

# SecurityFocus Microsoft Newsletter #77

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-03/0079.html>

---

**From:** Marc Fossi ([mfossi@securityfocus.com](mailto:mfossi@securityfocus.com))

**Date:** 03/11/02

Date: Mon, 11 Mar 2002 13:07:23 -0700 (MST)  
From: Marc Fossi <[mfossi@securityfocus.com](mailto:mfossi@securityfocus.com)>  
To: Focus-MS <[focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)>

SecurityFocus Microsoft Newsletter #77

---

This Issue is Sponsored by: GFI, Ltd.

Still think 1 anti-virus for Exchange is enough?

Get real! Proper Exchange Server security requires:

- \* Multiple virus engines – Don't depend on 1 engine only
- \* Email content/attachment checking – Quarantine dangerous emails
- \* Exploit shield – Email intrusion detection & defence
- \* Threats engine – Analyses/defuses HTML scripts, .exe files, etc

Get all this with Mail Security for Exchange 2000!

Get your FREE evaluation here: <http://www.gfi.com/securityfocus/>

---

## I. FRONT AND CENTER

1. Ten Windows Password Myths
2. Network Intrusion Detection Signatures, Part Four
3. Building an Anti Virus Engine
4. A Postcard From Brazil
5. In the Air Tonight
6. The American Management Training Association, Washington DC

## II. MICROSOFT VULNERABILITY SUMMARY

1. Novell GroupWise Web Root Disclosure Vulnerability
2. ReBB Image Tag Cross-Site Scripting Vulnerability
3. Microsoft SQL Server xp\_dirtree Buffer Overflow Vulnerability
4. Microsoft Windows NT Security Policy Bypass Vulnerability
5. Endymion MailMan Alternate Templates File Disclosure Vulnerability
6. Endymion Sake Mail Null Character File Disclosure Vulnerability
7. Multiple Vendor Radius Short Vendor-Length Field Denial Of...
8. MailServer by SH39 Denial of Service Vulnerability
9. TalentSoft Web+ Webpsvc Buffer Overflow Vulnerability
10. CVS Server Global Variable Denial Of Service Vulnerability

11. Microsoft IIS Authentication Method Disclosure Vulnerability
12. Multiple Vendor Java Virtual Machine Session Hijacking...

### III. MICROSOFT FOCUS LIST SUMMARY

1. Incident **\*\*FIXED\*\*** (Thread)
2. Web Services(Thread)
3. Web Services(Thread)
4. Assistance Needed(Thread)
5. MS02-009 : 2 in 1(Thread)
6. Bogus Microsoft Security Announcement(Thread)
7. SQL and Account Permissions(Thread)
8. Patch for the "Microsoft IIS False Content-Length Field DoS...
9. Another ISAPI filter : deny user authentication through...
10. Removing the NTLM Hashes from the AD & SAM?(Thread)
11. SecurityFocus Microsoft Newsletter #76(Thread)
12. Transfer files open shares vs ftp(Thread)
13. Windows XP Internet sharing issue.(Thread)
14. MS02-012/Q313450(Thread)
15. IIS SMTP component allows mail relaying via Null Session(Thread)
16. What about these exploits?(Thread)

### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. MailSecurity for Exchange 2000
2. Administrator Assistant Tool Kit
3. Windows Encryption Tool Kit

### V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. CHX-I Packet Filter v1.0
2. Port Scan Attack Detector (psad) v0.9.6
3. DECLASSFY v1.11
4. John the Ripper 1.6.31dev

### VI. SPONSORSHIP INFORMATION

#### I. FRONT AND CENTER

---

1. Ten Windows Password Myths  
by Mark Burnett

With all of our advances in security technology, one aspect remains constant: passwords still play a central role in system security. The difficulty with passwords is that all too often they are the easiest security mechanism to defeat. Selecting good passwords requires education. System administrators need to be educated and that education needs to be passed on to end users. This article will debunk some common myths surrounding passwords Windows 2000 and XP.

<http://online.securityfocus.com/infocus/1554>

2. Network Intrusion Detection Signatures, Part Four  
by Karen Kent Frederick

This is the fourth in a series of articles on understanding and developing signatures for network intrusion detection systems. In part one we discussed the basics of network IDS signatures and then took a closer look

at signatures that focus on IP, TCP, UDP and ICMP header values. In the second installment we looked at some signature examples. In the previous article, we began to examine the topic of protocol analysis, which means that the intrusion detection system actually understands how various protocols, such as FTP, are supposed to work. In this article, we will continue to look at protocol analysis and how it can overcome attempts by attackers to obfuscate their exploits so that they cannot be detected by simple intrusion detection signature methods.

<http://online.securityfocus.com/infocus/1553>

### 3. Building an Anti Virus engine by Markus Schmall

The article will describe the basic ideas, concepts, components and approaches involved in developing an anti-virus program from scratch from a developer's/software engineer's point of view. It will focus on the main elements of an anti-virus engine (hereafter referred to as AV engine) and will exclude aspects like graphical user interfaces, real-time monitors, file system drivers and plug-ins for certain application software like Microsoft Exchange or Microsoft Office. Although AV engines running/scanning for single platforms (such as Palm OS or EPOC/Symbian OS) can be designed in the same way, this article will focus on designing multi-platform scanning engines, which are far more complex.

<http://online.securityfocus.com/infocus/1552>

### 4. A Postcard From Brazil by Richard Forno

In developing responses to Internet security issues, Brazilians have learned much from the experience of other nations. The student may now hold some lessons for the teacher.

<http://online.securityfocus.com/columnists/65>

### 5. In the Air Tonight By Tim Mullen

When I got started with all this computer stuff, my primary role was that of a network engineer. Someone would decide their company needed X, and I would get hired to install boxes, plug them all into the LAN, and make everything work so when someone put in Y, X popped out the other end. It was magic.

<http://online.securityfocus.com/columnists/64>

### 6. April 29 – 30, 2002, The American Management Training Association, Washington DC

Walk away with defensive tactics to protect your wireless networks – today! Join wireless security leaders to discuss: · Various types of wireless attacks – and defense strategies for each · The pros and cons of WLAN security technologies: WAP, WEP, 802.11x, dynamic WEP, VPN's, bluetooth, 3G, dynamic IPsec, and PKI · Wireless security strategies: What the CIO should know · Corroborating with law enforcement after an attack occurs · Case studies presented by leading wireless security practitioners Plus: A comprehensive post-conference workshop: "A How-To Guide to Implementing Wireless LAN Security Solutions

For more information please visit <http://www.frallc.com/page709462.htm#3>

## II. BUGTRAQ SUMMARY

-----

### 1. Novell GroupWise Web Root Disclosure Vulnerability

BugTraq ID: 4206

Remote: Yes

Date Published: Feb 28 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4206>

Summary:

Novell GroupWise is a directory service available from Novell. It is designed for use on the Microsoft Windows platforms.

A vulnerability has been reported in some versions of GroupWise. Reportedly, if a maliciously formatted web request is submitted to the GWWEB.EXE cgi process, an error message will be returned. This error message will include the full path of the script.

Knowledge of the path to the web root may aid an attacker in performing further intelligent attacks against the vulnerable host.

Other versions of GroupWise may share this vulnerability. This has not, however, been confirmed.

### 2. ReBB Image Tag Cross-Site Scripting Vulnerability

BugTraq ID: 4220

Remote: Yes

Date Published: Mar 04 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4220>

Summary:

ReBB is web forum software which will run on most Unix and Linux variants, as well as Microsoft Windows operating systems. It is written in PHP and may be back-ended by a number of databases.

ReBB allows users to include images in forum messages using image tags, with the following syntax:

[img]url of image[/img]

However, HTML tags are not adequately filtered from within the image tags. It is possible to inject arbitrary script code into forum messages via these image tags. As a result, ReBB is prone to cross-site scripting attacks. Script code will be executed in the browser of the user viewing the forum message and may allow an attacker to steal cookie-based authentication credentials or perform actions as the victim user.

### 3. Microsoft SQL Server xp\_dirtree Buffer Overflow Vulnerability

BugTraq ID: 4231

Remote: Yes

Date Published: Mar 05 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4231>

Summary:

A vulnerability has been reported in the xp\_dirtree function provided with SQL Server. XPs are DLL files that perform high level functions in SQL Server. When called, they invoke a function called Srv\_paraminfo() to parse the input parameters.

If an extremely large parameter is passed to the stored procedure xp\_dirtree, a buffer overflow condition will occur. This may result in stack data being overwritten, including the return address of a function call. This may, in turn, lead to the execution of arbitrary code as the SQL Server process. SQL Server usually runs with SYSTEM privileges.

Exploitation of this vulnerability with arbitrary, oversized data may result in a denial of service condition.

This may be related to an older, known problem with unsafe usage of the Srv\_paraminfo() function call. This issue is discussed in BID 2030, 2031, 2038, 2039, 2040, 2041, 2042, and 2043. This relationship has not been confirmed.

### 4. Microsoft Windows NT Security Policy Bypass Vulnerability

BugTraq ID: 4236

Remote: Yes

Date Published: Mar 06 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4236>

Summary:

Microsoft IIS is a popular web server package for Windows NT based platforms. Version 4.0 of IIS installs a remotely accessible directory, /IISADMPWD, which contains a number of vulnerable .HTR files. These are designed to allow system administrators the ability to provide HTTP based password change services to network users. Requesting one of the .htr files returns a form that requests the account name, current password, and changed password.

An issue has been reported which could allow NT users, with their local security policy set to "User cannot change password", to change their password via IISADMPWD. In addition, this issue has been reported to be exploitable on disabled user accounts.

5. Endymion MailMan Alternate Templates File Disclosure Vulnerability

BugTraq ID: 4222

Remote: Yes

Date Published: Mar 04 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4222>

Summary:

Endymion MailMan is a webmail application written in Perl. It will run on most Linux and Unix variants, in addition to Microsoft Windows operating systems.

Endymion MailMan is prone to an issue which may allow a remote attacker to break out of wwwroot and disclose the contents of arbitrary web-readable files.

Due to insufficient validation of input supplied to the ALTERNATE\_TEMPLATES CGI variable, Endymion MailMan is prone to directory traversal attacks. An attacker may view arbitrary web-readable files by crafting a malicious web request containing dot-dot-slash (../) sequences, followed by the name of the requested file, followed by a trailing null character (%00).

This issue may cause sensitive information to be disclosed to remote attackers.

6. Endymion Sake Mail Null Character File Disclosure Vulnerability

BugTraq ID: 4223

Remote: Yes

Date Published: Mar 04 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4223>

Summary:

Endymion Sake Mail is a webmail servlet, written in Java. It will run on most Unix and Linux variants, in addition to Microsoft Windows operating systems.

Endymion Sake Mail is prone to directory traversal attacks, potentially disclosing arbitrary web-readable files to remote attackers. Successful exploitation entails crafting a malicious web request, targetting an arbitrary web-readable file. The malicious request will include dot-dot-slash (../) sequences and a trailing null character (%00), causing the attacker's request to break out of wwwroot to disclose the contents of the targetted file.

This issue may cause sensitive information to be disclosed to remote attackers.

#### 7. Multiple Vendor Radius Short Vendor–Length Field Denial Of Service Vulnerability

BugTraq ID: 4230

Remote: Yes

Date Published: Mar 04 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4230>

Summary:

RADIUS is the RFC 2865–specified Remote Authentication Dial In User Service. The protocol has been developed and implemented by numerous vendors, and used on Microsoft Windows, Unix, and Linux operating systems.

A problem with the protocol implementation could make it possible for remote users to deny service to legitimate users of the service. The problem is in the handling of short Vendor–Length fields.

The specification of the RADIUS protocol allows for the use of vendor–specific options. These options may be designed for specific vendor implementations of the RADIUS protocol, and may not be compatible with implementations by other vendors.

A problem has been discovered in the handling of vendor–specific options. When a RADIUS packet is passed to a client or server, neither the client nor server validate the contents of the vendor–length field. When a RADIUS packet with a vendor–length specification of less than 2 is sent, the contents of the vendor–length field is interpreted as a negative number. This number may be passed to other functions of the RADIUS server or client, resulting in an unpredictable reaction, and a likely crash of the server or client.

This problem makes it possible for a remote user to supply a maliciously crafted RADIUS packet, and deny service to legitimate users of the service.

#### 8. MailServer by SH39 Denial of Service Vulnerability

BugTraq ID: 4232

Remote: Yes

Date Published: Mar 05 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4232>

Summary:

MailServer by SH39 is an SMTP/POP3 server for Microsoft Windows environments.

Reportedly, connecting to port 25 on a MailServer host, and submitting an unusual amount of arbitrary data (approx 2500 bytes) could initiate a denial of service condition.

This issue may be the result of an unchecked buffer. If this is the case, there is a possibility that arbitrary code may be executed on the vulnerable target. However, this has not yet been confirmed.

This has been reported to work when making a telnet connection to port 25.

#### 9. TalentSoft Web+ Webpsvc Buffer Overflow Vulnerability

BugTraq ID: 4233

Remote: Yes

Date Published: Mar 01 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4233>

Summary:

TalentSoft Web+ is an environment for developing web-based client/server applications. It will run on Microsoft Windows 9x/NT/2000 operating systems.

The Web+ executable does not perform sufficient bounds checking on strings that are passed to services. Malicious externally supplied data may be passed to the Webpsvc service, which by default is run with SYSTEM privileges.

In particular, an excessively long URL may cause stack variables to be overwritten, potentially resulting in the execution of attacker-supplied instructions. At the very least, this may cause a denial of service to the Web+ server.

Since the services in question run with SYSTEM privileges, successful exploitation resulting in arbitrary code execution will enable a remote attacker to fully compromise a host running the vulnerable software.

#### 10. CVS Server Global Variable Denial Of Service Vulnerability

BugTraq ID: 4234

Remote: Yes

Date Published: Mar 05 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4234>

Summary:

CVS Server is a freely available, open source software package designed for the management and distribution of source code. It is available for the Microsoft Windows, Linux and Unix platforms.

A problem with CVS server may make it possible to deny service to legitimate users. The problem is in an improperly set global variable.

Due to a programming error, a global variable used by the CVS Server program is improperly initialized. Because of this, a remote user may be able to create a set of circumstances that use the improperly initialized variable. This could result in the server reacting unpredictably, and

crashing.

This problem makes it possible for a remote user to launch a denial of service attack against legitimate users of the service.

#### 11. Microsoft IIS Authentication Method Disclosure Vulnerability

BugTraq ID: 4235

Remote: Yes

Date Published: Mar 05 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4235>

Summary:

Microsoft IIS supports Basic and NTLM authentication. It has been reported that the authentication methods supported by a given IIS server can be revealed to an attacker through the inspection of returned error messages, even when anonymous access is also granted.

When a valid authentication request is submitted for either message with an invalid username and password, an error message will be returned. This happens even if anonymous access to the requested resource is allowed. An attacker may be able to use this information to launch further intelligent attacks against the server, or to launch a brute force password attack against a known user name.

#### 12. Multiple Vendor Java Virtual Machine Session Hijacking Vulnerability

BugTraq ID: 4228

Remote: Yes

Date Published: Mar 04 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4228>

Summary:

Various Java virtual machine implementations contain a vulnerability that may allow for interception and hijacking of web requests.

The vulnerability is present when a client system is configured to use a HTTP proxy server. It is possible for malicious java code to redirect requests meant for the proxy server to an arbitrary host. This occurs transparently, without any client consent or knowledge.

This vulnerability can be exploited with a maliciously crafted Java applet, possibly embedded in a webpage. The victim must run the applet in a vulnerable virtual machine.

As a result a user's session information could be captured and be examined for sensitive information. Man-in-the-middle attacks may also be possible, as the response to any request may be crafted by the attacker.

It should be noted that all builds of Microsoft Virtual Machine prior to and including build 3802 are affected by this issue.

#### IV. MICROSOFT FOCUS LIST SUMMARY

---

1. Incident **\*\*FIXED\*\*** (Thread)

Relevant URL:

[4.3.2.7.2.20020307181036.048e3548@shit.intranet.shitcum.com](http://online.securityfocus.com/archive/88/4.3.2.7.2.20020307181036.048e3548@shit.intranet.shitcum.com)">http://online.securityfocus.com/archive/88/4.3.2.7.2

2. Web Services(Thread)

Relevant URL:

[OF15FB8145.40A24406-ON03256B75.0075BFB7@nam.pwcinternal.com](http://online.securityfocus.com/archive/88/OF15FB8145.40A24406-ON03256B75.0075BFB7@nam.pwcinternal.com)">http://online.securityfocus.com/archive/88/

3. Web Services(Thread)

Relevant URL:

[04F92BA33955D51195B700508B4AB6E90417048B@dslak13.dnznet.co.nz](http://online.securityfocus.com/archive/88/04F92BA33955D51195B700508B4AB6E90417048B@dslak13.dnznet.co.nz)">http://online.securityfocus.com/archive/88/

4. Assistance Needed(Thread)

Relevant URL:

[9fdcf797@lauradominion.com](http://online.securityfocus.com/archive/88/002b01c1c608$87252100$9fdcf797@lauradominion.com)">http://online.securityfocus.com/archive/88/002b01c1c608\$87252100\$9fdcf797@laur

5. MS02-009 : 2 in 1(Thread)

Relevant URL:

[http://online.securityfocus.com/archive/88/005701c1c5b3\\$8a7dc280\\$33680095@ws0433](http://online.securityfocus.com/archive/88/005701c1c5b3$8a7dc280$33680095@ws0433)

6. Bogus Microsoft Security Announcement(Thread)

Relevant URL:

[Pine.LNX.4.43.0203070821530.23976-100000@mail.securityfocus.com](http://online.securityfocus.com/archive/88/Pine.LNX.4.43.0203070821530.23976-100000@mail.securityfocus.com)">http://online.securityfocus.com/archive/88/

7. SQL and Account Permissions(Thread)

Relevant URL:

[fd613518@address.com](http://online.securityfocus.com/archive/88/010c01c1c590$86d0d500$fd613518@address.com)">http://online.securityfocus.com/archive/88/010c01c1c590\$86d0d500\$fd613518@address.co

8. Patch for the "Microsoft IIS False Content-Length Field DoS Vulnerability" (bid 3667)(Thread)

Relevant URL:

[3C8662C7.2070202@globalsis.com.ar](http://online.securityfocus.com/archive/88/3C8662C7.2070202@globalsis.com.ar)">http://online.securityfocus.com/archive/88/3C8662C7.2070202@globalsis.co

9. Another ISAPI filter : deny user authentication through IIS to users you want.(Thread)

Relevant URL:

[62916738AE78304392A417129871620A2582CE@kings-ms-exch01.kings.com](http://online.securityfocus.com/archive/88/62916738AE78304392A417129871620A2582CE@kings-ms-exch01.kings.com)">http://online.securityfocus.com/ar

10. Removing the NTLM Hashes from the AD & SAM?(Thread)

Relevant URL:

[http://online.securityfocus.com/archive/88/000501c1c45e\\$a8636260\\$c8d9a8c0@GARNHOME01](http://online.securityfocus.com/archive/88/000501c1c45e$a8636260$c8d9a8c0@GARNHOME01)

11. SecurityFocus Microsoft Newsletter #76(Thread)

Relevant URL:

[Pine.LNX.4.43.0203050808210.5896-100000@mail.securityfocus.com](http://online.securityfocus.com/archive/88/Pine.LNX.4.43.0203050808210.5896-100000@mail.securityfocus.com)">http://online.securityfocus.com/archive/88/P

12. Transfer files open shares vs ftp(Thread)

Relevant URL:

[http://online.securityfocus.com/archive/88/014201c1c3b9\\$ff3712d0\\$7507b33e@luscinia](http://online.securityfocus.com/archive/88/014201c1c3b9$ff3712d0$7507b33e@luscinia)

13. Windows XP Internet sharing issue.(Thread)

Relevant URL:

[0cdac797@lauradominion.com](http://online.securityfocus.com/archive/88/009f01c1c3eb$3304d490$0cdac797@lauradominion.com)">http://online.securityfocus.com/archive/88/009f01c1c3eb\$3304d490\$0cdac797@laur

14. MS02-012/Q313450(Thread)

Relevant URL:

[45BD889F8A1BD4118736009027FC6E7B01C8CDBD@optimdexch.optiglobe.com](http://online.securityfocus.com/archive/88/45BD889F8A1BD4118736009027FC6E7B01C8CDBD@optimdexch.optiglobe.com)">http://online.securityfocus.com

15. IIS SMTP component allows mail relaying via Null Session(Thread)

Relevant URL:

[5833B98BD25CB54B9896FFAE74780B24082B2D@server1.Home.KnobbeITS.com](http://online.securityfocus.com/archive/88/5833B98BD25CB54B9896FFAE74780B24082B2D@server1.Home.KnobbeITS.com)">http://online.securityfocus.com

16. What about these exploits?(Thread)

Relevant URL:

[http://online.securityfocus.com/archive/88/5209A1038EA9854CBB6F868F9C4053D41F6AE3@exchange.systemate.c](http://online.securityfocus.com/archive/88/5209A1038EA9854CBB6F868F9C4053D41F6AE3@exchange.systemate.com)

PRODUCTS FOR MICROSOFT PLATFORMS

#### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. MailSecurity for Exchange 2000

by GFI Software

Platforms: Windows 95/98, Windows NT, Windows 2000

Relevant URL:

<http://www.gfi.com/mailsecurity/index.html>

Summary:

The need to monitor email messages for dangerous, offensive or confidential content has never been more evident. The most deadly viruses, able to cripple your email system and corporate network in minutes, are being distributed worldwide via email in a matter of hours (for example, the Love Letter virus). Products that only perform anti-virus scanning do not provide sufficient protection. Worse still, email is likely to become the means for installing backdoors (Trojans) and other harmful programs to help potential intruders break into your network. Products restricted to anti-virus alone will never protect against this. Your only defense is to install a comprehensive email content checking and anti-virus solution to safeguard your mail server & network. Mail Security acts as an Email

Firewall and protects you from email viruses, exploits and threats, as well as email attacks targeted at your organization. Mail Security for Exchange 2000 is based on the new Microsoft VS API, and scans the Exchange information stores.

## 2. Administrator Assistant Tool Kit

by Aelita Software

Platforms: Windows NT

Relevant URL:

<http://www.aelita.com/products/AdminAssist.htm>

Summary:

Administrator Assistant Tool Kit is a set of tools that facilitates security management of Windows NT-based networks. It eliminates tedious and sometimes impossible file system and registry permission management as well as password auditing tasks. Administrator Assistant consists of FileAdmin, RegAdmin, and ScanPro.

## 3. Windows Encryption Tool Kit

by MaeDae Enterprises

Platforms: Windows 95/98, Windows 3.x, DOS

Relevant URL:

<http://www.maedae.com/products.html>

Summary:

The Windows Encryption Toolkit (WET) for Microsoft Windows has just been enhanced to add 32 bit support. The WET provides the data encryption routines from our famous ENCRYPT-IT for Windows and DOS in the form of easy to use 16 bit and 32 bit DLLs. These DLLs are now available for your use with C/C++, Visual Basic, and most other languages that support DLLs. WET and WET PRO (professional version) can even be used in spreadsheets, word processors, and any other product that supports DLLs.

## V. NEW TOOLS FOR MICROSOFT PLATFORMS

---

### 1. CHX-I Packet Filter v1.0

by IDRCI Inc.

Relevant URL:

[http://www.idrci.net/idrci\\_products.htm](http://www.idrci.net/idrci_products.htm)

Platforms: Windows 2000, Windows XP

Summary:

Designed to complement the CHX-I application firewall engine at the network level, the CHX-I Packet Filter can be used on Windows 2000/XP servers or workstations as a first level of defense. Its great graphic user interface and management flexibility allows for rapid filter creation and deployment.

### 2. Port Scan Attack Detector (psad) v0.9.6

by Michael Rash [mbr@cipherdyne.com](mailto:mbr@cipherdyne.com)

Relevant URL:

<http://www.cipherdyne.com/psad/>

Platforms: Linux

Summary:

Port Scan Attack Detector (psad) is a program written in Perl that is designed to work with Linux firewalling code (iptables in the 2.4.x kernels, and ipchains in the 2.2.x kernels) to detect port scans. It features a set of highly configurable danger thresholds (with sensible defaults provided), verbose alert messages that include the source, destination, scanned port range, begin and end times, TCP flags and corresponding nmap options (Linux 2.4.x kernels only), email alerting, and automatic blocking of offending IP addresses via dynamic configuration of ipchains/iptables firewall rulesets. In addition, for the 2.4.x kernels psad incorporates many of the TCP signatures included in Snort to detect highly suspect scans for various backdoor programs (e.g. EvilFTP, GirlFriend, SubSeven), DDoS tools (mstream, shaft), and advanced port scans (syn, fin, Xmas) which are easily leveraged against a machine via nmap.

### 3. DECLASFY v1.11

by Dan Mares [dmares@maresware.com](mailto:dmares@maresware.com)

Relevant URL:

<http://www.dmares.com/maresware/df.htm#DECLASFY>

Platforms: DOS, Windows 3.x, Windows 95/98

Summary:

DECLASFY is designed to meet Department of Defense standards from the rainbow series concerning declassification (wiping) of hard disks, and cleansing of floppy disks. Declassfy writes the entire disk with hex 0s, then 1s (0xff), then random characters or symbols as many time as the user wishes. Since it runs from a DOS boot it wipes the entire drive, not subject to drive access limitations of WINDOWS.

### 4. John the Ripper 1.6.31dev

by Solar Designer

Relevant URL:

<http://www.openwall.com/john/>

Platforms: BeOS, DOS, MacOS, Windows 2000, Windows 95/98, Windows NT

Summary:

John the Ripper is a password cracker, currently available for UNIX, DOS, WinNT/Win95. Its primary purpose is to detect weak UNIX passwords.

## VI. SPONSORSHIP INFORMATION

---

This Issue is Sponsored by: GFI, Ltd.

Still think 1 anti-virus for Exchange is enough?

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #77

Get real! Proper Exchange Server security requires:

- \* Multiple virus engines – Don't depend on 1 engine only
- \* Email content/attachment checking – Quarantine dangerous emails
- \* Exploit shield – Email intrusion detection & defence
- \* Threats engine – Analyses/defuses HTML scripts, .exe files, etc

Get all this with Mail Security for Exchange 2000!

Get your FREE evaluation here: <http://www.gfi.com/securityfocus/>

---

- *Previous message:* [Thor@HammerofGod.com](mailto:Thor@HammerofGod.com): "RE: Automatic Updates on XP Pro"
- *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)