# The Ten Most Critical
# Internet Security Vulnerabilities (Updated)
## The Experts' Consensus
Version 2.100 October 2, 2001
Copyright 2001, The SANS Institute

Stop the Break-Ins!

The majority of successful attacks on computer systems via the Internet can be traced to exploitation of one of a small number of security flaws. Most of the systems compromised in the Solar Sunrise Pentagon hacking incident were attacked through a single vulnerability. A related flaw was exploited to break into many of the computers later used in massive distributed denial of service attacks. Recent compromises of Windows NT-based web servers are typically traced to entry via a well-known vulnerability. Another vulnerability is widely thought to be the means used to compromise more than 30,000 Linux systems.

A few software vulnerabilities account for the majority of successful attacks because attackers are opportunistic – taking the easiest and most convenient route. They exploit the best-known flaws with the most effective and widely available attack tools. They count on organizations not fixing the problems, and they often attack indiscriminately, by scanning the Internet for vulnerable systems.

System administrators report that they have not corrected these flaws because they simply do not know which of over 500 potential problems are the ones that are most dangerous, and they are too busy to correct them all. A step by step tutorial by Mary Chaddock to help system administators get started with the top ten is available here.

The information security community is meeting this problem head on by identifying the most critical Internet security problem areas – the clusters of vulnerabilities that system administrators need to eliminate immediately. This consensus Top Ten list represents an unprecedented example of active cooperation among industry, government, and academia. The participants came together from the most security-conscious federal agencies, from the leading security software vendors and consulting firms, from the top university-based security programs, and from CERT/CC and the SANS Institute. A complete list of participants may be found at the end of this article.

Here is the experts' list of the Ten Most Often Exploited Internet Security Flaws along with the actions needed to rid your systems of these vulnerabilities.

Three Notes For Readers:

Note 1. This is a living document. It includes initial, step-by-step instructions and pointers for correcting the flaws. We will update these instructions as more current or convenient methods are identified and we welcome your input. This is a community consensus document – your experience in eliminating the vulnerabilities can help others

who come after you. To make suggestions e-mail info@sans.org with the subject Top Ten Comments. To get the latest version of the guidelines, e-mail info@sans.org with the subject Top Ten Fixes.

Note 2. You'll find references to CVE numbers – the Common Vulnerabilities and Exposures reference numbers that correspond with vulnerabilities. CAN numbers are candidates for CVE entries that are not yet fully verified. For more data on the award-winning CVE project, see http://cve.mitre.org.

Note 3. At the end of the list, you'll find an extra section offering a list of the ports used by commonly probed and attacked services. By blocking traffic to those ports at the firewall or other network perimeter protection device, you add an extra layer of defense that helps protect you from configuration mistakes.

## 1. BIND weaknesses: nxt, qinv and in.named allow immediate root compromise.

The Berkeley Internet Name Domain (BIND) package is the most widely used implementation of Domain Name Service (DNS) -- the critical means by which we all locate systems on the Internet by name (e.g., www.sans.org) without having to know specific IP addresses -- and this makes it a favorite target for attack. Sadly, according to a mid-1999 survey, about 50% of all DNS servers connected to the Internet are running vulnerable versions of BIND. In a typical example of a BIND attack, intruders erased the system logs, and installed tools to gain administrative access. They then compiled and installed IRC utilities and network scanning tools, which they used to scan more than a dozen class-B networks in search of additional systems running vulnerable versions of BIND. In a matter of minutes, they had used the compromised system to attack hundreds of remote systems abroad, resulting in many additional successful compromises. This illustrates the chaos that can result from a single vulnerability in the software for ubiquitous Internet services such as DNS.

### Systems Affected:
Multiple UNIX and Linux systems

### CVE Entries:
nxt CVE-1999-0833
qinv CVE-1999-0009
Other related entries: CVE-1999-0835, CVE-1999-0848, CVE-1999-0849, CVE-1999-0851

### Advice on correcting the problem:
A. Disable the BIND name daemon (named) on all systems that are not authorized to be DNS servers. Some experts recommend you also remove the DNS software.

B. On machines that are authorized DNS servers, update to the latest version and patch level. Use the guidance contained in the following advisories:

> For the NXT vulnerability: http://www.cert.org/advisories/CA-99-14-bind.html
> For the QINV (Inverse Query) and NAMED vulnerabilities:

http://www.cert.org/advisories/CA-98.05.bind_problems.html
http://www.cert.org/summaries/CS-98.04.html

C. Run BIND as a non-privileged user for protection in the event of future remote-compromise attacks. (However, only processes running as root can be configured to use ports below 1024 – a requirement for DNS. Therefore you must configure BIND to change the user-id after binding to the port.)

D. Run BIND in a chroot()ed directory structure for protection in the event of future remote-compromise attacks.

## 2. Vulnerable CGI programs and application extensions (e.g., ColdFusion) installed on web servers.

Most web servers support Common Gateway Interface (CGI) programs to provide interactivity in web pages, such as data collection and verification. Many web servers come with sample CGI programs installed by default. Unfortunately, many CGI programmers fail to consider ways in which their programs may be misused or subverted to execute malicious commands. Vulnerable CGI programs present a particularly attractive target to intruders because they are relatively easy to locate, and they operate with the privileges and power of the web server software itself. Intruders are known to have exploited vulnerable CGI programs to vandalize web pages, steal credit card information, and set up back doors to enable future intrusions, even if the CGI programs are secured. When Janet Reno's picture was replaced by that of Adolph Hitler at the Department of Justice web site, an in-depth assessment concluded that a CGI hole was the most probable avenue of compromise. Allaire's ColdFusion is a web server application package which includes vulnerable sample programs when installed. As a general rule, sample programs should always be removed from production systems.

### Systems Affected:
All web servers.

### CVE Entries:
** Sample CGI programs (All CGI)
**Remedy:**
Remove all sample CGI programs on a production server.

** CAN-1999-0736(IIS 4.0, Microsoft Site Server 3.0, which is included with Microsoft Site Server 3.0 Commerce Edition, Microsoft Commercial Internet System 2.0, and Microsoft BackOffice Server 4.0 and 4.5)

(see http://www.microsoft.com/technet/security/bulletin/ms99-013.asp )
**Remedy:**
Apply patch at : ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/Viewcode-fix/

CVE-1999-0067 (phf phone book program included with older NCSA and Apache server)
CVE-1999-0068 ('mylog.html' sample script shipped with the PHP/FI)
CVE-1999-0270 (IRIX 6.2, IRIX 6.3, IRIX 6.4)

CVE-1999-0346 (sample script shipped with the PHP/FI package)
CVE-2000-0207 (IRIX 6.5)

Most important CGI Vulnerabilities not including sample programs
CAN-1999-0467 (WebCom Guestbook CGI)

** CAN-1999-0509 (All CGI Web Servers)
Refer to http://www.cert.org/advisories/CA-96.11.interpreters_in_cgi_bin_dir.html
**Remedy:**
The solution to this problem is to ensure that the CGI bin directory does not include any general-purpose interpreters, for example

- PERL
- Tcl
- UNIX shells (sh, csh, ksh, etc.)

CVE-1999-0021 (Muhammad A. Muquit's wwwcount version 2.3)
CVE-1999-0039 (Outbox Environment Subsystem for IRIX)
CVE-1999-0058 (PHP/FI package written by Rasmus Lerdorf)
CVE-1999-0147 (Glimpse HTTP 2.0 and WebGlimpse)
CVE-1999-0148 (Outbox Environment Subsystem for IRIX)
CVE-1999-0149 (Outbox Environment Subsystem for IRIX)

** CVE-1999-0174 (All CGI Web Servers) Refer to,
http://xforce.iss.net/static/291.php
(More info at http://www.netspace.org/cgi-bin/wa?A2=ind9702B&L=bugtraq&P=R64 )
**Remedy:**
Remove the "view-source" script from the cgi-bin directory on your web server.

CVE-1999-0177 (O'Reilly Website 2.0 and earlier CGI)
CVE-1999-0178 (O'Reilly Website 2.0 and earlier CGI)
CVE-1999-0237 (Webcom's CGI Guestbook for Win32 web servers)
CVE-1999-0262 (fax survey CGI script on Linux )
CVE-1999-0279 (Excite for Web Servers)
CVE-1999-0771 (Compaq Management Agents and the Compaq Survey Utility)
CVE-1999-0951 (OmniHTTPd CGI program)
CVE-2000-0012 (MS SQL CGI program)
CVE-2000-0039 (AltaVista search engine)
CVE-2000-0208 (htsearch CGI script for ht://dig)

ColdFusion Sample Program Vulnerabilities
** CAN-1999-0455
** CAN-1999-0922
** CAN-1999-0923

ColdFusion Other Vulnerability
** CAN-1999-0760
** CVE-2000-0057

**Advice on correcting the problem:**
A. Do not run web servers as root

B. Get rid of CGI script interpreters in bin directories:

http://www.cert.org/advisories/CA-96.11.interpreters_in_cgi_bin_dir.html

C. Remove unsafe CGI scripts

http://www.cert.org/advisories/CA-97.07.nph-test-cgi_script.html
http://www.cert.org/advisories/CA-96.06.cgi_example_code.html
http://www.cert.org/advisories/CA-97.12.webdist.html

D. Write safer CGI programs:

http://www-4.ibm.com/software/developer/library/secure-cgi/
http://www.cert.org/tech_tips/cgi_metacharacters.html
http://www.cert.org/advisories/CA-97.24.Count_cgi.html

E. Don't configure CGI support on Web servers that don't need it.

F. Run your Web server in a chroot()ed environment to protect the machine against yet to be discovered exploits

## 3. Remote Procedure Call (RPC) weaknesses in rpc.ttdbserverd (ToolTalk), rpc.cmsd (Calendar Manager), and rpc.statd that allow immediate root compromise

Remote procedure calls (RPC) allow programs on one computer to execute programs on a second computer. They are widely-used to access network services such as shared files in NFS. Multiple vulnerabilities caused by flaws in RPC, are being actively exploited. There is compelling evidence that the vast majority of the distributed denial of service attacks launched during 1999 and early 2000 were executed by systems that had been victimized because they had the RPC vulnerabilities. The broadly successful attack on U.S. military systems during the Solar Sunrise incident also exploited an RPC flaw found on hundreds of Department of Defense systems.

**Systems Affected:**
Multiple UNIX and Linux systems

**CVE Entries:**
rpc.ttdbserverd - CVE-1999-0687, CVE-1999-0003, CVE-1999-0693 (-0687 is newer than -0003, but both allow root from remote attackers and it's likely that -0003 is still around a LOT; -0693 is only locally exploitable, but does give root)

rpc.cmsd – CVE-1999-0696
rpc.statd - CVE-1999-0018, CVE-1999-0019.

**Advice on correcting the problem:**
A. Wherever possible, turn off and/or remove these services on machines directly accessible from the Internet.

B. Where you must run them, install the latest patches:

> For Solaris Software Patches:
> http://sunsolve.sun.com
>
> For IBM AIX Software
> http://techsupport.services.ibm.com/support/rs6000.support/downloads
> http://techsupport.services.ibm.com/rs6k/fixes.html
>
> For SGI Software Patches:
> http://support.sgi.com/
>
> For Compaq (Digital Unix) Patches:
> http://www.compaq.com/support

Search the vendor patch database for tooltalk patches and install them right away.

A summary document pointing to specific guidance about each of three principal RPC vulnerabilities may be found at: http://www.cert.org/incident_notes/IN-99-04.html

For statdd: http://www.cert.org/advisories/CA-99-05-statd-automountd.html
For ToolTalk: http://www.cert.org/advisories/CA-98.11.tooltalk.html
For Calendar Manager: http://www.cert.org/advisories/CA-99-08-cmsd.html

## 4. RDS security hole in the Microsoft Internet Information Server (IIS)

Microsoft's Internet Information Server (IIS) is the web server software found on most web sites deployed on Microsoft Windows NT and Windows 2000 servers. Programming flaws in IIS's Remote Data Services (RDS) are being employed by malicious users to run remote commands with administrator privileges. Some participants who developed the "Top Ten" list believe that exploits of other IIS flaws, such as .HTR files, are at least as common as exploits of RDS. Prudence dictates that organizations using IIS install patches or upgrades to correct all known IIS security flaws when they install patches or upgrades to fix the RDS flaw.

**Systems Affected:**
Microsoft Windows NT systems using Internet Information Server

**CVE Entries:**
CVE-1999-1011

**Advice on correcting the problem:**

An outstanding guide to the RDS weakness and how to correct it may be found
at: http://www.wiretrip.net/rfp/p/doc.asp?id=29&iface=2

B. Microsoft has also posted relevant information at:

> http://support.microsoft.com/support/kb/articles/q184/3/75.asp
> http://www.microsoft.com/technet/security/bulletin/ms98-004.asp
> http://www.microsoft.com/technet/security/bulletin/ms99-025.asp

## 5. Sendmail and MIME buffer overflows as well as pipe attacks that allow immediate root compromise.

Sendmail is the program that sends, receives, and forwards most electronic mail processed on UNIX and Linux computers. Sendmail's widespread use on the Internet makes it a prime target of attackers. Several flaws have been found over the years. The very first advisory issued by CERT/CC in 1988 made reference to an exploitable weakness in sendmail. In one of the most common exploits, the attacker sends a crafted mail message to the machine running Sendmail, and Sendmail reads the message as instructions requiring the victim machine to send its password file to the attacker's machine (or to another victim) where the passwords can be cracked.

**Systems Affected:**
Multiple UNIX and Linux systems

**CVE Entries:**
CVE-1999-0047, CVE-1999-0130, CVE-1999-0131, CVE-1999-0203, CVE-1999-0204,
CVE-1999-0206.
CVE-1999-0130 is locally exploitable only.

**Advice on correcting the problem:**
A. Upgrade to latest version of Sendmail and/or implement patches for sendmail. See
http://www.cert.org/advisories/CA-97.05.sendmail.html

B. Do not run Sendmail in daemon mode (turn off the -bd switch) on machines that are neither mail servers nor mail relays.

## 6. sadmind and mountd

Sadmind allows remote administration access to Solaris systems, providing graphical access to system administration functions. Mountd controls and arbitrates access to NFS mounts on UNIX hosts. Buffer overflows in these applications can be exploited allowing attackers to gain control with root access.

**Systems Affected:**
Multiple UNIX and Linux systems
Sadmind: Solaris machines only

**CVE Entries:**
sadmind - CVE-1999-0977
mountd - CVE-1999-0002.

**Advice on correcting the problem:**

A. Wherever possible, turn off and/or remove these services on machines directly accessible from the Internet.

B. Install the latest patches:

> For Solaris Software Patches:
> http://sunsolve.sun.com
>
> For IBM AIX Software
> http://techsupport.services.ibm.com/support/rs6000.support/downloads
> http://techsupport.services.ibm.com/rs6k/fixes.html
>
> For SGI Software Patches:
> http://support.sgi.com/
>
> For Compaq (Digital Unix) Patches:
> http://www.compaq.com/support

C. More guidance at:

> http://www.cert.org/advisories/CA-99-16-sadmind.html
> http://www.cert.org/advisories/CA-98.12.mountd.html

**7. Global file sharing and inappropriate information sharing via NetBIOS and Windows NT ports 135->139 (445 in Windows2000), or UNIX NFS exports on port 2049, or Macintosh Web sharing or AppleShare/IP on ports 80, 427, and 548.**

These services allow file sharing over networks. When improperly configured, they can expose critical system files or give full file system access to any hostile party connected to the network. Many computer owners and administrators use these services to make their file systems readable and writeable in an effort to improve the convenience of data access. Administrators of a government computer site used for software development for mission planning made their files world readable so people at a different government facility could get easy access. Within two days, other people had discovered the open file shares and stolen the mission planning software.

When file sharing is enabled on Windows machines they become vulnerable to both information theft and certain types of quick-moving viruses. A recently released virus called the 911 Worm uses file shares on Windows 95 and 98 systems to propagate and causes the victim's computer to dial 911 on its modem. Macintosh computers are also vulnerable to file sharing exploits.

The same NetBIOS mechanisms that permit Windows File Sharing may also be used to enumerate sensitive system information from NT systems. User and Group information (usernames, last logon dates, password policy, RAS information), system information, and certain Registry keys may be accessed via a "null session" connection to the

NetBIOS Session Service. This information is typically used to mount a password guessing or brute force password attack against the NT target.

**Systems Affected:**
UNIX, Windows, and Macintosh systems.

**CVE Entries:**
SMB shares with poor access control - CAN-1999-0520
NFS exports to the world - CAN-1999-0554
These candidate entries are likely to change significantly before being accepted as full CVE entries.

**Advice on correcting the problem:**
A. When sharing mounted drives, ensure only required directories are shared.

B. For added security, allow sharing only to specific IP addresses because DNS names can be spoofed.

C. For Windows systems, ensure all shares are protected with strong passwords.

D. For Windows NT systems, prevent anonymous enumeration of users, groups, system configuration and registry keys via the "null session" connection.

Block inbound connections to the NetBIOS Session Service (tcp 139) at the router or the NT host.

Consider implementing the RestrictAnonymous registry key for Internet-connected hosts in standalone or non-trusted domain environments:

> NT4: http://support.microsoft.com/support/kb/articles/Q143/4/74.asp
> Win2000: http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

E. A quick, free, and secure test for the presence of NetBIOS file sharing, and its related vulnerabilities, effective for machines running ANY operating system, is available at the Gibson Research Corporation web site. Simply visit http://grc.com/ and click the "ShieldsUP" icon to receive a real-time appraisal of any system's NetBIOS exposure. Detailed instructions are available to help Microsoft Windows users deal with NetBIOS vulnerabilities.

F. For Macintosh systems, disable file sharing and web sharing extensions unless absolutely required. If file sharing must be enabled, ensure strong passwords for access, and stop file sharing during periods in which it is not required.

To permanently disable Web sharing in MacOS 8 or MacOS 9, remove two files and restart:

System Folder:Control Panels:Web Sharing
System Folder:Extensions:Web Sharing Extension

To permanently disable AppleShare/IP in MacOS 9, remove one file and restart:
System Folder:Extensions:Shareway IP Personal Bgnd

## 8. User IDs, especially root/administrator with no passwords or weak passwords.

Some systems come with "demo" or "guest" accounts with no passwords or with widely-known default passwords. Service workers often leave maintenance accounts with no passwords, and some database management systems install administration accounts with default passwords. In addition, busy system administrators often select system passwords that are easily guessable ("love," "money," "wizard" are common) or just use a blank password. Default passwords provide effortless access for attackers. Many attackers try default passwords and then try to guess passwords before resorting to more sophisticated methods. Compromised user accounts get the attackers inside the firewall and inside the target machine. Once inside, most attackers can use widely-accessible exploits to gain root or administrator access.

**Systems Affected:**
All systems.

**CVE Entries:**
Unix guessable (weak) password - CAN-1999-0501
Unix default or blank password - CAN-1999-0502
NT guessable (weak) password - CAN-1999-0503
NT default or blank password - CAN-1999-0504

These candidate entries are likely to change significantly before being accepted as full CVE entries.

**Advice on correcting the problem:**
A. Create an acceptable password policy including assigned responsibility and frequency for verifying password quality. Ensure senior executives are not exempted. Also include in the policy a requirement to change all default passwords before attaching computers to the Internet, with substantial penalties for non-compliance.

B1. VERY IMPORTANT! Obtain written authority to test passwords

B2. Test passwords with password cracking programs:

     For Windows NT: l0pthcrack http://www.l0pht.com
     For UNIX: Crack http://www.users.dircon.co.uk/~crypto

C. Implement utilities that check passwords when created.

     For UNIX: Npasswd, http://www.utexas.edu/cc/unix/software/npasswd
     For Windows NT:
     http://support.microsoft.com/support/kb/articles/Q161/9/90.asp

D. Force passwords to expire periodically (at a frequency established in your security policy).

E. Maintain password histories so users cannot recycle old passwords.

Additional information may be found at:

> http://www.cert.org/tech_tips/passwd_file_protection.html
> http://www.cert.org/incident_notes/IN-98.03.html
> http://www.cert.org/incident_notes/IN-98.01.irix.html

## 9. IMAP and POP buffer overflow vulnerabilities or incorrect configuration.

IMAP and POP are popular remote access mail protocols, allowing users to access their e-mail accounts from internal and external networks. The "open access" nature of these services makes them especially vulnerable to exploitation because openings are frequently left in firewalls to allow for external e-mail access. Attackers who exploit flaws in IMAP or POP often gain instant root-level control.

### Systems Affected:
Multiple UNIX and Linux systems

### CVE Entries:
CVE-1999-0005, CVE-1999-0006, CVE-1999-0042, CVE-1999-0920, CVE-2000-0091

### Advice on correcting the problem:
A. Disable these services on machines that are not e-mail servers.

B. Use the latest patches and versions. Additional information may be found at:

> http://www.cert.org/advisories/CA-98.09.imapd.html
> http://www.cert.org/advisories/CA-98.08.qpopper_vul.html
> http://www.cert.org/advisories/CA-97.09.imap_pop.html

C. Some of the experts also recommend controlling access to these services using TCP wrappers and encrypted channels such as SSH and SSL to protect passwords.

## 10. Default SNMP community strings set to 'public' and 'private.'

The Simple Network Management Protocol (SNMP) is widely used by network administrators to monitor and administer all types of network-connected devices ranging from routers to printers to computers. SNMP uses an unencrypted "community string" as its only authentication mechanism. Lack of encryption is bad enough, but the default community string used by the vast majority of SNMP devices is "public", with a few "clever" network equipment vendors changing the string to "private". Attackers can use this vulnerability in SNMP to reconfigure or shut down devices remotely. Sniffed SNMP traffic can reveal a great deal about the structure of your network, as well as the systems and devices attached to it. Intruders use such information to pick targets and plan attacks.

### Systems Affected:
All system and network devices.

**CVE Entries:**
default or blank SNMP community name (public) - CAN-1999-0517
guessable SNMP community name - CAN-1999-0516
hidden SNMP community strings - CAN-1999-0254, CAN-1999-0186

These candidate entries are likely to change significantly before being accepted as full CVE entries.

**Advice on correcting the problem:**
A. If you do not absolutely require SNMP, disable it.

B. If you are using SNMP, use the same policy for community names as used for passwords described in Vulnerability Cluster Number 8 above.

C. Validate and check community names using snmpwalk.

D. Where possible make MIBs read only. Additional information:

> http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid 210315

Recent virus attacks have illustrated how macro and script code could spread easily through e-mail attachments, and people were admonished to avoid opening potentially dangerous attachments. However, Windows users can also spread malicious viruses without opening attachments. Microsoft Outlook and Outlook Express will execute HTML and script code in an e-mail in their default installations. In addition, several so-called ActiveX components are incorrectly executable from an e-mail containing HTML and script code. Some of the vulnerable controls include the Scriplet.typlib (ships with IE 4.x and 5.x) and the UA control (Office 2000). Other vulnerabilities arising from the use of Active Scripting are that an e-mail could be used to install new software on a users computer.

A relatively benign virus known as the kak worm is already spreading through these mechanisms. A malicious version of kak can be anticipated at any time. We recommend that all users and administrators set Outlook and Outlook Express to read e-mail in the "Restricted Sites Zone" and then further disable all Active Scripting and ActiveX related settings in that zone. This is done in the Options dialog's Security tab, but can be automated using System Policies. Microsoft has made patches available for the individual problems and is readying a patch which will set the security settings in Outlook, but apparently has no plans on fixing Outlook Express.

**Systems Affected:**
All Windows systems with Internet Explorer 4.x and 5.x (even if it is not used) or Office 2000. Windows 2000 is not affected by some of the IE issues.

**CVE Entries:**
CVE-1999-0668
CAN-2000-0329

**Advice on correcting the problem:**
http://www.microsoft.com/security/bulletins/ms99-032.asp
http://www.microsoft.com/security/bulletins/MS99-048.asp
http://www.microsoft.com/technet/security/bulletin/MS00-034.asp

The fixes for the particular vulnerabilities discussed here are available from:

http://www.microsoft.com/msdownload/iebuild/scriptlet/en/scriptlet.htm
http://www.microsoft.com/msdownload/iebuild/ascontrol/en/ascontrol.htm
http://officeupdate.microsoft.com/info/ocx.htm

Set your Security Zone to restricted sites and then disable all active content in that zone.

Apply the patch to Outlook as soon as it becomes available at:

http://office.microsoft.com/Downloads/default.aspx

Updating your virus detection software, while important, is not a complete solution for this problem. You must also correct the flaws in Microsoft's software.

In this section, we list ports that are commonly probed and attacked. Blocking these ports is a minimum requirement for perimeter security, not a comprehensive firewall specification list. A far better rule is to block all unused ports. And even if you believe these ports are blocked, you should still actively monitor them to detect intrusion attempts. A warning is also in order. Blocking some of the ports in the following list may disable needed services. Please consider the potential effects of these recommendations before implementing them.

1. Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses, private (RFC1918 and network 127) and IANA reserved addresses. Also block source routed packets.
2. Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)
3. RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)
4. NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 – earlier ports plus 445(tcp and udp)
5. X Windows -- 6000/tcp through 6255/tcp
6. Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)
7. Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)
8. Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)
9. "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)
10. Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)
11. ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and destination unreachable messages **except** "packet too big" messages (type

3, code 4). (This item assumes that you are willing to forego the legitimate uses of ICMP echo request in order to block some known malicious uses.)

See also Top Ten Blocking Recommendations Using ipchains and Top Ten Blocking Recommendations Using Cisco ACLs in the SANS Infosec Reading Room.

Compaq (Digital Unix)

    http://www.compaq.com/support

FreeBSD

    http://www.freebsd.org/security/

HP HP-UX

    For the US, Canada, Asia-Pacific, & Latin America:
    http://us-support.external.hp.com

    For Europe:
    http://europe-support.external.hp.com

    Choose Individual Patches, then log in or create new login ID.

    To Retrieve a Security Patch Matrix:
    ftp://us-ffs.external.hp.com/export/patches/hp-ux_patch_matrix/

IBM AIX

    http://techsupport.services.ibm.com/support/rs6000.support/downloads
    http://techsupport.services.ibm.com/rs6k/fixes.html

SCO (OpenServer and Unixware)

    http://www.sco.com/security/ (Security Bulletins and Patches)
    http://www.sco.com/support/ftplists/index.html (General OS patches)

Sun Solaris

    http://sunsolve.sun.com (Recommended & Security Patches)

SGI

    http://support.sgi.com

Linux

Caldera
http://www.caldera.com/support/security/

Debian
http://www.debian.org/security/index.en.html

Mandrake
http://www.linux-mandrake.com/en/fupdates.php3

Red Hat
http://www.redhat.com/support/updates.html

SuSe
http://www.suse.com/support/download/updates/index.html
http://www.suse.de/en/support/security/index.html

# The Experts Who Helped Create The Top Ten and Top 20 Internet Vulnerability Lists

| Name | Company | Name | Company |
|------|---------|------|---------|
| Bill Hancock | Exodus Communications | Tony Sager | National Security Agency |
| Bill Hill | MITRE | Gene Schultz | Lawrence Berkeley Laboratory |
| Billy Austin | Intrusion.com | Eric Schultze | Foundstone |
| Chris Brenton | Dartmouth Inst. for Security Studies | Alan Paller | SANS Institute |
| Christopher Klaus | Internet Security Systems | Derek Simmel | Carnegie Mellon University |
| Clint Kreitner | Center for Internet Security | Gene Spafford | Purdue University CERIAS |
| Dave Mann | BindView | Frank Swift | Pilot Network Services |
| David Nolan | Arch Paging | | |
| Eric Cole | SANS Institute | Jim Ransome | RAZOR Research - BindView Development |
| Igor Gashinsky | NetSec Inc | Marcus Sachs | JTF-CNO US Department of Defense |
| Jesper Johansson | Boston University | Mary Chaddock | |
| Jim Magdych | Network Associates Inc. | Jeff Stutzman | Healthcare ISAC |
| Jimmy Kuo | Network Associates Inc. | Lance Spitzner | Sun Microsystems, GESS Team |
| Kathy Fithen | CERT Coordination Center | | |
| Kelly Cooper | Genuity | Vince Rowe | FBI, NIPC |
| Larry Merritt | National Security Agency | Viriya Upatising | Loxley Information Services Co. |
| Lee Brotzman | NASIRC Allied Technology Group Inc. | Ross Patel | ViaCode Ltd and Afentis Security Team |
| Matt Bishop | University of California Davis | Stephen Northcutt | SANS Institute |
| Mudge | @stake | Laurie Zirkle | Virginia Tech CIRT |
| Nick FitzGerald | Computer Virus Consulting Ltd. | | |
| Phil Benchoff | Virginia Tech CIRT | Ron Nguyen | Ernst & Young |
| Randy Marchany | Virginia Tech | Bob Todd | Advanced Research Corporation |
| Rob Clyde | Axent | | |
| Rob Clyde | Symantec | Chris Prosise | Foundstone Inc. |
| Robert Harris | EDS | | |
| Ron Jarrell | Virginia Tech CIRT | Greg Shipley | Neohapsis |
| Scott Conti | University of Massachusetts | Martin Roesch | Snort |
| Scott Craig | KMart | | |
| Scott Lawler | Veridian | Wayne Stenson | Honeywell |
| Shawn Hernan | CERT Coordination Center | Bruce Schneier | Counterpane Internet Security Inc. |
| Sten Drescher | Tivoli Systems | Greg Shipley | Neohapsis |
| Steve Christey | MITRE | Hal Pomeranz | Deer Run Associates |
| Tina Bird | Counterpane Internet Security Inc. | David Nolan | Arch Paging |
| Valdis Kletnieks | Virginia Tech CIRT | Ed Skoudis | Predictive Systems |
| William McConnell | Tre nd Consulting Services | Jeff Tricoli | FBI NIPC |