

HNS Newsletter
Issue 70 - 09.07.2001
<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: 2620

Table of contents:

- 1) General security news
- 2) Security issues
- 3) Security world
- 4) Featured products
- 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

BRITISH HACKER FINED IN EMIRATES

A Dubai court has fined a 22-year-old British computer engineer \$2,725 for hacking into the network of state-run telecoms company Etisalat in the United Arab Emirates (UAE). Mr Lee Ashurst from Oldham, England, who pleaded not guilty and told the Dubai court he did not realise what he was doing was illegal, was convicted of misusing "equipment, services or facilities provided by Etisalat".

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ireland.com/newspaper/breaking/2001/0702/breaking10.htm>

NAMING CONVENTIONS FOR MALWARE

This article provides a basic analogy between computer and biological viruses, leading into malware taxonomy as compared to biological taxonomy and the challenges thereof for malware taxonomy.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/greatanalogy1.html>

NOVELL TRIES ITS HAND AT SECURITY WITH ICHAIN

Best known for its networking software and frequent strategy shifts, Novell Inc. is set to roll out this summer new products in an effort to reshape itself as a security company. Novell last week spelled out the details of its forthcoming iChain 2.0 access-control software, which will include a host of enhanced security features, such as optional token-based authentication.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2781571,00.html>

OPEN SOURCE THE ANSWER TO DOG-EAT-DOG SECURITY

Many of today's PKI e-commerce security implementations leave a lot to be desired. For example, often a single application can get the digital certificate to stamp multiple transactions, while only asking for the end-user's password to use the certificate once. This means that for now, even PKI mixed with smartcards and authenticators may not be enough to get e-commerce over the barrier of gaining universal acceptance. On most occasions we are still being asked by the Internet security industry to simply trust with little tangible evidence either way until after the fact that other people's code, from every merchant and financial institution under the sun, will do the right thing on our system with our money. That's a lot to ask.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://it.mycareer.com.au/opinion/rewire/2001/07/03/FFXUWZU4NOC.html>

MALWARE TAXONOMY: INTRODUCTION

In this article we explore the concept of using biological taxonomy as an example for us to follow when naming viruses and other malware. The goal of a taxonomy/naming system is to enable humans to effectively and consistently communicate regarding identified elements and/or observations and hypothesis that make up the philosophy of a systematic classification system.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/greatanalogy2.html>

USENET MAY BE A VIRUS MINEFIELD

Gryaznov, a member of the VirusPatrol project at McAfee's Avert Labs, has been studying viruses on Usenet for more than five years. Despite the perception that Usenet is increasingly irrelevant in the face of the Web, its population is actually growing, he says. The volume of Usenet posts grew 20 percent from January 2001 to April 2001, he says. And those new visitors are likely to encounter a flood of viruses, including Trojan horses, backdoors, and tools used to take over PCs for use in denial of service attacks, he says.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/news/article/0,aid,54424,00.asp>

USER GROUP PROPOSES OS SECURITY STANDARDS

The Center for Internet Security (CIS), a coalition of internet user groups,

yesterday released the first set of minimum security standards for operating systems. Starting off with specs for Solaris, the user group plans to introduce similar standards for Windows, as well as for Linux and other Unix systems. The group said that the definition of minimum security standards is an attempt to encourage vendors to ship more secure operating systems. Solaris was selected as the starting model because it is so often used as a critical part of the infrastructure in financial, military and ecommerce systems.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1123597>

TRUSTIX XSENTRY FIREWALL 1.5 REVIEW

This firewall is a solid offering from Trustix AS. As you may have guessed, this is the same company that had become famous for their distribution, Trustix Secure Linux. Obviously they have security on the brain. It shows. What I liked about XEntry is that you can configure the firewall from a workstation very easily. There is very little to be done on the server itself. While other firewall suites have this functionality, Trustix has made the job very easy and intuitive. Great for the stressed system administrator.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.thedukeofurl.org/reviews/misc/xsentry15/>

MOST HACKING HIDES REAL THREATS

The high profile of such relatively inconsequential online political warfare as denial-of-service attacks and playful site defacement has the general public distracted from much graver risks. That's especially true in Europe, according to experts, where many Internet users are newer to the medium and less attuned to the dangers of such threats as smart viruses. "Do Europeans care about information warfare?" asks Christiane Schultzki-Haddouti, a German journalist who specializes in information warfare. "Not much. Compared to America, Europe is still sleeping."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0%2C1283%2C44955%2C00.html>

UNICODE BUG RESTYLED AS DOS TOOL

The infamous Unicode IIS Web server exploit can also be used as a denial of service attack tool. Gray hat hacker Big Poop has published a site on the Internet explaining how the Unicode bug, which permits the execution of commands on a Web server, can be used to tie up system resources so that legitimate users can't access a site - a classic DoS attack technique.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/20155.html>

OS X FLAWS DRAW HACKERS' EYES

The rising popularity of the current Mac OS X and the new operating system's foundation in the ubiquitous Unix operating system have started to draw the scrutiny of hackers and security experts. The result: Electronic mailing lists dedicated to security are seeing the first reports of Mac OS X vulnerabilities. The vulnerabilities are considered mild, partly due to Apple's focus on desktop PCs and minimal presence in servers and other Internet infrastructure. But that could change as hackers get more ambitious and Apple tries to move into new markets.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,5093670,00.html>

THE RUX FIRECRACKER TROJAN

The trojan was discovered by Astonsoft developers. This is a trojan whose primary distinction is that it attempts to kill the users firewall before it does anything else. Vulnerable are AT Guard, Zone Alarm and or MC Afee Firewall.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=www.astonsoft.com\rax.htm>

MOBILE SECURITY: ALL TIED UP

Today we can do e-commerce sans wires - over the air. The dream of millions of dollars worth of business being initiated, conceived, collaborated, and executed by a mobile workforce is already a reality to some, but not quite for all... As with e-commerce, security plays a big part in the mobile revolution - ensuring that privacy, trust and reliability of transactions are not compromised. ZDNet Asia brings you the solutions already available, how some carriers are using them, as well as comments from industry players on mobile security.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnetasia.com/telecom/specialreports/cellphone/>

DEFAACEMENT SPREE IN AUSTRALIA

There has been a defacement rampage in Australia whn at least 48 pages of well-known Australian sites (such as those belonging to bookseller Dymocks, cable TV channel Sky Channel, a charity of the Alfred Hospital in Melbourne, the Penrith City council, and Web development company Nethead) have been defaced. Since June 28, the defacer known as L4m4 has struck well-known Australian sites such as those belonging to bookseller Dymocks, cable TV channel Sky Channel, a charity of the Alfred Hospital in Melbourne, the Penrith City council, and Web development company Nethead. The defacements were all gathered by the Alldas archive.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/167607.html>

GOVERNMENT, MILITARY SCRAMBLE FOR ENCRYPTION TECHNOLOGY

The government and military are investing more heavily in encryption technology as a defence against hackers who are beginning to deploy more sophisticated cracking techniques. That's the conclusion of a study by industry analysts Frost & Sullivan who said sales of encryption technologies to military and government agencies, along with contractors, are growing from \$176 million to a projected \$457.6 million by 2007.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/20193.html>

SECURE ONLINE BEHAVIOR, PART THREE

This the third article in a three-part series devoted to helping readers develop secure habits when using the various components of the Internet. This installment will focus on the World Wide Web. Unfortunately, the Web, was designed for ease of communication, rather than for security. While software programs such as firewalls, intrusion detection systems, and antivirus software can be provide protection, the best way to for users to ensure their security while surfing the Web is to learn and practice secure behaviors.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/basics/articles/sechabits3.html>

ADDRESSING SECURITY ISSUES IN LINUX

Once you have Linux up and running on your computer or your network and have installed your applications, you are all ready to go, right? Well, yes and no. Your system may be running, but until you consider security issues you are potentially leaving yourself open to serious trouble. Security encompasses a number of different aspects, from passwords and permissions, to data encryption, virus protection, firewalls and VPNs, software bugs, data backup, and even physical security (keylocks, bolt-down cables, and alarms, to name a few). In this extensive overview of Linux security issues, IBM's Mark Chapman points out various security issues, briefly describes strategies for dealing with them, and lists many products available to help you in your goal of a safe, secure Linux environment.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www-106.ibm.com/developerworks/linux/library/l-sec/>

THE DIRT ON BIG BROTHER

Is your computer watching you? The spectre of Big Brother just got a giant step closer thanks to a controversial piece of software called DIRT. Sold only to police, military and intelligence agencies, DIRT is causing a small furor in civil liberties circles. It offers government operatives a powerful tool to break into your home through the Internet and read everything on your computer, without ever leaving their offices. The brainchild of former NYPD cop Frank Jones, DIRT stands for Data Interception by Remote Transmission. Depending on the model, it reportedly costs anywhere from a few thousand dollars to over \$200,000.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://cryptome.org/DIRT-bags.htm>

MAX VISION BEGINS 18-MONTH TERM

Computer security consultant and confessed cyber intruder Max Butler will serve out his 18-month prison term at the privately-run Taft Correctional Institution in central California, sources say. Butler, known as 'Max Vision' to friends and associates, pleaded guilty last September to launching an automated intrusion program that cracked hundreds of military and defense contractor computers over a few days in 1998. Butler was sentenced in federal court in San Jose, California in May, and he surrendered to the custody of US Marshals last week.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/20222.html>

MANDRAKE SINGLE NETWORK FIREWALL REVIEW

Raymond writes: "I shall talk about Single Network Firewall from a consultant's viewpoint. That is, I will talk about how its function helps me as a security consultant to accomplish my work. I will talk little on its technical merits, as I personally don't think wrestling with Single Network Firewall for just one day qualifies me to talk about its technical flaws, or merits, or the lack thereof."

Link: <http://www.aeonxe.com/article.php?story=20010704040418557>

MALWARE TAXONOMY: CHALLENGES

The first article of this series illustrated generic similarities between biological and computer viruses. The second article overviewed biological and computer virus naming taxonomies. This last article discusses the challenges for a malware taxonomy in the context of the previous two articles.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/greatanalogy3.html>

IDS TERMINOLOGY, PART ONE: A-H

Intrusion Detection Systems (IDS) are still very much in their infancy, but in terms of development they are growing at an extraordinary rate. The terminology associated with IDS is also growing at rapidly. This article, the first of a two-part series, is intended to introduce readers to some IDS terminology, some of it basic and relatively common, some of it somewhat more obscure.

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

HANDHELDS: GETTING A GRIP ON SECURITY

The first, simple generation of PDAs was more or less protected from abuse through its limited capacity, which could not hold complex viruses or store large amounts of sensitive data. But newer PDAs will soon reach 128Mb in size, which is sufficient to store 10,000 personal or company addresses, 400 emails and 3000 documents with notes. Companies spend billions of pounds a year on IT security systems for desktop computers, but very little is invested in securing the mobile workforce. Companies should have this area covered within their security policy but, in reality, very few have the necessary security tools to ensure protection against breaches.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/Features/1123705>

IT DIRECTORS NOT GAMBLING ON SECURITY

At three different security events - the South West Insurance Forum, the NHS Security Conference and the Infosecurity Exhibition - IT directors were asked about security and revealed an alarmingly lax approach to the issue. Only 5 percent of respondents in the insurance sector saw security as a priority and, while 40 percent in the health sector cited security as their number one IT priority, only half were prepared to invest more than one tenth of their IT budget on the issue. Nearly half blamed the high implementation costs of security measures and over a third admitted feeling confused by the diversity of platforms on the market.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2090840,00.html>

Security issues

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

FEW VULNERABILITIES IN VWEBSERVER AND SMALLHTTP

ASP file source disclosing: Adding a unicated space character at the end of requested URL, vWebServer shows the ASP file instead of executing it.

DOS device filename vulnerability: Under Windows 9x, using any DOS device names (aux, con, prn, ...) as a filename or directory crashes Windows.

vWebServer doesn't filter those requests.

Very long URL vulnerability: Requesting a very long URL (i tried 8192 bytes long) will resulted in Error #5, File error. After requesting 2-3 times the same URL, web server will no longer response anything. Restart needed.

Link: <http://www.net-security.org/text/bugs/994075370,53246,.shtml>

WFTPD V3.00 R5 DIRECTORY TRAVERSAL

Append a dot to the lnk filename to fool WFTPD into accepting a *.lnk file, and we can traverse the homedirectory.

Link: <http://www.net-security.org/text/bugs/994075520,65273,.shtml>

BROKER 5.9.5.0 DIRECTORY TRAVERSAL

Users with write permissions can traverse directories, by uploading a lnk file pointing to the desired file / directory

Link: <http://www.net-security.org/text/bugs/994075572,2540,.shtml>

ARGOSOFT 1.2.2.2 *.LNK UPLOAD DIRECTORY TRAVERSAL

Users with write permissions can traverse directories, by uploading a lnk file pointing to the desired file / directory.

Link: <http://www.net-security.org/text/bugs/994075624,88729,.shtml>

BISONFTP SERVER V4R1 VULNERABILITY

BisonFTP Server V4R1 allows any user to upload *.bdl (a file format invented to make links to directories) :

PUT \local.bdl remote.bdl

If we create a *.bdl pointing to the harddrive's root (using our own copy of BisonFTP Server) and we CD to that link, we can browse the entire drive and we have the same rights as we have in our homedirectory + we can dive into subdirs whilst keeping the same rights.

Link: <http://www.net-security.org/text/bugs/994242895,83853,.shtml>

TRENDMICRO INTERSCAN WEBMANAGER VULNERABILITY

Trend Micro InterScan WebManager is a software which provides malicious mobile code protection, URL filtering and traffic management. A buffer overflow vulnerability exists in HttpSave.dll which is used as web management console feature in InterScan WebManager version 1.2. This problem can allow remote users to execute arbitrary commands with SYSTEM privilege.

Link: <http://www.net-security.org/text/bugs/994243172,66502,.shtml>

CALDERA - WEBMIN ROOT ACCOUNT LEAK

When starting system daemons from the webmin webfrontend, webmin does not clear its environment variables. Since these variables contain the authorization of the administrator, any daemon gets these variables. A simple attack would be to write a CGI scripts which just dumps all environment variables and wait for the administrator to restart apache using webmin. There is also a environment variable leakage in cron script creation, and a file viewing vulnerability, which makes an upgrade necessary.

Link: <http://www.net-security.org/text/bugs/994364078,55655,.shtml>

POPDELAYD & SENDMAIL RELAY AUTHENTICATION BUG

On some cobalt raq3 servers (with the popdelayd add-on packet installed) and in general on any system running the popdelayd script with sendmail is possible to "inject" this string in the syslog using sendmail logging. So anyone can insert a fake string with his own IP wich will be parsed by popdelayd and that will permit the use of sendmail as a relay.

Link: <http://www.net-security.org/text/bugs/994364157,33797,.shtml>

CESARFTPD & CERBERUS FTPD STACK OVERFLOW

Long arguments for USER, PASS, PORT, DELE, REST, RMD, and MKD (perhaps others as well) sent to CesarFTPd will cause a stack overflow.

Link: <http://www.net-security.org/text/bugs/994364215,56352,.shtml>

MICROSOFT IIS LOCAL AND REMOTE DOS

Opening and reading of device files (com1, com2, etc.) using Scripting.FileSystemObject will crash ASP-processor (asp.dll).

Link: <http://www.net-security.org/text/bugs/994364282,4209,.shtml>

REMOTE BUFFER OVERFLOW IN RADIUS IMPLEMENTATIONS

ISS X-Force has discovered buffer overflow vulnerabilities in two popular Remote Authentication Dial-In User Server (RADIUS) implementations. RADIUS was originally designed to manage user authentication into dial-up terminal servers and similar devices. It has since been used as a standard for access control and user authentication for numerous Internet infrastructure devices, including routers, switches, and 802.11 Wireless Access Points.

Link: <http://www.net-security.org/text/bugs/994419416,12254,.shtml>

CALDERA - OPENSSSH COOKIE FILE PROBLEM

Due to unsafe temporary directory usage an local attacker could remove any file called 'cookies' on the system.

Link: <http://www.net-security.org/text/bugs/994419927,53503,.shtml>

WINDOWS MS-DOS DEVICE NAME DOS VULNERABILITIES

This post is some kind of reply to all previous posts about win32 (server) applications filtering out MS-DOS Device Names (DDNs) to prevent requests for files such as \CON\CON from crashing the operating system. As these vulnerabilities exist due to a very internal operating system flaw (ring0 device drivers), I don't think it is the application programmer's fault nor their responsibility to provide filtering for a bug where they don't know the exact cause or background of. Because the flaw is within the operating system I think it's obvious that the *operating system* itself is patched, instead of

rewriting the applications running under it to have filtering... The reason for this is simple : it creates a false feeling of security. In alot of cases where applications have filtering for these bugs, they don't filter every DDN nor do they provide a *real* solution to the problem (checking whether the requested path contains a DDN using OS calls), as is the case with the OS patch. Conclusion : applications should not filter out DDNs, because they don't fix the problem (basically they make it even worse), the OS patch is better because it fixes *ALL* problems, and if it wouldn't then that's where this discussion should be about.

Link: <http://www.net-security.org/text/bugs/994421068,51056,.shtml>

Security world

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

TIME'S PORTRAYAL OF ALL VNC AS 'SPYWARE' - [04.07.2001]

Tridia Corporation, a global provider of eSupport tools that empower remote system administration for live collaboration, security, support, and training announced that TIME magazine's portrayal of all VNC (virtual network computing) software as "spyware" is not accurate. Given the situation portrayed in the article, similar spying results would prove virtually impossible with the highly secure TridiaVNC - a VNC hybrid. As experts on the topic, Tridia Corporation purposely improved TridiaVNC beyond the basic, insecure, remote access features of VNC. For security, TridiaVNC includes access notification, passwords, and timeouts for passwords. A soon to be announced TridiaVNC Pro version will grow the currently available remote access features and security.

Press release:

< <http://www.net-security.org/text/press/994248484,38882,.shtml> >

ISS Q2 FINANCIAL RESULTS BELOW EXPECTATIONS - [04.07.2001]

Internet Security Systems, Inc. (ISS), a leading global provider of security management solutions for the Internet, announced that its financial results for the second quarter ended June 30, 2001 are below its previously stated expectations.

Press release:

< <http://www.net-security.org/text/press/994248584,4441,.shtml> >

ENTEGRITY LAUNCHES ASSUREPARTNER PROGRAM - [04.07.2001]

Entegrity Solutions Corp., a leader in access management and application security software and services, launched its AssurePartner(TM) Program, a cooperative technology, marketing and sales initiative developed to help speed e-business application security deployment. The Entegrity AssurePartner Program provides systems integrators, software vendors and developers such as Unisys, Y-Point and EuroSignCard with the proven solutions, training and support they need to successfully deliver secure access management capabilities to their customers and strengthen and expand their rapid deployments of secure e-business initiatives.

Press release:

< <http://www.net-security.org/text/press/994248657,17572,.shtml> >

NCIRCLE POISED TO CHANGE IT SECURITY WORLD - [04.07.2001]

nCircle Network Security, Inc., a pioneer in next-generation network security, immediate availability of the industry's first network security risk management system delivering bonafide intrusion prevention. IP360 is a scalable, cost effective solution that integrates non-invasive, continuous vulnerability assessment, wirespeed, intelligent traffic monitoring, and centralized management and reporting.

Press release:

< <http://www.net-security.org/text/press/994248743,46690,.shtml> >

SOPHOS: TOP TEN VIRUSES IN JUNE 2001 - [04.07.2001]

This is the latest in a series of monthly charts counting down the ten most frequently occurring viruses as compiled by Sophos, a world leader in corporate anti-virus protection.

Press release:

< <http://www.net-security.org/text/press/994364416,51654,.shtml> >

GROUPSHIELD FOR DOMINO DELIVERS VIRUS PROTECTION - [05.07.2001]

McAfee, a division of Network Associates, Inc., announced that its award winning McAfee GroupShield solution for Lotus Domino has received IBM ServerProven validation. "Customers tell us they need programs to help make their business cost more predictable, whether they are a small business in startup mode or an established enterprise expanding their capabilities. In today's e-business world the greatest challenges revolve around finding the right tools to insure Internet security and virus protection."

Press release:

< <http://www.net-security.org/text/press/994367161,36545,.shtml> >

ETRUST EZ ANTIVIRUS EARNS ICOSA LABS CERTIFICATION - [05.07.2001]

Computer Associates International, Inc. announced that eTrust EZ Antivirus for Windows 98/ME, Windows NT Workstation, and Windows 2000 Professional have received ICOSA Labs Anti-Virus Scanning certification, endorsing the product's ability to reduce the security risks caused by viruses and other damaging malware. eTrust EZ Antivirus is one of several solutions offered by my-eTrust.com, a web-based storefront for small office and home users.

Press release:

< <http://www.net-security.org/text/press/994367217,22303,.shtml> >

Featured products

The HNS Security Database is located at:

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

Submissions for the database can be sent to: staff@net-security.org

F100/C FIREWALL BOX

Suitable for more complex configurations or extra large sites (more than 500 users). This modular line of firewall appliances enables you to multiply the Ethernet 10/100Mbps/s interfaces (3, 6, ...) and uses an add-on VPN accelerator card to achieve very high digital transmission rates.

Read more:

< <http://www.security-db.com/product.php?id=642> >

This is a product of NETASQ, for more information:

< <http://www.security-db.com/info.php?id=147> >

WTLS PLUS

WTLS Plus combines Certicom's ECC, SSL, and embedded platform expertise to offer a highly efficient WAP security solution. The toolkit provides for plug and-play integration, enabling WAP developers to quickly and reliably add WTLS functionality to their servers and client devices. It reduces cost by substantially shortening development schedules while ensuring that sensitive applications achieve the highest industry standards for security. Certicom's WTLS Plus provides both client and server software and is interoperable with products throughout the WAP marketplace. WTLS Plus is compliant with the WTLS specification developed by the WAP Forum.

Read more:

< <http://www.security-db.com/product.php?id=371> >

This is a product of Certicom, for more information:
< <http://www.security-db.com/info.php?id=78> >

LANGUARD FILE INTEGRITY CHECKER

LANguard File Integrity Checker is a utility that provides intrusion detection by checking whether files have been changed, added or deleted on a Windows 2000/NT system. If this happens it will alert the administrator by email. Since hackers need to change certain system files to gain access, this FREEWARE utility provides a great means to further secure any servers open to attack. After installing LANguard File Integrity Checker, a new service will be added to your system. You can configure which files & folders LANguard file checker should scan for changes and added files. Alerts can be sent to one or more email addresses. The service can run at scheduled intervals by using the task scheduler in Windows 2000 or the AT command in Windows NT.

Read more:
< <http://www.security-db.com/product.php?id=641> >

This is a product of GFI Software Ltd., for more information:
< <http://www.security-db.com/info.php?id=146> >

Security Software

All programs are located at:
<http://net-security.org/various/software>

DESKLOCK SECURITY SYSTEM 2.4.1D

Desklock Security allows administrators and parents to easily block access to certain areas of a Windows computer. Restrictions include blocking of user defined programs, control panels, start menu, desktop, and network options. Also available is the ability to freeze all desktop icons in place and disable the right mouse context menu. Desklock supports multiple administrator accounts making it a snap to use in a business or university environment.

Info/Download:
< <http://www.net-security.org/various/software/994246640,23846,windows.shtml> >

SASTK 0.1.2.1

SASStk - Slackware Administrators Security tool kit. We aim to provide a set of tools and utilities to install and maintain a reasonable level of security for the Slackware Linux distribution.

Info/Download:

< <http://www.net-security.org/various/software/994247604,12032,linux.shtml> >

ZEBEDEE 2.2.2

Zebedee is a simple program to establish an encrypted, compressed "tunnel" for TCP/IP or UDP data transfer between two systems. This allows traffic such as telnet, ftp and X to be protected from snooping as well as potentially gaining performance over low-bandwidth networks from compression.

Info/Download:

< <http://www.net-security.org/various/software/994249630,1654,windows.shtml> >

IPTRAP 0.3

IPtrap listens to several TCP ports to simulate fake services (X11, Netbios, DNS, etc). When a remote client connects to one of these ports, his IP address gets immediately firewalled and an alert is logged. It runs with iptables and ipchains, but any external script can also be launched. IPv6 is supported.

Info/Download:

< <http://www.net-security.org/various/software/994249799,6650,linux.shtml> >

METALOG 0.5

Metalog is a modern replacement for syslogd and klogd. The logged messages can be dispatched according to their facility, urgency, program name and/or Perl-compatible regular expressions. Log files can be automatically rotated when they exceed a certain size or age. External shell scripts (ex: mail) can be launched when specific patterns are found. Metalog is easier to configure than syslogd and syslog-ng, accepts unlimited number of rules and has (switchable) memory bufferisation for maximal performance.

Info/Download:

< <http://www.net-security.org/various/software/994249160,79077,linux.shtml> >

Defaced archives

[04.07.2001]

Original: <http://www.fiat.co.il/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/04/www.fiat.co.il/>

OS: Windows

Original: <http://www.delmar.cec.eu.int/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/04/www.delmar.cec.eu.int/>

OS: Windows

[05.07.2001]

Original: <http://business.worldonline.fr/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/05/business.worldonline.fr/>

OS: Windows

Original: <http://www.acer.com.my/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/05/www.acer.com.my/>

OS: Windows

Original: <http://thestore.sonymusic.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/05/thestore.sonymusic.com/>

OS: Windows

Original: <http://www.dealerx.packardbell.com.au/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/05/www.dealerx.PackardBell.com.au/>

OS: Windows

Original: <http://www.y2k.siemens.dk/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/05/www.y2k.siemens.dk/>

OS: Windows

[06.07.2001]

Original: <http://www.citroen.be/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/06/www.citroen.be/>

OS: Windows

Original: <http://www.bergen.telenor.no/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/06/www.bergen.telenor.no/>

OS: Windows

Original: <http://www.sparc.org/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/06/www.sparc.org/>

OS: Solaris

Original: <http://www.issa.int/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/06/www.issa.int/>

OS: Windows

[07.07.2001]

Original: <http://www.hrl.il.ibm.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/07/www.hrl.il.ibm.com/>

OS: Windows

Original: <http://www.radio.telenor.no/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/07/www.radio.telenor.no/>

OS: Windows

Original: <http://www.sco.co.jp/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/07/www.sco.co.jp/>

OS: SCO

Original: <http://www.sco.com.tw/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/07/www.sco.com.tw/>

OS: SCO

Original: <http://www2.unesco.org/>

Defaced: <http://defaced.alldas.de/mirror/2001/07/07/www2.unesco.org/>

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, summer is just around the corner.

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>