

HNS Newsletter
Issue 73 - 30.07.2001
<http://net-security.org>
<http://security-db.com>

This is a newsletter delivered to you by Help Net Security. It covers weekly roundups of security events that were in the news the past week. Visit Help Net Security for the latest security news - <http://www.net-security.org>.

Subscribe to this weekly digest on:
<http://www.net-security.org/text/newsletter>

Archive of the newsletter in TXT and PDF format is available here:
<http://www.net-security.org/news/archive/newsletter>

Current subscriber count to this digest: 2654

Table of contents:

- 1) General security news
- 2) Security issues
- 3) Security world
- 4) Featured articles
- 5) Security software
- 6) Defaced archives

=====
LANguard Security Event Log Monitor

=====
LANguard SELM is a network wide event log monitor that retrieves logs from all NT/2000 servers and workstations and immediately alerts the administrator of possible intrusions. Through network wide reporting, you can identify machines being targeted as well as local users trying to hack internal company information. LANguard analyses the system event logs, therefore is not impaired by switches, IP traffic encryption or high-speed data transfer.

Download your evaluation copy from:
<http://www.net-security.org/cgi-bin/ads/ads.pl?banner=gfitxt>

=====

General security news

TELSTRA ACCUSED OF PLAYING DOWN HACKER THEFT
Telstra has been accused of keeping its customers in the dark after computer hackers obtained confidential customer details from one of its email networks and posted them on the Internet. The user names and passwords for the private email accounts of customers of Telstra's BigPond ADSL troubleplagued network were collected by a virus activated by a computer hacker late last week. A list of 69 names and passwords were then sent to other Australian based websites, but some Telstra customers say they suspect countless more customers could be affected.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://it.mycareer.com.au/breaking/2001/07/23/FFX7K2U4HPC.html>

TRIPWIRE IN THE ENTERPRISE

Elena Khan writes: "I work for Adero, Inc., a start-up that specializes in global caching of Web content. We first opened shop in Massachusetts two years ago, moved a couple of times to bigger facilities, and finally found a home in the Boston suburb of Waltham. As our company grew, however, so did our need for intrusion detection. Our security team recommended Tripwire, and the operations team (my group) was tasked with implementing it on 200 machines (comprising four discrete functional groups) that were already deployed worldwide."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sysadminmag.com/articles/2001/0108/0108a/0108a.htm>

PERSONAL FIREWALLS UNDER FIRE

So let's assume your corporate network is secured by a good firewall, such as FW-1, Raptor, Gauntlet, PIX or any of the many other enterprise-class firewalls out there. So far, so good. But what about the security of your remote users? How many employees have laptops in addition to their office PCs? How many full-time telecommuters does your company have? How many of these users store sensitive data on their home office PCs, laptops or handhelds? How many of these devices hook directly into your corporate network?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infosecuritymag.com/articles/july01/cover.shtml>

DEF CON 9 - OPEN LETTER TO THE COMMUNITY

The Dark Tangent writes: "Having just finished my 9th DEF CON, I have a few thoughts - I am looking for feedback from the community to help decide the next steps for the future of DEF CON."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.defcon.org/TEXT/9/open-letter-dc9.txt>

SECURING THE WIRELESS INTERNET USING "KILOBYTE" SSL

"Kilobyte" SSL (KSSL) is a small-footprint, client-side-only implementation of SSL v3.0 for handheld and wireless devices. The process of developing connectivity applications for these devices requires consideration of the unique characteristics of a wireless environment, such as weaker CPUs, network latency, low bandwidth, and intermittent connectivity. This article provides an overview of these design considerations while using the KSSL APIs.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://dcb.sun.com/practices/howtos/kssl.jsp>

SIL - MY DATE WITH FEDERAL PRISON

Well I sit ready to surrender myself in next week for a two year federal bid without regrets. I decided to fight Big Brother and lost, but at least I fought and that's what matters in my heart. Anyways so why the hell am I writing this? Because if I don't let someone know than it will all be in vain, and I have an intuition some would probably know what to make of it.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.disgraced.org/sayinggoodbye.html>

HACKERS/KIDS/EXPERTS

Vectra Corporation technical architect Damon Wynne - "Most computer hackers are just bored kids with too much time on their hands, according to an industry expert who likens them to street vandals, and only ten percent of hackers really know what they're doing".

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infowar.com/hacker/01/hack_071801c_j.shtml

UPDATE ON ETISALAT 'HACKING' CASE

Lawyers acting for a young Briton who was fined for hacking into the UAE's Internet system have appealed against his conviction, but the Public Prosecutor is demanding a tougher sentence.

Link: <http://www.gulf-news.com/Articles/news.asp?ArticleID=22747>

NOT ILLEGAL IN RUSSIA

In an interview with a local Las Vegas television station, Sklyarov denied doing anything wrong and accused Adobe of bullying him. "I wrote the program to demonstrate security flaws, not to violate copyright law," he said. "It's not illegal in Russia."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.themoscowtimes.com/stories/2001/07/23/045.html>

INTERVIEW WITH LSD

Croatian security web site Active Security did an interview with Last Stage of Delirium, group of skilled people that are actively present in the security scene and well known for winning the Argus challenge.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.active-security.org/LSD_eng.html

ADOBE U-TURN ON EBOOK HACKER

Adobe has dropped the charges against Russian programmer Dmitry Sklyarov, who was arrested for copyright infringement of its eBook product. The about turn comes after protestors rallied in more than 20 US cities Monday, urging the sale of Adobe stock and a boycott of Adobe products.

Link: http://www.macworld.co.uk/news/main_news.cfm?NewsID=3238

WHITE HOUSE WEB SITE MOVES TO LINUX

The White House Web site has been moved onto a Linux platform after its administrators managed to successfully side step an attack by the Code Red worm. Netcraft reports that Whitehouse.gov is now being hosted by peering firm AboveNet and that the site uses a Netscape-Enterprise/3.6 Web server on a Linux platform. Prior to its forced move, Netcraft suggests the site was run on a Sun server, but the data on this is far from conclusive.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/20587.html>

SSH CHROOTGROUPS

Chroot alters the effective root directory of a user or process to one specified by the root user. Thus far, chroot has not been widely used for creating secure user environments; the difficulties involved with creating a functional cage are an obstacle that still needs to be overcome. This article will provide an overview

of SSH ChRootGroups feature; which provides a quick and easy way for administrators to lock users inside a chrooted cage.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/linux/articles/chroot.html>

LINUX KERNEL-LEVEL TROJAN

This document on Linux Today describes the Kernel Intrusion System (KIS) trojan that affects Linux 2.2 and 2.4 systems. The specific version of the KIS trojan analyzed is labeled 0.9.

Link: http://linuxtoday.com/news_story.php?ltsn=2001-07-23-005-20-SC-KN

HOW TO PROTECT YOUR PC FROM THE SIRCAM WORM

This worm can infect and re-infect networked computers without you even knowing - and then email your private documents to others. Find out here how to make your system secure against the latest email worm.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2091860,00.html>

THE ONLY FITTING PUNISHMENT FOR VIRUS WRITERS? DEATH!

David Coursey writes: "My proposal is simple: When you find a virus author, kill him (or her). I don't really care how this is accomplished, but will offer some suggestions before explaining why I think the punishment makes sense."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/anchordesk/stories/story/0,10738,2795678,00.html>

JUSTICE CREATING CYBERCRIME UNITS

Federal Computer Week reports that the Justice Department is creating 10 specialized prosecutorial units that will be dedicated to fighting cybercrime.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.fcw.com/fcw/articles/2001/0723/web-doj-07-23-01.asp>

DECSS CASE COULD CHANGE YOUR IT SHOP

A legal battle over DVD encryption, currently in appeals court, could shape the future of IT. The parties involved say the ability to innovate and do business in a digital world is at stake.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.informationweek.com/thisweek/story/IWK20010711S0010>

SWISSONLINE'S GOT COMPROMIZED

Swiss hackers were able to infiltrate the mail server of SwissOnline, Switzerland's third largest Internet service provider (ISP), and gain access to 250,000 e-mail addresses and passwords, including some for the embassies of France, Sweden and Israel.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/168272.html>

PEER TO PEER - SECURITY RISKS

In a word: lots. File sharing of any type usually involves risks. FTP sites are routinely probed for directories that can be used to store and download files, or for files that are improperly protected and available publicly (such as billing

data being moved via ftp from mainframe systems to others). Attackers regularly scan for NFS and SMB to find systems with improper permissions that can be exploited...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityportal.com/closet/closet20010725.html>

WHY THE SIRCAM WORM IS ONLY THE BEGINNING FOR NEW VIRUSES

Jose Nazario, who spoke at this year's Black Hat Security Briefing, is a biochemist who makes biological parallels with computer viruses. The problem with the current group of worms, according to Nazario, is that they are all too highly visible, unable to infect specific targets, and too easily blocked by antivirus vendors. Nazario predicted that future worms will be written with a specific goal in mind, such as infecting a specific large network or spreading a political or hacktivism message within a specific group of industry servers. And they will do so with greater stealth.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/anchordesk/stories/story/0,10738,2797739,00.html>

LINUX AT DEF CON 9

Quite a number of the attendees run Linux and there were several talks focused specifically on Linux security. During one, the Kernel Intrusion System (KIS) was released. Writing kernel modules seems to be an emerging trend for root kits and other Linux cracker tools. Once the attacker gains root access, they can modify the kernel or dynamically insert a module that completely hides all their processes and network connections from the unsuspecting admin.

Link: <http://www.linux.com/enhance/newsitem.phtml?sid=1&aid=12478>

FBI MUST REPORT ON E-MAIL WIRETAPS

The U.S. House of Representatives passed a measure on Monday that would require the FBI to report how it uses the controversial e-mail wiretap system formerly known as Carnivore.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.msnbc.com/news/604180.asp>

PATCH YOUR TELNETD

According to Newbytes report, all of the "high-profile" web sites that were defaced in the past few weeks - FreeBSD web site, TiVo Inc., the SANS Institute, Themes.org and a Microsoft site in Belgium, were penetrated through security hole in telnetd. Also you can catch the thread regarding the leaked exploit on antiSecurity board.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/168280.html>

MICROSOFT SERVICES FOR UNIX 2.0 MEMORY LEAKS

Among the components provided by Services for Unix (SFU) 2.0 are services that implement the NFS (Network File System) and Telnet protocols. Both services contain memory leaks that could be triggered by a user request. An attacker who repeatedly sent such a request could deplete the kernel memory on the server to the point where performance slowed and the system could potentially fail.

Link:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-039.asp>

STEVE GIBSON VS. THOMAS C. GREENE

The long-awaited ear-to-ear debate on the Win-XP raw-sockets implementation involving Steve Gibson and The Register's Thomas C. Greene on the radio show Online Tonight with David Lawrence is available as mirrored on HNS.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.net-security.org/mirror/the-register/>

HNS SECURITY DATABASE UPDATE

HNS Security Database was updated with about 15 new companies and 60 new products. Some of the companies added - Exodus Communications, Breakwater, Barbedwires Technologies, Uniskill, En Garde Systems, MDD, etc.

Link: <http://www.security-db.com/>

CONGRESS NO HAVEN FOR HACKERS

Even as the world's geeks march against the Digital Millennium Copyright Act, key legislators and lobbyists are dismissing concerns about the controversial law as hyperbole. The law that led to the arrest of Russian programmer Dmitry Sklyarov last week and an immediate outcry among programmers continues to enjoy remarkably broad support on Capitol Hill. No bill has yet been introduced in Congress to amend the DMCA for one simple reason: Official Washington loves the law precisely as much as hackers and programmers despise it.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/business/0,1367,45522,00.html>

HAL 2001 - COPS, CRIMES AND BEER

If you are going to this year's Hackers At Large convention, be sure to behave. HAL staff did a brief article on things you shouldn't do if you don't want to exchange your tent for a jail. We are also visiting HAL2001 so do mail us if you want to buy us a beer or if you need a beer :)

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.hal2001.org/hal/04Network/04crimes/index.html>

LUCENT HIT BY HACKING DOUBLE WHAMMY

Lucent suffered a double hack attack yesterday when its XL.com website was defaced twice in a matter of hours. A defacer calling himself Feltonspray got to the networking giant's XL.com site first, leaving the simple message: "Ops another site OWN3D by Feltonspray."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1124242>
Link: <http://www.safemode.org/mirror/2001/07/24/xl.com/>

OPENSSE KEY MANAGEMENT, PART 1

In this series, you'll learn how RSA and DSA authentication work, and see how to set up passwordless authentication the right way. In the first article of the series, Daniel Robbins focuses on introducing the RSA and DSA authentication protocols and showing you how to get them working over the network.

Link: <http://www-106.ibm.com/developerworks/library/l-keyc?open&l=805,t=grl,p=openSSH>

HUGE IDENTITY THEFT UNCOVERED

Key personal data belonging to hundreds of individuals have been shared in an Internet chat room, in what one expert says could become one of the largest identity theft cases ever. The data include Social Security numbers, driver's license numbers, date of birth and credit card information - everything a criminal would need to open an online bank account, apply for a credit card, even create the paperwork necessary to smuggle illegal immigrants.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.msnbc.com/news/604496.asp>

INCIDENT RESPONSE - INVESTIGATING COMPUTER CRIME

Joe "Zonker" Brockmeier writes: "Incident Response is the first book I've seen that deals solely with how to gather forensic evidence and recover after an attack. I'm always up for a book that covers a new topic, or at least a new angle, so I tore into this one with great interest. Overall, the book was an interesting read. There are a few quibbles here and there, but the book contains some decent information."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://unixreview.com/articles/2001/0107/0107m/0107m.htm>

JAM ECHELON DAY

A large group of individuals in the Global Internet Community have set out to bring attention to the communications monitoring system known as ECHELON. We are hosting a mirror for Jam Echelon Day, where you can find all the information on this surveillance system and the ways how to be a part of this notable effort.

Link: <http://www.net-security.org/text/press/996145547,87978,.shtml>

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.net-security.org/mirror/jam-echelon/>

CAPITOL HILL LIKES DMCA

Wired - The law that led to the arrest of Russian programmer Dmitry Sklyarov last week and an immediate outcry among programmers continues to enjoy remarkably broad support on Capitol Hill. No bill has yet been introduced in Congress to amend the DMCA for one simple reason: Official Washington loves the law precisely as much as hackers and programmers despise it.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/print/0,1294,45522,00.html>

CBA HACK THREAT

Threats made last week by a hacker to access Commonwealth Bank Australia accounts have raised fresh concerns about the risks of e-commerce.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.thestandard.com.au/articles/display/0,1449,14824,00.html>

WINDOWS 2000 TERMINAL SERVICE DoS

The Windows 2000 Terminal Service and Windows NT 4.0 Terminal Server Edition contains a memory leak in one of the functions that processes incoming Remote Data Protocol data via port 3389. Each time an RDP packet containing a specific type of malformation is processed, the memory leak depletes overall server memory by a small amount.

Link: <http://www.net-security.org/text/bugs/996153501,98683,.shtml>

RSA POSES \$200,000 CRYPTO CHALLENGE

RSA Security is running a factoring challenge that offers would-be code breakers a prize of up to \$200,000 for finding the two numbers of the kind used to create ultra-secure 2048-bit encryption key.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/20638.html>

REP: GIVE FAIR USE A FAIR SHAKE

Rep. Rick Boucher - "It's a broad overreach to have a person arrested under the federal criminal laws simply because they made software that circumvents a technological measure". Boucher said his office will draft a bill to be introduced later this year. Also from his homepage - "Representative Boucher's Speech on Fair Use".

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,45548,00.html>

FBI CYBER-BRANIACS INFECT THEMSELVES WITH SIRCAM

We've long been at a loss to identify a single job that the FBI's elite Net-security squad at the NIPC performs adequately. In May the Congressional General Accounting Office released a scathing report cataloging NIPC's chronic dysfunction, so it was with delicious irony that on Wednesday, after managing to infect its own networks with the SirCam e-mail worm, NIPC told Congress that it would disgrace itself a good deal less often if it had a bigger budget.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/20678.html>

COMPUTER SECURITY DEGREE

A Pennsylvania university will offer a bachelor's degree in computer security. "There's a real need in the computer industry for these kinds of workers, because the newspapers are always full of stories about hackers and threats to the infrastructure," said Richard Amori, chairman of the university's computer science department.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/01/07/27/news18.html>

ETHICAL HACKING 101

Ankit Fadia has launched into the public eye by writing a book about his recent his computer-hacking adventures. After breaking into the websites of several Indian computer magazines, the 16-year-old boy spent about two weeks this summer churning out the 600-page tome titled "The Unofficial Guide to Ethical Hacking."

Link: http://www.upside.com/texis/mvm/executive_briefing?id=3b607b211

USING AN OPENBSD FIREWALL TO SHARE A CABLE MODEM

Setting up an OpenBSD firewall is a straightforward process. This paper assumes that you have already installed OpenBSD 2.9 and that you are comfortable in a UNIX environment.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://gridley.acns.carleton.edu/~lowem/pages/openbsd.html>

HEY SIRCAM, WHERE'D YOU GO?

Security experts said that SirCam's stunningly sudden slowdown is most likely due to increased awareness of the virus after heavy mainstream media coverage earlier this week, along with people and companies upgrading their antiviral software to protect against SirCam.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/business/0,1367,45570,00.html>

INDIA HACKERS SCARED STRAIGHT?

Indian hackers always thought they were too sophisticated to fall into the hands of the rough cops in this country, who various human rights groups routinely accuse of brutality. But that feeling evaporated after one of the four people arrested recently in connection with a hacking incident accused Mumbai police of breaking his hand during interrogation.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/culture/0,1284,45569,00.html>

HACKERS ARE TOO RISKY TO HIRE, SAYS TRUSECURE CEO

Security companies that want to be taken seriously don't hire hackers, whether their exploits have been for good or bad purposes, according to Adam Joseph, CEO and president of Trusecure. Joseph said hackers undoubtedly have great skills in penetrating companies' computer systems but he and other security professionals are working on a different level - the business of risk prevention.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1124273>

CISCO TO BUY VPN SECURITY COMPANY

In a move to tune up its part in the arena for virtual private network services, Cisco Systems said it has agreed to acquire Allegro Systems for approximately \$181 million.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdn/stories/news/0,4586,5094831,00.html>

FOUR NEW WAYS TO STUFF SOMEONE'S WIN MACHINE

We've seen another spike in Microsoft security bulletins during the past few days. Funny how these things seem to run in cycles...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/20715.html>

IT'S BED TIME FOR CODE RED WORM - BUT IS IT SLEEPY?

As midnight races around the world tonight, Code Red is supposed to be putting itself to sleep on the thousands of Windows-based Web servers it probably still infects. But security experts won't be sleeping easily, because they're not convinced that the worm's own stasis self-timer - designed to kick in on the 28th day of the month - means the threat is over.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/168450.html>

HACKING VEGAS AT BLACK HAT AND DEF CON

Since 1992 Las Vegas has been descended upon each July by an underground

society that is--even by Las Vegas standards--conspicuously dressed, unpredictable and in some cases downright scary. They speak English only part of the time, tend to mistrust outsiders, and many of their habits and leisure activities are of questionable legality. Not surprisingly, their public events are always well-attended by representatives of the law enforcement community.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www2.linuxjournal.com/articles/tradeshaw/0038.html>

HACKER ARREST MAY SPUR REVIEW OF DIGITAL RULES

He's an unlikely poster child for a movement to change a major U.S. law. But the plight of Russian programmer Dmitry Sklyarov, who was arrested last week, is again shining the spotlight on a controversial law designed to expand copyright protections into the digital age.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1005-200-6699001.html>

MICROSOFT BULLETINS FAIL PGP VERIFICATION

In order to protect against forgery, Microsoft's security response center digitally signs its bulletins with PGP before e-mailing them to the more than 100,000 subscribers to its security notification service. But if recipients attempt to verify the messages' authenticity, PGP will issue a warning that the signer of the bulletin is invalid. "The problem is that Microsoft's bulletins effectively look as if they're forged. And telling a Microsoft forgery from someone else's is virtually impossible," Paul Murphy, head of information technology at Gemini Genomics.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cosmiverse.com/tech07270102.html>

PC SPIES EYE CHILDREN, LOVERS, EMPLOYEES

What would you do if you discovered your spouse, parent or employer spied on your computer activity, secretly watching the Web sites you visit, the e-mails you read and even the passwords you use?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/internet/07/27/computer.surveillance/index.html>

Security issues

All vulnerabilities are located at:
<http://net-security.org/text/bugs>

TIVOLI SECUREWAY POLICY DIRECTOR VULNERABILITY

Web Seal Policy director does not handle URLs in hex code correct. It is possible to perform web traversals by appending %2e, to access the underlying web server.

Link: <http://www.net-security.org/text/bugs/995916612,85021,.shtml>

PERMISSION PROBLEMS WITH ARKEIA

While working with the commercial version of Arkeia backup software I noticed it creates most of it's "database" files with the permissions of 666. This was version 4.2.8-2 of the server, and I had noticed this several updates ago, so it's been going on for some time. The database files are located in /usr/knox/arkeia/dbase. I have tried resetting the permissions on the files, but they get reset again when backup runs again.

Link: <http://www.net-security.org/text/bugs/995981023,72798,.shtml>

SECURITY HOLE IN PHPLIB 7.2 PREPEND.PHP3

The PHPLib Team announces phplib-7.2d, available now. This release fixes the recently discovered hole in prepend.php3 that can allow a remote attacker to inject non-local code into any phplib based script.

Link: <http://www.net-security.org/text/bugs/995981374,10024,.shtml>

NETBSD - INSUFFICIENT CHECKING SENDMSG(2)

Due to insufficient length checking in the kernel, sendmsg(2) can be used by a local user to cause a kernel trap, or an 'out of space in kmem_map' panic.

Link: <http://www.net-security.org/text/bugs/995992013,58936,.shtml>

NETBSD - SSHD(8) "COOKIES" FILE MISHANDLING

sshd(8) allows users to delete files named "cookies" from arbitrary directories if X11 forwarding is enabled. Therefore, rogue local users can abuse this to remove any file named "cookies" using root privileges.

Link: <http://www.net-security.org/text/bugs/995992212,20925,.shtml>

NETBSD - LOCAL USER MAY GAIN SUPERUSER PRIVILEGES

A race condition between the setuid/setgid handling in the execve(2) system call and the ptrace(2) system call can allow a local user to cause a setuid-root executable to execute arbitrary code as the superuser.

Link: <http://www.net-security.org/text/bugs/995992334,59006,.shtml>

SOLARIS DTMAIL BUFFER OVERFLOW VULNERABILITY

NSFOCUS Security Team has found a buffer overflow vulnerability in the dtmail of Solaris handling MAIL environment variable, exploitation of which could allow an attacker to run arbitrary code with the privilege of mail group.

Link: <http://www.net-security.org/text/bugs/996007321,46237,.shtml>

CISCO LOCAL DIRECTOR DENIAL OF SERVICE

If your Cisco local directors are configured to do all port mappings (0:0) and not port-bound virtuals (port-to-port mappings), you can easily DOS the local director by causing the "no answer reassign" to surpass its default threshold counter of 8.

Link: <http://www.net-security.org/text/bugs/996008636,47610,.shtml>

SUSE SECURITY ANNOUNCEMENT: XLI/XLOADIMAGE

xli, aka xloadimage, a image viewer for X11 is used by Netscape's plugger to display TIFF-, PNG- and Sun-Raster-images. The plugger configuration file is /etc/pluggerrc. Due to missing boundary checks in the xli code a buffer overflow could be triggered by an external attacker to execute commands on the victim's system. An exploit is publically available.

Link: <http://www.net-security.org/text/bugs/996010334,12852,.shtml>

CERT - BUFFER OVERFLOW IN TELNETD

The telnetd program is a server for the Telnet remote virtual terminal protocol. There is a remotely exploitable buffer overflow in Telnet daemons derived from BSD source code. This vulnerability can crash the server, or be leveraged to gain root access.

Link: <http://www.net-security.org/text/bugs/996058309,88769,.shtml>

OPENUNIX, UNIXWARE: SU BUFFER OVERFLOW

Long values of the TERM variable can cause the su command to have a memory fault. This might be exploited by an unauthorized user to gain privileges.

Link: <http://www.net-security.org/text/bugs/996058438,60486,.shtml>

MAMBO SITE SERVER V3.0.X VULNERABILITY

Any user can gain administrator privileges.

Link: <http://www.net-security.org/text/bugs/996084978,59609,.shtml>

SGI SECURITY - NETPRINT DSO EXPLOIT

A modification to netprint exploit reported on SGI Security Advisories 19961203-01-PX and 19961203-02-PX allows root access on IRIX 6.5 systems that have open lp accounts.

Link: <http://www.net-security.org/text/bugs/996153392,15380,.shtml>

MICROSOFT - WINDOWS 2000 TERMINAL SERVICE DoS

The Windows 2000 Terminal Service and Windows NT 4.0 Terminal Server Edition contains a memory leak in one of the functions that processes incoming Remote Data Protocol data via port 3389. Each time an RDP packet containing a specific type of malformation is processed, the memory leak depletes overall server memory by a small amount.

Link: <http://www.net-security.org/text/bugs/996153501,98683,.shtml>

SCO - TELNETD AYT OVERFLOW?

Based on the results from the Telnet AYT scanner, SCO OpenServer may be vulnerable.

Link: <http://www.net-security.org/text/bugs/996154421,18204,.shtml>

TCP SEQUENCES IN SONICWALL SOHO FIREWALL

This may not seem bad, but to me it seems that this defeats the point of NAT if somebody can steal your sessions. Note the section on TCP sequence prediction. This was a Sonicwall SOHO firewall.

Link: <http://www.net-security.org/text/bugs/996154938,58090,.shtml>

CONECTIVA LINUX SECURITY ANNOUNCEMENT - IMP

1. A remote attacker could trick the server into fetching scripts from another host and then execute them. This could be used to get access to the server running this webmail system.
2. An attacker might also execute malicious javascript code in the browser of an user who is reading an email sent by the attacker with special "javascript:" encodings.
3. An attacker could make the server read a file called "prefs.lang" and execute it as PHP code. The attacker would have to be able to create that file first, which implies at least some sort of write access, such as one provided by a shell account, or ftp upload.

Link: <http://www.net-security.org/text/bugs/996155032,47418,.shtml>

MANDRAKE LINUX SECURITY UPDATE ADVISORY: ELM

A buffer overflow exists in the elm email client when handling very long message-ids. This would overwrite other header fields and could potentially cause further damage.

Link: <http://www.net-security.org/text/bugs/996155095,34316,.shtml>

DRAKE LINUX SECURITY UPDATE ADVISORY: SQUID

The Squid proxy server has a serious security flaw in versions 2.3.STABLE2 through 2.3.STABLE4. This problem surfaces when Squid is used in httpd_accel mode. If you configure httpaccelwith_proxy off then any request to Squid is allowed. Malicious users may use your proxy to portscan remote systems, forge email, and other activities.

Link: <http://www.net-security.org/text/bugs/996155118,37442,.shtml>

SNAPSTREAM PVS VULNERABILITY

It is possible to navigate outside of the HTTP base directory, and download any file from the host for which the filename is known. The HTTP server runs in the context of the logged in user. SSD.ini, which contains a great deal of information regarding the target system can be retrieved remotely using the method detailed above.

Link: <http://www.net-security.org/text/bugs/996168206,4858,.shtml>

APACHE DIRECTORY LISTING VULNERABILITY

You can access files/directories under the http root by subtracting the number of slashes from the appended url equal to the number of characters in the file or directory name you are attempting to access.

Link: <http://www.net-security.org/text/bugs/996234653,92502,.shtml>

OPENSERVR /ETC/POPPER BUFFER OVERFLOW

The popper daemon /etc/popper was subject to a buffer overflow that could be used by a malicious user.

Link: <http://www.net-security.org/text/bugs/996234778,70595,.shtml>

MICROSOFT - MALFORMED RPC REQUEST SERVICE FAILURE

Several of the RPC servers associated with system services in Microsoft Exchange, SQL Server, Windows NT 4.0 and Windows 2000 do not adequately validate inputs, and in some cases will accept invalid inputs that prevent normal processing. The specific input values at issue here vary from RPC server to RPC server.

Link: <http://www.net-security.org/text/bugs/996235672,87928,.shtml>

WINDOWS MEDIA PLAYER BUFFER OVERFLOW

An unchecked buffer exists in the functionality used to process Windows Media Station files. This unchecked buffer could potentially allow an attacker to run code of his choice on the machine of another user. The attacker could either send a specially malformed file to another user and entice her to run or preview it, or he could host such a file on a web site and cause it to launch automatically whenever a user visited the site. The code could take any action on the machine that the legitimate user himself could take.

Link: <http://www.net-security.org/text/bugs/996235783,23218,.shtml>

SERIOUS PHPNUKE VULNERABILITY

After testing just a few scripts on phpnuke I have noticed the following:
Some fields in the registration form allow code and fail to filter out the tags.

e.g Interests: src=http://www.anything.com/defaced.gif>

Also when faking a form and posting from local file (user.php.html) after editing a few fields like the avatar picture for example, it is possible to escape surtain dirs with the ../../../../dir/pic.gif in the options field.

001.gif

002.gif

This tells user.php to save the avatar path as
http://www.target.com/../../dir_on_server/anyfile.ext and loads the file when the user info of the attacker is viewed.

The preview of the Registration Form allows Javascript in the body. (not the user.php) but it does not allow ' or " . BUT you can user / instead of ' so this helps to will in variables in javascript. This can damage the site and make it look ugly.

Link: <http://www.net-security.org/text/bugs/996267678,33303,.shtml>

ENTRUST - GETACCESS VULNERABILITY

due to missing input-validation it is possible to run(start) java-programs on the "getaccess"-machine. combined with public accessibly uploads or any other possibility to create class-files on the server this vulnerability could be used to run arbitrary system commands on the target machine (or change getAccess parameters and steal any user ac count you want BTW). It should also be possible(but not proven yet) to exploit default-,install- or demo classes within Java or getAccess whic h would make the file-upload (creation) part unneeded!

(uninstall.class is very likely an effective DOS).

Link: <http://www.net-security.org/text/bugs/996267746,12544,.shtml>

Security world

All press releases are located at:
<http://net-security.org/text/press>

NEW BILINGUAL TROJAN EMANATING FROM MEXICO - [23.07.2001]

Aladdin Knowledge Systems, a global leader in the field of Internet content and software security, announced its eSafe content security solution automatically protects corporate networks against the Win32.Sircam trojan, a new malicious threat that sends either English or Spanish language emails with malicious payload.

Press release:

< <http://www.net-security.org/text/press/995889756,97816,.shtml> >

SONICWALL REVENUES INCREASE 61% IN SECOND QUARTER - [23.07.2001]

SonicWALL, Inc., a leading provider of Internet security solutions, reported revenues of \$26.6 million for the second quarter ended June 30, 2001, representing an increase of 61% compared to revenues of \$16.5 million for the same period of 2000. Revenues increased by 8% sequentially over the \$24.6 million reported in the first quarter of 2001.

Press release:

< <http://www.net-security.org/text/press/995889809,32056,.shtml> >

SECURE COMPUTING AWARDED DARPA CONTRACT - [23.07.2001]

Secure Computing Corporation, a leading provider of enterprise access control software and services, announced that it has received a contract from the Defense Advanced Research Projects Agency (DARPA) to develop advanced VPN solutions that provide mobile and remote users authenticated, high bandwidth access to enterprise networks. Technologies developed under this effort will be leveraged in future capabilities for Sidewinder™, Secure's firewall and VPN gateway, as well as the 3Com Embedded Firewall. This contract award demonstrates Secure Computing's continued commitment to acquire research contracts that contribute to the advancement of both Department of Defense and commercial solutions.

Press release:

< <http://www.net-security.org/text/press/995915637,2332,.shtml> >

ANTI-PIRACY SELF-REPORTING SOFTWARE RELEASED - [23.07.2001]

The Software-Police announced the release of its powerful, ground-breaking online anti-piracy security software reporting system. This information technology service program is capable of capturing over 127,500,000 illegal uses of software per hour. The Israel-based firm is selling its intellectual property at a trade summit convened by the Honorable James S. Gilmore II, Governor of Virginia, at the end of July.

Press release:

< <http://www.net-security.org/text/press/995917288,58796,.shtml> >

INTRUSION.COM'S 'SECURED BY CHECK POINT' APPLIANCES - [23.07.2001]

Intrusion.com, Inc., a leading provider of enterprise security solutions for the information-driven economy, announced four new integrated security appliances at breakthrough price points. Each appliance provides high performance, high density security solutions that are expandable and easy to deploy.

Press release:

< <http://www.net-security.org/text/press/995917393,63020,.shtml> >

EUROPEANS ARE FAR FROM UNITED ON E-SECURITY - [23.07.2001]

Companies in Europe are divided over the potential threat to business from viruses, hack attacks and other forms of sabotage, according to research conducted by security specialist Evidian. Despite this, multinationals are still refusing to take local security issues into account when devising corporate policy. In France, Benelux, Spain and Germany, viruses are seen as the major threat, with 40% of companies identifying this form of attack as the most prevalent. In the UK, deliberate sabotage by employees or ex-employees was identified as the biggest area of concern, while in Scandinavia over 50% claimed it was accidental damage caused by an employee. In Italy, financial fraud was identified as the biggest headache.

Press release:

< <http://www.net-security.org/text/press/995917497,39507,.shtml> >

SOPHOS: INDUSTRIAL ESPIONAGE WORM STRIKES - [24.07.2001]

Sophos Anti-Virus, a world leader in corporate anti-virus protection, warned of a new worm which could prove highly damaging to unprotected businesses. The Sircam worm (also known as W32/Sircam-A), steals commercially sensitive or personal documents from the infected PC. It then forwards these files to all of the infected users' email contacts. Sophos has already received over two hundred reports of the worm from corporates and predicts it may be the one

of the year's hardest-hitting viruses.

Press release:

< <http://www.net-security.org/text/press/995980692,27163,.shtml> >

PENTASAFE PROVIDES IT SECURITY TO VALUEOPTIONS - [24.07.2001]

PentaSafe Security Technologies Inc. announced that ValueOptions, Inc., the largest privately owned behavioral health managed care company in the US, has purchased PentaSafe's VigilEnt Security Solution to manage the security of their information assets. PentaSafe's products will enable ValueOptions to simplify and centralize security auditing, vulnerability assessment, host-based intrusion detection, and security management on all of their systems throughout the US. "Security, confidentiality and privacy are key concerns to us at ValueOptions," said Bob Esposito, CTO of at ValueOptions. "We have always taken a proactive, not reactive, approach to keeping our customers' healthcare records and information secure. With our exponential growth however, we need a more cohesive solution to security management, especially now that we are faced with the challenge of complying with new government regulations such as HIPAA."

Press release:

< <http://www.net-security.org/text/press/995983032,59570,.shtml> >

INSTARAK SECURE SERVER APPLIANCE LAUNCHED - [24.07.2001]

eSoft Inc., announced the introduction of the InstaRak secure server appliance. The new product has been designed to meet the needs of service providers and their customers to provide a secure, end-to-end solution for web, DNS and mail services for multiple domains. eSoft is pioneering the delivery of secure server appliances by integrating server features with security protection making the InstaRak the most secure server on the market today.

Press release:

< <http://www.net-security.org/text/press/995983119,88038,.shtml> >

SECURITY MONITOR RELEASED BY HIDEAWAY.NET - [24.07.2001]

Hideaway.Net launches its Security Monitor. The Security Monitor application enables anyone from home PC users to IT professionals to keep track of the latest vulnerabilities, patches, virus alerts, and security news in a quick and easy manner. It can be fully customized to filter content and alarm the user if security holes or patches are released for specific platforms. While not in use, the Monitor runs unobtrusively in the user's system tray.

Press release:

< <http://www.net-security.org/text/press/995983389,43104,.shtml> >

F-SECURE WARNS OF SIRCAM WORM - [24.07.2001]

F-Secure Corporation is alerting computer users worldwide about a new, rapidly spreading e-mail worm called Sircam. Sircam is a mass mailing e-mail worm with the ability to spread through Windows Network shares. F-Secure anti-virus detects and disinfects the worm. The worm was found in the wild on July 17 in the USA. After that the worm has been spreading globally. In addition of USA, infections have been reported in Asia, South America, India and Europe. Northern Europe and Scandinavia have been spared the worst hits because of the holiday season in these countries.

Press release:

< <http://www.net-security.org/text/press/995987410,97127,.shtml> >

MCAFFEE ENTERS JAPANESE MARKET - [24.07.2001]

McAfee.com, a leading provider of Web security services, and Sourcenext, a leading Japanese computer software developer and publisher, announced a strategic alliance making Sourcenext the exclusive provider of Japanese language versions of McAfee.com's anti-virus, firewall, privacy and PC utilities applications to over 200 retail outlets in the Japanese market. Sourcenext will also be delivering these services online to its customer base of over a million people. This agreement represents McAfee.com's first localized services for the emerging Asian market and is part of McAfee.com's overall initiative to offer its Internet security services to consumers outside the United States.

Press release:

< <http://www.net-security.org/text/press/996007735,72887,.shtml> >

MCAFFEE AVERT RAISES SIRCAM TO HIGH RISK - [24.07.2001]

Due to an increase of infected users, McAfee AVERT (Anti-Virus Emergency Response Team), a division of Network Associates, Inc. (Nasdaq: NETA), raised its risk assessment of the recently discovered SirCam worm to HIGH risk. W32/SirCam@MM is a destructive mass-mailing (@mm) worm that sends copies of itself to all the e-mail addresses in the infected users' address books. In addition, SirCam sends files with extensions .GIF, .JPG, .JPEG, .MPEG, .MOV, .MPG, .PDF, .PNG, .PS, and .ZIP in the MY DOCUMENTS folder out of the existing environment. AVERT has received more than 300 samples of the virus directly, and has also received reports of hundreds more customers being infected, or reporting the virus being stopped since its discovery on July 17, 2001.

Press release:

< <http://www.net-security.org/text/press/996007854,33984,.shtml> >

SECURITY EXPERTS AT TECHMECCA CONFERENCE - [24.07.2001]

Internationally-renowned technologist and author Bruce Schneier will provide an eye-opening presentation on Internet security issues as part of an all-star lineup of speakers featured at the first annual TechMecca financial services technology conference. The event, which is expected to draw bank, credit union and savings

and loan executives from across the country, will be held Nov. 28-30, 2001 in Arlington, Texas.

Press release:

< <http://www.net-security.org/text/press/996007993,1831,.shtml> >

PROTECTING CONSUMERS FROM IDENTITY THEFT - [24.07.2001]

Whether online or in the real world, identity theft -- the unauthorized use of personal information -- is an increasingly frequent problem for consumers. Identity theft can range from the theft of address and contact information to the illegal use of social security numbers and credit card details. According to the Federal Bureau of Investigation, consumers are regularly exposed to this range of risks and the Internet adds another element to the risk mix, making it more difficult for consumers to identify and measure the reliability of merchants to whom they are trusting transactions.

Press release:

< <http://www.net-security.org/text/press/996008062,95583,.shtml> >

ERUCES AND DATAWISE FORM ALLIANCE - [25.07.2001]

ERUCES, Inc., a provider of innovative security software that completely prohibits unauthorized users from reading or tampering with protected data, and DataWise, Inc., a solution integrator providing services for mid to large sized financial and medical organizations, today announced an alliance in which DataWise will sell the ERUCES Tricryption Engine with its integration services.

Press release:

< <http://www.net-security.org/text/press/996069735,29773,.shtml> >

SYMANTEC WEB SECURITY ANNOUNCED - [25.07.2001]

Symantec Corporation, a world leader in Internet security, announced Symantec Web Security, a high performance, integrated gateway solution that provides Symantec's industry-leading virus protection and web filtering for web-based traffic (HTTP and FTP). Symantec Web Security is an integrated, single-scan anti-virus and web filtering solution that provides IT administrators with a fast, easy-to-use tool to protect networks from unknown malware threats and non business related web content. Symantec Web Security also contains heuristic technologies, in addition to its list-based filtering, ensuring speed and protection for organizational networks.

Press release:

< <http://www.net-security.org/text/press/996069822,2853,.shtml> >

SIRCAM WORM NOT SCARED OFF BY ANTI-VIRUS PRODUCTS - [25.07.2001]

The current assault by the new SirCam email virus - a fast-spreading destructive worm - is a fresh reminder that organizations can only be safe against email attacks such as this if they have installed an email content checking gateway at email server level. Because the SirCam worm can disguise itself by morphing and adopting different Subject lines each time it spreads, anti-virus protection alone is not enough, warned GFI, developer of Mail essentials for Exchange/SMTP, the leading email content checking and anti-virus solution.

Press release:

< <http://www.net-security.org/text/press/996075432,89223,.shtml> >

JAM ECHELON DAY OCTOBER 21ST - [26.07.2001]

A large group of individuals in the Global Internet Community have set out to bring attention to the communications monitoring system known as ECHELON. Two years ago, when this idea was launched, the existence of ECHELON was denied by all of the participating agencies. Now with the recent issuing of the report by the "Temporary Committee on the ECHELON Interception System" its existence and invasive practices are no longer in doubt.

Press release:

< <http://www.net-security.org/text/press/996145547,87978,.shtml> >

EXAULT TO PROVIDE QUALYS'S VULNERABILITY SCANNING - [26.07.2001]

Qualys, Inc., a leading provider of enterprise network vulnerability assessment and monitoring solutions, announced that Exault, Inc. a leader in network security and performance technology consulting, has added QualysGuard online network vulnerability scanning to its suite of offerings. With online vulnerability scanning, Exault clients will be able to automatically inspect their computer networks via the Internet on an ongoing basis to rapidly pinpoint and evaluate security risks.

Press release:

< <http://www.net-security.org/text/press/996155581,68445,.shtml> >

NCIPHER ANNOUNCES NEW E-SECURITY QUALIFICATION - [26.07.2001]

nCipher plc, a leading developer of Internet security products for e-commerce and Public Key Infrastructure (PKI) applications, announced its partnership with NetConnect Ltd to bring expert training in the field of cryptographic hardware security and key management with the launch of the nCipher Certified Systems Engineer (nCSE) qualification.

Press release:

< <http://www.net-security.org/text/press/996155631,50569,.shtml> >

CRYPTOMATHIC AND ALADDIN PARTNER - [27.07.2001]

Aladdin Knowledge Systems, a global leader in the field of Internet content and software security, announced that Cryptomathic, a leading e-Security software provider and PKI specialist, joined Aladdin's eToken Solutions partner program with a PKI application offering seamless usage of the eToken for authentication and signing.

Press release:

< <http://www.net-security.org/text/press/996236249,35514,.shtml> >

RAINBOW TECHNOLOGIES CREATES ESECURITY DIVISION - [27.07.2001]

Rainbow Technologies, Inc., a leading provider of high-performance security solutions for the Internet and eCommerce, announced the creation of Rainbow eSecurity, a new division focusing on the commercial security industry which combines all of the desktop, software security, and Internet and network infrastructure security solutions into a single business unit. Shawn Abbott, president of Rainbow iVEA, was named president of this new business unit, reporting directly to Walt Straub, Rainbow CEO. Rainbow Technologies now has three core divisions, Rainbow eSecurity for commercial security markets, Rainbow Mykotronx for custom and high-assurance security technologies, and Rainbow Spectria for eBusiness services.

Press release:

< <http://www.net-security.org/text/press/996268265,17505,.shtml> >

HNS Security Database

HNS Security Database consists of a large database of security related companies, their products, professional services and solutions. HNS Security Database will provide a valuable asset to anyone interested in implementing security measures and systems to their companies' networks. Visit us at <http://www.security-db.com>

Featured articles

All articles are located at:
<http://www.net-security.org/text/articles>

Articles can be contributed to staff@net-security.org

INSTALLATION OF A SECURE WEB SERVER

Apart from firewalls, which aim at protecting internal networks against attacks from the internet, web servers are the second important field requiring a high degree of security. This article shows how this can be done on a Linux system within just 45 minutes. Of course, the same can also be done on other operating systems. Below is an example based on the SuSE Linux 6.4 distributions.

Read more:
< <http://www.net-security.org/text/articles/index-download.shtml#SuSE> >

BLACKHAT 2001 ATTRITION SLIDE PRESENTATION

This is the presentation that the Attrition staff presented at the BlackHat Briefings. It shows how they managed their defacement mirror as well as the problems related with that.

Read more:
< <http://www.net-security.org/text/articles/index-download.shtml#Attrition> >

IS YOUR NETWORK SECURE?

This story, albeit fictional characters, is reality for hundreds of companies who make a home on the Internet. What did all of them do wrong? The problem can be traced to their criteria for picking a website hosting and design company. The person responsible for doing the screening will be given, or has to create, a guideline of what a certain website design and hosting company has to meet. How many of these guidelines have security in mind? Take a minute to look at the Attrition, web defacement mirror to find out...

Read more:
< <http://www.net-security.org/text/articles/secure.shtml> >

IMPLEMENTING A SECURE NETWORK

Scenario: You have just been hired as the Senior Administrator for a large law firm in Southern California. Your first responsibility as the Senior Systems Administrator is to assess the current network including looking for possible security and efficiency problems. To your surprise, well maybe not so much of

a suprise, the current network is an open field for any possible intruder. The webserver is running Windows NT 3.5 without any patches, and your firewall is FreeBSD 2.2.8. The majority of the workstations are running Windows 95 all with open, unprotected shares, and all bypassing the company's already insecure firewall to access the Internet.

Read more:

< <http://www.net-security.org/text/articles/securenetwork.shtml> >

NETWORK SNIFFERS

Sniffers are tools, also known as network analyzers, used for monitoring network traffic. As such, if used by authorized personnel, can prove to be of a great value. But, on the other hand, sniffers represent significant threat to your network, and are very hard to detect.

Read more:

< <http://www.net-security.org/text/articles/sniffers.shtml> >

Security Software

All programs are located at:

<http://net-security.org/various/software>

RPC TOOLS V1.0

The RPC tools package contains three separate tools for obtaining information from a system that is running RPC services. rpcdump allows you to dump the contents of the endpoint mapper database. ifids is similar to rpcdump but allows you to query a single RPC server and can even allow you to query an RPC server which is not listed in the endpoint map obtained with rpcdump above. walksam is a tool which allows you to dump the information of each user found within the SAM database via Named Pipes or using the additional protocol sequences used by Windows 2000 domain controllers. rpcdump, ifids, and walksam are demonstration programs from the Null Session and MSRPC concepts discussed at BlackHat Windows 2000.

Info/Download:

< <http://www.net-security.org/various/software/995280389,51943,windows.shtml> >

VLAD THE SCANNER

VLAD the Scanner is an open-source security scanner that checks for the SANS Top Ten security vulnerabilities commonly found to be the source of a system compromise. It has been tested on Linux, OpenBSD, and FreeBSD. It requires several Perl modules to run (see the README for more details).

Info/Download:

< <http://www.net-security.org/various/software/995280648,48921,linux.shtml> >

ETTERCAP 0.5.2

Ettercap is a network sniffer/interceptor/logger for switched LANs. It supports active and passive dissection of many protocols (even ciphered ones, like SSH and HTTPS). Data injection in an established connection and filtering (substitute or drop the payload) on the fly is also possible, keeping it alive. You can sniff connections between local and remote hosts through a gateway using the MAC based sniffing mode. Plugins are supported. It has the ability to check whether you are in a switched LAN or not, and to use OS fingerprints to let you know the geometry of the LAN.

Info/Download:

< <http://www.net-security.org/various/software/995283835,54458,linux.shtml> >

GNOSCAN 0.1.1

GnoScan is a multi-threaded network scan and security utility with an intuitive graphical user interface. It runs under GNOME. This is not the world's first port scanner, but certainly one of the most easy ones to use.

Info/Download:

< <http://www.net-security.org/various/software/995285332,25648,linux.shtml> >

KNOCKER 0.2.0

Knocker is a simple and easy-to-use TCP security port scanner written in C. It is able to analyze hosts and the network services which are running on them.

Info/Download:

< <http://www.net-security.org/various/software/995285702,46427,linux.shtml> >

VSHELL 1.1.1 OFFICIAL

VShell Server is a secure access server for Windows NT and Windows 2000, supporting the Secure Shell protocol (SSH2). VShell can be used for secure network access, system administration, and file transfer. In conjunction with an SSH2 client such as SecureCRT, VShell provides an encrypted session that includes a command shell and TCP/IP data tunneling using port forwarding. SFTP and SCP support allows secure FTP applications, such as SecureFX, to connect

for secure file transfers. System administrators can use any SSH2 client, such as SecureCRT or Linux and Unix clients, to access the server PC through the secure command shell. Using NT and DOS utilities, you can start and stop the server, add and remove users, copy files, and even reboot the machine.

Info/Download:

< <http://www.net-security.org/various/software/995396801,23614,windows.shtml> >

PESTPATROL

PestPatrol is a utility, similar to anti-virus products, but instead of scanning for viruses it scans for worms and Trojans, and even tools and utilities used by hackers and maybe even trusted employees. Used along with anti-virus software, PestPatrol will keep you safe from malicious objects, commonly referred to as Pests. You routinely scan for viruses, why not make PestPatrol part of your daily routine?

Info/Download:

< <http://www.net-security.org/various/software/995535909,90381,windows.shtml> >

Defaced archives

[25.07.2001]

Original: <http://www.hackers.nl/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/25/www.hackers.nl/>

OS: FreeBSD

[26.07.2001]

Original: <http://www.stenaline.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/26/www.stenaline.com/>

OS: Windows

Original: <http://www2.stenaline.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/26/www2.stenaline.com/>

OS: Solaris

Original: <http://www.macromedia.co.za/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/26/www.macromedia.co.za/>

OS: Windows

[27.07.2001]

Original: <http://www.microsoft.com.sa/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/27/www.microsoft.com.sa/>

OS: FreeBSD

Original: <http://www.apache.org.cn/>
Defaced: <http://defaced.alldas.de/mirror/2001/07/27/www.apache.org.cn/>
OS: FreeBSD

Original: <http://webservices.cnet.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/07/27/webservices.cnet.com/>
OS: Windows

Original: <http://www.sprite.com.br/>
Defaced: <http://defaced.alldas.de/mirror/2001/07/27/www.sprite.com.br/>
OS: Windows

[28.07.2001]

Original: <http://abv-sfo1-ws10.cnet.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/07/28/abv-sfo1-ws10.cnet.com/>
OS: Windows

Original: <http://www.attrition.org/>
Defaced: <http://defaced.alldas.de/mirror/2001/07/28/www.attrition.org/>
OS: Linux

Original: <http://www.sanyo.ne.jp/>
Defaced: <http://defaced.alldas.de/mirror/2001/07/28/www.sanyo.ne.jp/>
OS: FreeBSD

Original: <http://abv-sfo1-ws5.cnet.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/07/28/abv-sfo1-ws5.cnet.com/>
OS: Windows

Original: <http://www.borland.it/>
Defaced: <http://defaced.alldas.de/mirror/2001/07/28/www.borland.it/>
OS: Windows

[29.07.2001]

Original: <http://www.renault.co.za/>
Defaced: <http://defaced.alldas.de/mirror/2001/07/29/www.renault.co.za/>
OS: Windows

Original: <http://www.creative.or.jp/>
Defaced: <http://defaced.alldas.de/mirror/2001/07/29/www.creative.or.jp/>
OS: FreeBSD

Original: <http://www.audi.lu/>
Defaced: <http://defaced.alldas.de/mirror/2001/07/29/www.audi.lu/>
OS: Windows

=====
Help Net Security T-Shirt available

=====
Thanks to our affiliate Jinx Hackwear we are offering you the opportunity
to wear a nifty HNS shirt :) The image speaks for itself so follow the link
and get yourself one.

Get one here: <http://207.21.213.175:8000/ss?click&jinx&3af04db0>

=====
Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org
<http://net-security.org>
<http://security-db.com>