



VULNERABILITY ASSESSMENT  
WHITEPAPER

---

INTRODUCTION, IMPLEMENTATION AND  
TECHNOLOGY DISCUSSION

## Security Vulnerabilities of Computers & Servers

### Security Risks Change Daily

New and diverse computer security threats are being discovered every day. They come as software bugs that affect the software we use to communicate, connect to the Internet, share files, etc.

A sampling of the many companies and products that have had security bugs reported include:

3com, Apache, Checkpoint, Cisco, Coldfusion, Compaq, Computer Associates, Groupwise, HP, IBM, IIS, Informix, Internet Explorer, Lotus, Microsoft, Napster, Netscape, Nortel, Novell, NT, Oracle, Pix, Realserver, Redhat, Roxen, Samba, Shiva, Solaris, Sun, Suse, Tektronix, Tripwire, Ultraseek, Webalizer, Webcart, Webshield, Wingate, and Zeus.

These discoveries (bugs) are published on the Internet to keep responsible users aware of new threats. Unfortunately, the hackers are also aware of these bugs.

Each month programs are written and distributed on the Internet to help users identify and fix these issues in their systems. Sometimes hackers are the source for these programs. These discovery programs average about one per business day.

Subsequently, each month hackers have new ways to automatically test for holes and vulnerabilities on your computer or network. Remember, these new security weaknesses didn't exist the month, week, or day before their discovery. Thus, **ANY SOLUTION FOR SECURING DATA OR PROTECTING NETWORKS MUST BE UPDATED REGULARLY TO PROPERLY PROTECT YOUR SYSTEM FROM THESE NEW THREATS.**

### Most Attacks are Automated

Because of the millions of computers on the web, many people will tell themselves that their small organization or home system is nothing of consequence and should not be threatened by hackers. This would be true if it wasn't so easy to automate an attack on millions of computers through programming.

Hackers will write a computer program called an Internet virus or worm, which can indiscriminately test millions of different computers for weaknesses. Upon discovery of a computer with a weakness, the worm will copy itself to the target computer and begin probing a different set of randomly selected computers. Optionally, the worm may use the security weakness it discovered to run commands on the target computer and simply destroy the target by deleting key system files.

You may have heard of worms like Code-red, Slammer, and Nimda. These are all Internet-based viruses that cost billions in destroyed data, repair labor, and lost productivity.

Many computer users understand the concept of computer viruses. Virus detection software is designed to test for the presence of a virus file. Since many of these attacks will never copy themselves to the target computer, it's important to understand that **VIRUS PROTECTION SOFTWARE ALONE WILL NOT PROTECT YOU FROM THESE NETWORK-BASED SECURITY THREATS!** The best protection is to identify weaknesses before hackers and worms are able to exploit them.

## Doesn't My Firewall Protect My Computer?

The function of a firewall is to block ports. If you have absolutely no ports open and they are all stealth, your system is reasonably secure (there are still some potential threats). If you open a port because you need some service on your server or computer, you expose your system to all possible attacks associated with that service or port. ONCE YOU OPEN UP PORTS ON A FIREWALL, MOST FIREWALLS NO LONGER PROTECT YOUR COMPUTER FROM ANY ATTACKS ON THAT PORT.

Additionally, many firewalls require extensive configuration. The only way to confirm that your firewall is performing as you believe is to test the operation of your firewall from the Internet side. SecurityMetrics offers a Free Server Firewall test. In case after case, network administrators are surprised either by open ports or exposed vulnerabilities that they thought were protected by their firewall. There is no substitute for making sure your firewall is performing correctly. You do this by testing the firewall, and any other accessible machines behind your firewall (in your DMZ), from the hackers point of reference.

## How Do I Test My Computer?

You can use the same automated programs hackers use to test your own computers, identify possible weaknesses, and fix vulnerabilities before they become a problem. SecurityMetrics provides testing services, which are updated nightly, so that you can test your computers, servers, or other network devices like firewalls for the latest security weaknesses. In order to determine what tool to use to test your computer(s), you need to understand a few basic concepts about how computers communicate.

Every computer that communicates on the Internet uses an Internet Protocol (IP) address. Some IP addresses are Public and others are Private. Any computer with a Public IP address means that it is directly accessible from any other computer on the Internet. Any computer can present information requests or commands, which it can either deny or accept, and respond accordingly. You could relate this to direct dialing with the telephone where any direct marketing salesperson or other individual could dial this number directly.

When a computer is behind a router, firewall or proxy server, it may be using a Private IP address. This means that any requests for information or commands must pass through the router, firewall, or proxy server in order to be delivered to the destination computer. These security measures provide a good layer of protection. You could relate this to dialing into a company switchboard in order to connect to someone within the organization. All employees can dial out through the switch as they wish, but direct marketers or other undesirable calls have to come to the switchboard to ask permission to speak with someone inside the organization.

If you have a Public IP address, you should use the SecurityMetrics Site Certification, Perimeter Check, or Desktop Check service to test your computer or server. If you have a Private IP address, you need the SecurityMetrics Appliance at your site to test your computer or server.

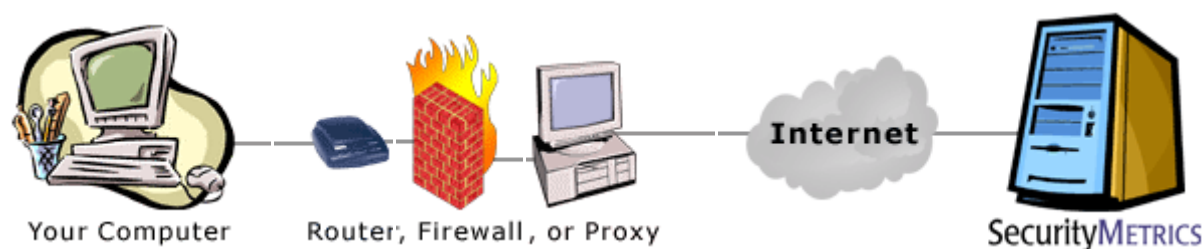
The simplest way to determine if your computer uses a public or private IP address is to use the Free Port Scan at [www.securitymetrics.com/portscan.adp](http://www.securitymetrics.com/portscan.adp). Select the "Home Office/Personal Firewall Test" option. At the top of the portscan results, it will indicate whether or not there is a

firewall, router or proxy between your computer and the Internet. If so, you are using a Private IP address. If not, you are using a Public Address.

## Automatic Connection Analyzer

Your computer reported an IP address of **256.61.45.256**, but your actual IP address is **10.0.0.100**.

There is a router, proxy, or firewall between you and the Internet. Your port scan results may reflect the security of your router, firewall or proxy instead of your computer.



In the case above, the 10.0.0.100 is your computer and it's using a private IP address.

## Automatic Connection Analyzer

Internet **attackers** and worms **can directly probe** your computer for open ports and vulnerabilities, because your computer (**256.63.145.199**) is connected directly to the Internet.



In this case, the 256.63.145.199 is your computer and it is directly connected to the Internet with a public IP address.

## SecurityMetrics Vulnerability Assessment Technology

The vulnerability assessment security testing provided by SecurityMetrics is a superior service. SecurityMetrics combines multiple types of security tests into a single testing environment. These testing components are the most up-to-date technologies available for vulnerability assessment.

The SecurityMetrics Appliance uses five components in each vulnerability assessment scan:

- Port scan of up to 20,000 TCP ports and the most common UDP ports
- Vulnerability assessment of over 1,500 industry standard vulnerabilities
- Brute force testing of 698 of the most common default username/password combinations on FTP and Telnet ports
- Mail open-relay testing which determines if your system is being used as a mail relay
- Website spidering two levels deep to find HTML errors or XSS code

# securityMETRICS

Vulnerability assessment is perhaps the most ignored security technology today. It is inexpensive and deadly to IT administrators who have never used the technology for their systems. One of our favorites quotes on the use of vulnerability assessment is found on page 125 in “Linux Exposed”:

“There is one simple countermeasure that will protect you, should a hacker scan your machines with a [vulnerability assessment scanner] – scan your own systems first. Make sure to address any problems reported by the scanner, and then a scan by a hacker will give him no edge.”

It is difficult to beat a good vulnerability assessment system. It is hard to recover from the use of a poor VA system. False-positives can become extremely time consuming, frustrating and a waste of time.

A good vulnerability assessment system will point out holes you could never have found yourself and tell you of password problems, programming errors and basic architecture issues without the high price tag of a security consultant.

## **Concise Reporting Which Includes Solution Instructions**

All security components are launched at each target when a test is initiated. Concise security reports are available when all the various security components finish analyzing the target. Large disorganized reports hinder the security resolution process. SecurityMetrics reports contain instructions, security patch links, and helpful information needed to immediately repair identified issues.

SecurityMetrics has also developed a Pass/Fail scoring system for vulnerability assessments. Each security issue is rated according to its risk to your security. If your computer or server passes our tests, you can be assured that you are protected from thousands of potential hacking attacks.

Anyone in a large organization who has to manage hundreds or thousands of computers understands that a 20-page report per computer system is unmanageable.

# securityMETRICS

Below is a sample report illustrating SecurityMetrics Vulnerability Assessment reports.

Executive Summary		
Test Result: <b>Fail</b>	Date: <b>2003-05-22</b>	Target IP: <b>10.0.0.31</b>
Test ID: <b>33</b>	Test Length: <b>1.20 Minutes</b>	DNS Entry: <b>No DNS entry</b>
Total Risk: <b>14</b>	Start Time: <b>13:55:35</b>	Finish Time: <b>13:56:48</b>
Full OS Description: <b>Windows NT 3.51 SP5, NT4 or 95/98/98SE</b>		

The computer **fails** because a risk of 4 or more was found. Look in the Security Vulnerabilities section below for instructions to reduce your security risk.

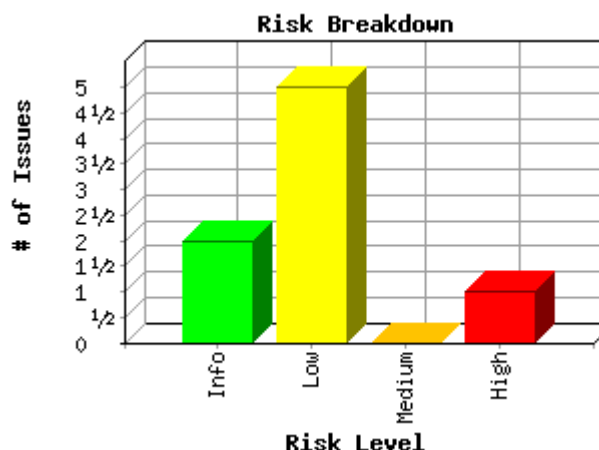
Attackers typically use foot printing, port scanning and security vulnerability testing to find security weaknesses on computers. This report provides information on all these categories.

### Footprinting

Find public information regarding this IP, which an attacker could use to gain access: [IP Information](#)

### Port Scan

Attackers use a port scan to find out what programs are running on your computer. Most programs have known security weaknesses. Disable any unnecessary programs listed below.



Port Scan					
Protocol	Port	Program	Status	Summary	Turn Off
ALL		Firewall	Absent	Your computer does not appear to be behind a firewall. We recommend installing and using a properly configured firewall.	
ICMP	Ping		Accepting	Your computer is answering ping requests. Hackers use Ping to scan the Internet to see if computers will answer. If your computer answers then a hacker will know your computer exists and your computer could become a hacker target. You should install a firewall or turn off Ping requests.	<a href="#">HowTo</a>
UDP	137	netbios-ns	Open	The NetBIOS Name Service (NBNS) provides a means for hostname and address mapping on a NetBIOS-aware network. NBNS does not specify a method for authenticating communications, and as such, machines running NetBIOS services are vulnerable to attacks.	<a href="#">HowTo</a>
UDP	138	netbios-dgm	Open	The Netbios Datagram Service exposes characteristics of the system. A hacker can use the information exposed to break into the system. If you are a dial up user then turn off NetBeui for your dial up connection. Turn off file sharing if possible.	<a href="#">HowTo</a>
TCP	139	netbios-ssn	Open	NetBIOS is a networking protocol used by Microsoft Windows to provide easy networking. If this port is open, any computer with Microsoft Windows can connect to yours and potentially use shared resources on your computer. This makes it possible for an attacker to copy, delete, or modify your data or install malicious programs on your computer.	<a href="#">HowTo</a>

## Security Vulnerabilities

An attacker probes your computer for weaknesses using vulnerability detection tools. The following section lists all security vulnerabilities detected on your computer.

Each vulnerability is ranked by risk on a scale of 0 to 9, with 9 being critical. The computer will fail if any vulnerability has a risk of 4 or more.

Security Vulnerabilities				
Protocol	Port	Program	Risk	Summary
tcp	0	general/tcp	7	The remote host has predictable TCP sequence numbers. An attacker may use this flaw to establish spoofed TCP connections to this host. <b>Solution</b> : If the remote host is running Windows, see <a href="http://www.microsoft.com/technet/security/bulletin/ms99-046.asp">http://www.microsoft.com/technet/security/bulletin/ms99-046.asp</a> <b>Risk Factor</b> : High CVE : CVE-1999-0077
udp	137	netbios-ns	3	The remote host has the following MAC address on its adapter : 0x4a 0x42 0x20 0x20 0x20 0x20 If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. <b>Risk Factor</b> : Serious Low CVE : CAN-1999-0621
icmp	0	general/icmp	1	The remote host answered to an ICMP_MASKREQ query and sent us its netmask (255.255.255.0) An attacker can use this information to understand how your network is set up and how the routing is done. This may help him to bypass your filters. <b>Solution</b> : reconfigure the remote host so that it does not answer to those requests. Set up filters that deny ICMP packets of type 17. <b>Risk Factor</b> : Low CVE : CAN-1999-0524
icmp	0	general/icmp	1	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols. <b>Solution</b> : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). <b>Risk Factor</b> : Low CVE : CAN-1999-0524
tcp	0	general/tcp	1	The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things. <b>Solution</b> : Contact your vendor for a patch <b>Risk Factor</b> : Low
tcp	0	general/tcp	1	The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things. <b>Solution</b> : Contact your vendor for a patch <b>Risk Factor</b> : Low
tcp	0	general/tcp	0	Remote OS guess : Windows NT4 or 95/98/98SE CVE : CAN-1999-0454

## Evaluate For Yourself

Those who have public IP addresses can evaluate the SecurityMetrics Vulnerability Assessment service by running the Free Server Firewall Test found at [www.securitymetrics.com/portscan.adp](http://www.securitymetrics.com/portscan.adp). Select the "Business Server/Firewall Test" option and follow the instructions.

A 30-day evaluation is available for organizations that would like to assess the SecurityMetrics Appliance—Intrusion Detection/Prevention System.