacker penetration or attack. This assessment tested for 14453 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.



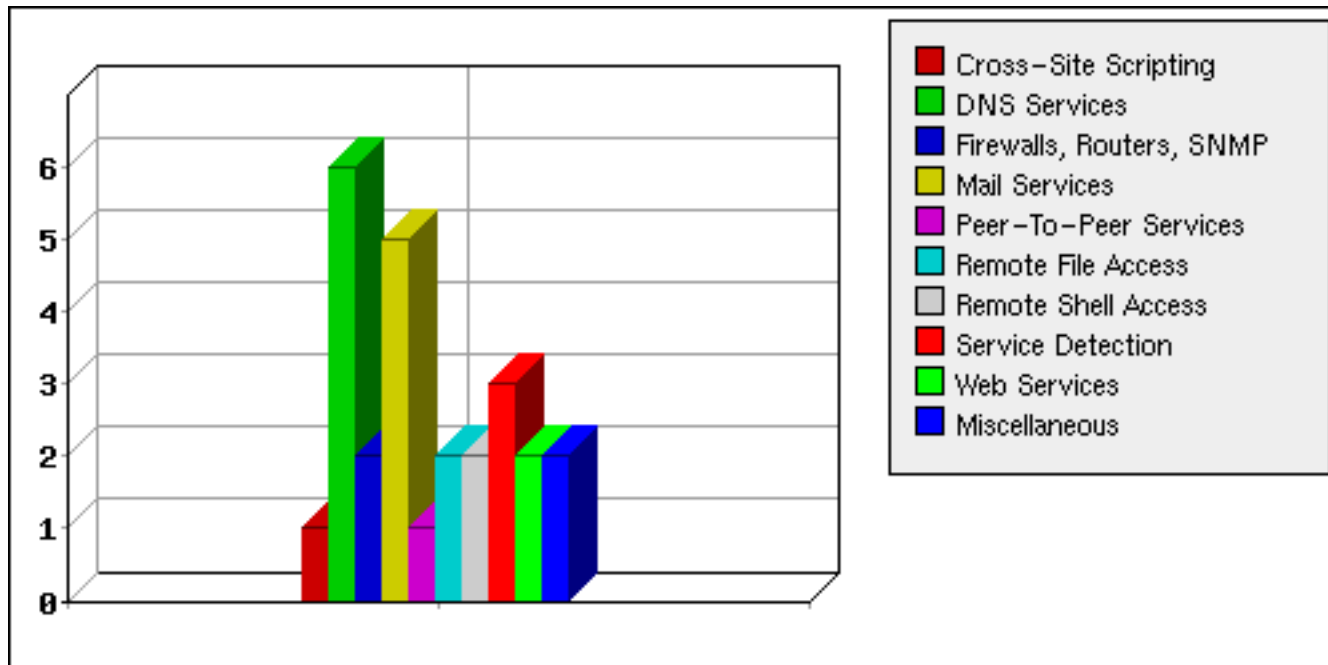
# Vulnerable Hosts

This SAAZScan analysis scanned 1 total IP addresses. Of those, 1 host was 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								
IP Address	OS Fingerprint	Ports	Risk-5	Risk-4	Risk-3	Risk-2	Risk-1	Threats
1.2.3.4	Linux Kernel 2.6.7	7	0	4	3	3	16	26

# Vulnerable Threat Families

The 26 total discovered vulnerabilities are spread across 10 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	Risk 5	Risk 4	Risk 3	Risk 2	Risk 1	Total
Cross-Site Scripting	0	1	0	0	0	1
DNS Services	0	2	1	0	3	6
Firewalls, Routers, SNMP	0	0	0	1	1	2
Mail Services	0	0	0	1	4	5
Miscellaneous	0	1	1	0	0	2
Peer-To-Peer Services	0	0	0	1	0	1
Remote File Access	0	0	0	0	2	2
Remote Shell Access	0	0	0	0	2	2
Service Detection	0	0	0	0	3	3
Web Services	0	0	1	0	1	2

# 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: 1.2.3.4 - sample.report.com

Risk	Port	Protocol	ID	Summary
Critical	domain (53/tcp)	None	10539	Determines if the remote name server allows recursive queries
Critical	domain (53/udp)	None	12217	DNS Cache Snooping
Critical	general/tcp	None	10336	Performs portscan / rpc scan / os recognition
Critical	www (80/tcp)	None	11213	http TRACE XSS attack
High	domain (53/tcp)	None	10595	Determines if the remote name server allows zone transfers
High	general/tcp	None	12213	Check for TCP approximations on the remote host
High	www (80/tcp)	None	14771	Checks for Apache <= 1.3.33
Medium	general/tcp	None	11618	Sends a SYN+FIN packet and expects a SYN+ACK
Medium	smtp (25/tcp)	None	10249	EXPN and VRFY checks
Medium	www (80/tcp)	None	11778	Looks for *.mp3,avi,asf,mpg,wav,ogg)
Low	domain (53/tcp)	None	11002	detects a running name server
Low	domain (53/tcp)	None	10028	Sends a VERSION.BIND request
Low	domain (53/udp)	None	11951	detects a name server type and version
Low	general/icmp	None	10114	Performs an ICMP timestamp request
Low	general/tcp	None	11936	Determines the remote operating system
Low	imaps (993/tcp)	None	11414	Grab and display the IMAP banner
Low	imaps (993/tcp)	None	10863	Displays the server certificate
Low	pop3s (995/tcp)	None	10185	POP Server Detection

<b>Low</b>	pop3s (995/tcp)	None	10863	Displays the server certificate
<b>Low</b>	smtp (25/tcp)	None	11421	SMTP server fingerprinting
<b>Low</b>	ssh (22/tcp)	None	10267	SSH Server type and version
<b>Low</b>	ssh (22/tcp)	None	10881	Negotiate SSHd connections
<b>Low</b>	submission (587/tcp)	None	11421	SMTP server fingerprinting
<b>Low</b>	www (80/tcp)	None	11419	Displays office files
<b>Low</b>	www (80/tcp)	None	11032	Directory Scanner
<b>Low</b>	www (80/tcp)	None	10107	HTTP Server type and version

# Threat Differential

This section lists all of the differences in discovered threats for all hosts in this assessment. Differences are derived based on the results obtained on the date shown. Hosts that were scanned during a previous scan but not during a later scan are considered dead and will be listed. Similarly, hosts scanned during the latest scan only are considered new and will be listed as well.

Host	Scanner	This Date	Baseline
1.2.3.4 - sample.report.com	External	Sep 28, 2006	Aug 28, 2006

## 12 Newly Discovered Threats

- 10881 - ssh (22/tcp) - SSH protocol versions supported
- 11414 - imaps (993/tcp) - Get the IMAP Banner
- 11032 - www (80/tcp) - Directory Scanner
- 11419 - www (80/tcp) - Office files list
- 12213 - general/tcp - TCP sequence number approximation
- 11213 - www (80/tcp) - HTTP TRACE Method Enabled
- 10336 - general/tcp - Nmap
- 11618 - general/tcp - Remote host replies to SYN+FIN
- 10595 - domain (53/tcp) - DNS AXFR
- 10863 - pop3s (995/tcp) - SSL Certificate
- 10863 - imaps (993/tcp) - SSL Certificate
- 11002 - domain (53/tcp) - DNS Server Detection

## 14 Threats No Longer Present

- 10539 - domain (538/tcp) - Usable remote name server
- 10539 - domain (539/tcp) - Usable remote name server
- 10539 - domain (537/tcp) - Usable remote name server
- 11951 - domain (533/udp) - DNS Server Fingerprint
- 11951 - domain (532/udp) - DNS Server Fingerprint
- 14771 - www (801/tcp) - Apache <= 1.3.33 htpasswd local overflow
- 14771 - www (803/tcp) - Apache <= 1.3.33 htpasswd local overflow
- 14771 - www (802/tcp) - Apache <= 1.3.33 htpasswd local overflow
- 10107 - www (8011/tcp) - HTTP Server type and version
- 10107 - www (8066/tcp) - HTTP Server type and version
- 10107 - www (8044/tcp) - HTTP Server type and version
- 10107 - www (8033/tcp) - HTTP Server type and version
- 10107 - www (8055/tcp) - HTTP Server type and version
- 10107 - www (8022/tcp) - HTTP Server type and version

## Network Characteristics

This section is not specific to security threats or vulnerabilities. Rather, the Network Characteristics section provides general information about how each host in this assessment responded to some standard basic network testing. The information in this section may be useful to gain an understanding of the characteristics of the hosts as seen from a remote network across the Internet.

## 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
1.2.3.4 - sample.report.com	0%	14.2	14.2	14.2

## Reverse DNS

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
1.2.3.4	sample.report.com	192.168.3.3	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: 1.2.3.4 - sample.report.com

Hop	IP Address	Hostname	Time (ms)
7	1.2.20.110	gw2-7-100.phx1.puregig.net	3.1
8	1.2.20.1	gw.phx1.puregig.net	6.6
9	1.2.11.100	gw3-4-56.phx1.puregig.net	10.8
10	1.2.3.1	gw.report.com	12.9
11	1.2.3.4	sample.report.com	18.4

## Online Public Database Search

There are various public databases, accessible via the Internet, which may contain information about your network, systems, and company. Under normal circumstances, this information is not confidential and does not contain any errors. However, it is also possible for these public databases to contain sensitive and/or incorrect data. If this is the case, the potential impact could vary widely. It may be a simple typo, it may allow your network to be hijacked by hackers, or it may expose proprietary information to the Internet.

In the sections Whois Domain and Whois Arin, online public databases were queried for information about each host in this assessment. Because this information is specific to your network, Zenith Infotech can not automatically determine if this information is correct or not. Please review the results listed in those sections for each of these queries to ensure that the information is both correct and non-confidential.

## IP Address Registries

The ARIN IP Address registry was queried for each host in this assessment. The results of this query should show the owner (and associated contacts) for each host. This should probably be your company directly, your ISP, or maybe even your hosting provider (if applicable). The entity listed below is considered the authoritative owner of the host.

Host(s): 1.2.3.4

```
OrgName          Sample Software Systems, Inc.
OrgID            ISP
Address          1682 N Sample St, Suite 201
City             Anytown
StateProv        AZ
PostalCode       85602
Country          US
NetRange         1.2.0.0 - 1.2.255.255
CIDR             1.2.0.0/16
NetName          DSS1
NetHandle        NET-1-2-0-0-1
Parent           NET-1-2-0-0-0
NetType          Direct Allocation
NameServer       NS1.ISP.NET
NameServer       NS2.ISP.NET
Comment
RegDate          1990-06-12
Updated          2001-08-01
TechHandle       SAMPLE-ARIN
TechName         Smith, Jane
TechPhone        +1-555-326-1000
TechEmail        jane.smith@isp.net
OrgTechHandle    SAMPLE-ARIN
OrgTechName      Smith, John
OrgTechPhone     +1-555-326-1000
OrgTechEmail     john.smith@isp.net
# ARIN WHOIS database, last updated 2006-10-15 19:10
```

# Domain Name Registries

This section attempted to resolve the domain name for each host in this assessment. Then, that domain name, if any, was searched in the Internic and domain name registry databases. The results of this query should report the owner (and associated contacts) for the domain name, if any, associated the host. This should probably be your company directly, your ISP, or maybe even your hosting provider (if applicable). The entity listed below is considered the authoritative owner of the domain name, if any, associated with the host.

Host(s): 1.2.3.4

Whois Server Version 1.3

Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to <http://www.internic.net> for detailed information.

Domain Name: REPORT.COM  
Registrar: TUCOWS INC.  
Whois Server: whois.opensrs.net  
Referral URL: <http://domainhelp.tucows.com>  
Name Server: NS2.ISP.NET  
Name Server: NS1.ISP.NET  
Name Server: NS1.REPORT.COM  
Status: ACTIVE  
Updated Date: 16-aug-2003  
Creation Date: 09-oct-2001  
Expiration Date: 09-oct-2005

&gt;&gt;&gt; Last update of whois database: Sat, 16 Oct 2006 06:58:29 EDT &lt;&lt;&lt;

Domain name: SAMPLE-REPORT.COM

Administrative Contact:

Sample Reports, Hostmaster hostmaster@report.com  
555 N. Central Ave.  
Suite 101  
Anytown, AZ 85301  
US  
(555) 123-5678

Technical Contact:

Sample Reports, Hostmaster hostmaster@report.com  
555 N. Central Ave.  
Suite 101  
Anytown, AZ 85301  
US  
(555) 123-5678

Registration Service Provider:

Sample ISP, noc@isp.net  
555-123-1000  
<http://www.report.net>  
This company may be contacted for domain login/passwords,  
DNS/Nameserver changes, and general domain support questions.

Registrar of Record: TUCOWS, INC.  
Record last updated on 16-Aug-2003.  
Record expires on 09-Oct-2005.  
Record created on 09-Oct-2001.

Domain servers in listed order:

NS1.REPORT.COM	1.2.3.1
NS1.ISP.NET	6.3.2.1

Domain status:  
ACTIVE

# 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: 1.2.3.4 - sample.report.com

## Determines if the remote name server allows recursive queries

	Risk	Port	Protocol	ID
<b>Family:</b> DNS Services	<b>Critical</b>	domain (53/tcp)	None	10539

The remote name server allows recursive queries to be performed by the host running nessusd.

If this is your internal nameserver, then forget this warning.

If you are probing a remote nameserver, then it allows anyone to use it to resolve third parties names (such as www.nessus.org). This allows hackers to do cache poisoning attacks against this nameserver.

If the host allows these recursive queries via UDP, then the host can be used to 'bounce' Denial of Service attacks against another network or system.

See also : <http://www.cert.org/advisories/CA-1997-22.html>

Solution: Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it).

If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf

If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command

Then, within the options block, you can explicitly state:  
'allow-recursion { hosts\_defined\_in\_acl }'

For more info on Bind 9 administration (to include recursion), see:  
<http://www.nominum.com/content/documents/bind9arm.pdf>

If you are using another name server, consult its documentation.

CVE: [CVE-1999-0024](#)

BugTraq ID: [136](#), [678](#)

---

## DNS Cache Snooping

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

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_Cache_Snooping_1.1.pdf)

---

**Performs portscan / rpc scan / os recognition**

Family:  
Miscellaneous

Risk	Port	Protocol	ID
Critical	general/tcp	None	10336

Nmap found that this host is running Linux 2.4.0 - 2.5.20

---

**http TRACE XSS attack**

Family:  
Cross-Site Scripting

Risk	Port	Protocol	ID
Critical	www (80/tcp)	None	11213

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://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>

---

#### Determines if the remote name server allows zone transfers

**Family:**  
DNS Services

Risk	Port	Protocol	ID
High	domain (53/tcp)	None	10595

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](#)

---

#### Check for TCP approximations on the remote host

**Family:**  
Miscellaneous

Risk	Port	Protocol	ID
High	general/tcp	None	12213

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

---

<a href="#">Checks for Apache &lt;= 1.3.33</a>	Risk	Port	Protocol	ID
<b>Family:</b> Web Services	High	www (80/tcp)	None	14771

The remote host appears to be running a version of Apache which is older than 1.3.32.

There is a local buffer overflow in htpasswd command in this version, which may allow a local user to gain the privileges of the httpd process.

\*\*\* Note that Nessus solely relied on the version number  
\*\*\* of the remote server to issue this warning. This might  
\*\*\* be a false positive

See also : <http://xforce.iss.net/xforce/xfdb/17413>

Solution: Upgrade to Apache 1.3.32 when available

---

<a href="#">Sends a SYN+FIN packet and expects a SYN+ACK</a>	Risk	Port	Protocol	ID
<b>Family:</b> Firewalls, Routers, SNMP	Medium	general/tcp	None	11618

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](#)

---

<a href="#">EXPN and VRFY checks</a>	Risk	Port	Protocol	ID
<b>Family:</b> Mail Services	Medium	smtp (25/tcp)	None	10249

The remote SMTP server answers to the EXPN and/or VRFY commands.

The EXPN command can be used to find the delivery address of mail aliases, or even the full name of the recipients, and the VRFY command may be used to check the validity of an account.

Your mailer should not allow remote users to use any of these commands, because it gives them too much information.

Solution: if you are using Sendmail, add the option :

O PrivacyOptions=goaway

in /etc/sendmail.cf.

CVE: [CAN-1999-0531](#)

---

<a href="#">Looks for *(mp3,avi,asf,mpg,wav,ogg)</a>	Risk	Port	Protocol	ID
<b>Family:</b> Peer-To-Peer Services	<b>Medium</b>	www (80/tcp)	None	11778

Here is a list of files which have been found on the remote web server. Some of these files may contain copyrighted materials, such as commercial movies or music files.

If any of this file actually contains copyrighted material and if they are freely swapped around, your organization might be held liable for copyright infringement by associations such as the RIAA or the MPAA.

- /mp3/Alcohol.mp3

Solution: Delete all the copyrighted files

---

<a href="#">detects a running name server</a>	Risk	Port	Protocol	ID
<b>Family:</b> DNS Services	<b>Low</b>	domain (53/tcp)	None	11002

A DNS server is running on this port. If you do not use it, disable it.

---

<a href="#">Sends a VERSION.BIND request</a>	Risk	Port	Protocol	ID
<b>Family:</b> DNS Services	<b>Low</b>	domain (53/tcp)	None	10028

BIND 'NAMED' is an open-source DNS server from ISC.org. Many proprietary DNS servers are based on BIND source code.

The BIND based NAMED servers (or DNS servers) allow remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind', will typically prompt the server to send

the information back to the querying source.

The remote bind version is : None

Solution:

Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts.

---

	Risk	Port	Protocol	ID
<b>detects a name server type and version</b>				
<b>Family:</b> DNS Services	<b>Low</b>	domain (53/udp)	None	11951

The remote name server could be fingerprinted as being : ISC BIND 9.2.3

---

	Risk	Port	Protocol	ID
<b>Performs an ICMP timestamp request</b>				
<b>Family:</b> Firewalls, Routers, SNMP	<b>Low</b>	general/icmp	None	10114

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](#)

---

	Risk	Port	Protocol	ID
<b>Determines the remote operating system</b>				
<b>Family:</b> Service Detection	<b>Low</b>	general/tcp	None	11936

The remote host is running Linux Kernel 2.4

---

	Risk	Port	Protocol	ID
<b>Grab and display the IMAP banner</b>				
<b>Family:</b> Mail Services	<b>Low</b>	imaps (993/tcp)	None	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.

---

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

Here is the SSLv2 server certificate:

Certificate:

Data:

Version: 1 (0x0)

Serial Number: 1 (0x1)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=US, ST=Arizona, L=Phoenix, O=Sample/Email=hostmaster@sample.report.com

Validity

Not Before: Sep 8 07:40:46 2002 GMT

Not After : Sep 8 07:40:46 2003 GMT

Subject: C=US, ST=Arizona, L=Phoenix, O=Sample, CN=sample.report.com/Email=hostmaster@sample.report.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (2048 bit)

Modulus (2048 bit):

00:a4:70:b5:e2:78:bd:aa:5b:00:b4:98:8f:97:6e:  
78:de:50:b9:a2:f0:de:9d:a6:26:fd:e2:55:8c:5a:  
ca:70:5f:f5:26:2a:22:7a:07:db:ad:d3:01:eb:3d:  
82:39:23:ff:91:8b:f3:bc:44:59:9d:f4:cf:44:da:  
70:1d:d8:e9:cd:30:4b:dc:5c:7b:5e:71:c3:70:c6:  
aa:6b:0c:1d:ff:2b:23:cb:63:3a:9c:5a:cb:ed:4a:  
a4:b8:57:28:01:b5:a6:c9:7b:b1:8d:30:7c:09:67:  
5e:eb:77:71:45:7d:ab:0a:62:b0:5a:67:79:90:11:  
97:22:4f:2b:90:04:ea:7a:92:90:65:ab:2f:be:92:  
0c:04:fd:4b:95:9d:b2:89:e5:7d:54:c1:cc:13:57:  
cd:f6:26:8b:40:9b:4d:87:7d:99:3a:66:52:71:a9:  
a4:4e:72:16:ad:0f:a7:34:5d:99:68:6e:9a:01:57:  
0f:04:ed:5d:d4:27:72:a0:af:3a:56:52:89:34:63:  
2d:1e:62:34:3e:07:8d:51:ad:36:0b:d3:06:1d:09:  
34:95:56:a9:53:56:60:4d:42:74:25:3e:08:79:28:  
79:09:29:92:db:61:6d:13:e8:bc:e0:b5:c5:c5:3a:  
78:cd:6d:c1:f4:40:1e:84:ce:7b:d0:6a:e9:87:56:  
78:31

Exponent: 65537 (0x10001)

Signature Algorithm: md5WithRSAEncryption

55:c7:a8:e0:91:bc:33:c0:c3:19:84:24:9d:3d:39:55:13:fe:  
17:7a:71:ab:fc:76:e0:9f:62:e9:a4:19:ba:34:e8:e1:28:4e:  
d8:6a:66:8d:4d:c0:55:4f:3d:12:1f:2c:fc:e3:8e:99:f5:63:  
c2:8d:77:b8:51:3c:eb:cb:32:13:2b:40:ad:1d:76:73:a5:d4:  
e6:05:58:ae:d8:64:75:4e:23:8b:93:e9:8f:9d:8e:9e:fc:7a:  
a7:01:81:f5:a1:5a:98:d6:56:43:d0:6f:14:45:82:56:f3:b7:  
e0:75:28:74:92:79:7f:bc:3f:e8:1e:0e:07:fa:a3:20:63:be:  
40:b6:20:08:a4:eb:09:02:5d:ce:b3:49:ba:f2:c2:15:f0:bd:  
97:94:e7:03:f4:0d:0c:a4:95:d5:aa:06:c6:1a:52:cf:8b:f7:  
63:b2:75:ce:86:9a:13:b5:22:97:04:c0:cf:37:ee:01:99:48:  
ac:59:18:45:e4:21:80:48:ed:29:65:1d:c6:06:a3:09:bf:d9:  
8c:d2:77:10:4b:cb:3c:2b:1f:e0:01:28:ba:0a:e5:9b:88:66:  
3d:90:7e:11:d4:ec:62:12:58:21:33:85:7a:60:f2:8c:b5:74:  
d8:f2:00:af:61:41:d3:95:28:2c:3e:7a:de:71:b6:0b:1e:33:  
da:b6:38:73

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.

---

**Displays the server certificate**

Risk	Port	Protocol	ID
Low	pop3s (995/tcp)	None	10863

Family:  
Service Detection

Here is the SSLv2 server certificate:

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=US, ST=Arizona, L=Phoenix, O=Sample, CN=sample.report.com/Email=hostmaster@sample.report.com

Validity

Not Before: Sep 10 07:30:21 2003 GMT

Not After : Sep 7 07:30:21 2013 GMT

Subject: C=US, ST=Arizona, L=Phoenix, O=Sample, CN=sample.report.com/Email=hostmaster@sample.report.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:e2:9b:ef:ac:8d:80:fc:36:23:49:55:72:47:21:

4e:6e:ba:99:58:47:5e:df:00:00:42:b1:78:a8:22:

d5:44:a2:ad:7a:6f:82:d3:d2:71:08:5f:a2:e1:1c:

5e:4b:c0:a9:29:38:3e:55:1a:3a:25:cc:fa:e8:0d:

d4:6e:ee:45:8f:5e:e3:b3:02:28:33:cd:99:9f:a4:

56:d8:88:5c:41:cb:49:e6:93:68:7f:2b:41:14:1e:

88:ff:85:28:74:7e:3c:b9:eb:5c:8a:49:d7:56:f8:

d6:ff:df:b0:3a:49:53:fd:fb:3d:0d:81:85:0a:b7:

39:ce:81:db:a6:77:3f:74:9f

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

84:D3:94:7E:B2:52:26:D9:A5:85:3C:FD:93:34:DA:9E:0F:EA:CD:EA

X509v3 Authority Key Identifier:

keyid:84:D3:94:7E:B2:52:26:D9:A5:85:3C:FD:93:34:DA:9E:0F:EA:CD:EA

DirName:/C=US/ST=Arizona/L=Phoenix/O=Sample/CN=sample.report.com/Email=hostmaste

r@sample.report.com

serial:00

X509v3 Basic Constraints:

CA:TRUE

Signature Algorithm: md5WithRSAEncryption

0b:ce:d6:c7:f8:56:9a:aa:d3:13:b2:d6:69:33:01:bb:1c:90:  
5b:04:da:cf:f8:70:af:49:2a:3f:b2:32:33:46:95:2a:c3:18:  
72:a3:c6:d3:85:70:df:3d:8f:a6:34:60:1c:e8:27:e3:87:19:  
98:d5:a7:8e:d6:6a:09:f3:2b:1f:3f:92:a5:5c:79:31:a6:f5:  
0e:52:d2:a1:ce:2c:a5:30:e1:87:92:c8:8d:37:94:12:23:1a:  
db:96:d7:b8:31:ae:97:f6:54:74:13:25:37:b1:7e:08:43:b8:  
44:94:e0:0d:52:55:e4:7c:af:88:e1:1c:e6:6e:1a:9a:b0:8e:  
ce:72

---

<a href="#">SMTP server fingerprinting</a>	Risk	Port	Protocol	ID
<b>Family:</b> Mail Services	<b>Low</b>	smtp (25/tcp)	None	11421

This server could be fingerprinted as being Sendmail 8.12.2

---

<a href="#">SSH Server type and version</a>	Risk	Port	Protocol	ID
<b>Family:</b> Remote Shell Access	<b>Low</b>	ssh (22/tcp)	None	10267

Remote SSH version : SSH-2.0-OpenSSH\_3.8.1p1 Debian 1:3.8.1p1-8

---

<a href="#">Negotiate SSHd connections</a>	Risk	Port	Protocol	ID
<b>Family:</b> Remote Shell Access	<b>Low</b>	ssh (22/tcp)	None	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

---

<a href="#">SMTP server fingerprinting</a>	Risk	Port	Protocol	ID
<b>Family:</b> Mail Services	<b>Low</b>	submission (587/tcp)	None	11421

This server could be fingerprinted as being Sendmail 8.12.2

---

<a href="#">Displays office files</a>	Risk	Port	Protocol	ID
<b>Family:</b> Remote File Access	<b>Low</b>	www (80/tcp)	None	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.

---

<b>Directory Scanner</b>	<b>Risk</b>	<b>Port</b>	<b>Protocol</b>	<b>ID</b>
<b>Family:</b> Remote File Access	<b>Low</b>	www (80/tcp)	None	11032

The following directories were discovered:  
/cgi-bin, /icons, /images, /mailman, /mp3

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

---

<b>HTTP Server type and version</b>	<b>Risk</b>	<b>Port</b>	<b>Protocol</b>	<b>ID</b>
<b>Family:</b> Web Services	<b>Low</b>	www (80/tcp)	None	10107

The remote web server type is :

Apache/1.3.31

The 'ServerTokens' directive is set to ProductOnly however we could determine that the version of the remote server by requesting a non-existent page.

## 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 - sample.report.com

<b>Path:</b> /index.php?SqlQuery=test%20 This might be interesting... has been seen in web logs from an unknown scanner. (GET)	<b>Nikto</b> <b>Port:</b> 80
<b>Path:</b> /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)	<b>Nikto</b> <b>Port:</b> 80
<b>Path:</b> /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)	<b>Nikto</b> <b>Port:</b> 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
10539	<b>Critical</b>	Usable remote name server <a href="#">CVE-1999-0024</a> , <a href="#">BID-136</a> , <a href="#">BID-678</a>
11213	<b>Critical</b>	HTTP TRACE Method Enabled <a href="#">CVE-2004-2320</a> , <a href="#">BID-9506</a> , <a href="#">BID-9561</a> , <a href="#">BID-11604</a> , <a href="#">OSVDB-877</a> , <a href="#">OSVDB-3726</a>
10595	<b>High</b>	DNS AXFR <a href="#">CVE-1999-0532</a> , <a href="#">OSVDB-492</a>
12213	<b>High</b>	TCP sequence number approximation <a href="#">CVE-2004-0230</a> , <a href="#">BID-10183</a> , <a href="#">OSVDB-4030</a> , IAVA-2004-A-0007
14771	<b>High</b>	Apache <= 1.3.33 htpasswd local overflow <a href="#">BID-13777</a> , <a href="#">BID-13778</a> , <a href="#">OSVDB-10068</a>
10249	<b>Medium</b>	EXPN and VRFY commands <a href="#">CVE-1999-0531</a> , <a href="#">OSVDB-12551</a>
11618	<b>Medium</b>	Remote host replies to SYN+FIN <a href="#">BID-7487</a> , <a href="#">OSVDB-2118</a>
10028	<b>Low</b>	Version of BIND <a href="#">OSVDB-23</a>
10114	<b>Low</b>	icmp timestamp request <a href="#">CVE-1999-0524</a>
11032	<b>Low</b>	Directory Scanner OWASP-CM-006

# Education

The Education report is written to provide a very high level explanation of network and information security. This report will also show some statistics about the need for security, dispel common myths about security, and define (in plain English) many of the terms used throughout this document.

This particular section is non-technical and is geared toward non-technical individuals, business management, and/or executives. For the stated audience, this report should be a prerequisite to the other reports in this document. If you are already familiar with Zenith Infotech documents, or if you are a technical professional, you may wish to simply skim this Education report. However, if you are a non-technical person, it is strongly recommended that you read this report.

## What is Network and/or Information Security

Before you can understand the concept of network security, you must decide what security means to you and your company. Perhaps to you, feeling secure means knowing that you are safe from any outsider gaining access to your confidential files and private company information. If this is the case, use this policy to evaluate what goes on with your network because the same private information is also stored in your computer systems.

Network security simply means preventing unauthorized use of your computer network. Taking the necessary precautions to protect your network will help to keep unauthorized users, or hackers, from gaining access to your computer system or network. Network security can also assist you in detecting whether or not a hacker tried breaking into your system, and what damage, if any, was done.

When it comes to network security, most companies fall somewhere between two boundaries: complete access and complete security. A completely secure computer is one that is not connected to the network, not plugged in, and physically unreachable by anyone. Obviously, a machine like this does not serve much of a purpose in your office. On the other hand, a computer with complete access is very easy to use, requiring no passwords or authorization to provide information. Unfortunately, having a machine with complete access means anyone could access it. This could spell disaster for you and your organization.

# Security Threat Risk Factor Definitions

## Urgent Risk

Urgent (Level 5) vulnerabilities provide remote intruders with remote root or remote administrator capabilities. With this level of vulnerability, hackers can compromise the entire host. Level 5 includes vulnerabilities that provide remote hackers full file-system read and write capabilities, remote execution of commands as a root or administrator user.

## Critical Risk

Critical (Level 4) vulnerabilities provide intruders with remote user, but not remote administrator or root user capabilities. Level 4 vulnerabilities give hackers partial access to file-systems (for example, full read access without full write access). Vulnerabilities that expose highly sensitive information also qualify as level 4 vulnerabilities.

## High Risk

High Risk (Level 3) vulnerabilities provide hackers with access to specific information stored on the host, including security settings. This level of vulnerabilities could result in potential misuse of the host by intruders. Examples of level 3 vulnerabilities include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, susceptibility to denial of service (DoS) attacks, and unauthorized use of services (for example, mail relaying).

## Medium Risk

Medium Risk (Level 2) vulnerabilities expose some sensitive information from the host, such as precise versions of services. With this information, hackers could research potential attacks to try against a host.

## Low Risk

Low Risk (Level 1) vulnerabilities are informational, such as open ports.

# Security Threat Family Definitions

## AIX Local Checks

Local operating system and application level security checks for AIX.

## Backdoors

Access to application files, system data, or confidential information.

## Centos Local Checks

Local operating system and application level security checks for Centos.

## Cross-Site Scripting

Threats related to improper sanitation of untrusted input in web pages.

## DNS Services

Vulnerabilities with domain name servers and configurations.

## Database Services

Exploits in database servers, services, and configurations.

## Debian Local Checks

Local operating system and application level security checks for Debian.

## Denial of Service

Threats of DoS attacks exploits used to launch other DoS attacks.

## FTP Services

Vulnerabilities of FTP (file sharing) applications, servers, or services.

## Fedora Local Checks

Local operating system and application level security checks for Fedora.

## Firewalls, Routers, SNMP

Threats or attack methods related to firewall and router devices and the SNMP protocol.

## FreeBSD Local Checks

Local operating system and application level security checks for FreeBSD.

## Gentoo Local Checks

Local operating system and application level security checks for Gentoo.

## HP-UX Local Checks

Local operating system and application level security checks for HP-UX.

## MacOS X Local Checks

Local operating system and application level security checks for MacOS X.

## Mail Services

Threats dealing with e-mail server problems or exploits.

## Mandrake Local Checks

Local operating system and application level security checks for Mandrake.

## Microsoft Bulletins

Local operating system and application level security checks for Microsoft Windows.

## **Miscellaneous**

Various threats and attacks that do not fit into any other family.

## **Netware**

Problems with Netware operating systems, applications, and services.

## **Peer-To-Peer Services**

Threats of exposed private data through file sharing services.

## **Red Hat Local Checks**

Local operating system and application level security checks for Red Hat.

## **Remote File Access**

Unauthorized access to files or data on your systems.

## **Remote Shell Access**

Vulnerability of user or service-level accounts and information.

## **Service Detection**

Tests for services, ports, and versions.

## **Slackware Local Checks**

Local operating system and application level security checks for Slackware.

## **Solaris Local Checks**

Local operating system and application level security checks for Solaris.

## **SuSE Local Checks**

Local operating system and application level security checks for SuSE.

## **Ubuntu Local Checks**

Local operating system and application level security checks for Ubuntu.

## **Unix**

Problems, exploits, or attack methods related to UNIX systems or common UNIX services.

## **Web Services**

Problems exposed by web servers, configurations, or CGI scripts.

## **Windows**

Problems with Windows operating systems, applications, and services.

# Definitions of Technical Terms

## ARIN

American Registry of Internet Numbers. This is the primary governing body that regulates Internet IP addresses. Other similar registries include APNIC and RIPE.

## CGI

Common Gateway Interface. A standard structure and protocol for running external programs from a web server. For example, a program to process e-commerce credit card purchases would likely use CGI.

## CVE / CAN

Common Vulnerabilities and Exposures / CANDidate. A dictionary that tracks information about known network and information security vulnerabilities.

## DoS

Denial of Service. DoS is a specific type of network attack which can make servers and/or routers crash and typically results in a network outage.

## DNS

Domain Name System/Service. A protocol used on the Internet for translating hostnames into Internet addresses. For example, DNS is the service that would translate www.google.com into the IP address 216.239.57.104. DNS is basically a phone book for the Internet.

## Domain Name

Strings of alphanumeric characters used to name/identify computers, networks, and organizations on the Internet.

## Exploit

A vulnerability in software or computer configurations that can be used for breaking security or otherwise attacking an Internet host over the network.

## Family

The classification system used to determine the general category or type of service affected by a particular security threat. For example, security threats specific to Microsoft Windows systems would be classified in the "Windows" family in the security threats database.

## Fingerprint

To identify by means of a distinctive mark or characteristic. For example, fingerprints are used to remotely identify which services, servers, operating systems, etc... that are running on any network.

## Firewall

Any of a number of security schemes that prevent unauthorized users from gaining access to a computer network. Generally, a firewall is a hardware device installed on a network to help protect the network from hackers and attacks.

## Hacker

A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. Many times the term is also used to describe a person who breaks into computer systems and/or networks.

## Host

See Server.

## IP Address

A numerical representation of a computer's address on the Internet.

## MTA

Mail Transport Agent. The program running on a server to perform email functions and protocols. For example, when you send an email, your ISP's mail server uses an MTA to process the message.

## **Nessus**

Open source security scanning engine used by most security professionals world-wide.

## **Network**

An interconnected group of computers and electronic systems. A LAN is an example of a network. The Internet is another (albeit much more complex) example of a network.

## **Port**

A computer's network interface is divided into several channels - each channel is called a "port." A port is used by specific hardware or software components to service requests on a network. For example, web servers typically use port number 80 to accept connections from users' web browsers. Generally, each computer has 65,535 unique ports.

## **Port Scan**

The process of examining a group of ports on a computer to determine which ones are active. A port scan does not identify which applications/services are running on a computer, what any active ports are used for, or any security threats on the computer. It only determines which ports are active.

## **Protocol**

A standard procedure for regulating data transmission between computers. For example, an email server uses a specific set of protocols so that anyone on the Internet can send email to anyone else on the Internet - regardless of which software or ISP either party is using.

## **Risk Factor**

The classification system used to determine the severity or potential impact of a particular security threat.

## **Security Scan**

The process of using various information security methodologies and techniques to audit the level of security for a computer, application, service, and/or network.

## **Security Threat**

See Exploit.

## **Server**

A computer that provides some service(s) to other computers that are connected to it via a network. For example, a web server provides web pages to your computer via the Internet.

## **Service**

Work performed, or offered by, a server. For example, a web server offers the service of providing web pages to a web browser.

## **SSL**

Secure Sockets Layer. A protocol designed to provide encrypted secure communications on the Internet. SSL is very commonly used to secure the transmission of e-commerce transactions. However, SSL does not provide any security for data after the initial transmission of the transaction.

## **TCP/IP**

Transmission Control Protocol / Internet Protocol. A suite of data networking and communications protocols for communication between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols.

## **Virus**

A rogue computer program that searches out other programs and infects them by embedding a copy of itself in them, so that they become Trojan horses. When these programs are executed, the embedded virus is executed too, thus propagating the infection. This normally happens invisibly to the user.

## **Vulnerability**

See Exploit.

## **VPN**

Virtual Private Network. The use of encryption in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.

## **Whois**

An Internet directory service for looking up information on a remote server. Whois is commonly used to lookup information about people, companies, IP addresses, computers, and domain names.