

Net-Sec mini letter  
Issue 9 - 24.04.2000  
<http://net-security.org>

- 1) Security news
- 2) Security issues
- 3) HNS

- 1) Security news

#### DIGITAL CERTIFICATES & ENCRYPTION

Lance Spitzner wrote a white paper dedicated to Digital Certificates & Encryption, how they work and apply to Internet Commerce.

Link: <http://rootprompt.org/article.php3?article=354>

#### OPEN SOURCE

"One of the great rallying cries from the Open Source community is the assertion that Open Source Software is, by its very nature, less likely to contain security vulnerabilities, including back doors, than closed source software. The reality is far more complex and nuanced." - read article by Elias Levy on Security Focus.

Link: <http://www.securityfocus.com/commentary/19>

#### MICROSOFT TO BOOST WINDOWS, UNIX INTEGRATION

Bowing to the requirements of users who run systems with multiple operating environments, Microsoft is at work merging its Interix product line into the next version of its Windows Services for Unix.

Link: <http://www.infoworld.com/articles/pi/xml/00/04/17/000417piindia.xml>

#### mod\_SSL 2.6.3

This module provides strong cryptography for the Apache 1.3 webserver via the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols by the help of the Open Source SSL/TLS toolkit OpenSSL, which is based on SSLeay from Eric A. Young and Tim J. Hudson.

Link: <http://www.modssl.org/>

#### FEARS OF ETHICAL HACKERS

UK security vendors have reacted angrily to the news that a group of the world's most experienced hackers have joined forces to launch their own company. It looks like that they don't like to share their piece of the cake...

Link:

<http://www.silicon.com/public/door?REQUNIQ=956019205&6004REQEVENT=&REQINT1=37026&REQSTR1=newsnow>

#### GUGGENHEIM MUSEUM SITE DEFACED

Computer hackers supporting the armed Basque separatist group ETA sabotaged the Web page of the Guggenheim Museum in the Basque city of Bilbao over the weekend, a museum official said Monday.

Link: <http://www.lasvegassun.com/sunbin/stories/tech/2000/apr/17/041700923.html>

#### FIREWALL

Network Associates plans to announce that it is adding personal firewall technology to its security e-appliance server. The addition will let system integrators include centrally managed intrusion-detection capabilities to enterprise customers' systems.  
Link: <http://www.techweb.com/wire/story/TWB20000418S0005>

#### SECURITY HOLE IN NETSCAPE

There is a security hole in Netscape Communicator 4.x which allows a malicious Web site to read HTML files on a user's hard drive (including the user's bookmarks file and browser cache files, which reveal Web-surfing history). The exploit works by setting a cookie whose value contains JavaScript code.

Link: <http://www.peacefire.org/security/jscookies/>

#### MAFIABOY A COPYCAT

The Canadian teen-ager known as Mafiaboy, who was arrested in connection with an attack against the CNN Web site in February, is an amateur who simply copied tactics used by far more sophisticated attackers who may never be caught, security analysts say.

Link: <http://www.computerworld.com/home/print.nsf/all/000420D73A>

#### MORE ON MAFIABOY

"I'm highly skeptical. I don't think they've found the person who did the attacks. I think law enforcement is stalling the press and public to keep them off their backs while they find the real person" B.K DeLong (McIntyre from Attrition.org) said about Mafiaboy case.

Link: <http://www.wired.com/news/politics/0,1283,35785,00.html>

#### MORE ON MAFIABOY CASE

APB News reports that in order to get the information, knowledge and software to launch the attack, Mafiaboy allegedly was making requests in IRC rooms, on mailing lists, through instant-messaging service ICQ and in Usenet discussion groups.

Link: [http://www.apbnews.com/newscenter/internetcrime/2000/04/20/hacker0420\\_01.html](http://www.apbnews.com/newscenter/internetcrime/2000/04/20/hacker0420_01.html)

#### CGI MADE SECURE

"Writing secure CGI scripts is a particularly important topic because crackers love to hack sites through Web servers (and other common services), and the best way to nail a Web server is through CGI security problems". Read IBM's whitepaper on the topic.

Link: <http://www-4.ibm.com/software/developer/library/secure-cgi/>

## 2) Security Issues (as posted to BugTraq mailing list)

Note: If you are following the links below, be sure to add "," on the end of each URL (If you don't, 404 error will be heading your way:)

PS: All added vulnerabilities could be found on : <http://www.net-security.org/text/misc/bugs>

#### Weak Token in Mail.Com Application

Posted @ 14.4.2000

Free Web mail services powered by mail.com (two underlying free Web mail applications were identified, and this vulnerability pertains to only one of them. Services that use the other

application are not vulnerable as far as we know. The free Web mail offered directly by mail.com is not vulnerable)

Link: <http://www.net-security.org/cgi-bin/bugs/fullnews.cgi?newsid955672928,31728>,

Performance Copilot for IRIX 6.5 vulnerability

Posted @ 14.4.2000

/usr/etc/pmcd has a fail-open security model, allowing anyone to perform queries by default. This exposes potentially sensitive information (ps -efl, df, etc) to anyone on the net. pmcd will accept garbage connections and grow large heaps not released upon tearing down the connection, thus permitting a DoS

Link: <http://www.net-security.org/cgi-bin/bugs/fullnews.cgi?newsid955677342,71261>,

Backdoor in MS FP extensions

Posted @ 16.4.2000

The NT 4 Option Pack ships with a particular ISAPI .dll in /\_vti\_bin/\_vti\_aut/ named dwssr.dll, which is mixed in with the Microsoft FrontPage extensions (the version I have is 3.0.2.1105). This particular .dll allows you to read .asp (and .asa) files under the web root, providing you know the 'password' (obfuscated encoding scheme) of which to ask it. And, as implied by the title, the constant key used in the encoding is "Netscape engineers are weenies!".

Link: <http://www.net-security.org/cgi-bin/bugs/fullnews.cgi?newsid955853149,33108>,

BindView RAZOR Team Analysis of DVWSSR.DLL

Posted @ 18.4.2000

The risks of having dwssr.dll are not as severe as originally reported in media outlets Friday morning, but still severe enough that system administrators responsible for NT systems to investigate. The risks involve whether or not a certain DLL is loaded, how rights are set, and potentially how Front Page 98 is used.

Link: <http://www.net-security.org/cgi-bin/bugs/fullnews.cgi?newsid956019126,43896>,

Remote DoS attack in Real Networks Real Server

Posted @ 22.4.2000

The Ussr Labs team has recently discovered a memory problem in the RealServer 7 Server. What happens is, by performing an attack with specially-malformed information to port 7070 it will cause the process containing the services to stop responding.

Link: <http://www.net-security.org/cgi-bin/bugs/fullnews.cgi?newsid956368558,30994>,

Microsoft's corner:

Microsoft Security Bulletin #25

<http://www.net-security.org/cgi-bin/bugs/fullnews.cgi?newsid955810581,12760>,

Microsoft Security Bulletin #25 (updated)

<http://www.net-security.org/cgi-bin/bugs/fullnews.cgi?newsid955998017,76171>,

Microsoft Security Bulletin #26

<http://www.net-security.org/cgi-bin/bugs/fullnews.cgi?newsid956330697,52433>,

Microsoft Security Bulletin #27

<http://www.net-security.org/cgi-bin/bugs/fullnews.cgi?newsid956330814,11111>,

Microsoft Security Bulletin #28

[http://www.net-security.org/cgi-bin/bugs/fullnews.cgi?newsid956485486,86260,](http://www.net-security.org/cgi-bin/bugs/fullnews.cgi?newsid956485486,86260)

### 3) HNS

HNS forum:

<http://www.net-security.org/various/discussion>

#Security:

<http://www.net-security.org/various/irc>

Bookstore:

<http://www.net-security.org/various/bookstore>

(new books were added this week)

Vote for HNS on Webfringe > <http://www.webfringe.com/?net-sec>

HNS Staff

[staff@net-security.org](mailto:staff@net-security.org)

<http://net-security.org>