National Infrastructure Protection Center CyberNotes

Issue #4-99 *February 17, 1999*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between January 27 and February 12, 1999. The table provides the operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Allaire[1]	ColdFusion 4.0	Code snippets from sample applications make it possible to make HTTP calls from the machine and to execute Denial-of-Service (DoS) attacks.	Remove the CFDOCS directory or restrict access to the directory. A maintenance release is scheduled for April 1999.	ColdFusion Sample Code vulnerability	**High**	Bug discussed in newsgroups and Web sites. Exploit script not required for the exploit.
Allaire[2]	ColdFusion Application Server 2.X, 3.X, 3.1.X and ColdFusion Server 4.X	Machines loaded with the Expression Evaluator (sample application) will allow authorized individuals to read and delete files on the server.	Remove all sample applications and code from production servers and obtain patch for Expression Evaluator at: http://www.allaire.com	ColdFusion Expression Evaluator unauthorized access	**High**	Bug discussed in newsgroups and Web sites. Exploit script not required for the exploit. Other related hacker tools can be utilized to gain privileged access.

[1] Allaire Security Bulletin, ASB99-02.
[2] Allaire Security Bulletin, ASB99-01.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Allaire[3]	ColdFusion Server – all versions with Microsoft SQL and ColdFusion Server 4.0 Enterprise with Sybase SQL	It is possible to send malicious Structured Query Language (SQL) statements to a database through a dynamic query. ColdFusion may mishandle numbers, if not quoted, or a string that is processed with the PreserveSingleQuotes() function.	Allaire has prepared a technical brief that provided guidance on this subject. The brief is titled "Securing Databases for ColdFusion Applications" and is available at: http://www.allaire.com.	ColdFusion SQL statements in dynamic queries.	**High**	Bug discussed in newsgroups and Web sites.
Cisco with Livingston[4]	ComOS 3.8.2-PM3 ComOS 3.7L-Or-HS	DoS will occur if a large number of bytes are directed at the access port, such as port 23.	Restrict telnet access to only those machines requiring access. Configure "service tcp-keepalives-in" or configure timeouts on TTY lines.	Router Access Port DoS	Medium (Note: The risk may be higher under certain conditions.)	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.
Cyrix[5]	HARDWARE CPU	No privileged users can cause systems to lock up by issuing three opcodes. Testing has not been done to determine if bug may be invoked remotely.	No workarounds or patches known at time of publishing.	Cyrix bug	Low/ Medium	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.
HP-UX[6] 11.0/800	Operating System	Patch PHCO_13214 will change the file usr/bin/newgrp to suid root.	Informational comment only.	PHCO_13214 suid root	Low	Bug discussed in newsgroups.
IPSWITCH	IMail[7]	Local user can gain unauthorized, privileged access to IMail, including account creation/deletion and reading.	No workarounds or patches known at time of publishing.	IMail 1920 key attack	Medium	Bug discussed in newsgroups and Web sites. Exploit script not required for the exploit.
Linux[8]	Operating System - PLP Line Printer Control (lpc) program under SuSE 5.2	Local user can gain root access through a buffer overflow.	Patch code available, along with alternative line printer suites.	Linux /usr/bin/lpc buffer overflow	Low/ Medium	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.
Linux – Multiple vendors	wu-ftpd	Unauthorized user can gain root access through a buffer overflow.	Upgrade available for wu-ftpd. Red Hat updates available at: ftp://updates.redhat.com/5.2 Slackware updates available at: ftp://ftp.cdrom.com/pub/linux/slackware-current/slakware/n8 SCO updates available at: ftp://ftp.sco.com/SSE/	Palmetto.ftpd – remote root overflow	**High**	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.

[3] Allaire Security Bulletin, ASB99-04.
[4] BUGTRAQ, February 5, 1999.
[5] BUGTRAQ, February 4, 1999.
[6] BUGTRAQ, February 5, 1999.
[7] ibid.
[8] BUGTRAQ, February 3, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Linux[9] - RedHat 5.x and below	MILO/Alpha	A local user running MILO can cause an Alpha based Linux machine to become unstable, lock up, or reboot.	New version available at: ftp://genie.ucd.ie/pub/alpha/milo/milo-latest	Non-Privileged Halt of Linux/Alpha	Low	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.
Microsoft[10]	BackOffice 4.0 Setup utility	The REBOOT.INI file that is created by the Setup utility contains plaintext passwords for the SQL Executive logon, Exchange Services Account, and possibly others.	No workarounds or patches known at time of publishing.	Microsoft REBOOT.INI	Medium/ High	Bug discussed in newsgroups and Web sites.
Microsoft[11]	Internet Information Server (IIS)	Virtual servers in the same physical directory can leak information through the cache.	Disable the cache.	Active Server Pages (ASP) Caching BUG	Medium	Bug discussed in newsgroups.
Microsoft[12]	IIS with Site Server 2.0	If an administrator does not create a directory called "users" then on the first successful upload a "users" directory will be created. This directory will default to the EVERYBODY group and this group will have change access (including write permission).	If not needed remove Site Server including the files: cpshost.dll uploadn.asp uploadx.asp upload.asp repost.asp postinfo.asp If needed, check that no directory accessible from the web has write permissions.	IIS and Site Server users directory write	Medium/ High	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.
Microsoft[13]	Word	Microsoft Word will issue a warning if a document containing a macro is opened. If a template contains a macro, the user receives no such warning. The template can be referenced by URL and thus load the contents from the Internet with out the user's knowledge.	Patch available at: http://officeupdate.microsoft.com/nonIE4/DownloadDetails/wd97spnonie4.htm Note: If you load Service Release 2 (SR-2), update this patch will be removed.	Word 97 template Vulnerability	**High**	Exploit Script now available. **Virus Bulletin has reported that at least two viruses exploit or use this hole as a means of distribution.**

[9] KSR[T] Advisory #009
[10] NTBUGTRAQ, February 9, 1999.
[11] NTBUGTAQ, January 27, 1999.
[12] BUGTRAQ, January 30, 1999.
[13] Microsoft Security Bulletin, MS99-002.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows[14] 95, 98, and NT[15]	IIS and File Transfer Protocol (FTP)	Refer to CyberNotes #3-99	Patch available for various versions at: ftp://ftp.microsoft.com/bussys/iss	IIS DoS FTP	Low/ Medium	Script identified at time of publishing but does not appear to be posted. Explanation of exploit available in newsgroups.
Microsoft Windows NT[16] 4.0	NT 4.0 with Service Pack 4 (SP4)	If a user password is changed from a DOS, Windows 3.1, Windows for Workgroups, OS/2, or Macintosh client then, it is possible to log in from a Windows NT machine to the user account without a password.	Patch available at: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP4/Msv1-fix/	Authentication Processing Error in Windows NT 4.0	Medium/ High	Bug discussed in newsgroups and Web sites. Exploit script not required for the exploit.
Microsoft Windows NT[17] 4.0 with SP3 and SP4	Operating System	If a user changes his/her password and then locks the workstation, the new password will not be accepted.	The user will discover the problem the first time he/she attempts to unlock the workstation.	NT4 locking	Low	**No attacks using this bug have been reported.**
Multiple[18]	FTP PASV mode	Unauthorized user may use the PASV command of FTP to gain access to information or cause a DoS condition.	Various solutions suggested, including updating the Request for Comment (RFC).	FTP PASV "Pizza Thief"	Low	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.
Multiple[19]	Nobo (Back Orifice program detector)	If sufficient information is received in a short period of time, Nobo may not be able to process the information resulting in a DoS condition.	Nobo V1.3 corrects this problem.	Nobo buffer overflow	Low	Bug discussed in newsgroups and Web sites.
Norton[20]	For Your Eyes Only[21]	Product contains backdoor password.	No workarounds or patches known at time of publishing.	Backdoor password for Norton For Your Eyes Only	Medium	Bug discussed in newsgroups and Web sites. Password discussed on IRC channel.

[14] eEye Digital Security Team, Advisory Code IISE01.
[15] BUGTRAQ, January 25, 1999.
[16] Microsoft Security Bulletin (MS99-004).
[17] BUGTRAQ, February 2, 1999.
[18] InfoWar Security Advisory #01
[19] BUGTRAQ, February 4, 1999.
[20] IRC channel discussion, February 4, 1999.
[21] NTSECURITY, February 6, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Rational Software[22]	Clear Case v3.2	Unauthorized local user can gain root access. This condition allows a user to suid any file.	No workarounds or patches known at time of publishing.	Clear Case root exploitable race condition	High	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.
SeattleLabs [23]	SLMail 3.1	Sending the "vrfy" or "expn" commands composed of 2,041 characters will cause the program to terminate.	No workarounds or patches known at time of publishing.	SLMail Vulnerabilities	Low	Bug discussed in newsgroups. Exploit script not required for the exploit.
SeattleLabs [24]	SLMail 3.1	A DoS and a buffer overflow condition exist. If the "helo" command is sent to port 27 followed by 819 to 849 characters, a potential DoS condition occurs. If 855 to 2,041 characters are sent, a buffer overflow occurs.	No workarounds or patches known at time of publishing. SeattleLabs representatives report that they are working on a fix and it will be included in Slmail 3.2 maintenance release.	SLMail Vulnerabilities	Low/ Medium	Bug discussed in newsgroups. Exploit script not required for the exploit.
Sun Solaris[25] 2.4 to 2.6	Common Desktop Environment (CDE)	Unauthorized user can gain root access through several vulnerabilities.	Patches available at: http://sunsolve.com/sunsolve/pubpatches/patches.html	Sun Solaris CDE	**High**	Bug discussed in newsgroups and Web sites.
Sun Solaris[26] 7, 7_x86, 2.6, 2.5.1, many others	Operating system (sdtcm_convert)	Unauthorized user can gain root access through a buffer overflow.	Patches available at: http://sunsolve.sun.com/sunsolve/pubpatches/patches.html.	sdtcm_convert buffer overflow	**High**	Bug discussed in newsgroups and Web sites.
Sun Solaris[27] 7, 7_x86, 2.6, 2.5.1, many others	Operating system (man/catman)	When run as root, the man or catman commands may overwrite arbitrary files.	Patches available at: http://sunsolve.sun.com/sunsolve/pubpatches/patches.html	Sun Solaris man/catman overwrite	Low/ Medium (Note: The full extent of this bug has not been reviewed.)	Bug discussed in newsgroups and Web sites.
Unix	Pine 4.04	If not truncated, a message with a From line containing 10,000 characters causes Pine to fail. It may be possible to place data in memory.	No workarounds or patches known at time of publishing.	Pine 10,000 character From line	Low/ Medium	Bug discussed in newsgroups and Web sites.
Unix[28]	HARDWARE Modem	If a user has access to the modem tty when dialing into the system, he/she can get passwords or cause a DoS condition.	Workarounds are (1) provide login access through modems connected to terminal servers, (2) use the mgetty-1.1.20 programs provided "ptylogin" as the login program, or (3) use the rlogin program.	Unix Modem problem	Low	Script identified at time of publishing but does not appear to be posted. Explanation of exploit available in newsgroups.

[22] L0pht Advisory – Rational Software ClearCase root exploitable race conditions.
[23] eEye Digital Security Team, Advisory Code AD02041999.
[24] idid.
[25] Sun Microsystems, Inc. Security Bulletin #00185.
[26] Sun Microsystems, Inc. Security Bulletin #00183.
[27] Sun Microsystems, Inc. Security Bulletin #00184.
[28] BUGTRAQ, January 27, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix[29]	Pine up to 4.1	The mailcap file distributed with the metamail MIME-support package, while implementing RFC-1524 correctly, introduces the possibility that an unauthorized user can manipulate the system to execute arbitrary commands.	Remove the metamail package from Pine. The metamail package is not required by Pine. If this is not possible, set the "mail-search-path" to a personal mailcap file path. Note - A number of patches have been provided by individuals, but many of these patches only serve to move the vulnerability down one nesting level.[30]	Remote exploit on Pine 4.1	Medium/ High	Bug discussed in newsgroups.
Unix[31]	Wget 1.5.3	When invoked with the -N option, it attempts to change the permissions of symlinks but changes permissions at the target files.	Workaround has been posted in several newsgroups.	Wget-1.5.3 chmod + symlinks	Low	Bug discussed in newsgroups.
Unix[32]	WS_FTP Server 1.0.1.E and 1.0.2.E	A DoS condition occurs if a "cwd" command is composed of over 875 characters.	No workarounds or patches known at time of publishing.	WS_FTP Server Remote DoS attack	Low/ Medium	Bug discussed in newsgroups and Web sites. Exploit script not required for the exploit.
Unix - HP-UX[33]	rpc.pcnfsd	Unauthorized remote user can gain root access. This vulnerability allows the printer spool directory to be made world writeable.	Patch available for this problem. User should consult the patch matrix from Hewlett-Packard.	HP-UX rpc.pcnfsd	**High**	Bug discussed in newsgroups and Web sites.
Unix – Digital Unix[34] 4.0 Updated since issuance of CyberNotes #3-99	Operating System (inc)	Buffer overflow condition exists in the /usr/bin/mh/inc file. This condition can allow an unauthorized user to gain root access.	No workarounds or patches known at time of publishing.	Digital Unix inc buffer overflow	**High**	**Exploit Script now available.** Explanation of exploit available in newsgroups.
Unix – Digital Unix[35] 4.0 prior to 4.0D Updated since issuance of CyberNotes #3-99	Operating System (at)	Buffer overflow condition exists in the "at" program that can allow an unauthorized user to gain root access.	Upgrade to Digital Unix 4.0D or obtain appropriate patch at: ftp://ftp.service.digital.com/public/dunix	Digital Unix at buffer overflow	**High**	**Exploit Script now available.** Explanation of exploit available in newsgroups.

[29] BUGTRAQ, February 8, 1999.
[30] BUGTRAQ, February 10, 1999.
[31] BUGTRAQ, February 2, 1999.
[32] eEye Digital Security Team, Advisory Code AD02021999.
[33] HP Daily Security Bulletins Digest, HPSBUX9902-091.
[34] BUGTRAQ, January 25, 1999.
[35] BUGTRAQ, January 25, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix - NetBSD[36] 19980603 to 19990208	netstat	Non-privileged user can read any kernel memory location.	Update to a source newer than 19990208. Disable netstat for non-root users: chmod 555 /usr/bin/netstat Patch available at: ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/patches/19990208-netstat	NetBSD netstat kernel viewing	Medium	Bug discussed in newsgroups and Web sites.
Unix -IBM AIX[37]	Navio NC browser install	One of the configuration scripts for the Navio NC browser sets permission of the /tmp directory to NFS exported and world read/writeable.	Users should check to see if /tmp has been exported and change NFS and permissions where appropriate.	Navio NC /tmp permission change	Medium	Bug discussed in newsgroups and Web sites. Exploit script not required for the exploit. Other related hacker tools can be utilized to gain privileged access.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - Any vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

[36] NetBSD Security Advisory 1999-002.
[37] BUGTRAQ, January 29, 1999.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between January 27 and February 12, 1999, listed by date of script, script name, script description, and comments. **Items listed in boldface/red (if any) are attack scripts for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or represent scripts that hackers/crackers are utilizing**. During this period, 31 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
Feb 11, 1999	All-access.c	Unix source code that will retrieve and decrypt Microsoft Access 97 database passwords.	
Feb 11, 1999	**All-access.exe**	**Win32 executable that will retrieve and decrypt Microsoft Access 97 database passwords.**	
Feb 11, 1999	Ftpchk.pl	Denial-of-Server (DoS) code used against ProFTPD servers	
Feb 11, 1999	**Net-RawIP v0.05c**	**Perl module that manipulates raw Internet Protocol (IP) packets and Ethernet headers. The version is ported to Perl 5.005 and BSD, and includes the oshare script (causes Microsoft Windows 98 machines to lock).**	
Feb 11, 1999	Novell Admin Exploit	Exploit code and description of vulnerability that allows a user to gain supervisor access to Novell NetWare 2.x, 3.x, and 4.x.	
Feb 10, 1999	Ms-access97-passwds.c	Program written in C that checks for Microsoft Access 97 database password weaknesses.	
Feb 10, 1999	Pepsi5.c	Random source host User Datagram Protocol (UDP) flooder.	
Feb 10, 1999	**Pwrspoof.tgz**	**Domain Name Server (DNS) spoofer.**	
Feb 8, 1999	**Net-RawIP v0.05b**	**Perl module that manipulates raw IP packets and Ethernet headers.**	
Feb 8, 1999	**Nmap v 2.06**	**Network-scanning tool that has a variety of scanning modes, including stealth, Xmas, and Null stealth. This release adds more operating system fingerprinting and several bug fixes. Note: This tool continues to be used by hackers. A number of systems become unstable when scanned if patches are not applied.**	
Feb 8, 1999	**RCR Bot v1.1**	**A plug-in for Back Orifice that is an IRC client. Once logged into a server, the infected machine can be remotely administered through IRC /msg or /query commands.**	
Feb 6, 1999	Router-tcpaccess-DoS	Code for conducting DoS attacks against a wide variety of routers.	
Feb 6, 1999	Slmail	Text that describes the procedure for exploiting the SLMail vulnerability. See SLMail Vulnerabilities in "Bugs, Holes & Patches" above.	
Feb 6, 1999	Spoof.0.1.tar.gz	IP/UDP/Transmission Control Protocol (TCP) spoofing.	
Feb 6, 1999	Thermoprog	Brute force password cracker.	
Feb 6, 1999	Windows-FAT-recursion	Explanation of how to perform a DoS attack against Microsoft Windows using FAT and allowing FTP uploads.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
Feb 4, 1999	Cprobe.sh	Scanning program that checks for 23 known Common Gateway Interface (CGI) script vulnerabilities.	
Feb 4, 1999	How to Break out	Detailed description of how to break out (user exceeds allowed access level) of restricted shells and menus.	
Feb 4, 1999	**Net-RawIP v0.04e**	**Perl module that manipulates raw IP packets and Ethernet headers.**	
Feb 4, 1999	NT4ALL	Code that allows any user (even Guest user) with write access to \WINNT\SYSTEM32 to log in with any password.	
Feb 4, 1999	pcapture	Tool for capturing packets on a network (network sniffer).	
Feb 4, 1999	**Smashdu.c**	**Code that exploits several buffer overflow conditions in Digital Unix. See Unix – Digital Unix in "Bugs, Holes & Patches" above.**	
Feb 3, 1999	lanlord v0.2-1	Identifies who owns machines at specific IP addresses. It runs on the Dynamic Host Configuration Protocol (DHCP) Server as a CGI script and uses CSS to modify output.	
Feb 3, 1999	**Net-RawIP v0.05a**	**Perl module that manipulates raw IP packets and Ethernet headers. The version is ported to Perl 5.005 and BSD.**	
Feb 1, 1999	**Chronicle Remote Registry Query Tool v1.0b**	**Determines the current service pack/hotfix level of all Microsoft Windows NT machines within a domain.**	
Feb 1, 1999	**Nessus 990201**	**Security audit tool that has 180 plug-ins for checking known security holes.**	
Feb 1, 1999	Slurpie v2.0b	Password cracker designed to run in a distributed environment.	
Feb 1, 1999	**Spoofscan.c**	**Program that conducts portscans from a spoofed IP. It spoofs the address of a machine located on the same Ethernet segments and then sniffs the responses.**	
Jan 30, 1999	Nmapstub.pl	Code that reads the nmap output and puts it into port and host structures. It then calls any routine that is requested, on a host by host basis.	
Jan 30, 1999	**Pmap_tools**	**Collection of tools that checks for portmap/rpc/rpcbind vulnerabilities.**	
Jan 28, 1999	**GnuSniff**	**Network packet sniffer.**	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line CyberNotes Script Analysis. While this section is intended only for short descriptions, contributions should include a full technical analysis of the script along with release instructions. The release options are: releasable to everyone, limited (originator-defined list of organizations), or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail requesting the full technical analysis of "X" where "X" is the script name. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the individual or organization unless otherwise requested.

Nmap - The output of a Nmap scan provides crucial information to the hacker. First, it provides a list of services that are active on the remote host. Second, by sending invalid tcp packets, Nmap performs a TCP stack analysis of the remote system. Since these anomalous packets are not covered by the RFCs, each operating system handles them differently. Nmap compares the responses to these packets against an internal database and provides a 'best guess' as to the operating system and version number running there. This combination allows the hacker to target the specific vulnerabilities on a given host, providing a higher success rate and a much lower attack signature. Finally, Nmap tells the user how difficult tcp sequence number prediction is for the remote host. This information can be used to target hosts that have a high potential for session hijacking. Such measures might be employed when a remote system has no vulnerable services running, or when it is shielded behind a firewall.[38]

Nmap was a winner of Infoworld's first annual Golden Guardian award and is described as:

> "the port scanner extraordinaire that we rely on regularly to get a quick birds-eye view of a network. Besides identifying open ports in every shape and form, nmap can identify OSes via TCP fingerprinting. The capability to send non-Request for Comment-compliant packets to an IP stack does have its downsides, however. It can hang some kernels, so use it carefully. Despite this rare condition, the capability will forever change how risk assessments are performed. With the exception of commercial vulnerability-detection tools, nothing else comes close to nmap for rapid network-security assessments."[39]

Trends

1. Several hackers/hacker groups appear to be using coordinated scans and probes from different sites.
2. Large numbers of scans and attacks continue to be directed at machines running the Linux operating system.
3. Scanning for Internet Message Access Protocol (IMAP) and POP continues.
4. Significant increase in reports of NetBus and Back Orifice scanning.
5. Significant increase in the number of scans directed specifically against Domain Name Servers.
6. Viruses are now being written to capture and transmit information.

Note: In the last edition of CyberNotes, in the "Trends" section #5, the acronym IMAP should have been defined as Internet Message Access Protocol.

Viruses

In the last few weeks, there has been an increase in reports of many people receiving e-mail messages containing Trojan horse programs. Along with the increase in Trojan horse programs, several viruses have either been reported in the press or exhibit new techniques/trends that the reader should made be aware of. Anti-virus vendors recommend that their users update the anti-virus definition packages on a regular basis (every two weeks).

IE0199.exe Trojan horse - This message, which appears to be sent from IEsupport@microsoft.com, informs the recipient that the attached program fixes a number of bugs in Internet Explorer. The program, if run, deletes sndvol32.exe from the System32 directory and installs a file called sndvol.exe in the System directory. A Registry key %SystemRoot%\System\sndvol.exe is added to the infected machine. Once installed, the Trojan horse launches a DoS attack against a Web site in Bulgaria.

---

[38] Excerpt from a report by the US Navy's SHADOW team, Naval Surface Warfare Center – Dahlgren Division.

[39] Infoworld, The more the merrier: 1998's Golden Guardian award given to three top security solutions, February 15, 1999.

To remove the program manually, you must remove the sndvol.exe file from the System directory, remove the Registry key, and reinstall a clean copy of sndvol32.exe into the System32 directory. Most major anti-virus vendors have included code in their latest data file updates to detect this Trojan horse program.

Happy99.exe Trojan horse - This program has been distributed via e-mail, newsgroups and Web software distribution sites. Happy99.exe is the most common name of this Trojan horse, but reports have identified the use of other files names. When run, the program displays fireworks graphics and installs two files (ska.exe and ska.dll) in the System directory. The program then attempts to spam e-mail recipients and newsgroups to which the infected machine has sent or received messages. Sites with an e-mail filtering capability can filter messages with the header "X-Spanska: Yes." Most major anti-virus vendors have included code in their latest data file updates to detect this Trojan horse program.

WM97.Caligula (aka. WM97.Cali) - This virus has received a great deal of press in the last two weeks for its attempt to steal PGP keys and then send the keys via FTP back to a site on the Internet. On the 31st of each month, this virus displays the following:

> "WM97/Caligulq ©Opic [CodeBreakers 1998]
> "No cia,"
> "No nsa,"
> "No satellite,"
> "Could map our veins."

This virus also disables the macro warning prompt to save the normal.dot Word template, disables ToolsMacro - VB Editor, and disables the menu items: ToolsMacro, ToolsCustomize, ViewToolbars. This virus has been posted on a number of virus writers' Web sites. Most major anti-virus vendors have included code in their latest data file updates to detect this virus program.

W97M.Footprint[40] - This virus overwrites the footers of all open documents and attempts to overwrite the macros in open documents. One of the indicators of infection is the placement of two files (footprint.$$$ and footprint.$$1) on the C drive. This virus has infected several US Government sites. Most major anti-virus vendors have included code in their latest data file updates to detect this virus program.

O97M/Triplicate - This is a new virus that, at the time of publication, **could not be detected by many anti-virus packages**. This virus is unique in that it is the first virus known to infect Microsoft Word, Excel, and PowerPoint files. Triplicate disables PowerPoint's macro protection, but this ability appears only to work from an infected Word file. Several anti-virus vendors' technical support centers were contacted and reported that detection for this new virus should be available in the near future.

[40] CIAC advisory J-025.