



HackerView Vulnerability Assessment

Silicon Forest Technology Group

IP Address Analyzed	1.2.3.4
Operating System Fingerprint	Unknown version of Linux web server running Apache
Technical Attention Priority	Immediate – Questionable services running
Type of Analysis	External Scan
Analysis Date / Time	October 14, 2008
Security Threats Discovered	200 open ports (various threat levels)
Serious Threats Discovered	2
Document ID #	HV8295-02

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

*****THIS IS AN EXAMPLE HACKERVIEW THAT LACKS SPECIFICS AND PCI REMEDIATION DATA*****

Executive Summary

This document provides the results of the vulnerability assessment performed by iSecurityPolicy against 1.2.3.4 on Tuesday, October 15, 2008. The information contained within this document is considered extremely confidential and should be treated as such.

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. iSecurityPolicy tested for over 20,000 different potential security vulnerabilities.

Payment Card Industry (PCI) scan summary: **NON-COMPLIANT** (see attachment for specific scan results)

During the process of this analysis, iSecurityPolicy discovered 200 open ports and 17 closed ports. This is abnormally high for a server. Of the discovered security threats, 2 of them are considered Serious Risks: weak SSL ciphers on port 443 (SSL) and the hosting of online gaming services on port 3724 (battlenet). It appears an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) may have noticed the scanning and closed ports temporarily.

A hacker would be able to ascertain a lot of information about this server from simple scans:

- Linux server running Apache (web server)
- The server is primarily a web server, but it also is acting in a role of an FTP server (port 21), file server (port 7000), possible game server (port 3724), and other services.
- Running Intrusion Detection System(s) (IDS) – Black Ice and NetProwler
- Veritas NetBackup is being used to backup data off-site to another server
- Three different types of remote management services are installed: Big Brother, VNC, and GroupWise

It is highly recommended that each service identified by this vulnerability assessment be validated as a necessary service. If the service is not essential, it should be shut off. The more services running on the server, the more avenues are available for a hacker to breach your network security. It only takes one weakness to gain control.

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.

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 18 security threats discovered on 1.2.3.4, 0 (0%) are considered High Risk and 2 (11%) are considered Medium Risk.

High Risk Security Threats Summaries

ID	Family	Summary
N/A	N/A	Battlenet – online gaming server

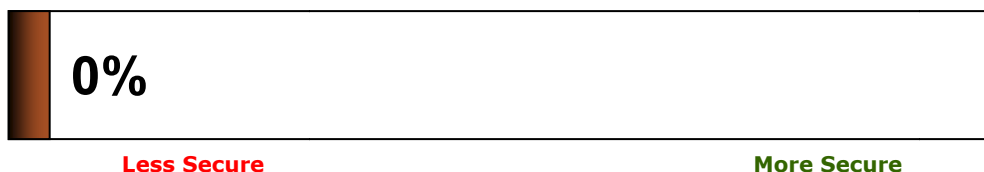
Medium Risk Security Threats Summaries

ID	Family	Summary
N/A	Web Services	The IIS server appears to have the .SHTML ISAPI filter mapped (ports 80 & 443)

Comparative Security Ranking

iSecurityPolicy 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 iSecurityPolicy 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 iSecurityPolicy has analyzed.

This Comparative Security Ranking gives an indication of how 1.2.3.4 compares to all of the other systems iSecurityPolicy has analyzed. For example, a rating of 100% would mean that 1.2.3.4 is more secure than every other system iSecurityPolicy 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 the HackerView scan services.



Most single-function servers that are considered "hardened" have minimal services running. In general, most secure servers have less than 6-10 ports open on the perimeter firewall. Having 200 ports open and communicating with external hosts is considered not hardened, especially with services such as FTP and gaming applications on a production web server.

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"/>	N/A	N/A

Outstanding Medium Risk Security Threats

Complete	ID	Summary
<input type="checkbox"/>	10937	Unmap the .SHTML extension

Other Items

Complete	ID	Summary
<input type="checkbox"/>	Recommended	Disable all non-essential services / ports
<input type="checkbox"/>	Recommended	Install (and update regularly) high quality anti-virus software
<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 iSecurityPolicy 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 iSecurityPolicy 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.

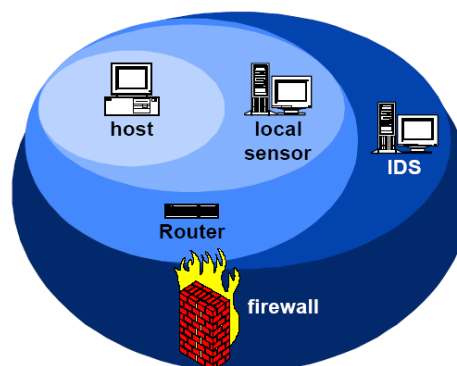
Just as you should frequently update your anti-virus software, it is also good practice to analyze your network's security regularly. New security threats and vulnerabilities are discovered daily and the iSecurityPolicy database of security threats generally grows by 5-10 new vulnerabilities every week. iSecurityPolicy 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 iSecurityPolicy's trained experts guide you through a needs assessment and install the hardware and software solution to meet your needs.

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.

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 (iSecurityPolicy) 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)
100%	4	0	0	0	0

Traceroute Response

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

Hop	Travel Time	IP	Hostname	TTL	Country	Time
1	0.5 ms	36.36.240.2 AS14361	c-v1102-d1.acc.dca2.hippie.net.	255	US	Unknown: 82e5d7e3
2	0.5 ms [+0ms]	36.36.224.249 AS0	gec3.core2.dca2.hippie.net.	254	US	Unix: 21:07:28.599
3	1.5 ms [+1ms]	36.36.224.185 AS0	iar2-ge-2-0-0.washington.savvis.net.	252	US	Unix: 22:08:59.301
4	1.7 ms [+0ms]	204.24.226.61 AS3561	acr1-loopback.washington.savvis.net.	252	US	Unix: 22:08:59.334
5	1.7 ms [+0ms]	204.24.227.21 AS3561	bcs2-so-2-3-0.washington.savvis.net.	250	US	Unix: 22:08:59.365
6	15 ms [+13ms]	204.30.192.61 AS3561	dcr2-so-7-1-0.atlanta.savvis.net.	250	US	Unix: 22:08:59.413
7	37 ms [+21ms]	204.30.192.70 AS3561	dcr2-so-2-0-0.dallas.savvis.net.	249	US	Unix: 22:08:59.493
8	68 ms [+30ms]	204.30.194.153 AS3561	dcr1.lay-so-3-2-0.losangeles.savvis.net.	247	US	Unix: 22:08:59.577
9	101 ms [+33ms]	208.172.35.62 AS3561	Ahr4-pos-0-0.irvine2oc2.savvis.net.	246	US	Unix: 22:08:59.648
10	101 ms [+0ms]	116.39.96.83 AS3561	csr193-ve214.irvine2oc2.savvis.net.	54	US	[Router did not respond]
11	101 ms [+0ms]	[Unknown]	[Unknown - Firewall did not respond]			
12	101 ms [+0ms]	1.2.3.4 AS3561	[Reached Destination] unknown.savvis.net	118	US	[Router did not respond]

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 as 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 not 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.

How I am searching:

Asking i.root-servers.net for 18.174.59.64.in-addr.arpa PTR record:

i.root-servers.net says to go to figwort.arin.net. (zone: 64.in-addr.arpa.)

Asking figwort.arin.net for 18.174.59.64.in-addr.arpa PTR record:

figwort.arin.net [192.42.93.32] says to go to dns04.savvis.net. (zone: 174.79.64.in-addr.arpa.)

Asking dns04.savvis.net for 18.174.59.64.in-addr.arpa PTR record: Reports that no PTR records exist [from 18.174.59.68].

Answer:

No PTR records exist for 1.2.3.4. [Neg TTL=3600 seconds]

Details:

dns04.savvis.net. (an authoritative nameserver for 174.79.64.in-addr.arpa., which is in charge of the reverse DNS for 1.2.3.4) says that there are no PTR records for 1.2.3.4.

To get reverse DNS set up for 1.2.3.4, you need to speak to your Internet provider. You could also check with dns@savvis.com., who is in charge of the 174.79.64.in-addr.arpa. zone.

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:

```
IP address:          1.2.3.4
Reverse DNS:         [No reverse DNS entry per dns01.savvis.net.]
Reverse DNS authenticity: [Unknown]
ASN:                 358961
ASN Name:           SAVVIS
IP range connectivity: 2
Registrar (per ASN): ARIN
Country (per IP registrar): US [United States]
Country Currency:   USD [United States Dollars]
Country IP Range:   64.79.160.0 to 64.79.175.255
Country fraud profile: Normal
City (per outside source): Cary, North Carolina
Private (internal) IP? No
IP address registrar: whois.arin.net
Known Proxy?       No
```

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:

Using 0 day old cached answer (or, you can [get fresh results](#)).
Hiding E-mail address (you can [get results with the E-mail address](#)).

```
OrgName: Savvis
OrgID: SAVVI-2
Address: 3300 Regency Parkway
City: Cary
StateProv: NC
PostalCode: 27511
Country: US
```

```
ReferralServer: rwhois://rwhois.savvis.net:4321/
```

```
NetRange: 64.79.160.0 - 64.79.175.255
CIDR: 64.79.160.0/20
NetName: SAVVIS
NetHandle: NET-64-79-160-0-1
Parent: NET-64-0-0-0-0
NetType: Direct Allocation
NameServer: DNS01.SAVVIS.NET
NameServer: DNS02.SAVVIS.NET
NameServer: DNS03.SAVVIS.NET
NameServer: DNS04.SAVVIS.NET
Comment:
RegDate:
Updated: 2004-10-07
```

```
OrgAbuseHandle: ABUSE11-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-877-393-7878
OrgAbuseEmail: *****@savvis.net
```

```
OrgNOCHandle: NOC99-ARIN
OrgNOCName: Network Operations Center
OrgNOCPHONE: +1-800-213-5127
OrgNOCEmail: *****@savvis.net
```

OrgTechHandle: [UIAA-ARIN](#)
 OrgTechName: US IP Address Administration
 OrgTechPhone: +1-800-213-5127
 OrgTechEmail: *****@savvis.net

ARIN WHOIS database, last updated 2006-04-05 19:10
 # Enter ? for additional hints on searching ARIN's WHOIS database.

Google Search Engine

In this section, the IP address 1.2.3.4 was queried using the Google search engine. Specifically, iSecurityPolicy 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 18 possible security threats discovered on 1.2.3.4, 0 (0%) are considered High Risk, 2 (11%) are considered Medium Risk, 3 (17%) are considered Low Risk, and 13 (72%) 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

Port: N/A Family: N/A Risk: High	N/A
---	-----

Medium Risk Security Threat Details

Port: http (80/tcp) Family: Web Services Risk: Medium Threat ID: 10937	
Port: ms-wbt-server (3389/tcp) Family:	Synopsis : It may be possible to get access to the remote host. Description :


<p>Web Services</p> <p>Risk: Medium</p> <p>Threat ID: 10937</p> <p>ms-wbt-server (3389/tcp)</p>	<p>The remote version of Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man in the middle attack.</p> <p>An attacker may exploit this flaw to decrypt communications between client and server and obtain sensitive information (passwords, ...).</p> <p>Solution: Force the use of SSL as a transport layer for this service.</p> <p>See Also : http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?c544b1fa</p> <p>Risk Factor : Medium / CVSS Base Score : 6 (AV:R/AC:H/Au:NR/C:P/A:P/I:P/B:N) CVE : CVE-2005-1794 BID : 13818 Other references : OSVDB:17131 Plugin ID : 18405</p> <p> Port is open Plugin ID : 11219</p> <p> Synopsis : The remote Windows host has Terminal Services enabled.</p> <p>Description : Terminal Services allows a Windows user to remotely obtain a graphical login (and therefore act as a local user on the remote host).</p> <p>If an attacker gains a valid login and password, he may be able to use this service to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.</p> <p>Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.</p> <p>Solution: Disable Terminal Services if you do not use it, and do not allow this service to run across the Internet.</p> <p>Risk Factor : None Plugin ID : 10940</p>
--	--

Low Risk Security Threat Details

<p>Port: http (80/tcp)</p> <p>Family: Web Services</p> <p>Risk:</p>	<p>Information found on port http (80/tcp)</p> <p>The remote host appears to be running a version of IIS which allows remote users to determine which authentication schemes are required for confidential webpages.</p> <p>Specifically, the following methods are enabled on the remote webserver: - IIS NTLM authentication is enabled</p>
--	--

<p>Low</p> <p>Threat ID: 11871</p>	<p>Solution : None at this time Risk factor : Low CVE : CVE-2002-0419 BID : 4235 Nessus ID : 11871</p>
<p>Port: https (443/tcp)</p> <p>Family: Web Services</p> <p>Risk: Low</p> <p>Threat ID: 11871</p>	<p>Information found on port https (443/tcp)</p> <p>The remote host appears to be running a version of IIS which allows remote users to determine which authentication schemes are required for confidential webpages.</p> <p>Specifically, the following methods are enabled on the remote webserver: - IIS NTLM authentication is enabled</p> <p>Solution : None at this time Risk factor : Low CVE : CVE-2002-0419 BID : 4235 Nessus ID : 11871</p>
<p>Port: https (443/tcp)</p> <p>Family: Web Services</p> <p>Risk: Low</p> <p>Threat ID: 20007</p>	<p>Information found on port https (443/tcp)</p> <p>Synopsis :</p> <p>The remote service encrypts traffic using a protocol with known weaknesses.</p> <p>Description :</p> <p>The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.</p> <p>See also :</p> <p>http://www.schneier.com/paper-ssl.pdf</p> <p>Solution :</p> <p>Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.</p> <p>Risk factor :</p> <p>Low / CVSS Base Score : 2 (AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N) Nessus ID : 20007</p>

Other Risk Security Threat Details

<p>Port: callbook (2000/tcp)</p> <p>Family: Port Scanner</p> <p>Risk: Other</p>	<p> Port is open Plugin ID : 11219</p>
---	--

<p>Threat ID: 11219</p>	
<p>Port: http (80/tcp)</p> <p>Family: Web Services</p> <p>Risk: Other</p> <p>Threat ID: 11219 10330 10107 24260</p>	<div data-bbox="462 283 495 325"></div> <p>Port is open Plugin ID : 11219</p> <div data-bbox="462 378 495 420"></div> <p>A web server is running on this port Plugin ID : 10330</p> <div data-bbox="462 472 495 514"></div> <p>Synopsis : A web server is running on the remote host.</p> <p>Description : This plugin attempts to determine the type and the version of the remote web server.</p> <p>Risk Factor : None</p> <p>Plugin output : The remote web server type is : Boa/0.94.13</p> <p>Plugin ID : 10107</p> <div data-bbox="462 1029 495 1071"></div> <p>Synopsis : Some information about the remote HTTP configuration can be extracted.</p> <p>Description : This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...</p> <p>This test is informational only and does not denote any security problem</p> <p>Solution: None.</p> <p>Risk Factor : None</p> <p>Plugin output : Protocol version : HTTP/1.0 SSL : no Pipelining : no Keep-Alive : yes Options allowed : (Not implemented) Headers :</p> <p>Date: Mon, 17 Dec 2007 18:57:33 GMT Server: Boa/0.94.13</p>

	<p>Connection: Keep-Alive Keep-Alive: timeout=10, max=1000 Content-Length: 1064 Last-Modified: Wed, 08 Nov 2006 06:51:28 GMT Content-Type: text/html</p> <p>Plugin ID : 24260</p>
<p>Port: http (80/tcp)</p> <p>Family: Web Services</p> <p>Risk: Other</p> <p>Threat ID: 10107</p>	
<p>Port: http (80/tcp)</p> <p>Family: Web Services</p> <p>Risk: Other</p> <p>Threat ID: 11874</p>	
<p>Port: http (80/tcp)</p> <p>Family: Web Services</p> <p>Risk: Other</p> <p>Threat ID: 10759</p>	
<p>Port: http (80/tcp)</p> <p>Family: Web Services</p> <p>Risk: Other</p> <p>Threat ID: 12234</p>	
<p>Port: https (443/tcp)</p> <p>Family:</p>	

<p>Web Services</p> <p>Risk: Other</p> <p>Threat ID: 10330</p>	
<p>Port: https (443/tcp)</p> <p>Family: Web Services</p> <p>Risk: Other</p> <p>Threat ID: 10330</p>	
<p>Port: https (443/tcp)</p> <p>Family: Web Services</p> <p>Risk: Other</p> <p>Threat ID: 10863</p>	<p>Information found on port https (443/tcp) Here is the SSLv2 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 368276 (0x59e94) Signature Algorithm: sha1WithRSAEncryption Issuer: C=US, O=Equifax, OU=Equifax Secure Certificate Authority Validity Not Before: Dec 23 22:16:34 2005 GMT Not After : Dec 24 22:16:34 2006 GMT Subject: C=US, O=*.teamlogicit.com, OU=https://services.choicepoint.net/get.jsp?GT60490495, OU=See www.geotrust.com/resources/cps (c)05, OU=Domain Control Validated - Power Server ID(TM), CN=*.teamlogicit.com Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:c8:7d:96:9c:7f:b7:2e:fa:2b:6d:51:14:f1:75: 5f:93:96:49:04:9e:6c:55:81:ff:d9:e8:4d:0c:60: f5:cc:c5:d3:25:e9:8a:5a:94:5d:67:dd:00:4e:16: 6a:a7:5c:16:01:c0:06:45:48:ec:f5:90:e0:83:79: c2:b1:7c:a5:76:36:67:7c:49:65:90:78:34:57:b0: 4e:5a:16:1f:da:c4:f1:10:fb:09:a0:e9:3c:c4:12: 8e:2a:7e:e1:9d:c2:e1:66:51:c6:7b:12:d2:5c:70: 94:42:ac:92:2a:77:23:a8:2e:1d:e0:b8:38:cf:21: 33:99:c5:a1:28:a8:ec:45:cf Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Key Usage: critical Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment X509v3 Subject Key Identifier: 86:91:77:C5:77:77:20:1C:57:76:C4:99:E6:6C:9E:7F:0C:07:63:40 X509v3 CRL Distribution Points: URI:http://crl.geotrust.com/crls/secureca.crl X509v3 Authority Key Identifier: keyid:48:E6:68:F9:2B:D2:B2:95:D7:47:D8:23:20:10:4F:33:98:90:9F:D4 X509v3 Extended Key Usage:</p>

	<p>TLS Web Server Authentication, TLS Web Client Authentication Signature Algorithm: sha1WithRSAEncryption 2d:0c:76:2c:1d:64:e9:c3:dd:39:a7:92:1a:77:f4:2f:0c:08: ab:51:09:59:7f:d0:17:f9:df:9a:dc:61:b3:7c:60:a3:2d:c1: 7d:1b:98:91:b1:f4:c1:fb:3f:44:d5:f0:3e:e0:39:61:2e:2b: d8:37:11:d2:ca:19:a0:2a:dd:47:6a:ec:e0:47:9b:e7:65:14: b1:ed:23:8d:14:85:68:90:6f:9b:75:04:b5:e6:da:ed:3f:59: b2:85:84:d5:82:54:48:dc:88:0c:07:81:bb:a7:c6:f2:39:3c: a3:66:79:2f:d1:8f:fe:07:c3:a8:7b:8a:5a:aa:81:ea:83:5c: 2d:b5</p> <p>Here is the list of available SSLv2 ciphers: RC4-MD5 EXP-RC4-MD5 RC2-CBC-MD5 EXP-RC2-CBC-MD5 DES-CBC-MD5 DES-CBC3-MD5</p> <p>The SSLv2 server offers 4 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack</p> <p>Solution: disable those ciphers and upgrade your client software if necessary. See http://support.microsoft.com/default.aspx?scid=kb;en-us;216482 or http://httpd.apache.org/docs-2.0/mod/mod_ssl.html#sslciphersuite</p> <p>This SSLv2 server also accepts SSLv3 connections. This SSLv2 server also accepts TLSv1 connections.</p> <p>Nessus ID : 10863</p>
<p>Port: https (443/tcp)</p> <p>Family: Web Services</p> <p>Risk: Other</p> <p>Threat ID: 11032</p>	
<p>Port: https (443/tcp)</p> <p>Family: Web Services</p> <p>Risk: Other</p> <p>Threat ID: 10330</p>	
<p>Port: https (443/tcp)</p> <p>Family: Web Services</p>	

Risk: Other	
Threat ID: 10330	
Port: mt-term-serv (3389/tcp)	
Family: Remote File Access	
Risk: Other	
Threat ID: 10330	

External Advisories

Of the 18 possible security threats discovered on 1.2.3.4, there were 3 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
10937	Medium	ISAPI filter in Front Page Server Extensions
		CVE : CVE-2002-0072 , BID : 1066, 4479 , IAVA:2002-A-0002, Nessus ID : 10937
11871	Low	Information leaks in IIS
		CVE : CVE-2002-0419 , BID : 4235 , Nessus ID : 11871
20007	Low	Remote service accepts connections encrypted using SSL 2.0
		Nessus ID : 20007

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 iSecurityPolicy 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 iSecurityPolicy 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 iSecurityPolicy 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, iSecurityPolicy 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 iSecurityPolicy 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, iSecurityPolicy 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 iSecurityPolicy?

Traditionally, information security is complex, time consuming and very expensive for businesses. iSecurityPolicy 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.

iSecurityPolicy'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 iSecurityPolicy 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

iSecurityPolicy 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 iSecurityPolicy 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 iSecurityPolicy 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 iSecurityPolicy security threats database.

FINGERPRINT

To identify by means of a distinctive mark or characteristic. For example, iSecurityPolicy 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. iSecurityPolicy uses Nessus as a security scanning engine to help with the iSecurityPolicy 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 iSecurityPolicy 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 iSecurityPolicy security threats database.

SCAN

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

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.