



The Top 20 Internet Security Vulnerabilities

and
How to Eliminate Them

SANS CDI East @ NIGHT – The SANS Institute © 2003

1

Agenda

- The need for a Top 20 list
- Building the list
- Differences from last year
- The Windows vulnerabilities
- The Unix vulnerabilities
- Top 20 team topics
- Questions

SANS CDI East @ NIGHT – The SANS Institute © 2003

2

The Need for a List

- Common complaints:
 - “I don’t know where to start”
 - “My scans show hundreds of vulnerabilities, now what?”
- Most intrusions begin by exploiting a known vulnerability
- Most intrusions can be prevented by closing common security exposures

Through the Eyes of a Hacker

- Attackers are opportunistic
 - Taking the easiest and most convenient route
 - Exploiting the best-known flaws with widely available tools
- They count on organizations not fixing the problems
 - Scanning the Internet for vulnerable systems
 - Often attacking indiscriminately

Through the Eyes of a Sysadmin

- System administrators are overwhelmed
 - May not know which of the hundreds of potential problems are the ones that are most dangerous
 - Too busy to correct them all
- They count on software companies to issue timely patches
 - But patch management is VERY HARD

The SANS Top 10 List

- First published in June 2000
- Updated to include 20 issues in 2001
 - 7 General vulnerabilities
 - 6 Windows vulnerabilities
 - 7 Unix/Linux vulnerabilities
- Split into two top-10 lists in 2002
 - 10 Windows vulnerabilities
 - 10 Unix/Linux vulnerabilities

2003 In Review

- Events in 2003 demonstrated the continued need for a Top 20 List
- Worms
 - SQL-Slammer via UDP
 - Blaster and Nachi via TCP
 - Swen and SoBig via e-mail
- New Vulnerabilities
 - SSH, SSL, BIND, Sendmail
 - Microsoft Windows, IE, Office

SQL-Slammer Worm

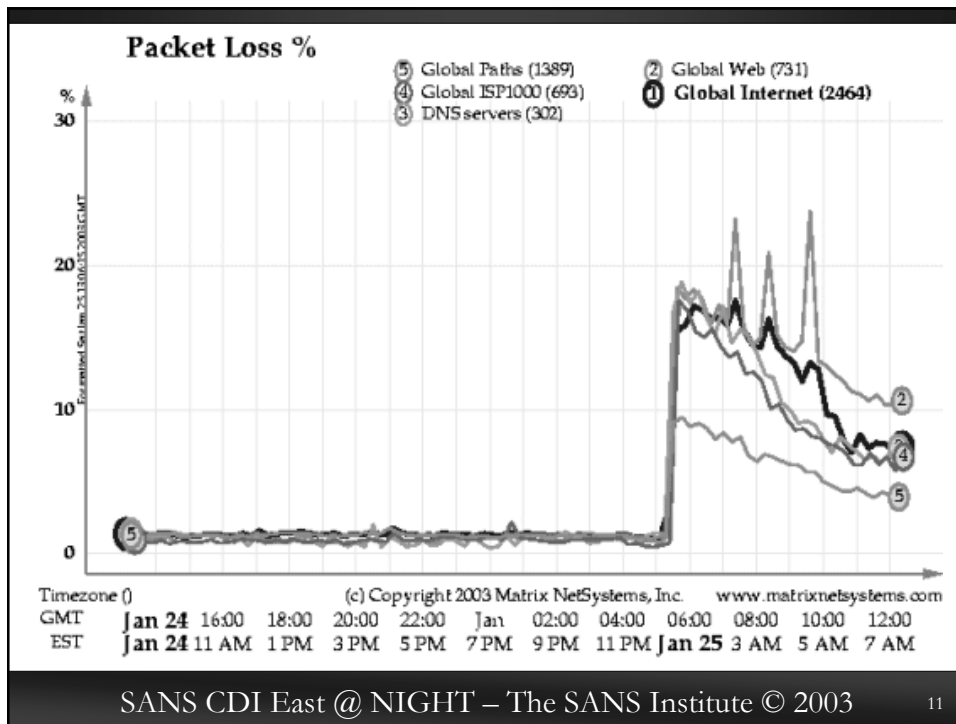
- 376-byte (small!) UDP packet
- Exploited a well documented vulnerability in Microsoft SQL Server and Microsoft SQL Desktop Engine (MSDE) systems
- Began spreading early on a Saturday morning – around 1 am EST
- Saturated the Internet within 10 minutes

SQL-Slammer Worm (2)

- Containment was easy
 - block UDP port 1434
- By 6 am EST all major ISPs were aware of the problem
- Some businesses did not get word until Monday morning
- Affected airline scheduling, bank ATM machines, and emergency services

Was SQL-Slammer Preventable?

- Microsoft Security Bulletin issued on July 25, 2002
- Patching was difficult, some patches caused additional problems
- Exploits published in November
- Worm hits on January 25, 2003



Blaster Worm

- Microsoft RPC/DCOM bulletin published on July 17, 2003
- Internet disruptions predicted by DHS
 - Warning issued on July 24
 - Expected a worm or similar type of malware
- A concurrent bulletin from Cisco was also troubling
 - Affected all versions of Cisco IOS after 10.3

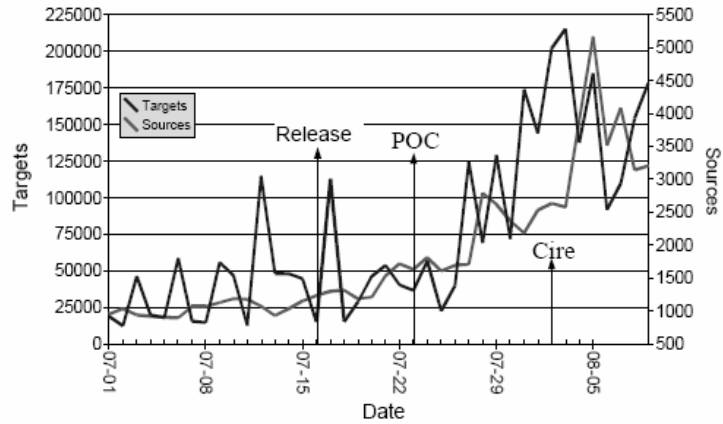
Blaster Worm (2)

- First proof-of-concept exploits appeared one week after bulletin release
 - Early exploits required specific memory offsets
 - Breakthrough occurred when “universal offsets” were published for Windows 2000 and Windows XP
- IRC “bots” were updated in early August

Internet Storm Center View

- TCP port 135 activity rose steadily in last half of July
- Large increase as IRC bots spread in early August
- On August 11th, ISC detected over 3500 new sources every 10 minutes
- Over 200,000 hosts compromised in next several hours

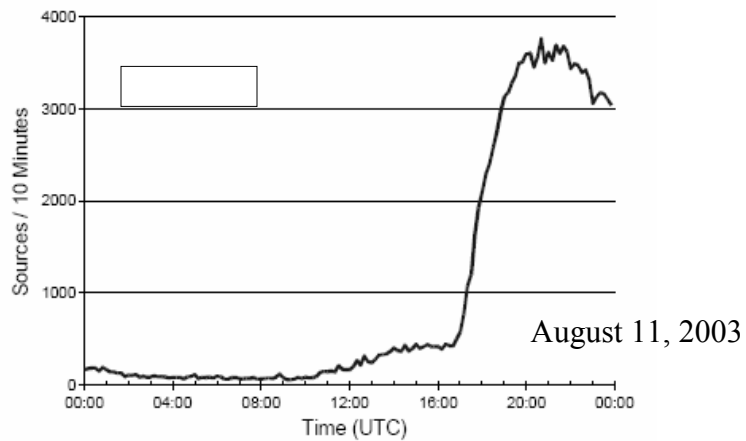
Port 135 Activity



SANS CDI East @ NIGHT – The SANS Institute © 2003

15

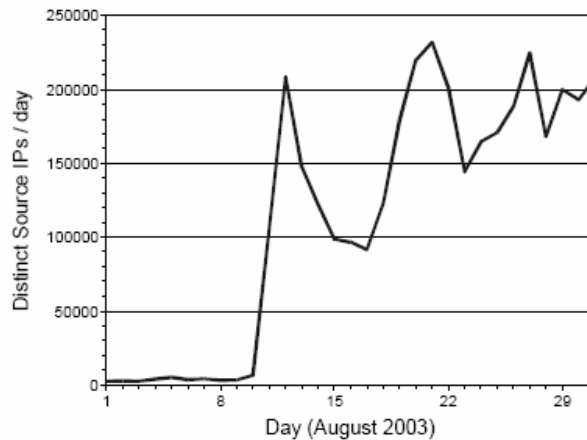
Sources Scanning for Port 135



SANS CDI East @ NIGHT – The SANS Institute © 2003

16

Blaster Summary



SANS CDI East @ NIGHT – The SANS Institute © 2003

17

Was Blaster Preventable?

- Microsoft Security Bulletin issued on July 17, 2003
- Patching is easy, but many users and sysadmins ignore or wait
- Exploits published within one week
- Worm hits on August 10, 2003

SANS CDI East @ NIGHT – The SANS Institute © 2003

18

Cleanup and Prevention

- Estimated cleanup costs for SQL-Slammer and Blaster have risen to over \$1 Billion each
- Both exploited vulnerabilities that had patches available
- Both could have been prevented

A Million Monkeys...

- Impact of random hacking can be greatly reduced with proactive defenses
- Damages can be minimized by reducing Internet exposure
- By addressing the most common holes, we raise the bar above the skills of the average "script kiddie"

Typical Kiddie-Hacker Methodology

- Scan for exposed systems
- Compile list and share with friends
- Wait for a proof-of-concept or working exploit to be published
- Launch the exploit against list
- Rinse, repeat

Best Defenses

- Patch, Patch, Patch!
- Make good design decisions
 - Use secure shell for remote login
 - Have restrictive perimeter policies
 - Include host based firewalls and IDSs
- Follow industry best practices
 - Log everything, trust nobody
 - Turn off unused services
 - Least privilege access

The Bottom Line

- A small number of vulnerabilities account for a large share of successful attacks
- Our folks in the trenches need the tools and information to help them eliminate these items

The SANS Top 20 Internet Security Vulnerabilities

4th Annual List - Released
October 8, 2003

Development Started in May 2003

- Two primary groups worked on the list
- SANS community
 - Staff, faculty, and alumni
 - Participants from past teams
- Writing team
 - Agencies such as DoE, NSA, and NISCC
 - Companies such as Qualys and Afentis
 - Universities including Arizona State, University of Massachusetts, and Virginia Tech

Development Goals

- Objectives
 - S.M.A.R.T (Specific Measurable Achievable Realistic and Timebased)
 - CVE and CAN data should only include remote root level compromises or equivalent
 - Keep the outlines as short and logical as possible
- Ensure that we implement the lessons learned from 2002

Development Process

- Requests for nominations go to the team
- Individual team members reached their own conclusions by
 - Turning to their IDS and logging systems
 - Nominating vulnerabilities that affect them most
 - Using on-line resources like icat.nist.gov
 - Asking their security teams for collective input

Development Process (2)

- Group Discussions
 - Nominations discussed in the open
 - E-mail was the primary communication medium
- Everyone is Heard
 - Every single concern or issue was taken under advisement and ALL sound feedback was integrated into the processes
- Hub and Spoke Communication Model

The Voting Rounds

- April and May – team formation
- Early June - nomination request goes out and team members submit chosen vulnerabilities
- Early July - master file of all nominations is sent out for vote
- Mid July - votes come back and the Top 20 begins to emerge
- August - tie breakers
- We have a new Top 20!

Announcement in Washington October 8, 2003

Released in Conjunction with:

- United States Department of Homeland Security
- United Kingdom's National Infrastructure Security Coordination Center
- Canada's Office of Critical Infrastructure Protection and Emergency Preparedness
- SANS Institute

The 2003 Top 20

Windows

- Internet Information Server (IIS)
- Microsoft SQL Server (MSSQL)
- Windows Authentication
- Internet Explorer (IE)
- Windows Remote Access Service
- Microsoft Data Access Components (MDAC)
- Windows Scripting Host (WSH)
- Microsoft Outlook and Outlook Express
- Windows Peer to Peer File Sharing (P2P)
- Simple Network Management Protocol (SNMP)

Unix

- BIND Domain Name System
- Remote Procedure Call (RPC)
- Apache Web Server
- General Unix Authentication
- Clear Text Services
- Sendmail
- Simple Network Management Protocol (SNMP)
- Secure Shell (SSH)
- Misconfiguration of Enterprise Services NFS/NIS
- Open Secure Sockets Layer (OpenSSL)

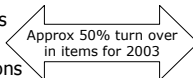
What's New in the Windows List?

2002 Top 20 List

- Internet Information Server (IIS)
- Microsoft Data Access Components (MDAC)
- Microsoft SQL Server
- Internet Explorer
- Windows Scripting Host (WSH)
- General Windows Authentication
- NETBIOS -- Unprotected Windows Networking Shares
- Anonymous Logon -- NULL Sessions
- LAN Manager Authentication -- Weak LM Hashing
- Remote Registry Access

2003 Top 20 List

- Internet Information Server (IIS)
- Microsoft Data Access Components (MDAC)
- Microsoft SQL Server
- Internet Explorer
- Windows Scripting Host (WSH)
- Windows Authentication
- Windows Remote Access Services
- Microsoft Outlook -- Outlook Express
- Windows Peer to Peer File Sharing (P2P)
- Simple Network Management Protocol (SNMP)



Black - Maintained placement on the list
 Blue - New Item for 2003
 Red - Bumped from the list

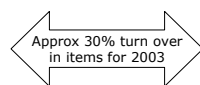
What's New in the Unix List?

2002 Top 20 List

- BIND/DNS
- Remote Procedure Call (RPC)
- Apache Web Server
- General Unix Authentication
- Sendmail
- Simple Network Management Protocol (SNMP)
- Secure Shell (SSH)
- File Transfer Protocol (FTP)
- R-Services -- Trust Relationships
- Line Printer Daemon (LPD)

2003 Top 20 List

- BIND/DNS
- Remote Procedure Call (RPC)
- Apache Web Server
- General Unix Authentication
- Sendmail
- Simple network Management Protocol (SNMP)
- Secure Shell (SSH)
- Clear Text Services
- Misconfiguration of Enterprise Services (NFS/NIS)
- Open Secure Sockets Layer



Black - Maintained placement on the list
Blue - New Item for 2003
Red - Bumped from the list

SANS CDI East @ NIGHT – The SANS Institute © 2003

33

Several Items Were Combined

- Remediating many vulnerabilities with common solutions
- A few examples:
 - Clear Text Services (R-Services, FTP, Telnet, SMTP, POP, etc.)
 - Windows Remote Access (DCOM-RPC, NetBIOS, Remote Registry, Anonymous Login, etc.)
 - WebDAV (ntdll.dll) belongs with IIS since it is the primary vector by which this exploit is accomplished

SANS CDI East @ NIGHT – The SANS Institute © 2003

34

Windows Vulnerabilities

- Internet Information Services (IIS)
- Microsoft SQL Server (MSSQL)
- Windows Authentication
- Internet Explorer (IE)
- Windows Remote Access Service
- Microsoft Data Access Components (MDAC)
- Windows Scripting Host (WSH)
- Microsoft Outlook and Outlook Express
- Windows Peer to Peer File Sharing (P2P)
- Simple Network Management Protocol (SNMP)

Defending Against The Windows Vulnerabilities

- Most of these issues can be mitigated with common security practices
- Examples include
 - Blocking tcp and udp ports 135 - 139, 445, 1025-1039, 1433 and 1434
 - Using Windows Update to patch
 - Using Microsoft Baseline Security Analyzer to verify

Defensive Measures for Internet Information Server

- Check for WebDAV (ntdll.dll) vulnerabilities
- HFNetcheck
- MBSA
- IIS Lockdown Wizard
 - special mention of URLScan next slide

Defensive Measures for Internet Information Server (2)

- URLScan overview (thanks to Jennifer Kolde)
 - IIS Lockdown is a tool for easily performing many of the basic (and necessary) fixes to IIS
 - URLScan is installed by IIS Lockdown
 - Application layer firewall that filters input to IIS before the data is passed to the web server
 - Filters specific request types (HEAD, TRACE, etc.), characters or metacharacters, or input longer than a specified length
 - Protects not only from specific attacks, but from general classes of attacks - both known and UNKNOWN

Defensive Measures for SQL Server Vulnerabilities

- SQL Server was the primary vulnerability behind worms such as SQLSnake and SQL-Slammer
- Apply patches and Service Packs
- Border router configurations
- Use strong passwords!

Defensive Measures for Windows Authentication Vulnerabilities

- Start with a good password policy
- Avoid weaker technologies
 - LANMAN authentication
- Use newer technologies
 - Windows XP with Windows 2003 Server
- Use tools to test your passwords
 - get permission!

Defensive Measures for Internet Explorer Vulnerabilities

- Stay up to date with patches and security fixes
- Securely configure your browser
 - Use Internet security zones
 - Privacy adjustments (cookies)
 - Miscellaneous (ActiveX, Java, Cross Site Scripting Attacks)
- Use a different browser

Defensive Measures for Remote Access Services

- Patch and apply Service Packs
- Securely configure
 - Disable file sharing where not absolutely needed
 - Remove anonymous logon
 - Restrict registry access
 - Monitor for RPC activity

Defensive Measures for Remote Access Services (2)

- Locate Microsoft LANs behind securely configured routers
 - Block the majority of this type of network traffic as far upstream as possible
- Identification of these issues is key to a successful defense

Defensive Measures for Data Access Components and Windows Scripting Host

- Stay up to date with patches and security fixes
- Download MDAC updates from <http://msdn.microsoft.com/downloads/list/dataaccess.asp>
- Use antivirus software
- Disable WSH file associations

Defensive Measures for Outlook and Outlook Express Vulnerabilities

- Use Antivirus Software
 - This is imperative in Outlook environments
- Stay current (windowsupdate.microsoft.com)
- Uninstall Outlook Express where not needed
 - Outlook Express may be re-installed silently if a service pack, significant roll-up, or operating system upgrade is installed
- Use conservative e-mail practices
 - File attachments

Defensive Measures for Peer to Peer Vulnerabilities

- P2P is unique
- Policy and policy enforcement is the primary defense against this phenomenon
 - Educate employees
 - Block known P2P ports at the firewall
- Network level identification and eradication
- Not only a threat of technical exploitation, but a real threat to your company's intellectual property

Defensive Measures for Simple Network Management Protocol

- Applicable to both Windows and Unix systems
 - Also appliances like routers and switches
- Identify, patch, remove/disable
- Secure border practices are essential
 - Be cautious with external SNMP monitoring
 - SNMP is a very standard method of intelligence gathering

Unix Vulnerabilities

- BIND Domain Name System
- Remote Procedure Call (RPC)
- Apache Web Server
- General Unix Authentication – No or Weak Passwords
- Clear Text Services
- Sendmail
- Simple Network Management Protocol (SNMP)
- Secure Shell (SSH)
- Misconfiguration of Enterprise Services NFS/NIS
- Open Secure Sockets Layer (OpenSSL)

Defending Against the Unix Vulnerabilities

- Solutions are more varied than with Microsoft Windows
 - Many different distributions
 - Most installations are customized
- General tenets include
 - Patching
 - Minimizing listening services
 - Securely configuring daemons
 - Turning on logging

Defensive Measures for BIND Vulnerabilities

- Upgrade!
 - All major versions of BIND (4.x, 8.x, and 9.x) are vulnerable to a number of remote exploits or denial of service attacks
- Patch when you cannot upgrade
- *chroot* your implementations of *named*
- Do not run BIND on non-DNS servers

Defensive Measures for Remote Procedure Call

- Turn off or remove if not needed
- Secure the border
 - Block tcp ports 111, [windows-135], 32770-32789
- Install patches from your vendor
 - See the Top 20 list at <http://www.sans.org/top20/#u2> for an extensive list

Defensive Measures for Apache Vulnerabilities

- Patch
- Do not run as root
- Securely Configure
 - Remove default scripts
 - Watch information disclosure (security through obscurity, modify tokens, disable directory indexing)
- *chroot* the entire Apache subdirectory tree
- Log all activity
- Watch your modules!

Defensive Measures for Unix General Authentication Vulnerabilities

- Have a solid password policy
- Use tools to test your passwords
 - get permission!
- Use shadow passwords
- Disable or remove accounts no longer in use

Defensive Measures for Clear Text Related Vulnerabilities

- Use encryption
- Disable or remove services where they are not needed (r-services, tftp, telnet)
- “Port forward” the protocol through ssh in order to secure it
 - example: - ssh -L [localport]:[targetmachine]:[remoteport] -l [username] [sshserver] -p [sshdport]

Defensive Measures for Sendmail Vulnerabilities

- Upgrade!
 - Sendmail has many vulnerabilities
 - Component of many common systems
- Securely configure
- Do not run in daemon mode
 - Turn off the “-bd” switch
- Turn off mail relaying for external users

Defensive Measures for Secure Shell Vulnerabilities

- Upgrade to most recent version of OpenSSH or SSH
- Use SSH2 when possible
- Verify good client side configuration
- SSH is unique in that it helps to mitigate many of the other Top 20 vulnerabilities
 - It is an ESSENTIAL tool

Defensive Measures for NFS/NIS Vulnerabilities

- Properly configure the */etc/exports* file to control access
- Block these services at gateways
- Disable where not needed
- Patch
- Tunnel NFS over SSH

Defensive Measures for OpenSSL Vulnerabilities

- Primary defense is to upgrade to the latest version
- If possible, use *ipfilters* or firewall rules to restrict system access

The Basic Remediation Process

- Choose a Top 20 scanning tool
- Scan your network
- Fix problems
- Scan again
- Fix problems that have become unfixed
 - Introduced by new, unremediated systems being put online
- Scan again...

Scanning Tools for the Top 20

- | | |
|--------------|--|
| • Qualys | sans20.qualys.com |
| • Foundstone | www.foundstone.com |
| • eEye | www.eeye.com/retina |
| • Nessus | www.nessus.org |
| • SAINT | www.saintcorporation.com |
| • Nmap | www.insecure.org |
| • Sara | www-arc.com/sara |
| • Vlad | razor.bindview.com/tools/vlad/ |

Patching and Updating

- Microsoft
 - windowsupdate.microsoft.com
 - office.microsoft.com
- Linux
 - www.debian.com/security
 - www.redhat.com/software/rhn/update
 - www.suse.com/us/private/support/security
- BSD
 - www.freebsd.org/security
 - www.openbsd.org/security.html

Items Removed from the 2002 Windows List

- NETBIOS
- Anonymous Logon
- Remote Registry Access
- LAN Manager Authentication
- General Windows Authentication

New Location of Removed Items

2002 List Items

- NETBIOS
- Anonymous Logon
- Remote Registry Access
- LAN Manager Authentication
- General Windows Authentication

2003 List Items

- Windows Remote Access
 - {combination of NETBIOS, Anonymous Logon, & Remote Registry Access. Includes DCOM RPC}
- Windows Authentication
 - {combination of LAN Manager Authentication, and General Windows Authentication}

Items Removed from the 2002 Unix List

- File Transfer Protocol
- R-Services - Trust Relationships
- Line Printer Daemon

New Location of Removed Items

2002 List Items

- File Transfer Protocol
- R-Services -- Trust Relationship
- Line Printer Daemon

We lost
LPD this year

2003 List Items

- Clear Text Services
 - {combination of "common" clear text programs. ftp, smtp, pop, telnet, tftp, rlogin, rsh, imap, http. Unfortunately, only the clear text vulnerability characteristics of FTP and the R-Services can be covered by a Clear Text Services item}
 - {We lost coverage of the other vulnerabilities involved in FTPD and the R-Services (buffer overflows, misconfiguration, trust issues, etc.)}
- No new item to absorb this topic

Persistent Items

- Why are there persistent items on the list from year to year?
- Could it be -
 - Overworked admins?
 - Laziness?
 - Lack of education?
 - Lack of a good way to track and install patches?

Answer - Yes, Yes, Yes, and Yes!

Action Plan

- Educate
- The team is a very powerful tool
- Update as new threats arise
- What did we learn? And where are we looking now? --> next slide..

Lessons Learned

- Can't fully secure these operating systems
 - But need to at least keep them patched
- Combine defensive techniques
 - Border devices
 - Network protocols
 - Host-based firewalls and IDSs
- Follow a basic remediation process (slide 59)

Additional Team Topics

- Some of the big issues
 - Whether we should discuss user behavior
 - Whether we should discuss architecture
 - Whether we should discuss non Windows and Unix products (such as Oracle, Lotus Notes, NetWare, Cisco, etc.)
 - Whether we should combine past items into common remediation items
- We have combined some remediation steps this year, how are we going to address more and more issues as the years go on?
- How did we come to the bottom of some of these questions?

The wonderful team who helped generate the 2003 Top 20

Adair Collins, US Department of Energy
Alan Paller, SANS Institute
Alex Lucas, United Kingdom National Infrastructure Security Co-ordination Center
Alexander Kotkov, CCH Legal Information Services
Anton Chuvakin, Ph.D., netForensics
BJ Bellamy, Kentucky Auditor of Public Accounts
Bradley Peterson, US Department of Energy
Cathy Booth, United Kingdom National Infrastructure Security Co-ordination Center - Incident Response CESG
Chris Benjes, National Security Agency
Christopher Misra, University of Massachusetts Amherst
Dave Dobrotka, Ernst & Young
Dominic Beecher, United Kingdom National Infrastructure Security Co-ordination
Ed Fisher, CableJiggler Consulting, LLC
Edward Skoudis, International Network Services
Edward W. Ray, MMICMAN LLC

Erik Kamerling, Pragmeta Networks/SANS Institute - Editor
Gerhard Eschelbeck, Qualys
Jeff Campione, Editor 2002
Jeff Ito, Indus Corporation
Jeni Li, Arizona State University
Kevin Thacker, United Kingdom National Infrastructure Security Co-ordination
Koon Yaw Tan, Infocomm Development Authority of Singapore (IDA)
Pedro Paulo Ferreira Bueno, MetroRED Telecom, Brazil
Pete Beck, United Kingdom National Infrastructure Security Co-ordination
Richard (Rick) Wanner, InfoSec Centre of Expertise (COE) CGI Information Systems & Management Consultants Inc.
Roland M Lascola, U.S. Dept. of Energy - Office of Independent Oversight and Performance Assurance
Ross Patel, Afentis Security
Russell Morrison, AXYS Environmental Consulting Ltd.
Scott A. Lawler, CISSP, Veridian Information Solutions
Stephen Northcutt, SANS Institute
Valdis Kletnieks, Virginia Tech
William Eckroade, U.S. Dept. of Energy

Additional Personnel

Thanks also to the following list of people for their excellent work in helping to edit, format and produce the 2003 list.

Audrey (Dalas) Bines, SANS Institute
Brian Corcoran, SANS Institute
Cara L. Mueller, SANS Institute

The Top 20 team would also like to thank the following SANS Alumni who donated their time to review and comment on the 2003 draft.

Paul Graham, CIT at the University at Buffalo (UB)
Jerry Berkman, UC Berkeley
Neil W Rickert, Northern Illinois University
Travis Hildebrand, US Department of Veteran Affairs
Christoph Gruber, WAVE Solutions
Mark Worthington, Affiliated Computer Services (ACS), Riverside Public Library
Matthew Nehawandian, CISSP

Questions
