



# Vulnerability Assessment

## Sample Company

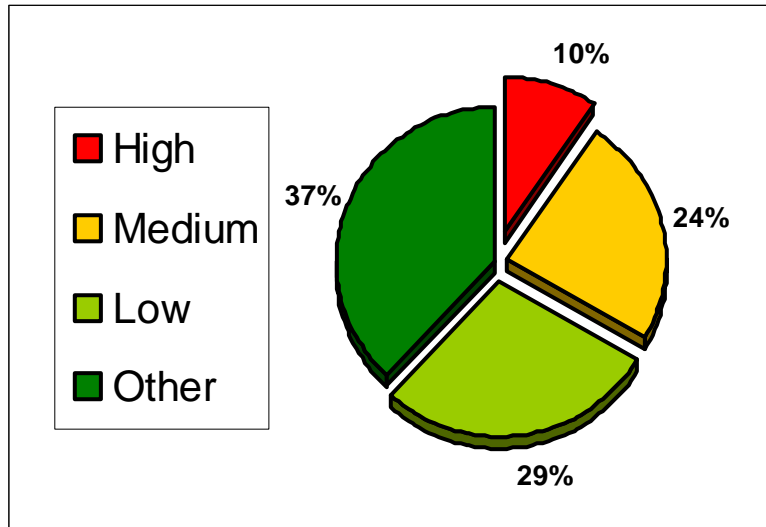
IP Address Analyzed	1.2.3.4
Operating System Fingerprint	Linux Kernel 2.6.7
Technical Attention Priority	Significant – Preventive Maintenance Required
Type of Analysis	External Scan
Analysis Date / Time	April 2, 2006 – 9:00AM (GMT-4)
Security Threats Discovered	21
Serious Threats Discovered	7
Document ID #	VA6092-01

**\* This report contains confidential company information \*  
Not For External Distribution**

# Executive Summary

This document provides the results of the vulnerability assessment performed by TeamLogic IT against 1.2.3.4 on Thursday, April 2, 2006 at 9:00AM (GMT-4). The information contained within this document is considered extremely confidential and should be treated as such.

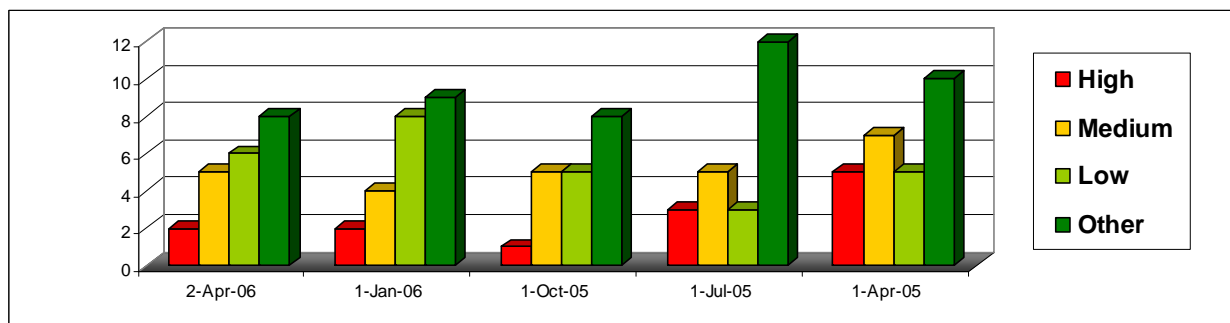
The graph below represents the seriousness of the security threats found during the assessment. The higher the percentage, the higher the priority should be for resolving the discovered security threats.



The scope of this analysis was to remotely audit and analyze the system and/or resources of 1.2.3.4. This provides a "hacker's eye view" of the system to discover its security vulnerabilities and weaknesses to possible hacker penetration or attack. TeamLogic IT tested for 9375 different potential security vulnerabilities.

During the process of this analysis, TeamLogic IT discovered 21 possible security threats. Of the discovered security threats, 7 of them are considered Serious Risks.

The graph below gives a historical perspective of the number of known security threats discovered for 1.2.3.4. Unexplained drastic changes should be looked into immediately.



Please recognize that network and information security is both a technical issue and a business issue. This document attempts to provide both high-level, plain-English information (in the Business Analysis Report section) and detailed technical information (in the Technical Analysis Report section). If you are a non-technical person, or if you are not familiar with scan reports, please consider reading the Education Report, located at the very bottom of this document.

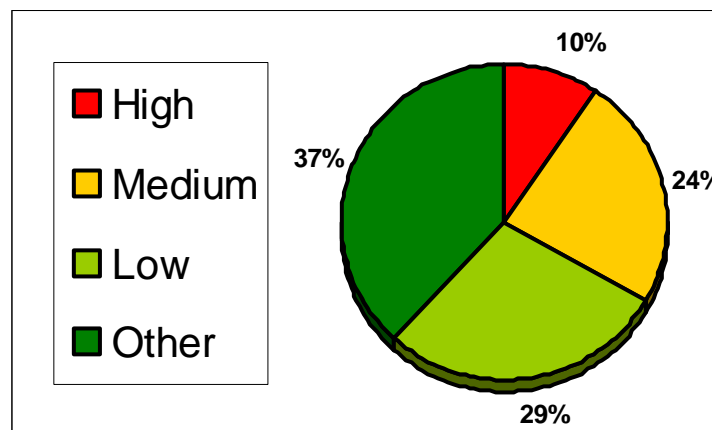
# Business Analysis Report

The Business Analysis Report is written to provide an analysis of the business-focused details of this document. This report examines the potential business impact of discovered security threats and quantifies relational data about the target network. The Business Analysis Report also provides an executive-level overview of the recommended immediate actions to be considered to address the security threats discovered.

This report attempts to be non-technical and the intended audience is non-technical individuals, business management, and/or executives. The Business Analysis Report presents the Scan results in plain-English, graphical, and summarized formats. For the intended audience, this report will contain the majority of the relevant information and data.

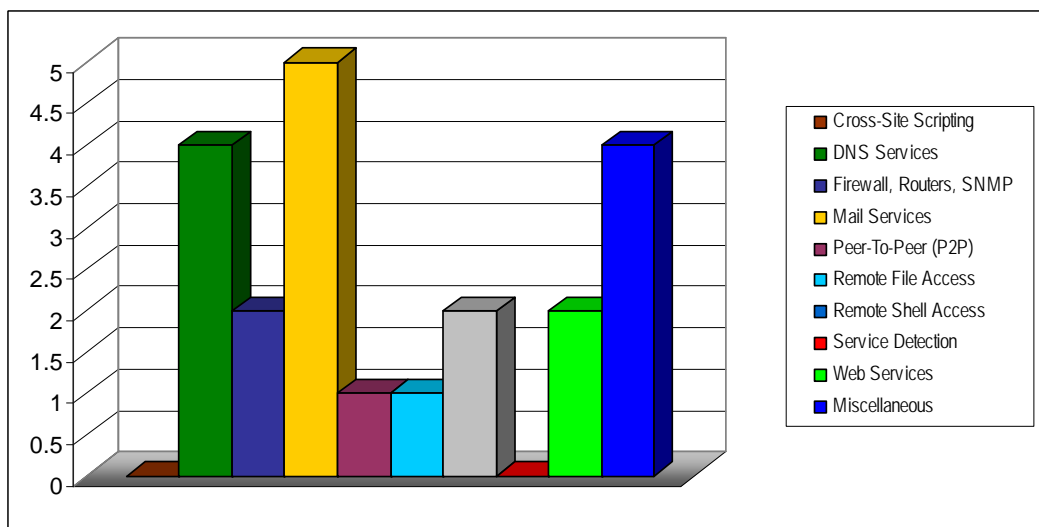
## Security Threats by Risk Factor

This scan discovered a total of 21 potential security threats to 1.2.3.4. Of this total number, 2 of the threats are classified as High Risk, 5 of the threats are classified as Medium Risk, 6 of the threats are classified as Low Risk, and 8 of the threats are classified as Other or an Information Risk.



## Security Threats By Family

The 21 potential security threats discovered on 1.2.3.4 are spread across different families of threat classifications. A large diversification of families (> 4) is cause for concern.



## Security Threats By Open Network Port

This scan analysis discovered a total of 7 open network ports on 1.2.3.4. 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 use. It is generally considered good practice to keep the number of open ports as low as possible. Sometimes hackers will target computers with a large number of open network ports because they might be easier 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.

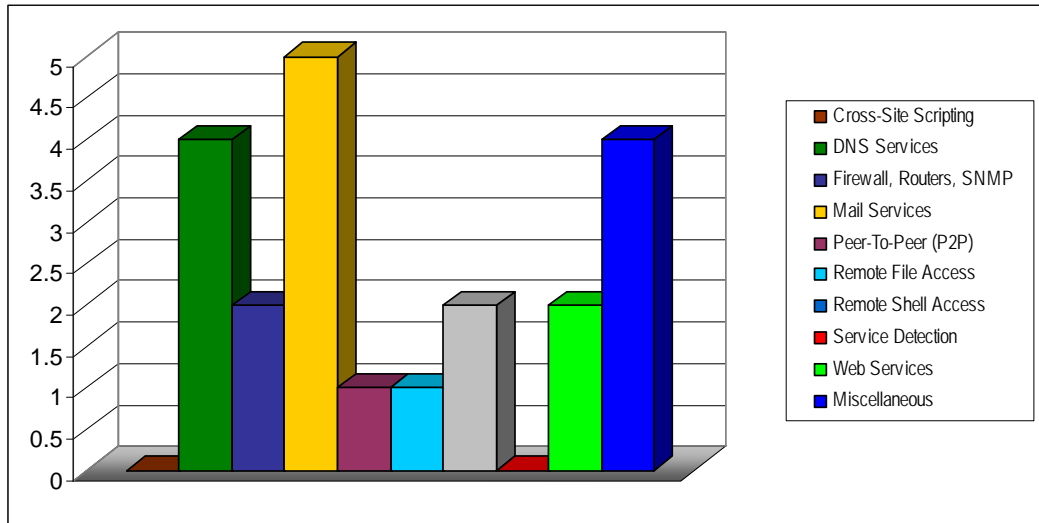
Port	Service	Fingerprint
22/tcp	ssh	OpenSSH 3.8.1p1 (protocol 2.0)
25/tcp	smtp	Sendmail 8.13.2/8.13.2/Debian-1
53/tcp	domain	ISC Bind None
80/tcp	www	Apache HTTPd
587/tcp	submission	Sendmail 8.13.2/8.13.2/Debian-1
993/tcp	ssl/imap	UW imapd 2003.339
995/tcp	ssl/pop3	UW Imap pop3 server 2003.83

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.

Port	High	Medium	Low	Other	Total
22/tcp	0	0	1	1	2
25/tcp	0	0	1	1	2
53/tcp	1	2	0	0	3
53/udp	0	0	0	1	1
80/tcp	1	0	1	2	4
587/tcp	0	0	0	1	1
993/tcp	0	0	0	2	2
995/tcp	0	0	1	1	2
general/icmp	0	0	1	0	1
general/tcp	0	2	0	1	3

## Security Threats By Family

This Scan analysis discovered a total of 21 potential security threats to 1.2.3.4. Of this total number, 7 of the threats are classified as a Serious Risk. High and Medium Risk threats are considered serious because they represent direct threats to 1.2.3.4. Low and Other Risk threats are still important, however these types of threats are usually either informational which help make attackers better prepared, or they cannot be closed without affecting service availability.



The 21 potential security threats discovered on 1.2.3.4 are spread across 8 different families of threat classifications. A large diversification of families (> 4) is cause for concern because these types of systems make more desirable targets for potential attackers. A relatively minor threat in one service could help an attacker exploit a more difficult and major threat in another service.

Family	High	Medium	Low	Other	Total
DNS Services	1	2	0	1	4
Firewalls, Routers, SNMP	0	1	1	0	2
Mail Services	0	0	2	3	5
Miscellaneous	0	1	0	3	4
Peer-To-Peer Services	0	0	0	1	1
Remote File Access	0	0	0	1	1
Remote Shell Access	0	0	1	1	2
Web Services	1	0	1	0	2

## Immediate Needs

This section will review the discovered security threats that are more probable to pose an immediate risk of attack to 1.2.3.4. This is determined by the risk factor of the discovered threats; any potential vulnerability classified as either High Risk or Medium Risk is automatically considered an "immediate need." Of the 21 security threats discovered on 1.2.3.4, 2 (10%) are considered High Risk and 5 (24%) are considered Medium Risk.

### High Risk Security Threats Summaries

ID	Family	Summary
10539	DNS Services	Useable remote name server
14771	Web Services	Apache <= 1.3.31 htpasswd local overflow

■ New     
 ■ Unmodified     
 ■ Modified     
 ■ Resolved

### Medium Risk Security Threats Summaries

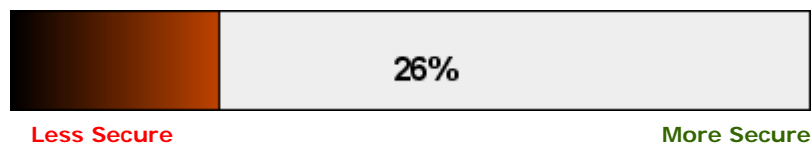
ID	Family	Summary
10028	DNS Services	Determine which version of BIND name daemon is running
10595	DNS Services	DNS AXFR
11213	Cross-Site Scripting	http TRACE XSS attack
11618	Firewalls, Routers, SNMP	Remote host replies to SYN+FIN
12213	Miscellaneous	TCP sequence number approximation

■ New     
 ■ Unmodified     
 ■ Modified     
 ■ Resolved

## Comparative Security Ranking

TeamLogic IT has assigned a score to this security analysis report. The score is based on the quantity and severity of the security threats discovered on 1.2.3.4. This score was then ranked against all the other scores, for all the other scan reports, from all of the TeamLogic IT customers. This formula produces a percentile ranking - the comparative rating of the quality of security for 1.2.3.4 versus all the other systems TeamLogic IT has analyzed.

This Comparative Security Ranking gives an indication of how 1.2.3.4 compares to all of the other systems TeamLogic IT has analyzed. For example, a rating of 100% would mean that 1.2.3.4 is more secure than every other system TeamLogic IT has analyzed, while a rating of 0% would mean that 1.2.3.4 is less secure than every other system analyzed. Since this is a comparative rating, a score of 100% does not guarantee that your system is completely secure nor does a lower rating mean your system will be attacked. Nonetheless, it does provide a general idea of how 1.2.3.4 compares to others using Scan.



## Resolution Checklist

This Security Resolution Checklist is intended to act as a bridge between the Business Analysis and Technical Analysis reports. The checklist is purposely designed to be a very high-level summary to help organize the workflow process of addressing potential security threats to your network. This report does not present any new information that is not available in the other reports of this document. Rather, sections of the other reports are simply summarized in this checklist to be a "common ground" between the distinctly different technical processes and business objectives.

### Outstanding High Risk Security Threats

Complete	ID	Summary
<input type="checkbox"/>	10539	Useable remote name server
<input type="checkbox"/>	14771	Apache <= 1.3.31 htpasswd local overflow

■ New     
 ■ Unmodified     
 ■ Modified     
 ■ Resolved

### Outstanding Medium Risk Security Threats

Complete	ID	Summary
<input type="checkbox"/>	10028	Determine which version of BIND name daemon is running
<input type="checkbox"/>	10595	DNS AXFR
<input type="checkbox"/>	11213	http TRACE XSS attack
<input type="checkbox"/>	11618	Remote host replies to SYN+FIN
<input type="checkbox"/>	12213	TCP sequence number approximation

■ New     
 ■ Unmodified     
 ■ Modified     
 ■ Resolved

### Other Items

Complete	ID	Summary
<input type="checkbox"/>	Recommended	Install a business-class firewall as a "front line" defense
<input type="checkbox"/>	Recommended	Install (and update regularly) high quality anti-virus software
<input type="checkbox"/>	Recommended	Perform a TeamLogic IT security analysis on all network devices
<input type="checkbox"/>	Recommended	Verify online database (ARIN, Domain, and Google) information
<input type="checkbox"/>	Recommended	Use TeamLogic IT's backup services for of all critical data. Test regularly
<input type="checkbox"/>	Recommended	Use TeamLogic IT's SystemWatch for patch management
<input type="checkbox"/>	Recommended	Use complex non-dictionary passwords for all users of all systems

## Suggested Next Steps

This section reviews some general security practices to consider. Each of these items may, or may not, be applicable to you, depending on the size, configuration, and usage of your network. Nonetheless, you should consider each of the items in this section, as they will help you to manage the awareness, protection, and reaction of your network to possible security attacks.

### Firewall Analysis

Every Internet-connected network, no matter how large or small, should seriously consider using a firewall. This would provide a reasonable "front line" defense against hackers or attacks. Firewalls can be either hardware or software and their pricing and effectiveness can vary significantly. The most expensive firewall may, or may not, be the best option. Likewise, the least expensive firewall may, or may not, provide adequate protection for your network.

In any case, firewalls are tasked with a complex and ever-changing job. Firewalls themselves can have security threats and it is not uncommon for a firewall to be configured incorrectly or to redirect ports to a server. Therefore, it is wise to have TeamLogic IT re-test your network's security after making any changes to your architecture (like installing a firewall). Although an excellent line of defense, a firewall alone does not automatically guarantee your networks' security.

## Security Analysis Scope and Frequency

The old saying is true: a chain is only as strong as its weakest link. The same is also true for your network and information security - all it takes is one vulnerability, on one piece of your network, to potentially spell disaster for the entire network.

Therefore, do not forget to have TeamLogic IT analyze the security of every Internet-connected device on your network. This includes servers, desktops, routers, firewalls, file servers, laptops - everything. If your network allows remote connections (for example, workers who telecommute and connect from their home office), don't forget to analyze the security of those remote devices too. Think of it this way: it is just as effective to break into your home using the bedroom window as it is using the front door. Every possible entry point needs to be secured.

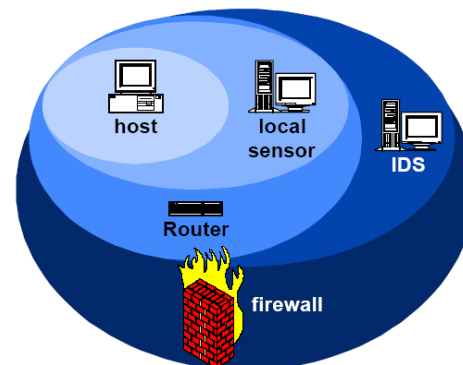
Just as you should frequently update your anti-virus software, it is also good practice to analyze your network's security regularly. New security threats and vulnerabilities are discovered daily and the TeamLogic IT database of security threats generally grows by 5-10 new vulnerabilities every week. TeamLogic IT constantly monitors security threats as they appear.

## Defense In-Depth Strategy

Layered defenses, or Defense In-Depth, is the approach of using multiple layers of security to guard against failure of a single security component. At your gateway to the Internet, you should at the very least maintain a business-class firewall and router. Most hardware manufacturers offer multifunction devices that can act as your router, firewall, intrusion detection system (IDS), and even a Demilitarized Zone (DMZ).

Routers have two or more interfaces that each connect to a network. When data is sent from your computer to a different network, the router receives that data on its interface (which is also the default gateway). The router then determines the best route to reach the destination address and forwards it out from a different interface.

Network Address Translation (NAT) is where a router hides internal IP addresses from sources outside the network. Only the router's IP address is visible to the Internet. A tunnel can be created through your firewall so that the computers on the Internet can communicate to one of the computers on a LAN. This is handy for running web servers, game servers, FTP servers, or even video conferencing.



A firewall is a term for any device (software or hardware) that prevents undesirable activity from either entering or exiting a network. A firewall filters all network packets to determine whether to forward them toward their destination. There are a number of firewall screening methods. A simple method is to screen requests to make sure they come from acceptable (previously identified) domain names and IP addresses.

An Intrusion Detection System (IDS) provides real-time security sentry (like a motion sensor) that protects the network from attack or unauthorized activity. An IDS analyzes the network datastream in search of activity signatures that have been deemed unauthorized, and then alarm and react to the activity. IDS can be passive or active defenses. Detection of break-ins or break-in attempts are found either manually or via software expert systems that operate on logs or other information available on the network.

A Demilitarized Zone (DMZ) is a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web servers, FTP servers, SMTP (e-mail) servers and DNS servers. The term comes from military use, meaning a buffer area between two enemies.

The most expensive or the most feature-rich gateway device might not always be the best for your needs. Let TeamLogic IT's trained experts guide you through a needs assessment and install the hardware and software solution to meet your needs.

## Security Notifications Newsletter

TeamLogic IT provides a free monthly email newsletter to its SystemWatch subscribers about new security threats. This newsletter gives you a simple, no-hassle way to stay on top of information about new security threats and to know when you may need to perform a security analysis / vulnerability assessment of your computers and/ or network.

# Technical Analysis Report

The Technical Analysis Report provides documentation and details of the technical-focused analysis conducted for this document. This report includes the technical details of an examination of the discovered security threats and quantifies relational data about the target network. The Technical Analysis Report also provides the in-depth details of each potential security threat discovered during the scan analysis.

This report is purposely technical and the intended audience is technical individuals, technical consultants, technical service providers, or in-house technology/engineering staff. The Technical Analysis Report presents all of the technical details and findings of the Scan analysis. For the intended audience, this report will contain the majority of the relevant information and data.

## Security Threats By Open Network Port

This scan analysis discovered a total of 7 open network ports on 1.2.3.4. 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 use. It is generally considered good practice to keep the number of open ports as low as possible. Sometimes hackers will target computers with a large number of open network ports because they might be easier 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.

Port	Service	Fingerprint
22/tcp	ssh	OpenSSH 3.8.1p1 (protocol 2.0)
25/tcp	smtp	Sendmail 8.13.2/8.13.2/Debian-1
53/tcp	domain	ISC Bind None
80/tcp	www	Apache HTTPd
587/tcp	submission	Sendmail 8.13.2/8.13.2/Debian-1
993/tcp	ssl/imap	UW imapd 2003.339
995/tcp	ssl/pop3	UW Imap pop3 server 2003.83

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.

Port	High	Medium	Low	Other	Total
22/tcp	0	0	1	1	2
25/tcp	0	0	1	1	2
53/tcp	1	2	0	0	3
53/udp	0	0	0	1	1
80/tcp	1	0	1	2	4
587/tcp	0	0	0	1	1
993/tcp	0	0	0	2	2
995/tcp	0	0	1	1	2
general/icmp	0	0	1	0	1
general/tcp	0	2	0	1	3

## Discovered Security Threat Summaries

This section provides a simple one-line summary for each discovered potential security threat on 1.2.3.4. These summaries are grouped by Risk Factor.

### High Risk Security Threats

ID	Family	Summary
10539	DNS Services	Useable remote name server
14771	Web Services	Apache <= 1.3.31 htpasswd local overflow

■ New
 ■ Unmodified
 ■ Modified
 ■ Resolved

### Medium Risk Security Threats

ID	Family	Summary
10028	DNS Services	Determine which version of BIND name daemon is running
10595	DNS Services	DNS AXFR
11213	Cross-Site Scripting	http TRACE XSS attack
11618	Firewalls, Routers, SNMP	Remote host replies to SYN+FIN
12213	Miscellaneous	TCP sequence number approximation

■ New
 ■ Unmodified
 ■ Modified
 ■ Resolved

### Low Risk Security Threats

ID	Family	Summary
10107	Web Services	HTTP Server type and version
10114	Firewalls, Routers, SNMP	icmp timestamp request
10185	Mail Services	POP3 Server type and version
10249	Mail Services	EXPN and VRFY commands
10267	Remote Shell Access	SSH Server type and version
12217	DNS Services	DNS Cache Snooping

■ New
 ■ Unmodified
 ■ Modified
 ■ Resolved

### Other Security Threats

ID	Family	Summary
10336	Miscellaneous	Nmap
10863	Miscellaneous	SSL ciphers - x2
10881	Remote Shell Access	SSH protocol versions supported
11032	Remote File Access	Directory Scanner
11414	Mail Services	IMAP Banner
11421	Mail Services	smtpscan - x2
11778	Peer-To-Peer Services	Web Server hosting copyrighted material
11951	DNS Services	DNS Server Fingerprint

■ New
 ■ Unmodified
 ■ Modified
 ■ Resolved

## Network Characteristics

This section is not specific to security threats or vulnerabilities. Rather, the Network Characteristics section provides general information about how 1.2.3.4 responded to some standard basic network testing. The information in this section may be useful to gain an understanding of the characteristics of 1.2.3.4 as seen from a remote network (TeamLogic IT) across the Internet.

### 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.

Packet Loss	Packets Sent	Packets Received	Minimum (ms)	Average (ms)	Maximum (ms)
0%	4	4	14.2	14.2	14.2

### Traceroute Response

The information below shows a traceroute originating from the TeamLogic IT network to 1.2.3.4.

Hop	Hostname	IP Address	Round-Trip Time
7	gw2-7-100.phx1.puregig.net	1.2.20.110	3.056
8	gw.phx1.puregig.net	1.2.20.1	6.611
9	gw3-4-56.phx1.purgig.net	1.2.11.100	10.81
10	gw.report.com	1.2.3.1	12.87
11	sample.report.com	1.2.3.4	18.397

### 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.

Reverse DNS turns an IP address into a hostname -- for example, it might turn 1.2.3.4 into host.example.com. For your domains, standard DNS (turning a hostname into an IP address, such turning host.example.com into 1.2.3.4) starts with the company (registrar) that you registered your domains with. You let them know what DNS servers are responsible for your domain names, and the registrar sends this information to the root servers (technically, the parent servers for your TLD). Then, anyone in the world can access your domains, and you can send them to any IP addresses you want. You have full control over your domains, and can send people to any IPs (whether or not you have control over those IPs, although you should have permission to send them to IPs that are not yours).

Reverse DNS works in a similar method. For your IPs, reverse DNS (turning 1.2.3.4 back into host.example.com) starts with your ISP (or whoever told you what your IP addresses are). You let them know what DNS servers are responsible for the reverse DNS entries for your IPs (or, they can enter the reverse DNS entries on their DNS servers), and your ISP gives this information out when their DNS servers get queried for your reverse DNS entries. Then, anyone in the world can look up the reverse DNS entries for your IPs, and you can return any hostnames you want (whether or not you have control over those domains, although you should have permission to point them to hostnames that are not on your domains).

The IP address 1.2.3.4 does have valid reverse DNS records. 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 the IP address into a valid hostname are shown below.

--

```

; <<>> DiG 9.2.1 <<>> -x 1.2.3.4
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1570
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;2.3.2.1.in-addr.arpa.          IN          PTR

;; ANSWER SECTION:
2.3.2.1.in-addr.arpa. 39552 IN CNAME 2.3.2.1.in-addr.arpa.
4.64-27.3.2.1.in-addr.arpa. 86400 IN PTR sample.report.com.

;; AUTHORITY SECTION:
64-27.20.99.140.in-addr.arpa. 86400 IN NS ns1.isp.net.

;; ADDITIONAL SECTION:
ns1.isp.net.          86400 IN A 1.2.3.2

;; Query time: 45 msec
;; SERVER: 192.168.3.3#53(192.168.3.3)
;; WHEN: Sat Oct 16 14:25:07 2004
;; MSG SIZE rcvd: 132

```

## 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 this section, three online public databases were queried for information about 1.2.3.4. Because this information is specific to your network, can not automatically determine if this information is correct or not. Please review the results listed below for each of these queries to ensure that the information is both correct and non-confidential.

## IP Address Registries

This section queried the ARIN IP Address registry for information about 1.2.3.4. The results of this query should show the owner (and associated contacts) for the 1.2.3.4 IP address. 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 IP address 1.2.3.4:

```

OrgName      Sample Software Systems, Inc.
OrgID        ISP
Address      1482 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      1990-04-12
Updated      2001-08-01
TechHandle   SAMPLE-ARIN
TechName     Smith, Jane
TechPhone    +1-555-324-1000
TechEmail    jane.smith@isp.net
OrgTechHandle SAMPLE-ARIN
OrgTechName  Smith, John
OrgTechPhone +1-555-324-1000
OrgTechEmail john.smith@isp.net
# ARIN WHOIS database, last updated 2006-01-15 19:00

```

## Domain Name Registries

This section attempted to resolve the domain name for 1.2.3.4. 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 with 1.2.3.4. 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 IP address 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

>>> Last update of whois database: Sat, 16 Oct 2004 06:58:29 EDT <<<

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.
```

## Google Search Engine

In this section, the IP address 1.2.3.4 was queried using the Google search engine. Specifically, TeamLogic IT searched for suspicious public information that may contain confidential details about 1.2.3.4, like password or login information. These results may show that confidential and/or sensitive information about 1.2.3.4 has been exposed to the public Internet. However, it is also possible that these results are completely innocent and no private data is available or exposed through Google's search engine. Click on the following link to review the results from this query:

[CLICK HERE TO VIEW THE GOOGLE SEARCH ENGINE QUERY FOR 1.2.3.4](#)

## All Discovered Security Threats Details

This section provides all the details about each discovered potential security threat on 1.2.3.4. These details are grouped by Risk Factor. Of the 21 possible security threats discovered on 1.2.3.4, 2 (10%) are considered High Risk, 5 (24%) are considered Medium Risk, 6 (29%) are considered Low Risk, and 8 (37%) are considered Other Risk.

If a threat has been modified, its heading will be color-coded using the following key:

■ New     
 ■ Unmodified     
 ■ Modified     
 ■ Resolved

### High Risk Security Threat Details

<p><b>Useable remote name server</b>          The remote name server allows recursive queries to be performed by the host running nssusd.</p> <p>If this is your internal nameserver, then forget this warning.</p> <p>If you are probing a remote nameserver, then it allows anyone to use it to resolve third parties names (such as www.nessus.org). This allows hackers to do cache poisoning attacks against this nameserver.</p> <p>If the host allows these recursive queries via UDP, then the host can be used to 'bounce' Denial of Service attacks against another network or system.</p> <p>See also : <a href="http://www.cert.org/advisories/CA-1997-22.html">http://www.cert.org/advisories/CA-1997-22.html</a></p> <p>Solution: Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it).</p> <p>If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf</p> <p>If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command</p> <p>Then, within the options block, you can explicitly state:          'allow-recursion { hosts_defined_in_acl }'</p> <p>For more info on Bind 9 administration (to include recursion), see:  <a href="http://www.nominum.com/content/documents/bind9arm.pdf">http://www.nominum.com/content/documents/bind9arm.pdf</a></p> <p>If you are using another name server, consult its documentation.</p> <p>CVE: <a href="#">CVE-1999-0024</a></p> <p>BugTraq ID: <a href="#">136</a>, <a href="#">678</a></p>	<p><b>Port:</b>          domain          (53/tcp)  <b>Family:</b>          DNS Services  <b>Risk:</b>  <span style="color: red;">High</span>  <b>Threat ID:</b>          10539</p>
<p><b>Apache &lt;= 1.3.31 htpasswd local overflow</b>          The remote host appears to be running a version of Apache which is older than 1.3.32.</p> <p>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.</p> <p>*** Note that Nessus solely relied on the version number          *** of the remote server to issue this warning. This might          *** be a false positive</p> <p>See also : <a href="http://xforce.iss.net/xforce/xfdb/17413">http://xforce.iss.net/xforce/xfdb/17413</a></p> <p>Solution: Upgrade to Apache 1.3.32 when available</p>	<p><b>Port:</b>          www          (80/tcp)  <b>Family:</b>          Web Services  <b>Risk:</b>  <span style="color: red;">High</span>  <b>Threat ID:</b>          14771</p>

<p>Additional Comments: NOTE FROM SAMPLE ENGINEER: This vulnerability will be resolved with our enterprise-wide upgrade tomorrow morning.</p>	
---	--

## Medium Risk Security Threat Details

<p><b>Determine which version of BIND name daemon is running</b> BIND 'NAMED' is an open-source DNS server from ISC.org. Many proprietary DNS servers are based on BIND source code.</p> <p>The BIND based NAMED servers (or DNS servers) allow remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind', will typically prompt the server to send the information back to the querying source.</p> <p>The remote bind version is : None</p> <p>Solution: Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts.</p> <p><b>DNS AXFR</b> 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.).</p> <p>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.</p> <p>Solution: Restrict DNS zone transfers to only the servers that absolutely need it.</p> <p>CVE: <a href="#">CAN-1999-0532</a></p>	<p><b>Port:</b> domain (53/tcp) <b>Family:</b> DNS Services <b>Risk:</b> Medium <b>Threat ID:</b> 10028</p> <p><b>Port:</b> domain (53/tcp) <b>Family:</b> DNS Services <b>Risk:</b> Medium <b>Threat ID:</b> 10595</p>
<p><b>http TRACE XSS attack</b> Your webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.</p> <p>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.</p> <p>An attacker may use this flaw to trick your legitimate web users to give him their credentials.</p> <p>Solution: Disable these methods.</p> <p>If you are using Apache, add the following lines for each virtual host in your configuration file :</p> <pre>RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE TRACK) RewriteRule .* - [F]</pre> <p>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.</p>	<p><b>Port:</b> www (80/tcp) <b>Family:</b> Cross-Site Scripting <b>Risk:</b> Medium <b>Threat ID:</b> 11213</p>

<p>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:</p> <pre>&lt;Client method="TRACE"&gt; AuthTrans fn="set-variable" remove-headers="transfer-encoding" set-headers="content-length: -1" error="501" &lt;/Client&gt;</pre> <p>If you are using Sun ONE Web Server releases 6.0 SP2 or below, compile the NSAPI plugin located at:  <a href="http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603">http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603</a></p> <p>See <a href="http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf">http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf</a>  <a href="http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html">http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html</a>  <a href="http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603">http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603</a>  <a href="http://www.kb.cert.org/vuls/id/867593">http://www.kb.cert.org/vuls/id/867593</a></p> <p><b>Additional Comments:</b>  NOTE FROM SAMPLE ENGINEER: This item was resolved on September 20, 2004.</p>	
<p><b>Remote host replies to SYN+FIN</b>  The remote host does not discard TCP SYN packets which have the FIN flag set.</p> <p>Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.</p> <p>See also : <a href="http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html">http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html</a>  <a href="http://www.kb.cert.org/vuls/id/464113">http://www.kb.cert.org/vuls/id/464113</a></p> <p>Solution: Contact your vendor for a patch</p> <p>BugTraq ID: <a href="#">7487</a></p>	<p><b>Port:</b>  general/tcp  <b>Family:</b>  Firewalls,  Routers, SNMP  <b>Risk:</b>  <b>Medium</b>  <b>Threat ID:</b>  11618</p>
<p><b>TCP sequence number approximation</b>  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 <a href="http://www.securityfocus.com/bid/10183/solution/">http://www.securityfocus.com/bid/10183/solution/</a></p> <p>CVE: <a href="#">CAN-2004-0230</a></p> <p>BugTraq ID: <a href="#">10183</a></p> <p>Other references : OSVDB: 4030, IAVA: 2004-A-0007</p>	<p><b>Port:</b>  general/tcp  <b>Family:</b>  Miscellaneous  <b>Risk:</b>  <b>Medium</b>  <b>Threat ID:</b>  12213</p>

## Low Risk Security Threat Details

<p><b>HTTP Server type and version</b>  The remote web server type is :</p> <p>Apache/1.3.31</p> <p>The 'ServerTokens' directive is set to ProductOnly however we could determine that the version of the remote server by requesting a non-existent page.</p>	<p><b>Port:</b>  www (80/tcp)  <b>Family:</b>  Web Services  <b>Risk:</b>  <b>Low</b>  <b>Threat ID:</b>  10107</p>
<p><b>icmp timestamp request</b></p>	<p><b>Port:</b></p>

<p>The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.</p> <p>This may help him to defeat all your time based authentication protocols.</p> <p>Solution: filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).</p> <p>CVE: <a href="#">CAN-1999-0524</a></p>	<p>general/icmp  <b>Family:</b>  Firewalls,  Routers, SNMP  <b>Risk:</b>  Low  <b>Threat ID:</b>  10114</p>
<p><b>POP3 Server type and version</b></p> <p>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.</p> <p>Versions and types should be omitted where possible.</p> <p>The version of the remote POP3 server is :  +OK sample.report.com v2003.83 server ready</p> <p>Solution: Change the login banner to something generic.</p>	<p><b>Port:</b>  pop3s  (995/tcp)  <b>Family:</b>  Mail Services  <b>Risk:</b>  Low  <b>Threat ID:</b>  10185</p>
<p><b>EXPN and VRFY commands</b></p> <p>The remote SMTP server answers to the EXPN and/or VRFY commands.</p> <p>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.</p> <p>Your mailer should not allow remote users to use any of these commands, because it gives them too much information.</p> <p>Solution: if you are using Sendmail, add the option :</p> <p>O PrivacyOptions=goaway</p> <p>in /etc/sendmail.cf.</p> <p>CVE: <a href="#">CAN-1999-0531</a></p>	<p><b>Port:</b>  smtp (25/tcp)  <b>Family:</b>  Mail Services  <b>Risk:</b>  Low  <b>Threat ID:</b>  10249</p>
<p><b>SSH Server type and version</b></p> <p>Remote SSH version : SSH-2.0-OpenSSH_3.8.1p1 Debian 1:3.8.1p1-8</p>	<p><b>Port:</b>  ssh (22/tcp)  <b>Family:</b>  Remote Shell  Access  <b>Risk:</b>  Low  <b>Threat ID:</b>  10267</p>
<p><b>DNS Cache Snooping</b></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><b>Port:</b>  domain  (53/udp)  <b>Family:</b>  DNS Services  <b>Risk:</b>  Low  <b>Threat ID:</b>  12217</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](http://community.sidestep.pt/~luis/DNS-Cache-Snooping/DNS_Cache_Snooping_1.1.pdf)

## Other Risk Security Threat Details

<p><b>Nmap</b> Nmap found that this host is running Linux 2.4.0 - 2.5.20</p>	<p><b>Port:</b> general/tcp <b>Family:</b> Miscellaneous <b>Risk:</b> <b>Other</b> <b>Threat ID:</b> 10336</p>
<p><b>SSL ciphers</b> 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:</p>	<p><b>Port:</b> imaps (993/tcp) <b>Family:</b> Miscellaneous <b>Risk:</b> <b>Other</b> <b>Threat ID:</b> 10863</p>

<p>d8:f2:00:af:61:41:d3:95:28:2c:3e:7a:de:71:b6:0b:1e:33: da:b6:38:73</p>	
<p><b>SSL ciphers</b> 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=hostmaster@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</p>	<p><b>Port:</b> pop3s (995/tcp) <b>Family:</b> Miscellaneous <b>Risk:</b> Other <b>Threat ID:</b> 10863</p>
<p><b>SSH protocol versions supported</b> The remote SSH daemon supports the following versions of the SSH protocol :</p> <ul style="list-style-type: none"> <li>. 1.99</li> <li>. 2.0</li> </ul> <p>SSHv2 host key fingerprint : 76:b8:68:fc:75:85:48:ba:56:f3:70:8c:af:da:ae:51</p>	<p><b>Port:</b> ssh (22/tcp) <b>Family:</b> Remote Shell Access <b>Risk:</b> Other <b>Threat ID:</b> 10881</p>
<p><b>Directory Scanner</b> The following directories were discovered: /cgi-bin, /icons, /images, /mailman, /mp3</p>	<p><b>Port:</b> www (80/tcp) <b>Family:</b></p>

<p>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</p>	<p>Remote File Access  <b>Risk:</b>  <b>Other</b>  <b>Threat ID:</b>  11032</p>
<p><b>IMAP Banner</b>  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.</p>	<p><b>Port:</b>  imaps (993/tcp)  <b>Family:</b>  Mail Services  <b>Risk:</b>  <b>Other</b>  <b>Threat ID:</b>  11414</p>
<p><b>smtpscan</b>  This server could be fingerprinted as being Sendmail 8.12.2</p>	<p><b>Port:</b>  smtp (25/tcp)  <b>Family:</b>  Mail Services  <b>Risk:</b>  <b>Other</b>  <b>Threat ID:</b>  11421</p>
<p><b>smtpscan</b>  This server could be fingerprinted as being Sendmail 8.12.2</p> <p><b>Additional Comments:</b>  NOTE FROM SAMPLE ENGINEER: This is the SMTP submission port for Sendmail. It corresponds to the existing port 25/TCP Sendmail process.</p>	<p><b>Port:</b>  submission (587/tcp)  <b>Family:</b>  Mail Services  <b>Risk:</b>  <b>Other</b>  <b>Threat ID:</b>  11421</p>
<p><b>Web Server hosting copyrighted material</b>  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.</p> <p>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.</p> <p>- /mp3/Alcohol.mp3</p> <p>Solution: Delete all the copyrighted files</p>	<p><b>Port:</b>  www (80/tcp)  <b>Family:</b>  Peer-To-Peer Services  <b>Risk:</b>  <b>Other</b>  <b>Threat ID:</b>  11778</p>
<p><b>DNS Server Fingerprint</b>  The remote name server could be fingerprinted as being : ISC BIND 9.2.3</p>	<p><b>Port:</b>  domain (53/udp)  <b>Family:</b>  DNS Services  <b>Risk:</b>  <b>Other</b>  <b>Threat ID:</b>  11951</p>

## External Advisories

Of the 21 possible security threats discovered on 1.2.3.4, there were 6 distinct 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	High	Useable remote name server on port domain (53/tcp) <a href="#">CVE-1999-0024</a> , <a href="#">BID-136</a> , <a href="#">BID-678</a>
10595	Medium	DNS AXFR on port domain (53/tcp) <a href="#">CAN-1999-0532</a>
11618	Medium	Remote host replies to SYN+FIN on port general/tcp <a href="#">BID-7487</a>
12213	Medium	TCP sequence number approximation on port general/tcp <a href="#">CAN-2004-0230</a> , <a href="#">BID-10183</a> , <a href="#">OSVDB-4030</a> , IAVA-2004-A-0007
10114	Low	icmp timestamp request on port general/icmp <a href="#">CAN-1999-0524</a>
10249	Low	EXPN and VRFY commands on port smtp (25/tcp) <a href="#">CAN-1999-0531</a>

## 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 TeamLogic IT 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.

## Why is Network Security Important?

---

You may have a good understanding of what network security is, but you may not know why it is so important. Being educated about what a hacker may be looking for on your system can help you understand why keeping your network secure is so critical.

There are several reasons for keeping your information secure. Of course the obvious reason that most people consider network security so important is to keep hackers away from their personal information. Intruders can gain access to your financial records, confidential client information, and private company data. However, this is not the only reason for security.

Most of us probably would not consider our communications and files to be top-secret information, but this does not mean we want others reading it. Many people believe if they only use their computers to send email, surf the Internet, or play computer games, they will not be targets for hacker attacks. Beware! Hackers may not care about your personal information; they may want to get into your network so they can attack other systems while making the attacks appear to be coming from you. Having this control over your network will enable them to mask their own identity. This could create a liability for your business, potentially even involvement in a federal investigation. Investing in a high-quality firewall is a good start to securing your network, but it is important to understand that firewalls are not threat-free. Having the best lock on your front door does not necessarily mean you will never be robbed. Likewise, having the best firewall does not automatically mean you will never be a victim of a hacker attack. It simply means that a hacker only has one thing to break to gain access to your entire network.

Hackers are discovering new vulnerabilities every day. Unfortunately, computer software is so complex that it is nearly impossible to ensure it is completely free of errors. Software vendors will often develop patches to address these errors after they are discovered. However, it is generally up to the user to find the patches and install them on their own computers.

## Ten Myths Versus Facts About Network Security

---

Many people and businesses unknowingly leave their private information readily available to hackers because they subscribe to some common myths about computer and network security. Below are ten myths and the facts to dispel them.

**MYTH** "I have virus protection software so I am already secure."

**FACT** Viruses and security threats are two completely different things. Your anti-virus software will not tell you about any of the security threats for which a TeamLogic IT vulnerability assessment will test your network, such as whether your financial or customer records are exposed to the Internet or whether your computer is vulnerable to various hacker attacks.

**MYTH** "I have a firewall so I don't need to worry about security threats."

**FACT** Firewalls are great and typically provide a good layer of security. However, firewalls commonly perform services such as port forwarding or network address translation (NAT). It is also surprisingly common for firewalls to be accidentally misconfigured (after all, to err is human). The only way to be sure your network really is secure is to test it. Among the security threats TeamLogic IT tests for, there is an entire category specifically for firewall vulnerabilities.

**MYTH** "I have nothing to worry about; there are too many computers on the Internet."

**FACT** People understand the need to lock their homes, roll up their car windows, and guard their purses and wallets. Why? Because if you don't, then sooner or later, you will be a victim. However, people are just starting to be aware that the same is true with their computers and networks. A single hacker can scan thousands of computers looking for ways to access your private information in the time it takes you to eat lunch.

**MYTH** "I know the security of my network and information is important, but all the solutions are too expensive and/or time consuming."

**FACT** While it is true that some network security products and services are very expensive and time consuming, Scan is a service specifically designed to be very robust, efficient, and effective, yet still affordable for anyone.

**MYTH** "I can't do anything about my network's security because I'm not a geek."

**FACT** While network security is a technical problem, TeamLogic IT has gone to great lengths to provide a solution that is comprehensible to non-technical people and geeks alike. You do not have to download, install, or configure anything. This document has a Business Analysis Report with everything explained in plain English and plenty of charts, graphs, and overviews. That report is specifically written for non-technical business people and home users.

**MYTH** "I know what is running on my computer and I am sure that it is secure."

**FACT** With the increased presence of spyware and other malicious software easily distributed on the Internet, it is impossible for a user to know everything that is running on a computer. Virtually all networked computers have one or more possible security threats or vulnerabilities. These threats could exist in your operating system, the software you run, your router/firewall, or anything else. As part of this document, you also receive a Comparative Security Ranking to let you know how the security of your network compares to all the other networks TeamLogic IT has analyzed.

**MYTH** "I tested my network a few months ago, so I know it is secure."

**FACT** New security threats and vulnerabilities are discovered daily. Just because your network tested well this month, does not mean it will still be secure next month - even if you didn't change anything. Just as you should frequently update your anti-virus software, it is also good practice to analyze your security regularly.

**MYTH** "Network and computer security is only important for large businesses."

**FACT** In reality, nothing could be further from the truth. Whether you are a casual home user or a large enterprise, your computer contains valuable and sensitive information. This could be financial records, passwords, business plans, confidential files, and any other private data. In addition to your private information, it is also important to protect your network from being used in denial of service attacks, as a relay to exploit other systems, as a repository for illegal software or files, and much more.

**MYTH** "A 'port scan' is the same thing as a security analysis scan and some web sites already give me that for nothing."

**FACT** Actually, a port scan and a security analysis scan are two very different things. In general terms, your computer's Internet connection has 65,535 unique service ports. These ports are used both by software running on your computer and by remote servers sending data to your computer (when you view a web page or check your email). A port scan will simply tell you which service ports are being used on your computer. It does not test any of these ports for security threats nor does it tell you where your network is vulnerable to possible hackers or attacks. When you get a security analysis scan, TeamLogic IT not only performs a thorough port scan, but also tests each open port for over 9,000 possible security threats and vulnerabilities.

**MYTH** "The best time to deal with network security is when a problem arises."

**FACT** The best time to deal with network security is right now, before a problem arises and to prevent you from ever becoming a victim. Think about it - the best time to lock the doors in your home is before a robbery occurs. Afterward it is already too late, the damage has been done. This is why it is critical to analyze your network's security now, to find and fix the vulnerabilities before a break-in happens.

## Who is TeamLogic IT?

---

Traditionally, information security is complex, time consuming and very expensive for businesses. TeamLogic IT works to eliminate all three of those problems. For the first time, robust network and information security services are fast, easy to use, and affordable for every business.

### THE GOOD NEWS

Businesses are becoming more aware of the critical importance of security for their computers, networks, confidential records, and electronic assets.

### THE BAD NEWS

These same businesses are frustrated when they discover that network security products and services are extremely expensive, complex, and unmanageable.

### THE RESULT

Many companies' computer security needs go unattended and their private data and networks remain exposed to hacker attacks.

TeamLogic IT's scan is an information security and hacker vulnerability assessment service. The system is automated and functions remotely. The customer does not need to download, install, or configure anything. This advanced technology emulates a team of "hackers" using thousands of unique methodologies and techniques to find the security threats, exposed private information, and attack vulnerabilities in any network. This data is then analyzed by a Certified Information Systems Security Professional (CISSP) and TeamLogic IT generates a detailed report that shows how the network could be attacked, what confidential information is exposed, the potential business impact of a hacker incident, and how to fix any security problems.

## Definition of Terms

---

TeamLogic IT tested your network for a total of 9,375 possible security threats. Each of these tests is classified by both a "family" (the type of security threat or the service that could be attacked) and a "risk factor" (the level of severity of the security threat or the probability that a hacker can exploit the vulnerability). This document also uses some terminology that may be unfamiliar to a non-technical audience. The following information provides an explanation of each family type and risk factor, and also defines some of the technical terminology used in this document.

### Security Threats Risk Factors Definitions

#### HIGH RISK

All security threats which can compromise the integrity of your data, expose your confidential information, be used to take your system(s) off-line, or can be used for denial of service (DoS) attacks are classified as high risk. These types of threats should be addressed first and are typically easy for a hacker to exploit and/or attack.

#### MEDIUM RISK

Security threats, which can open your system(s) to unauthorized access, expose your data/files/information, or cause certain portions of your network to crash (usually specific applications or services) are considered medium risk. Although usually (but not always) more complex to exploit, these types of threats are also very important to address.

#### LOW RISK

This classification of security threats is used for problems that typically cannot be used independently to gain unauthorized access to your data or compromise your system(s). However, these types of threats are commonly combined with other information to exploit your network.

#### OTHER RISK

This classification is used to provide informational data about your system(s). These types of security threats are typically not direct vulnerabilities, but they do expose additional information and data about your network. Hackers usually take this information to help them identify exactly how they will exploit or attack your network.

### 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.

#### 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.

### **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.

### **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.

### **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 Other Terminology**

### **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.

### **DEFENSE IN-DEPTH**

Defense In-Depth, is the approach of using multiple layers of security to guard against failure of a single security component.

### **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.

### **DMZ**

A Demilitarized Zone (DMZ) is a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.

### **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. For example, the domain name TeamLogic IT is www.sample-company.com.

### **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 by TeamLogic IT 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 TeamLogic IT security threats database.

### **FINGERPRINT**

To identify by means of a distinctive mark or characteristic. For example, TeamLogic IT uses a fingerprint 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.

### **GATEWAY**

A gateway is a network point (i.e. router) that acts as an entrance to another network.

### **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.

### **INTRUSION DETECTION SYSTEM**

An Intrusion Detection System (IDS) provides real-time security sentry (like a motion sensor) that protects the network from attack or unauthorized activity. An IDS analyzes the network datastream in search of activity signatures that have been deemed unauthorized, and then alarm and react to the activity. IDS can be passive or active defenses.

### **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 software used by most security professionals world-wide. TeamLogic IT uses Nessus as a security scanning engine to help with the TeamLogic IT scan service.

### **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.

### **NETWORK ADDRESS TRANSLATION**

Network Address Translation (NAT) is where a router hides internal IP addresses from sources outside the network. Only the router's IP address is visible to the Internet.

### **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 by TeamLogic IT to determine the severity or potential impact of a particular security threat. For example, security threats which could expose a company's financial records or customer databases would be considered "High Risk" in the TeamLogic IT security threats database.

### **SCAN**

The service offering which does remote automated hacker vulnerability analysis and security scanning. This report was generated using TeamLogic IT's scan service.

### **SECURITY SCAN**

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

### **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.