

Three Questions for the October 8, 2003 Top 20 Briefings.

Erik Kamerling
Editor of the 2003 Top 20
<http://www.sans.org/top20>
top20@sans.org



The SANS Top 20 List ~ A Consensus on
The Twenty Most Critical Internet Security
Vulnerabilities

In this briefing I am going to answer the following 3 questions for each operating platform

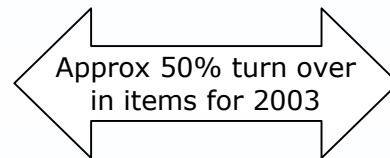
- **Q1:** What are the new items and issues covered in the 2003 Top 20 and why are they there?
 - Windows
 - UNIX
- **Q2:** At what expense did we obtain these new items? What vulnerabilities were bumped from the list?
 - Windows
 - UNIX
- **Q3:** Did we really lose our ability to defend against these vulnerabilities when the items were bumped?
 - Windows
 - UNIX

Question 1: What are the new items
and why are they included?

What are the differences between last year's Windows items and this year?

2002 Top 20 List - Where we are coming from.

- Windows
 - 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 - Where we have arrived.

- Windows
 - 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

High points of the *changes* with the Windows items that have maintained position on the list?

- Internet Information Server (IIS)
 - ntdll Web_DAV Buffer Overflow defense instructions -- <http://www.cert.org/advisories/CA-2003-09.html>
- Microsoft SQL Server
 - SQL-Slammer/SQL-Hell/Saphire Worm -- <http://www.cert.org/advisories/CA-2003-04.html>
- Internet Explorer
 - New Security Setting Guidelines for Internet Explorer
- Microsoft Data Access Components (MDAC)
 - Information on the Unchecked Buffer Overflow in MDAC, MS03-033
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-033.asp>. Also appearing as CAN-2003-0353
- Windows Scripting Host (WSH) -- Maintained it's position
 - Fully expanded and up to date "How to Protect Against It" section (including NTFS Permissions direction, expanded Antivirus info, etc.)

What items are totally new for the Windows Category?

- **Windows Authentication**
 - One of our great new items this year.
 - Combination of 2002 LAN Manager Authentication – Weak LM Hashing & General Windows Authentication – Accounts with No Passwords or Weak Passwords.
- **Windows Remote Access Services**
 - Another of our biggest new items this year, for those folks who use Windows.
 - combination of 2002 NetBIOS, Anonymous Logon, & Remote Registry Access. Including RPC DCOM outlines.
- **Microsoft Outlook -- Outlook Express**
 - First time appearing, was a close call in past years and it has finally made it.
 - Includes such excellent information as the need for Antivirus software, User Behavior considerations, program updating -- and even uninstalling Outlook.

continued

Continued..What items are totally new for the Windows Category?

- **Windows Peer to Peer File Sharing (P2P)**
 - First time appearing, and this item addresses some very important vulnerabilities that are rather new to the Top 20 file (Threats to Intellectual Property (legal), tunneling unauthorized traffic and data over authorized channels/remotely exploitable misconfigurations and weaknesses (technical), and social vulnerabilities in that there is ease of distribution of malicious code masquerading as legitimate materials in this communication medium (social)).
- **Simple Network Management Protocol (SNMP)**
 - It has been a close call in recent years to include SNMP as a Windows item, and this year it has made it into the Windows List

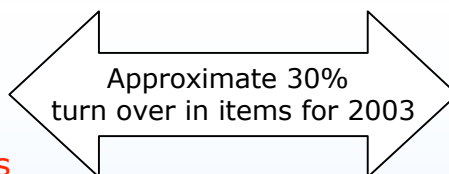
What are the differences between last year's UNIX items and this year?

2002 Top 20 List - Where we are coming from

- Unix
 - 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 - Where we have arrived

- Unix
 - 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

High points of the *changes* of the Unix items that have maintained position on the list?

- BIND/DNS
 - Updated - to include items such as CAN 2002-0651 (Buffer overflow in DNS Resolver), CAN 2002-1220 (Bind 8.3x denial of service via request of a subdomain), etc.
- Remote Procedure Call (RPC)
 - Updated - enhanced RPC Service and Program number information, enhanced description, and revised CVE and CAN.
- Apache Web Server
 - Updated - PHP vulnerabilities (CA-2002-05 CA-2002-21 CAN-2002-0985 CAN-2003-0097) covered under Apache.
- General UNIX Authentication
 - Reviewed and Updated.
- Sendmail
 - Updated to include items such as CA-2003-25 Buffer Overflow.

continued

High points of the *changes* with the Unix items that have maintained position on the list? Continued

- Simple network Management Protocol (SNMP)
 - Reviewed and Updated.
- Secure Shell (SSH)
 - Updated Description, vulnerability determination information, and “how to protect against it” data. SSH’s description has been updated to reflect it’s important role in remediating many of the other Top 20 clear text vulnerabilities.

What items are totally new for the Unix Category?

- **Clear Text Services**
 - Combination of U5 FTP, and U6 R-Services clear text aspects, with the addition of many other clear text programs like telnet – tftp – smtp – pop – imap - http - etc. This items outlines methods for detecting clear text transmissions through your network, and techniques for securing that traffic. With powerful security tools such as OpenSSL and OpenSSH.
- **Misconfiguration of Enterprise Services (NFS/NIS)**
 - Well rounded description of NFS/NIS security considerations, with comprehensive technical security instructions on steps like using NFSBug to test configurations, gateway port blocking considerations, and tunneling NFS over SSH!
- **Open Secure Sockets Layer**
 - Includes comprehensive description and defense information. Including information on OpenSSL buffer overflows and vulnerabilities such as (CAN-2002-0657 CAN-2002-0656 CAN-2002-0655)

What else is new in the file?

New Ports to Block at the Firewall list!

- The list of ports that we recommend are blocked at the firewall or gateway device has been greatly expanded.
- Too long to list here, go to <http://www.sans.org/top20> and see for yourself.
- Remember that the most secure approach is almost always to take a default deny stance on your routers and firewalls.

Malicious Code Defense Instructions

- The List now contains instructions to help defend your systems from some of the most destructive worms and malicious code today.
- **SQL_Slammer**
- MS Outlook Virus Propagation (includes **sobig** and others like it)
- Web_DAV Buffer Overflows
- RPC DCOM Exploits - Blaster
- **Code Red**
- **SQL Snake**
- Malicious Web Operators
- Klez, Sircam, Nimda
- **ILOVEYOU virus**
- etc.

Questions 2 & 3: What vulnerabilities were bumped from the list, and did we really lose our ability to defend against them?

Windows

What individual Windows vulnerabilities did we lose from the list in the voting process?

Did we Really Lose them? Or have they been absorbed into some new 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. Including DCOM RPC}
- Windows Authentication
 - {combination of LAN Manager Authentication, and General Windows Authentication}

UNIX

What individual UNIX vulnerabilities did we lose from the list in the voting process?

Did we Really Lose them?
Or have they been absorbed
into some new items?

2002 List Items

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

Looks like
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 lose coverage of the other vulnerabilities involved in FTPD and the R-Services (buffer overflows, misconfiguration, and trust issues to name a few)

? No new item to absorb this topic ?

Additional Information:

- A short overview of voting
- Items of discussion with the team for 2003

A Short Overview of the Voting Procedure

- May 2003 - We (SANS) asked the initial team to start thinking about the top 10 Windows and UNIX vulnerabilities that face their organizations
- Early June - A request goes out to the whole team for their Top 20 nominations (as brain food for the team: we include an attached rundown of all 2002 Top 20 enhancement comments and observations that we have collected from groups and agencies to this point)
- Feedback, nominations, and proposals come back - they are centrally tabulated into 1 large file.
- Early July - This file is sent back out to the team and we ask them to analyze, decide, and actually submit their votes to us.
- Mid July - All of the nominations are returned and counted and the Top 20 begins to emerge - results are back shortly and we quickly have 9 unix items and 9 windows items clearly placed.
- We naturally end up with tie votes on numerous items. e.g. It is a tie for UNIX 10th place (RServices,LPD,Samba,MySQL, OpenSSL) and for Win 10th place (ntdll.dll WebDav -- standalone, or SNMP)
- We do a tie breaker - the results are SNMP is tenth for Windows (WebDav was a shoe in under IIS), and the UNIX vote for OpenSSL inclusion as 10th place item comes in about a week later.
- The new Top 20 now shows itself. And we then go into research and writing mode to make the list come true.

October 8, 2003

SANS Institute -- Top 20 Project

17

Items of discussion with the team as we voted on vulnerabilities and started to build this file

- One of the biggest topics of discussion - and what turned out to be one of the most valuable decisions we could have made, was to focus some energy in the early stages on combining similar items into common groups. (FTP, smtp, pop, telnet) into a UNIX clear text services group, (Anon Login, Remote Registry Access, NETBIOS) into a Windows remote access item. WebDAV ntdll buffer overflow under IIS (since it is the primary avenue of compromise), etc. More on this type of combination effort later.
- There were many nominations this year - but the following items caused active discussion from the team and were common areas of desired focus
 - **The need to combine similar clear text programs into a common Clear Text Services item**
 - FTP should be merged into such a Clear Text item
 - The need to combine older items like w6 and w7 into 1 common authentication item
 - The need to combine older items like w4, w5, and w9 into a common remote access item (and later decided to include RPC -- DCOM)
 - **WebDav problems needed to be covered - and was absorbed into IIS**
 - Missing Patches and outdated software was a paramount topic that we needed to talk about in our remediation information for all items.
 - **Mention the pitfalls and dangers of standing up default installs**
 - We needed a security setting guideline for IE
 - User Behavior issues should be addressed in some way or manner
 - **Our CVE and CAN info needed a lot more attention and grooming to include new and pertinent vulnerabilities**
 - and so on...

continued

Continued.. Items of discussion with the team as we voted on vulnerabilities and started to build this file

Runners Up in the Voting Procedure

Unix Runners up! SAMBA, LPD, MYSQL, Snort, PHP, FTP

Windows Runners Up! Terminal Services, unchecked buffer in locator service, flaw in MS VM, Anonymous Login, Remote Registry

The SANS Top 20 List for 2003

•Windows

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

• Unix

- BIND/DNS
- 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

<http://www.sans.org/top20>

The Top 20 is a living document, so please check back frequently. As new critical threats emerge they will be outlined in this file.

The Team that created the 2003 version of the SANS 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
 - **SANS Personnel who helped**
- Audrey (Dalas) Bines, SANS Institute
- Brian Corcoran, SANS Institute
- Cara L. Mueller, SANS Institute
 - **SANS Alumni who reviewed and commented**
- 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

Additional Information

For more information please visit

<http://www.sans.org/top20>

There is no cost and no registration is required to download and use the Top 20

Questions should be directed to **top20@sans.org**



Erik Kamerling
Editor -- SANS Top 20 List
ekamerling@snaplen.com
607.437.7134