



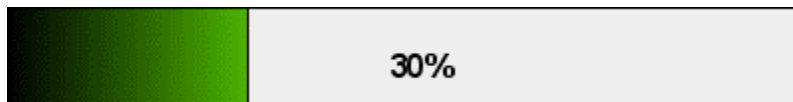
Knowledge is your Best Security

<b>IP ADDRESS ANALYZED</b>	XXX.XXX.XXX.XXX www.testsystem.com
<b>OPERATING SYSTEM FINGERPRINT</b>	Unknown
<b>TECHNICAL ATTENTION PRIORITY</b>	30%
<b>TYPE OF ANALYSIS</b>	External Scan
<b>ANALYSIS DATE</b>	Saturday - May 14, 2005 - 11:00 PM (GMT-5)
<b>SECURITY THREATS DISCOVERED</b>	13
<b>SEVERE THREATS DISCOVERED</b>	3
<b>DOCUMENT ID NUMBER</b>	6742 - 18339 - 20923

## Executive Summary

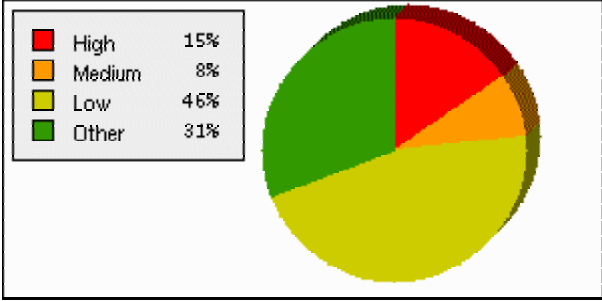
This document provides the results of the vulnerability assessment performed by Symtrex, Inc. against XXX.XXX.XXX.XXX on Saturday, May 14, 2005 at 11:00 PM (GMT-5). The information contained within this document is considered extremely confidential and should be treated as such.

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.

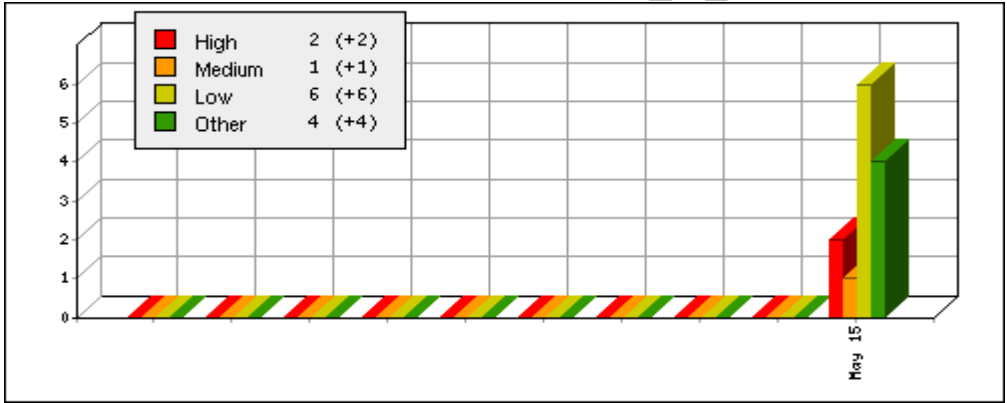


The scope of this analysis was to remotely audit and analyze the system and/or resources of XXX.XXX.XXX.XXX. This provides a "hacker's eye view" of the system to discover its security vulnerabilities and weaknesses to possible hacker penetration or attack. Symtrex, Inc. tested for 7793 different potential security vulnerabilities.

During the process of this analysis, Symtrex, Inc. discovered 13 possible security threats. Of the discovered security threats, 3 of them are considered severe.



The graph below gives a historical perspective of the number of known security threats discovered for XXX.XXX.XXX.XXX. 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 SymtrexVA reports, please consider reading the Education report, located at the very bottom of this document.

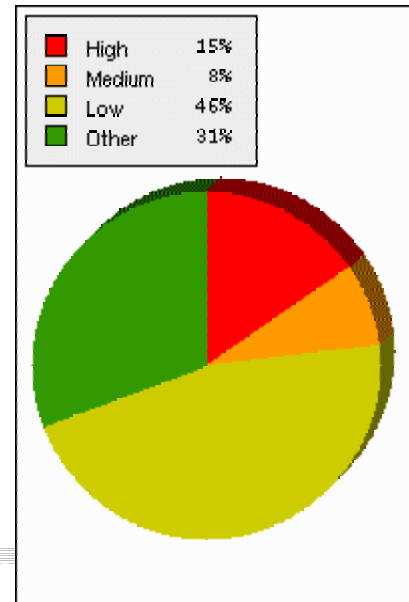
## Business Analysis Report

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 SymtrexVA results in plain-English, graphical, and summarized formats. For the intended audience, this report will contain the majority of the relevant information and data.

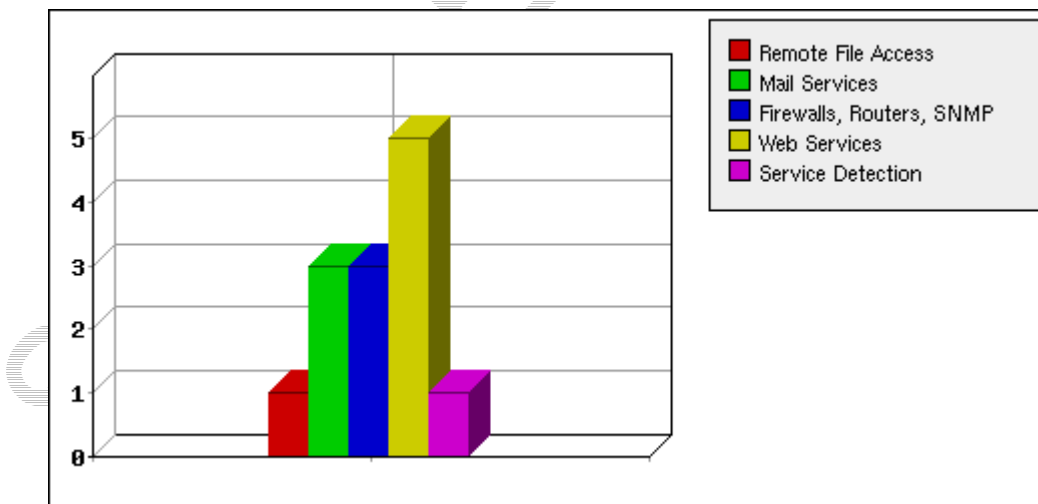
### Security Threats by Risk Factor

This SymtrexVA discovered a total of 13 potential security threats to XXX.XXX.XXX.XXX. Of this total number, 2 of the threats are classified as High Risk and 1 are classified as Medium Risk.



### Security Threats By Family

The 13 potential security threats discovered on XXX.XXX.XXX.XXX are spread across 5 different families of threat classifications. A large diversification of families (> 4) is cause for concern.



## Security Threats By Open Network Port

---

This SymtrexVA analysis discovered a total of 2 open network ports on XXX.XXX.XXX.XXX. 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
25/tcp	smtp	simple mail transfer
80/tcp	http	Microsoft IIS webserver 6.0

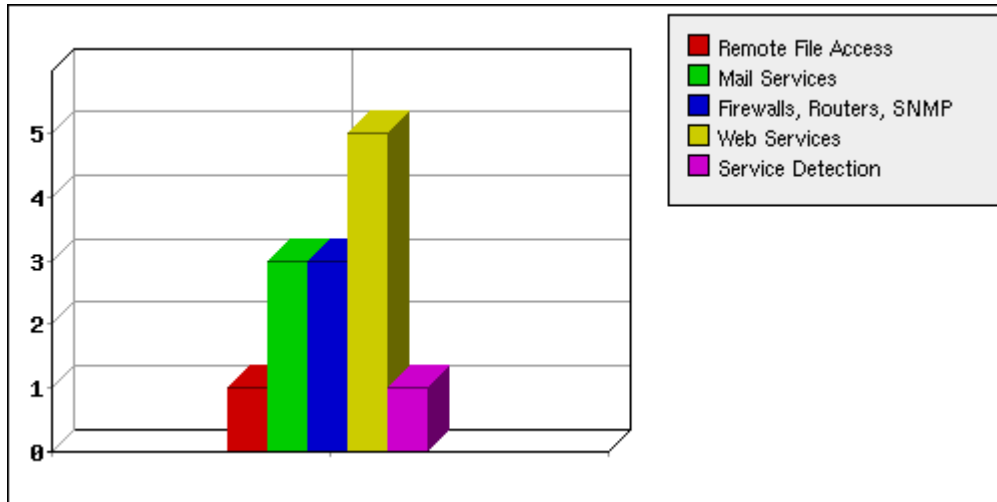
The following table shows a cross-reference of all discovered security threats by port number and Risk Factor. This analysis will help to determine which port represents the greatest overall risk to the target system.

Port	High	Medium	Low	Other	Total
25/tcp	0	0	2	1	3
80/tcp	1	0	2	3	6
500/udp	0	0	1	0	1
general/tcp	0	1	1	0	2
general/udp	1	0	0	0	1

## Security Threats By Family

---

This SymtrexVA analysis discovered a total of 13 potential security threats to XXX.XXX.XXX.XXX. Of this total number, 2 of the threats are classified as High Risk and 1 are classified as Medium Risk. The Medium and High Risk threats are considered serious because they represent direct threats to XXX.XXX.XXX.XXX. 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 13 potential security threats discovered on XXX.XXX.XXX.XXX are spread across 5 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
Firewalls, Routers, SNMP	1	1	1	0	3
Mail Services	0	0	2	1	3
Remote File Access	0	0	0	1	1
Service Detection	0	0	1	0	1
Web Services	1	0	2	2	5

## Immediate Needs

This section will review the discovered security threats that are more probable to pose an immediate risk of attack to XXX.XXX.XXX.XXX. 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 13 security threats discovered on XXX.XXX.XXX.XXX, 2 (15%) are considered High Risk and 1 (7%) are considered Medium Risk.

## High Risk Security Threats Summaries

ID	Family	Summary
11580	Firewalls, Routers, SNMP	UDP packets with source port of 53 bypass firewall rules
11874	Web Services	IIS Service Pack - 404

■ New      ■ Unmodified      ■ Modified      ■ Resolved

## Medium Risk Security Threats Summaries

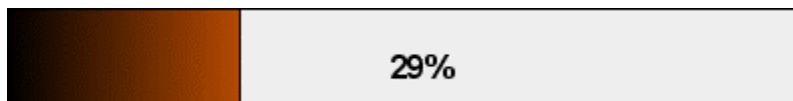
ID	Family	Summary
11618	Firewalls, Routers, SNMP	Remote host replies to SYN+FIN

■ New      ■ Unmodified      ■ Modified      ■ Resolved

## Comparative Security Ranking

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

This Comparative Security Ranking gives an indication of how XXX.XXX.XXX.XXX compares to all of the other systems Symtrex, Inc. has analyzed. For example, a rating of 100% would mean that XXX.XXX.XXX.XXX is more secure than every other system Symtrex, Inc. has analyzed, while a rating of 0% would mean that XXX.XXX.XXX.XXX 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 XXX.XXX.XXX.XXX compares to others using SymtrexVA.



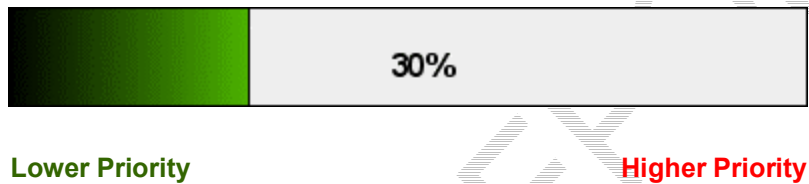
Less Secure

More Secure

## 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 work-flow 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"/>	11580	UDP packets with source port of 53 bypass firewall rules
<input type="checkbox"/>	11874	IIS Service Pack - 404

New  Unmodified  Modified  Resolved

### Outstanding Medium Risk Security Threats

Complete	ID	Summary
<input type="checkbox"/>	11618	Remote host replies to SYN+FIN

New  Unmodified  Modified  Resolved

## Other Items

Complete	Type	Item Summary
<input type="checkbox"/>	Recommended	Install a high quality firewall as a "front line" defense
<input type="checkbox"/>	Recommended	Install (and update regularly) high quality anti-virus software
<input type="checkbox"/>	Recommended	Perform Symtrex, Inc. security analysis on all network devices
<input type="checkbox"/>	Recommended	Verify online database (ARIN, Domain, and Google) information
<input type="checkbox"/>	Recommended	Make regular backups of all critical data. Test the backups for errors.
<input type="checkbox"/>	Recommended	Install latest patches and updates for operating system and applications
<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 Symtrex, Inc. 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 Symtrex, Inc. 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 Symtrex, Inc. database of security threats generally grows by 5-10 new vulnerabilities every week. Symtrex, Inc. has even seen more than 80 new security threats crop up in a single month.

## Security Notifications Newsletter

Symtrex, Inc. provides a free monthly email newsletter about the new security threats added to the Symtrex, Inc. database. 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 SymtrexVA 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 SymtrexVA analysis. For the intended audience, this report will contain the majority of the relevant information and data.

## Security Threats By Open Network Port

---

This SymtrexVA analysis discovered a total of 2 open network ports on XXX.XXX.XXX.XXX. 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.

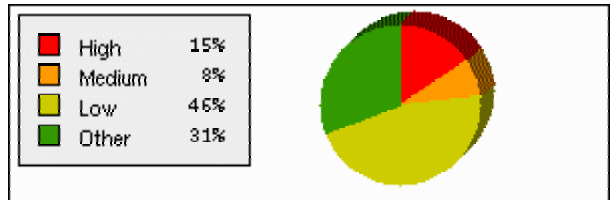
Port	Service	Fingerprint
25/tcp	smtp	simple mail transfer
80/tcp	http	Microsoft IIS webserver 6.0

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
25/tcp	0	0	2	1	3
80/tcp	1	0	2	3	6
500/udp	0	0	1	0	1
general/tcp	0	1	1	0	2
general/udp	1	0	0	0	1

## Discovered Security Threat Summaries

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



## High Risk Security Threats

ID	Family	Summary
11580	Firewalls, Routers, SNMP	UDP packets with source port of 53 bypass firewall rules
11874	Web Services	IIS Service Pack - 404

■ New     
 ■ Unmodified     
 ■ Modified     
 ■ Resolved

## Medium Risk Security Threats

ID	Family	Summary
11618	Firewalls, Routers, SNMP	Remote host replies to SYN+FIN

New       Unmodified       Modified       Resolved

## Low Risk Security Threats

ID	Family	Summary
10249	Mail Services	EXPN and VRFY commands
10263	Mail Services	SMTP Server type and version
10759	Web Services	Private IP address leaked in HTTP headers
11871	Web Services	Find if IIS server allows BASIC and/or NTLM authentication
11935	Firewalls, Routers, SNMP	IPSEC IKE detection
11936	Service Detection	OS Identification

New       Unmodified       Modified       Resolved

## Other Security Threats

ID	Family	Summary
10107	Web Services	HTTP Server type and version
11032	Remote File Access	Directory Scanner
11421	Mail Services	smtpscan
11699	Web Services	URLScan Detection

New       Unmodified       Modified       Resolved

## Ignored Security Threats

**NO THREATS IGNORED**

## Network Characteristics

---

This section is not specific to security threats or vulnerabilities. Rather, the Network Characteristics section provides general information about how XXX.XXX.XXX.XXX responded to some standard basic network testing. The information in this section may be useful to gain an understanding of the characteristics of XXX.XXX.XXX.XXX as seen from a remote network (Symtrex, Inc.) 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	Round-Trip Times	Minimum	Average	Maximum
0%	---->	66.0 (ms)	67.739 (ms)	69.696 (ms)

## Traceroute Response

---

The information below shows a traceroute originating from the Symtrex, Inc. network to XXX.XXX.XXX.XXX. This traceroute was performed using a maximum TTL value of 30, one UDP query per TTL, and a starting TTL of 5.

Hop	Hostname	IP Address	Round-Trip Time
5	Removed for security	XXX.XXX.XXX.XXX	14.638

6	Removed for security	XXX.XXX.XXX.XXX	46.923
7	Removed for security	XXX.XXX.XXX.XXX	47.026
8	Removed for security	XXX.XXX.XXX.XXX	46.876
13	Removed for security	XXX.XXX.XXX.XXX	66.813

---

## Reverse DNS Information

The IP address XXX.XXX.XXX.XXX 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.

Results have been removed for security reasons
--

---

## 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 XXX.XXX.XXX.XXX. 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 XXX.XXX.XXX.XXX. The results of this query should show the owner (and associated contacts) for the XXX.XXX.XXX.XXX 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 XXX.XXX.XXX.XXX:

Results have been removed for security reasons.

## Domain Name Registries

---

This section attempted to resolve the domain name for XXX.XXX.XXX.XXX. 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 XXX.XXX.XXX.XXX. 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 XXX.XXX.XXX.XXX:

Whois Server Version 1.3

Results have been removed for security reasons.

## Google Search Engine

---

In this section, the IP address XXX.XXX.XXX.XXX was queried using the Google search engine. Specifically, Symtrex, Inc. searched for suspicious public information that may contain confidential details about XXX.XXX.XXX.XXX, like password or login information. These results may show that confidential and/or sensitive information about XXX.XXX.XXX.XXX 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 XXX.XXX.XXX.XXX](#)**

## All Discovered Security Threats Details

---

This section provides all the details about each discovered potential security threat on XXX.XXX.XXX.XXX. These details are grouped by Risk Factor. Of the 13 possible security threats discovered on XXX.XXX.XXX.XXX, 2 (15%) are considered High Risk, 1 (7%) are considered Medium Risk, 6 (46%) are considered Low Risk, and 4 (30%) 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>UDP packets with source port of 53 bypass firewall rules</b></p> <p>It is possible to by-pass the rules of the remote firewall by sending UDP packets with a source port equal to 53.</p> <p>An attacker may use this flaw to inject UDP packets to the remote hosts, in spite of the presence of a firewall.</p> <p>Solution: Review your firewall rules policy</p> <p>BugTraq ID: <a href="#">7436</a>, <a href="#">11237</a></p>	<p><b>Port:</b> general/udp <b>Family:</b> Firewalls, Routers, SNMP <b>Risk:</b> <b>High</b> <b>Threat ID:</b> 11580</p>
<p><b>IIS Service Pack - 404</b></p> <p>The remote IIS server *seems* to be Microsoft IIS 6.0 - w2k3 build 3790</p>	<p><b>Port:</b> www (80/tcp) <b>Family:</b> Web Services <b>Risk:</b> <b>High</b> <b>Threat ID:</b> 11874</p>

## Medium Risk Security Threat Details

<p><b>Remote host replies to SYN+FIN</b></p> <p>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>
---	--

## Low Risk Security Threat Details

<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)</p> <p><b>Family:</b> Mail Services</p> <p><b>Risk:</b> Low</p> <p><b>Threat ID:</b> 10249</p>
<p><b>SMTP Server type and version</b></p> <p>Remote SMTP server banner : 220 www.testsystem.com SMTP Server CMSPraetor 5.10.4411 Ready ESMTP spoken here</p>	<p><b>Port:</b> smtp (25/tcp)</p> <p><b>Family:</b> Mail Services</p> <p><b>Risk:</b> Low</p> <p><b>Threat ID:</b> 10263</p>
<p><b>Private IP address leaked in HTTP headers</b></p> <p>This web server leaks a private IP address through its HTTP headers : /10.10.226.5</p> <p>This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server.</p> <p>There is a known issue with IIS 4.0 doing this in its default configuration. See <a href="http://support.microsoft.com/support/kb/articles/Q218/1/80.ASP">http://support.microsoft.com/support/kb/articles/Q218/1/80.ASP</a></p> <p>See the Bugtraq reference for a full discussion.</p> <p>CVE: <a href="#">CAN-2000-0649</a></p> <p>BugTraq ID: <a href="#">1499</a></p>	<p><b>Port:</b> www (80/tcp)</p> <p><b>Family:</b> Web Services</p> <p><b>Risk:</b> Low</p> <p><b>Threat ID:</b> 10759</p>
<p><b>Find if IIS server allows BASIC and/or NTLM authentication</b></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:</p> <ul style="list-style-type: none"><li>- IIS NTLM authentication is enabled</li></ul>	<p><b>Port:</b> www (80/tcp)</p> <p><b>Family:</b> Web Services</p> <p><b>Risk:</b> Low</p> <p><b>Threat ID:</b> 11871</p>

<p>Solution: None at this time</p> <p>CVE: <a href="#">CAN-2002-0419</a></p> <p>BugTraq ID: <a href="#">4235</a></p>	<p>11871</p>
<p><b>IPSEC IKE detection</b></p> <p>The remote host seems to be enabled to do Internet Key Exchange (IKE). This is typically indicative of a VPN server. VPN servers are used to connect remote hosts into internal resources.</p> <p>Solution: You should ensure that:</p> <ol style="list-style-type: none"> <li>1) The VPN is authorized for your Companies computing environment</li> <li>2) The VPN utilizes strong encryption</li> <li>3) The VPN utilizes strong authentication</li> </ol> <p>VPN Vendor signatures were generated from the ike-scan project written by Roy Hills and distributed by NTA Monitor.</p> <p>See also : <a href="http://www.nta-monitor.com/ike-scan/">http://www.nta-monitor.com/ike-scan/</a></p>	<p><b>Port:</b> isakmp (500/udp)</p> <p><b>Family:</b> Firewalls, Routers, SNMP</p> <p><b>Risk:</b> Low</p> <p><b>Threat ID:</b> 11935</p>
<p><b>OS Identification</b></p> <p>Nessus was not able to reliably identify the remote operating system. It might be: Microsoft Windows 2003 Server</p> <p>The fingerprint differs from these known signatures on 4 points.</p> <p>If you know what operating system this host is running, please send this signature to os-signatures@nessus.org :</p> <pre>:0:1:0:64:0:64:1:0:64:1:0:64:1:64:64:0:1:1:2:1:1:1:1:1:128:17520:MNWNNTNNS:0:0:0</pre>	<p><b>Port:</b> general/tcp</p> <p><b>Family:</b> Service Detection</p> <p><b>Risk:</b> Low</p> <p><b>Threat ID:</b> 11936</p>

## Other Risk Security Threat Details

<p><b>HTTP Server type and version</b></p> <p>The remote web server type is :</p> <p>Microsoft-IIS/6.0</p>	<p><b>Port:</b> www (80/tcp)</p> <p><b>Family:</b> Web Services</p> <p><b>Risk:</b> Other</p> <p><b>Threat ID:</b> 10107</p>
<p><b>Directory Scanner</b></p> <p>The following directories were discovered: /download, /images, /include, /styles</p> <p>While this is not, in and of itself, a bug, you should manually inspect</p>	<p><b>Port:</b> www (80/tcp)</p> <p><b>Family:</b> Remote File Access</p> <p><b>Risk:</b></p>

<p>these directories to ensure that they are in compliance with company security standards</p> <p>Other references : OWASP:OWASP-CM-006</p>	<p><b>Other</b> <b>Threat ID:</b> 11032</p>
<p><b>smtpscan</b></p> <p>smtpscan was not able to reliably identify this server. It might be: SLMail 5.1.0 The fingerprint differs from these known signatures on 2 point(s)</p> <p>If you known precisely what it is, please send this fingerprint to smtp-signatures@nessus.org : :250:250:500:250:501:250:550:214:252:550:500:250:250:250:250</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>URLScan Detection</b></p> <p>The remote web server is using URLScan to protect itself, which is a good thing.</p> <p>However since it is possible to determine that URLScan is installed, an attacker may safely assume that the remote web server is Internet Information Server.</p> <p>BugTraq ID: <a href="#">7767</a></p>	<p><b>Port:</b> www (80/tcp) <b>Family:</b> Web Services <b>Risk:</b> <b>Other</b> <b>Threat ID:</b> 11699</p>

## Symtrex Web Scanner

SymtrexVA tested XXX.XXX.XXX.XXX for additional web server vulnerabilities using the Symtrex web scanner. Any additional vulnerabilities discovered by Symtrex are listed below.

**Port 80 - /modules.php?name=Members\_List&letter=All&sortby=pass**

PHP Nuke module allows user names and passwords to be viewed. See [http://www.frog-man.org/tutos/PHP-Nuke6.0-Members\\_List-Your\\_Account.txt](http://www.frog-man.org/tutos/PHP-Nuke6.0-Members_List-Your_Account.txt) for other SQL exploits in this module. (GET)

**Port 80 - /exchange/**

Redirects to <http://www.testsystem.com/application/?cmd=checksessioncookie> , This may be interesting (Outlook exchange OWA server?)...

**Port 80 - /exchange/lib/AMPROPS.INC**

Redirects to <http://www.testsystem.com/application/lib/AMPROPS.INC?cmd=checksessioncookie> , Outlook Web Access server allows source code to be viewed by requesting the file directly from /exchange/lib/

**Port 80 - /exchange/lib/ATTACH.INC**

Redirects to <http://www.testsystem.com/application/lib/ATTACH.INC?cmd=checksessioncookie> , Outlook Web Access server allows source code to be viewed by requesting the file directly from /exchange/lib/

**Port 80 - /exchange/lib/DELETE.INC**

Redirects to <http://www.testsystem.com/application/lib/DELETE.INC?cmd=checksessioncookie> , Outlook Web Access server allows source code to be viewed by requesting the file directly from /exchange/lib/

**Port 80 - /exchange/lib/GETREND.INC**

Redirects to <http://www.testsystem.com/application/lib/GETREND.INC?cmd=checksessioncookie> , Outlook Web Access server allows source code to be viewed by requesting the file directly from /exchange/lib/

**Port 80 - /exchange/lib/GETWHEN.INC**

Redirects to <http://www.testsystem.com/application/lib/GETWHEN.INC?cmd=checksessioncookie> , Outlook Web Access server allows source code to be viewed by requesting the file directly from /exchange/lib/

**Port 80 - /exchange/lib/JSATTACH.INC**

Redirects to <http://www.testsystem.com/application/lib/JSATTACH.INC?cmd=checksessioncookie> , Outlook Web Access server allows source code to be viewed by requesting the file directly from /exchange/lib/

**Port 80 - /exchange/lib/JSROOT.INC**

Redirects to <http://www.testsystem.com/application/lib/JSROOT.INC?cmd=checksessioncookie> , Outlook Web Access server allows source code to be viewed by requesting the file directly from /exchange/lib/

**Port 80 - /exchange/lib/JSUTIL.INC**

Redirects to <http://www.testsystem.com/application/lib/JSUTIL.INC?cmd=checksessioncookie> , Outlook Web Access server allows source code to be viewed by requesting the file directly from /exchange/lib/

**Port 80 - /exchange/lib/LANG.INC**

Redirects to <http://www.testsystem.com/application/lib/LANG.INC?cmd=checksessioncookie> , Outlook Web Access server allows source code to be viewed by requesting the file directly from /exchange/lib/

**Port 80 - /exchange/lib/logon.inc**

Redirects to <http://www.testsystem.com/application/lib/logon.inc?cmd=checksessioncookie> , Outlook Web Access server allows source code to be viewed by requesting the file directly from /exchange/lib/

**Port 80 - /exchange/lib/PAGEUTIL.INC**

Redirects to <http://www.testsystem.com/application/lib/PAGEUTIL.INC?cmd=checksessioncookie> , Outlook Web Access server allows source code to be viewed by requesting the file directly from /exchange/lib/

**Port 80 - /exchange/lib/PUBFLD.INC**

Redirects to <http://www.testsystem.com/application/lib/PUBFLD.INC?cmd=checksessioncookie> , Outlook Web Access server allows source code to be viewed by requesting the file directly from /exchange/lib/

**Port 80 - /exchange/lib/RENDER.INC**

Redirects to <http://www.testsystem.com/application/lib/RENDER.INC?cmd=checksessioncookie> , Outlook Web Access server allows source code to be viewed by requesting the file directly from /exchange/lib/

**Port 80 - /exchange/lib/SESSION.INC**

Redirects to <http://www.testsystem.com/application/lib/SESSION.INC?cmd=checksessioncookie> , Outlook Web Access server allows source code to be viewed by requesting the file directly from /exchange/lib/

**Port 80 - /exchange/root.asp?acs=anon**

Redirects to <http://www.testsystem.com/application/root.asp?acs=anon?cmd=checksessioncookie> , This allows anonymous access to portions of the OWA server.  
<http://support.microsoft.com/support/exchange/content/whitepapers/owaguide.doc>

**Port 80 - /download/**

This might be interesting... (GET)

**Port 80 - /public/**

Redirects to <http://www.testsystem.com/public/?cmd=checksessioncookie> , This might be interesting...

**Port 80 - /localstart.asp**

Needs Auth: (realm "www.testsystem.com")

**Port 80 - /localstart.asp**

This may be interesting... (GET)

## External Advisories

---

Of the 13 possible security threats discovered on XXX.XXX.XXX.XXX, 7 of them also have external advisory sources for additional cross-reference information. To view the external advisory information, click on the reference number in the table below.

ID	Risk	Description and References
11580	High	UDP packets with source port of 53 bypass firewall rules on port general/udp <a href="#">BID-7436</a> , <a href="#">BID-11237</a>
11618	Medium	Remote host replies to SYN+FIN on port general/tcp <a href="#">BID-7487</a>
10249	Low	EXPN and VRFY commands on port smtp (25/tcp) <a href="#">CAN-1999-0531</a>
10759	Low	Private IP address leaked in HTTP headers on port www (80/tcp) <a href="#">CAN-2000-0649</a> , <a href="#">BID-1499</a>
11871	Low	Find if IIS server allows BASIC and/or NTLM authentication on port www (80/tcp) <a href="#">CAN-2002-0419</a> , <a href="#">BID-4235</a>
11032	Other	Directory Scanner on port www (80/tcp) OWASP-CM-006
11699	Other	URLScan Detection on port www (80/tcp) <a href="#">BID-7767</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 Symtrex, Inc. 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 2174 security threats for which an Symtrex, Inc. 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 2174 security threats Symtrex, Inc. 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, SymtrexVA 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, Symtrex, Inc. 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** Only 2% of networks receive a perfect score on an Symtrex, Inc. security scan. That means 98% of them 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 Symtrex, Inc. 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. Symtrex, Inc.' database of security threats generally grows by 5-10 new vulnerabilities every week. Sometimes, we have even seen more than 80 new security threats crop up in a single month! 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, Symtrex, Inc. not only performs a thorough port scan, but also tests each open port for 2174 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 Symtrex, Inc.

---

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

SymtremVA, is an automated information security and hacker vulnerability assessment service. The system is fully automated and functions remotely. The customer does not need to download, install, or configure anything. This advanced technology emulates a team of "hackers" using 7793 unique methodologies and techniques to find the security threats, exposed private information, and attack vulnerabilities in any network. This data is then automatically analyzed, manually reviewed, and Symtrem, Inc. 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

---

Symtrem, Inc. tested your network for a total of 7793 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.

### **HP-UX LOCAL CHECKS**

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

### **MACOS X LOCAL CHECKS**

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

### **MAIL SERVICES**

Threats dealing with e-mail server problems or exploits.

### **MANDRAKE LOCAL CHECKS**

Local operating system and application level security checks for Mandrake.

### **MICROSOFT BULLETINS**

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

### **MISCELLANEOUS**

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

## **NETWARE**

Problems with Netware operating systems, applications, and services.

## **PEER-TO-PEER SERVICES**

Threats of exposed private data through file sharing services.

## **RED HAT LOCAL CHECKS**

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

## **REMOTE FILE ACCESS**

Unauthorized access to files or data on your systems.

## **REMOTE SHELL ACCESS**

Vulnerability of user or service-level accounts and information.

## **SERVICE DETECTION**

Tests for services, ports, and versions.

## **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.

### **DoS**

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

### **DNS**

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 Symtrex, Inc. is www.symtrex.com.

## **SYMTREXVA**

The primary service offering which does remote automated hacker vulnerability analysis and security scanning. This report was generated using the Symtrex, Inc. SymtrexVA service.

## **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 Symtrex, Inc. 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 Symtrex, Inc. security threats database.

## **FINGERPRINT**

To identify by means of a distinctive mark or characteristic. For example, Symtrex, Inc. 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.

## **GOOGLE**

The most complete Internet search engine. Symtrex, Inc. uses the Google search engine as part of an Symtrex, Inc. analysis to look for hacked computers, disclosed passwords, and authentication information.

## **HACKER**

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

## **HOST**

See Server.

## **IP ADDRESS**

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

## **MTA**

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

## **NESSUS**

Open source security scanning software used by most security professionals world-wide. Symtrex, Inc. uses Nessus as a security scanning engine to help with the Symtrex, Inc. 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.

## **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 Symtrex, Inc. 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 Symtrex, Inc. security threats database.

## **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 Symtrex, Inc..

## **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.

---

**END OF REPORT**

---