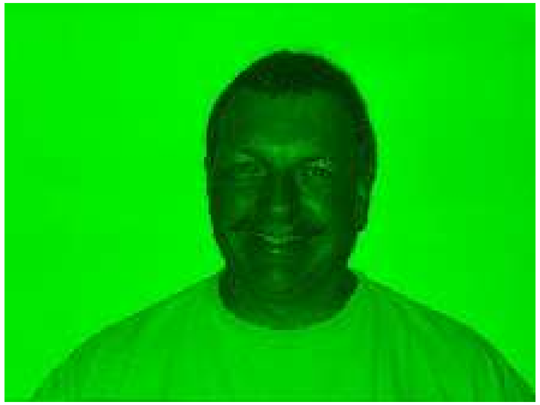
The NetBSD Update System

Maintaining "official" updates securely

Brought to you by



Alistair G. Crooks
agc@pkgsrc.org

Mon Jul 5 22:42:58 BST 2004

Problem set

- Security vulnerabilities
- DoS exploits
- XSS exploits
- Well-catered for on packages side by audit-packages
- Security Advisories have to carry instructions to update

Other approaches

- □Windows Update
- □RPMs
- □By hand
- □Prayer
- □Luck

Other approaches (2)

Help is at hand...

The building blocks

□ package naming conventions

□ audit-packages

□ pkg-vulnerabilities

□ signed packages

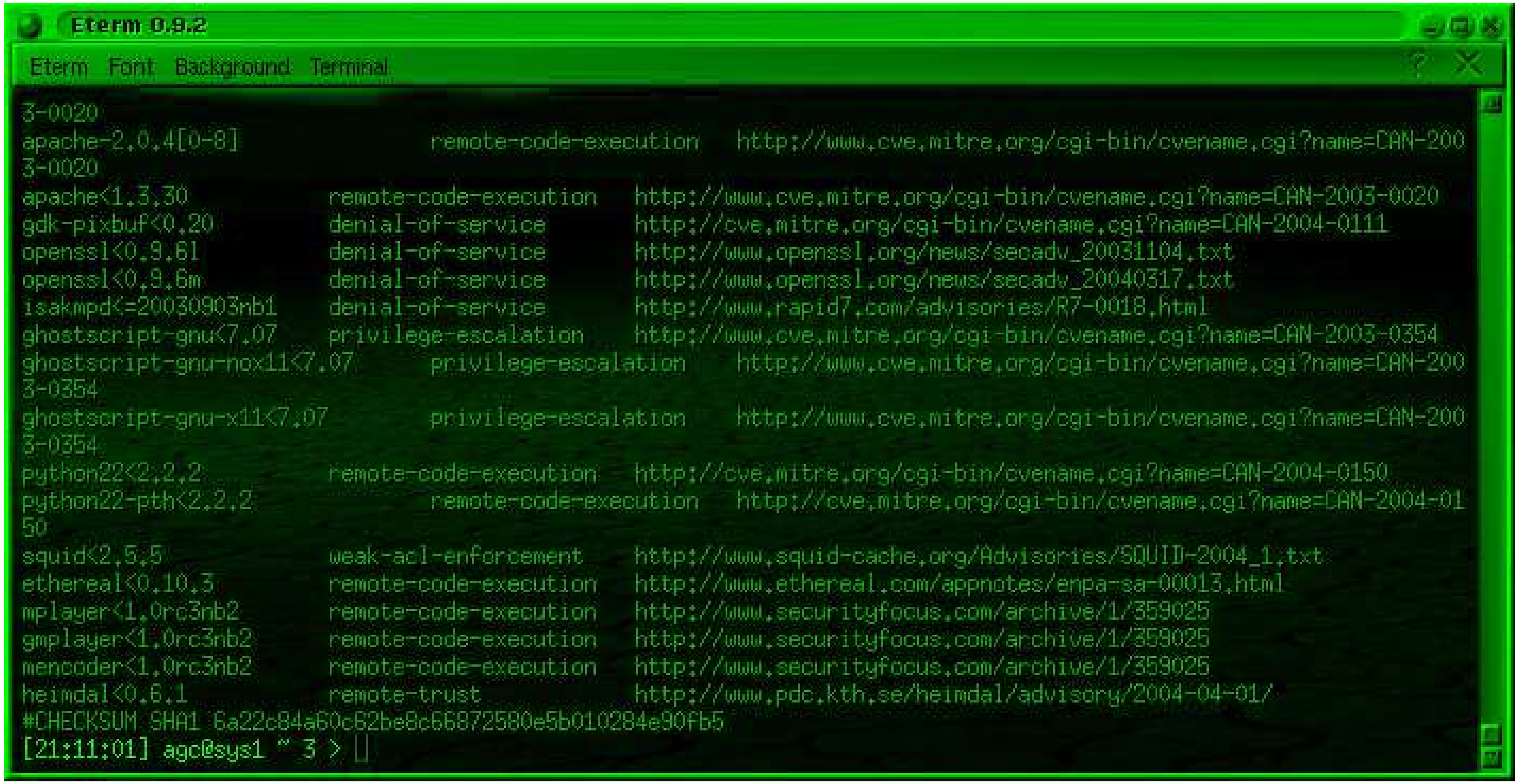
Package naming conventions

- A consistent numbering scheme
- Dewey-decimal-style numbering
  - Alpha
  - Beta
  - Release Candidate
  - Patch-level
  - Letters
  - NetBSD Version

audit-packages

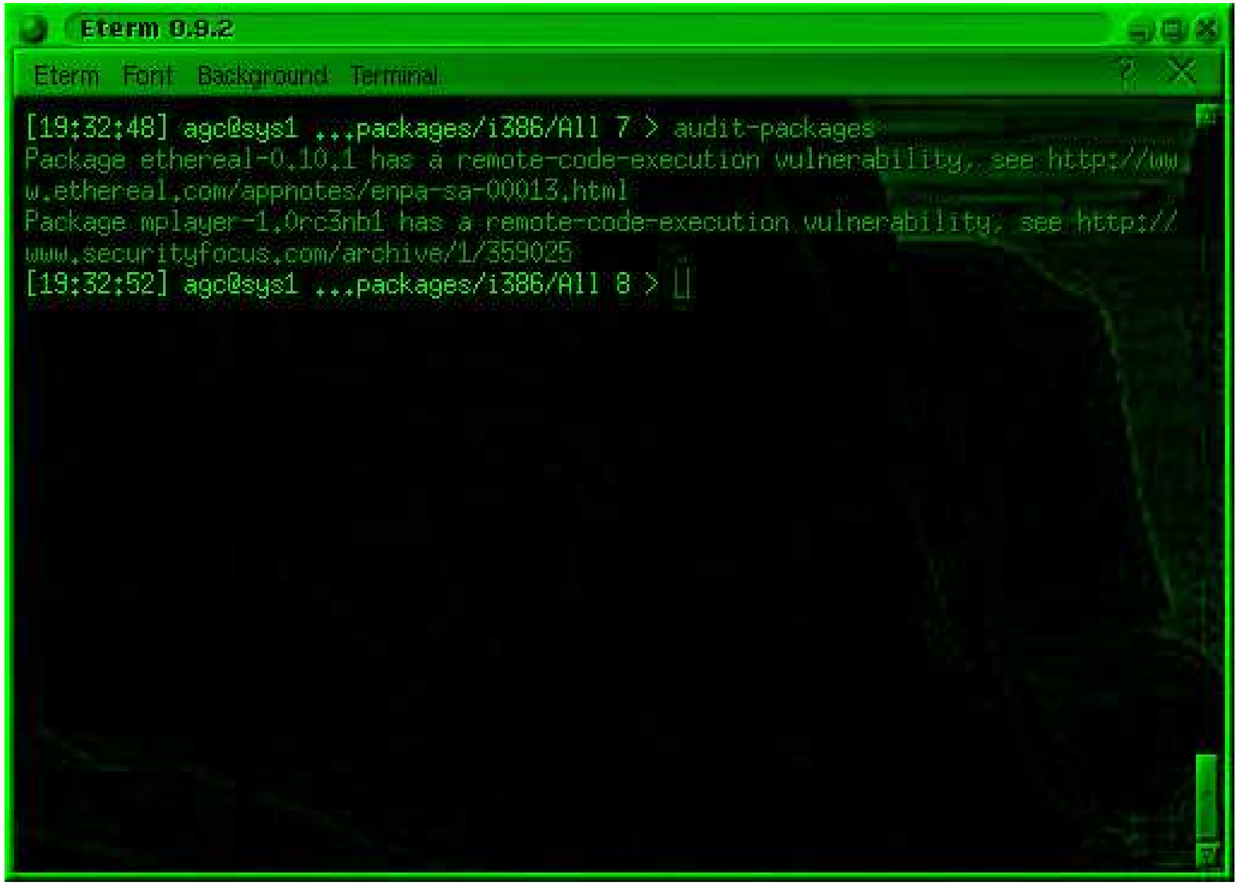
- A file is maintained on ftp.netbsd.org
- The pkg-vulnerabilities file
- download-vulnerability-list downloads the pkg-vulnerabilities file
- audit-packages scans the installed packages on the system

The pkg-vulnerabilities file



```
3-0020
apache-2.0.4[0-8]               remote-code-execution   http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-200
3-0020
apache<1.3.30           remote-code-execution   http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0020
gdk-pixbuf<0.20         denial-of-service       http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0111
openssl<0.9.6l          denial-of-service       http://www.openssl.org/news/secadv_20031104.txt
openssl<0.9.6m          denial-of-service       http://www.openssl.org/news/secadv_20040317.txt
isakmpd<=20030903nb1    denial-of-service       http://www.rapid7.com/advisories/R7-0018.html
ghostscript-gnu<7.07    privilege-escalation    http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0354
ghostscript-gnu-nox11<7.07      privilege-escalation    http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-200
3-0354
ghostscript-gnu-x11<7.07        privilege-escalation    http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-200
3-0354
python22<2.2.2          remote-code-execution   http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0150
python22-pth<2.2.2              remote-code-execution   http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-01
50
squid<2.5.5             weak-acl-enforcement    http://www.squid-cache.org/Advisories/SQUID-2004_1.txt
ethereal<0.10.3         remote-code-execution   http://www.ethereal.com/appnotes/enpa-sa-00013.html
mplayer<1.0rc3nb2       remote-code-execution   http://www.securityfocus.com/archive/1/359025
gmplayer<1.0rc3nb2      remote-code-execution   http://www.securityfocus.com/archive/1/359025
mencoder<1.0rc3nb2      remote-code-execution   http://www.securityfocus.com/archive/1/359025
heimdal<0.6.1           remote-trust            http://www.pdc.kth.se/heimdal/advisory/2004-04-01/
#CHECKSUM SHA1 6a22c84a60c62be8c66872580e5b010284e90fb5
[21:11:01] agc@sys1 ~ 3 >
```

Audit-packages in operation



```
[19:32:48] agc@sys1 ...packages/i386/All 7 > audit-packages
Package ethereal-0.10.1 has a remote-code-execution vulnerability, see http://ww
w.ethereal.com/appnotes/enpa-sa-00013.html
Package mplayer-1.0rc3nb1 has a remote-code-execution vulnerability, see http://
www.securityfocus.com/archive/1/359025
[19:32:52] agc@sys1 ...packages/i386/All 8 >
```

Digital Signing

Digitally-signed packages

□ Provenance of a package is assured

□ External vs. Internal signatures

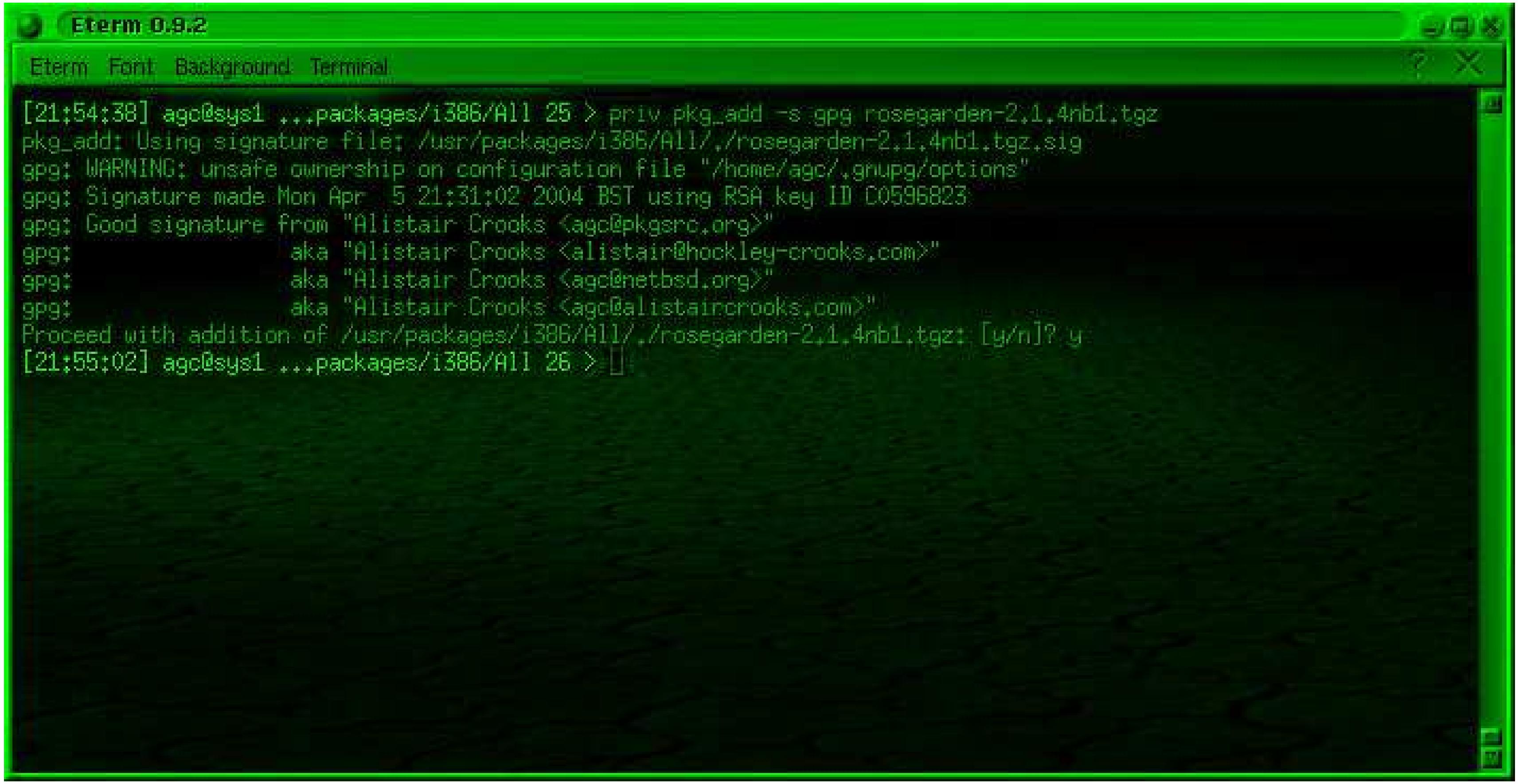
□ External signatures in pkgsrc since September 2001

□ Based on gpg

□ Automatically invoked by pkg_add(1)

□ Binary packages can be transferred by insecure media

Installing a digitally-signed package



```
[21:54:38] agc@sys1 ...packages/i386/All 25 > priv pkg_add -s gpg rosegarden-2.1.4nb1.tgz
pkg_add: Using signature file: /usr/packages/i386/All/./rosegarden-2.1.4nb1.tgz.sig
gpg: WARNING: unsafe ownership on configuration file "/home/agc/.gnupg/options"
gpg: Signature made Mon Apr  5 21:31:02 2004 BST using RSA key ID C0596823
gpg: Good signature from "Alistair Crooks <agc@pkgsrc.org>"
gpg:                 aka "Alistair Crooks <alistair@hockley-crooks.com>"
gpg:                 aka "Alistair Crooks <agc@netbsd.org>"
gpg:                 aka "Alistair Crooks <agc@alistaircrooks.com>"
Proceed with addition of /usr/packages/i386/All/./rosegarden-2.1.4nb1.tgz: [y/n]? y
[21:55:02] agc@sys1 ...packages/i386/All 26 > 
```

The NetBSD Update System

- Provide the functionality of Windows Update
- Digital signatures to verify the provenance of packages
- Transfer binary packages by insecure media
- Check if an update has already been installed
- Preserve previous files for "rollback"

Pre-requisites for NetBSD Update

- NetBSD packaging tools installed
- pkgsrc/security/gnupg package
- pkgsrc/pkgtools/pkg_tarup package

Stages in NetBSD Update

- Notification that updates are available
- Download the updates
- Install those updates

Windows Update

□ Site DoS measures early in 2004

□ Integrated in the base system

□ Checkpoints in the operating system

Other Update Systems

- □ Not to charge for them
- □ Quick turnaround for exploits

Stages in NetBSD Update

- □ Notification that updates are available
- □ Download updates file via ftp(1)
- □ Download updates and signatures
- □ Create "rollback" binary package of any existing files
- □ Attempt to install packages via a signed pkg_add
- □ Option to accept or reject here, depending upon package’s signature

Applicability of an Update

□Either a computer is vulnerable to an exploit, or not

□Update list has OS, version and architecture triplet

□Can announce vulnerability even if no fix is available

□(Operating system, version, architecture) triplet

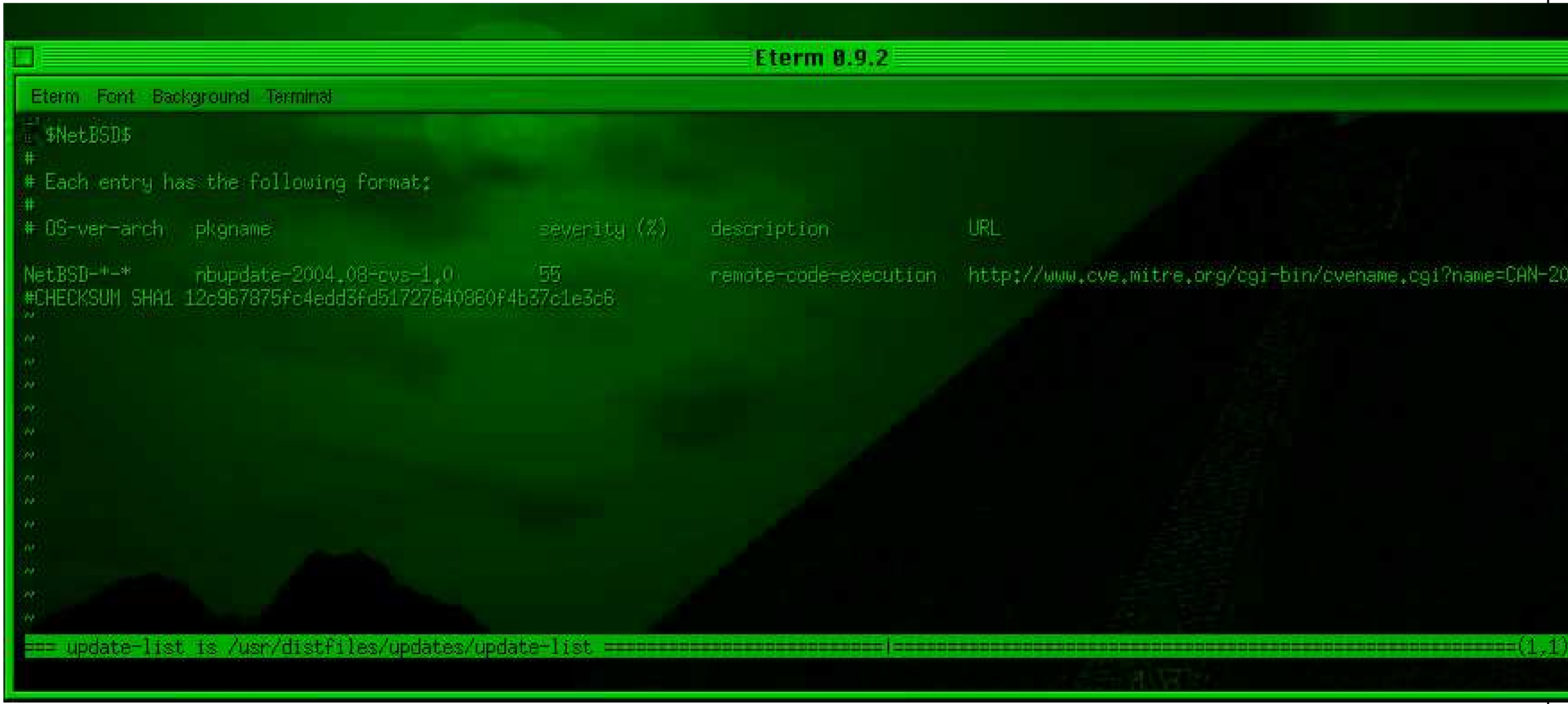
Vulnerability

- A package can either be installed on a computer, or not
- pkg_info(1) can be used to tell if an update is installed
- If not, the computer is deemed to be vulnerable, and needs the update applied
- A similar sequence to the audit-packages script

Downloading

- Download components via ftp(1)
- Security is not present in the transfer

The update-list file



```
# $NetBSD$
#
# Each entry has the following format:
#
# OS-ver-arch   pkgname                         severity (%)    description              URL

NetBSD-*-*      nbupdate-2004.08-cvs-1.0        55              remote-code-execution   http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-20
#CHECKSUM SHA1 12c967875fc4edd3fd51727640860f4b37c1e3c6
~
~
~
~
~
~
~
~
~
~
~
~
~
~
=== update-list is /usr/distfiles/updates/update-list ==========================|===========================================================(1,1)
```

Components which are downloaded

- binary package
- binary package detached signature
- rollback package DESCR file
- rollback package PLIST file

Checkpoints

- □System checkpoint facility on Microsoft Windows
- □Rollback binary packages and recovery

Installing the Update

□ Windows Update allows unattended installation of updates

□ NetBSD Update uses

```
pkg_add -s gpg update-name
```

□ Provenance information via gpg

Aspects of updating

□Changes to configuration files

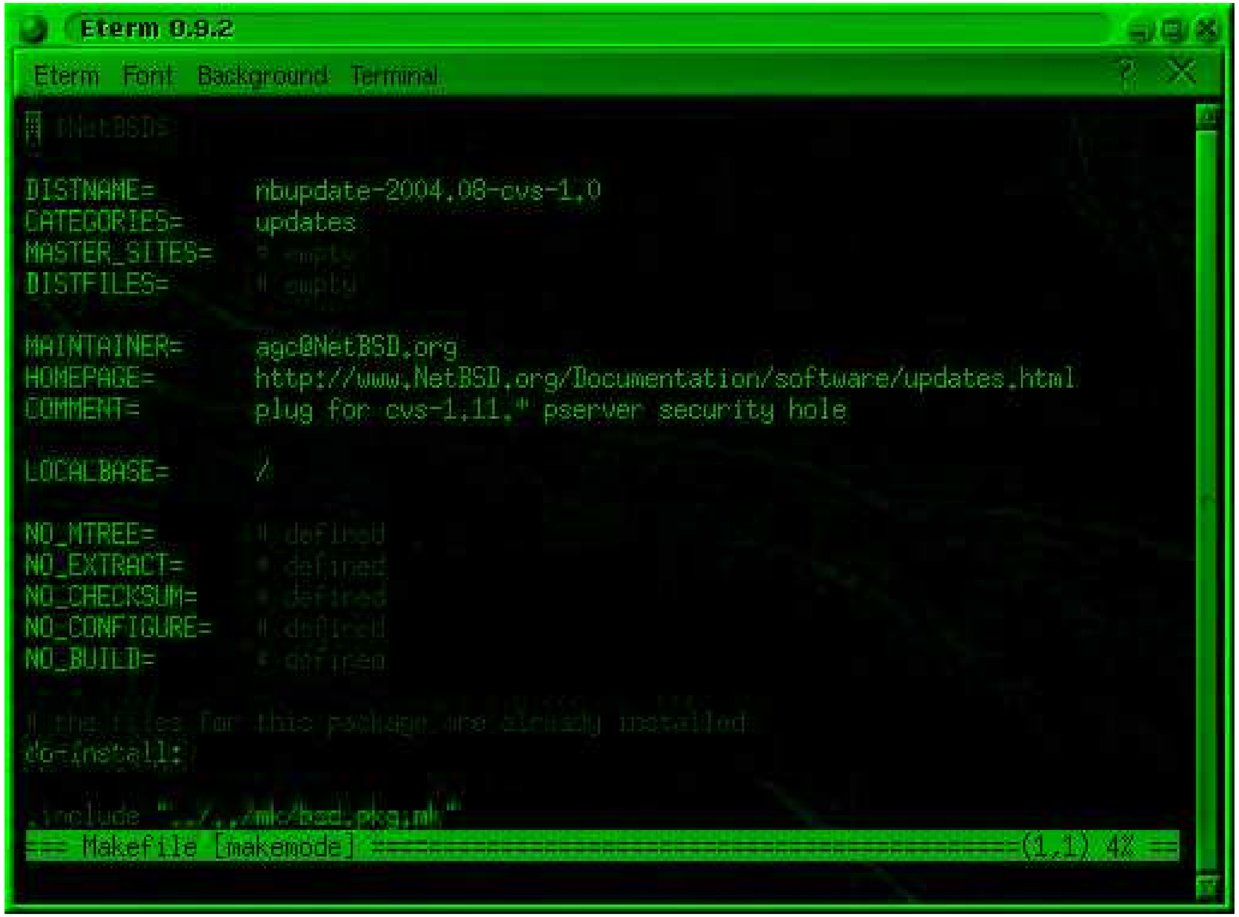
□Changes to kernel

Creating an update package

- □ Special pkgsrc entry is provided
- □ Modify PLIST and DESCR
- □ Files taken from a running system
- □ Binary package is signed by

```
gpg --sign --detach ${PKGNAME}
```

Template pkgsrc Makefile



```
# $NetBSD$

DISTNAME=       nbupdate-2004.08-cvs-1.0
CATEGORIES=     updates
MASTER_SITES=   # empty
DISTFILES=      # empty

MAINTAINER=     agc@NetBSD.org
HOMEPAGE=       http://www.NetBSD.org/Documentation/software/updates.html
COMMENT=        plug for cvs-1.11.* pserver security hole

LOCALBASE=      /

NO_MTREE=       # defined
NO_EXTRACT=     # defined
NO_CHECKSUM=    # defined
NO_CONFIGURE=   # defined
NO_BUILD=       # defined

# the files for this package are already installed
do-install:

.include "../../mk/bsd.pkg.mk"
=== Makefile [makemode] ==============================================(1,1) 4% ==
```

Implications

- an update can be backed out and replaced by previous contents
- less onus for security instructions in security advisories
- digital signature provenance needs to be kick-started
- reliance upon GPLed code in a BSD utility

Who can use it?

- Anyone using the NetBSD Packages Collection
- Not necessarily NetBSD
- Notification feature advises when updates are needed

pkgsrc platforms

□ AIX

□ BSDOS

□ Darwin

□ FreeBSD

□ IRIX

□ Interix

□ Linux

□ NetBSD

□ OpenBSD

□ SunOS

□ UnixWare

Extensibility

- Sun’s patch system organisation
- Any operating system you wish to support

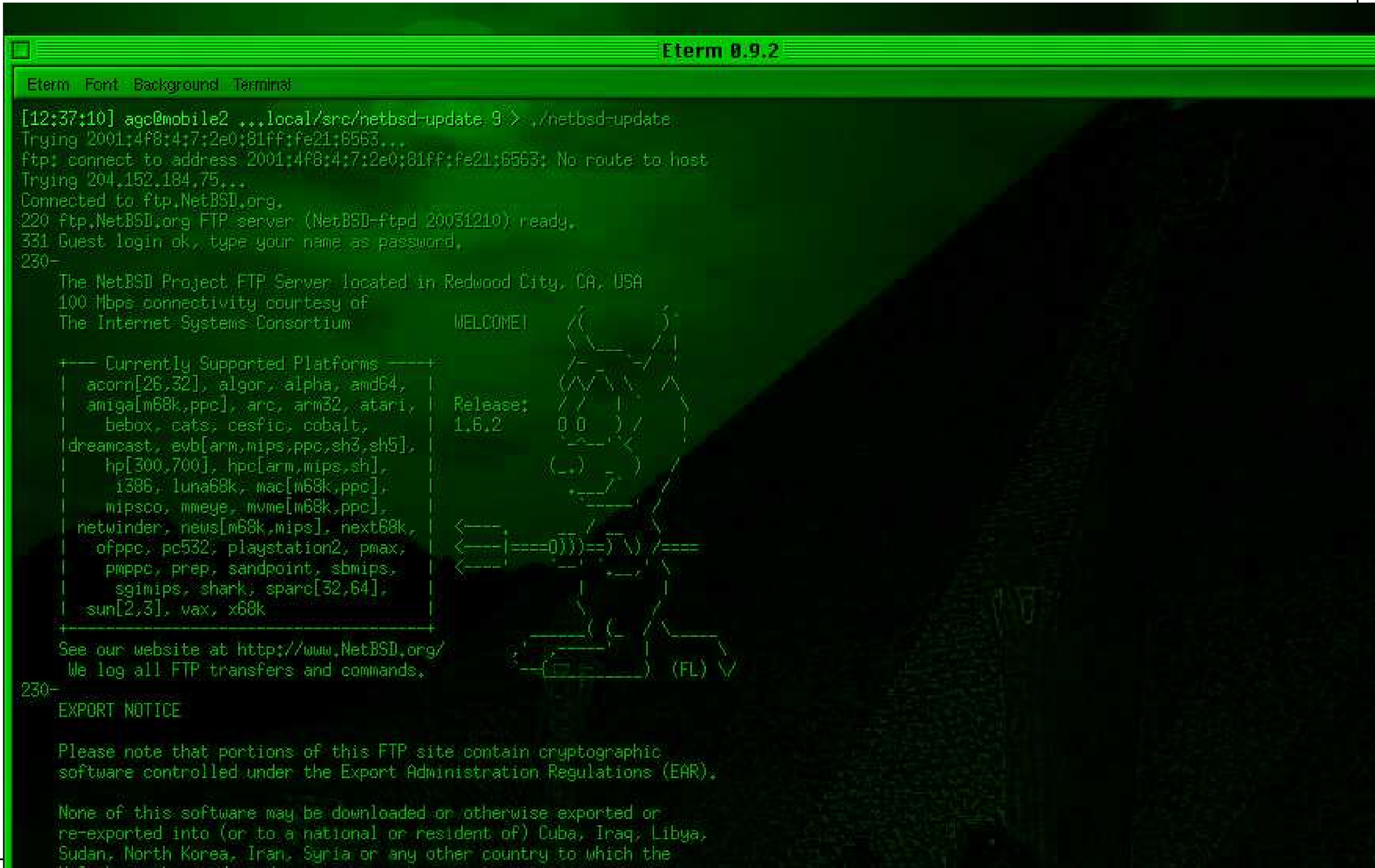
Who should use it?

- Anyone who is serious about security

Who should use it?

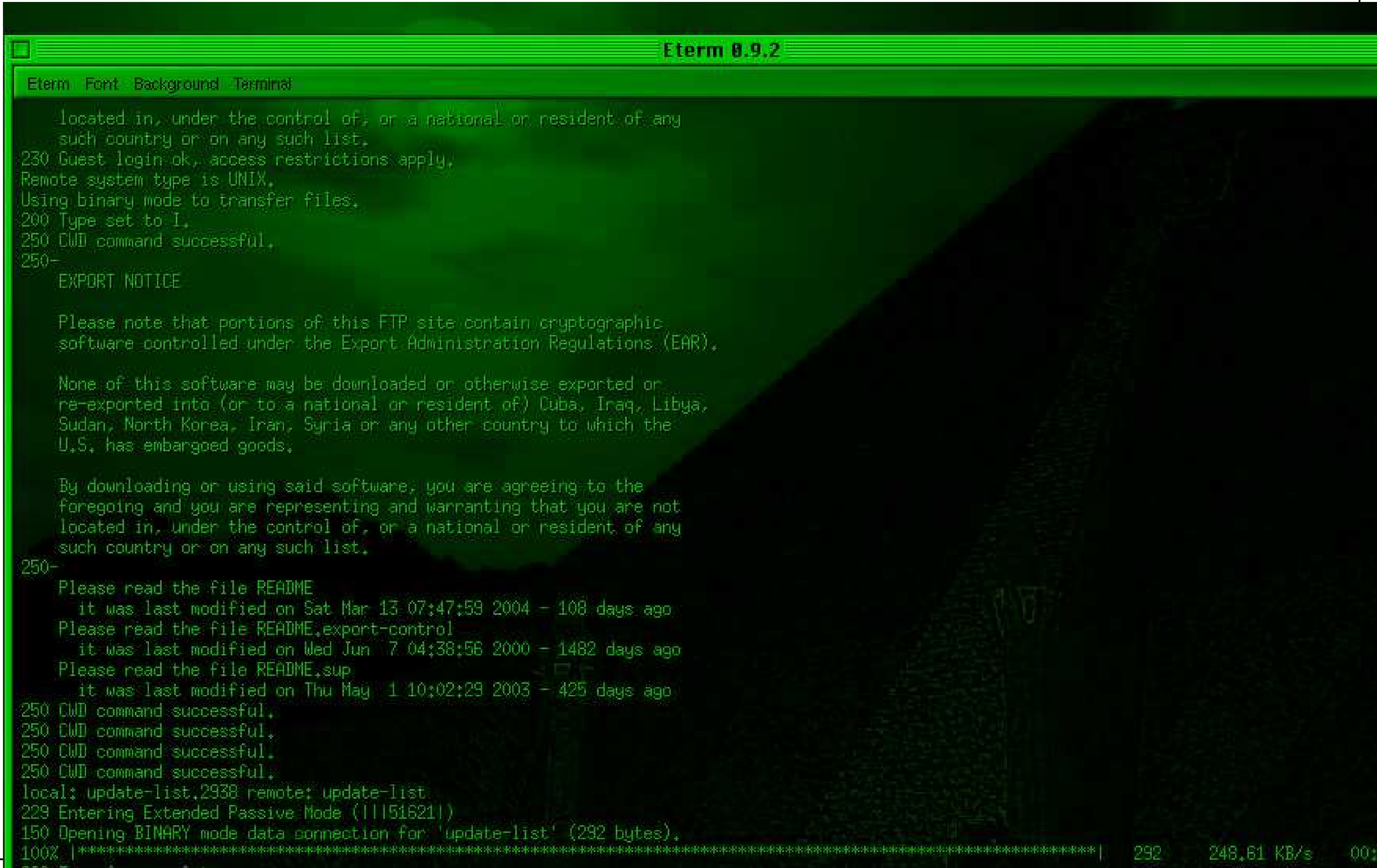
- Anyone who is serious about security

NetBSD Update in Action (1)



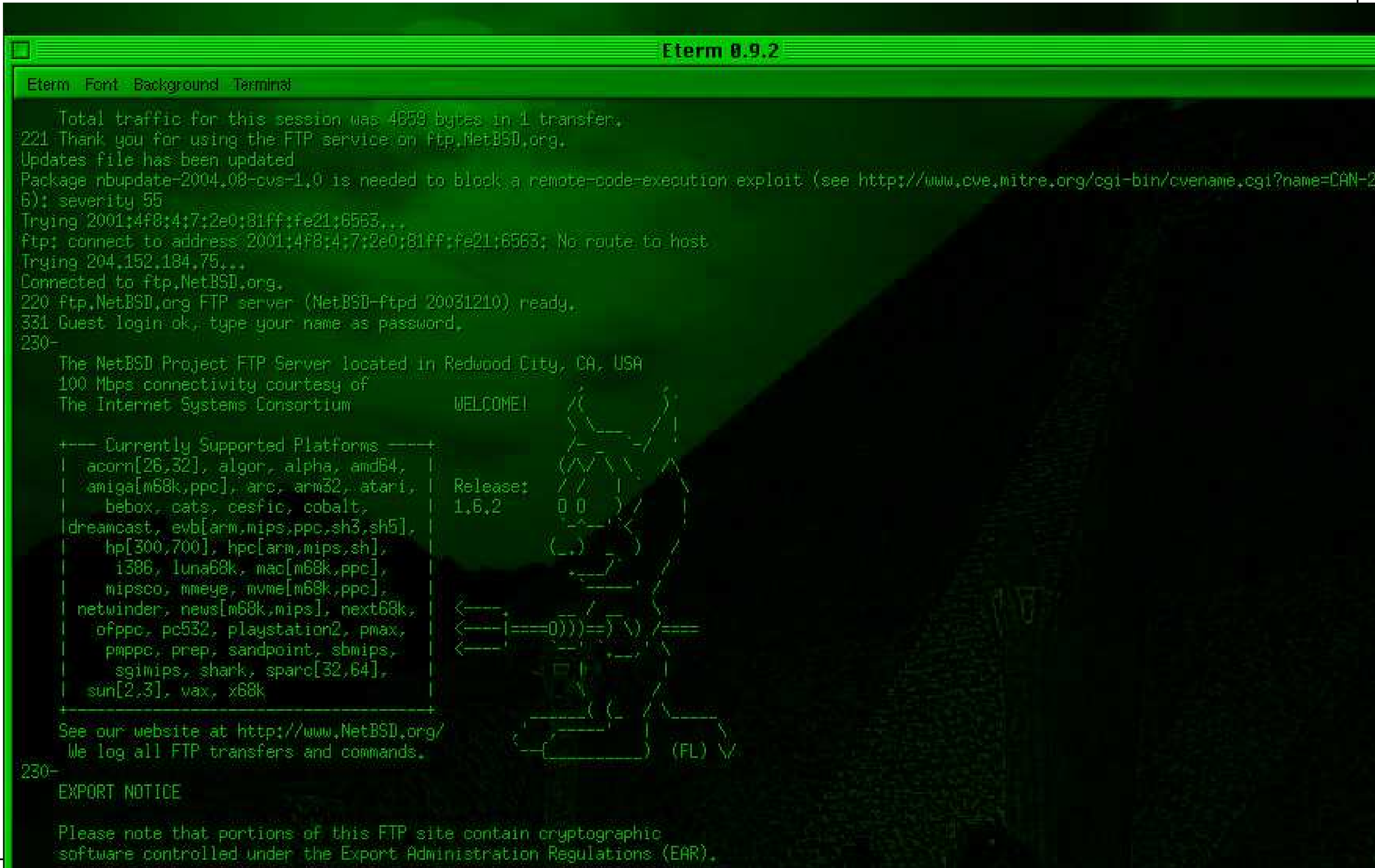
```
[12:37:10] agc@mobile2 ...local/src/netbsd-update 9 > ./netbsd-update
Trying 2001:4f8:4:7:2e0:81ff:fe21:6563...
ftp: connect to address 2001:4f8:4:7:2e0:81ff:fe21:6563: No route to host
Trying 204.152.184.75...
Connected to ftp.NetBSD.org.
220 ftp.NetBSD.org FTP server (NetBSD-ftpd 20031210) ready.
331 Guest login ok, type your name as password.
230-
    The NetBSD Project FTP Server located in Redwood City, CA, USA
    100 Mbps connectivity courtesy of                      ,        ,
    The Internet Systems Consortium           WELCOME!    /(        )`
                                                          \ \___   / |
    +--- Currently Supported Platforms -----+             /- _  `-/  '
    |  acorn[26,32], algor, alpha, amd64,   |            (/\/ \ \   /\
    |  amiga[m68k,ppc], arc, arm32, atari,  | Release:   / /   |  `    \
    |    bebox, cats, cesfic, cobalt,       | 1.6.2      O O   ) /    |
    |dreamcast, evb[arm,mips,ppc,sh3,sh5],  |            `-^--'`<     '
    |    hp[300,700], hpc[arm,mips,sh],     |           (_.)  _  )   /
    |     i386, luna68k, mac[m68k,ppc],     |            `.___/`    /
    |    mipsco, mmeye, mvme[m68k,ppc],     |              `-----' /
    | netwinder, news[m68k,mips], next68k,  | <----.     __ / __   \
    |   ofppc, pc532, playstation2, pmax,   | <----|====O)))==) \) /====
    |    pmppc, prep, sandpoint, sbmips,    | <----'    `--' `.__,' \
    |     sgimips, shark, sparc[32,64],     |              |        |
    |  sun[2,3], vax, x68k                  |               \       /
    +---------------------------------------+         ______( (_  / \______
    See our website at http://www.NetBSD.org/       ,'  ,-----'   |        \
     We log all FTP transfers and commands.         `--{__________)  (FL)  \/
230-
    EXPORT NOTICE

    Please note that portions of this FTP site contain cryptographic
    software controlled under the Export Administration Regulations (EAR).

    None of this software may be downloaded or otherwise exported or
    re-exported into (or to a national or resident of) Cuba, Iraq, Libya,
    Sudan, North Korea, Iran, Syria or any other country to which the
```

NetBSD Update in Action (2)



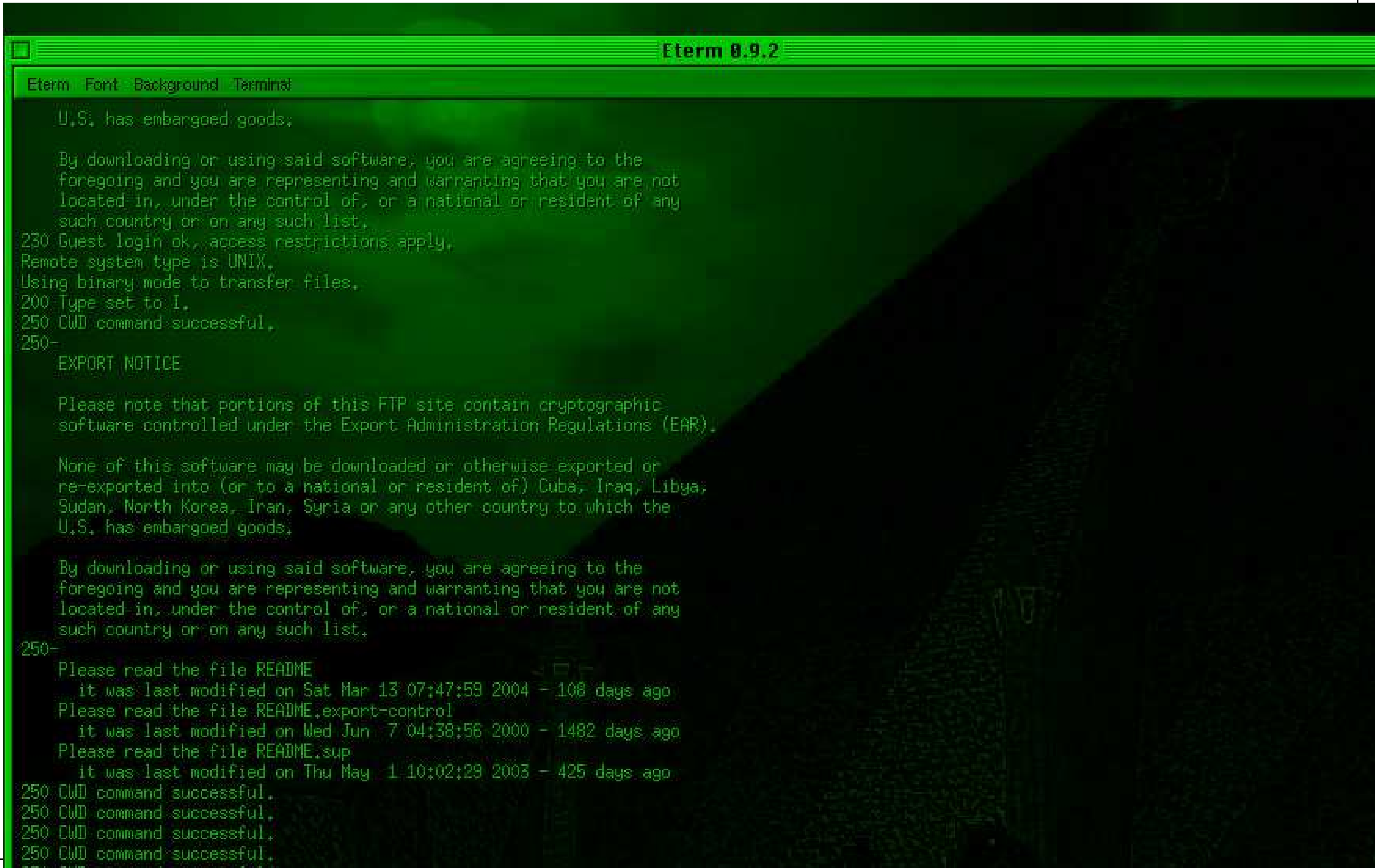
```
    located in, under the control of, or a national or resident of any
    such country or on any such list.
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
200 Type set to I.
250 CWD command successful.
250-
    EXPORT NOTICE

    Please note that portions of this FTP site contain cryptographic
    software controlled under the Export Administration Regulations (EAR).

    None of this software may be downloaded or otherwise exported or
    re-exported into (or to a national or resident of) Cuba, Iraq, Libya,
    Sudan, North Korea, Iran, Syria or any other country to which the
    U.S. has embargoed goods.

    By downloading or using said software, you are agreeing to the
    foregoing and you are representing and warranting that you are not
    located in, under the control of, or a national or resident of any
    such country or on any such list.
250-
    Please read the file README
      it was last modified on Sat Mar 13 07:47:59 2004 - 108 days ago
    Please read the file README.export-control
      it was last modified on Wed Jun  7 04:38:56 2000 - 1482 days ago
    Please read the file README.sup
      it was last modified on Thu May  1 10:02:29 2003 - 425 days ago
250 CWD command successful.
250 CWD command successful.
250 CWD command successful.
250 CWD command successful.
local: update-list.2938 remote: update-list
229 Entering Extended Passive Mode (|||51621|)
150 Opening BINARY mode data connection for 'update-list' (292 bytes).
100% |************************************************************************************************************|   292     248.61 KB/s    00
```

NetBSD Update in Action (3)



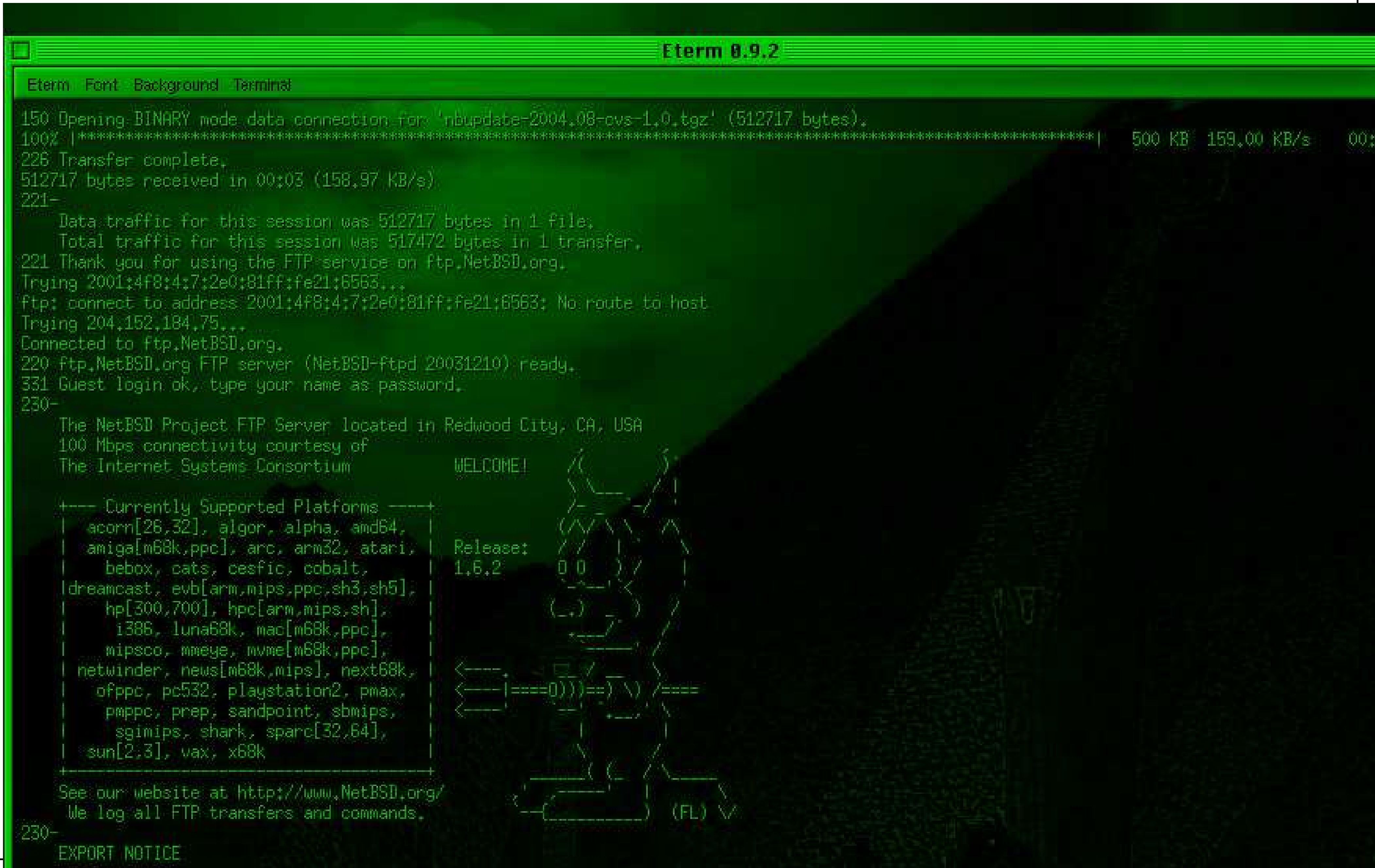
```
    Total traffic for this session was 4859 bytes in 1 transfer.
221 Thank you for using the FTP service on ftp.NetBSD.org.
Updates file has been updated
Package nbupdate-2004.08-cvs-1.0 is needed to block a remote-code-execution exploit (see http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2
6): severity 55
Trying 2001:4f8:4:7:2e0:81ff:fe21:6563...
ftp: connect to address 2001:4f8:4:7:2e0:81ff:fe21:6563: No route to host
Trying 204.152.184.75...
Connected to ftp.NetBSD.org.
220 ftp.NetBSD.org FTP server (NetBSD-ftpd 20031210) ready.
331 Guest login ok, type your name as password.
230-
    The NetBSD Project FTP Server located in Redwood City, CA, USA
    100 Mbps connectivity courtesy of
    The Internet Systems Consortium           WELCOME!

    +---- Currently Supported Platforms -----+
    |  acorn[26,32], algor, alpha, amd64,    |
    |  amiga[m68k,ppc], arc, arm32, atari,   |  Release:
    |    bebox, cats, cesfic, cobalt,        |  1.6.2
    |dreamcast, evb[arm,mips,ppc,sh3,sh5],   |
    |    hp[300,700], hpc[arm,mips,sh],      |
    |     i386, luna68k, mac[m68k,ppc],      |
    |    mipsco, mmeye, mvme[m68k,ppc],      |
    | netwinder, news[m68k,mips], next68k,   |
    |   ofppc, pc532, playstation2, pmax,    |
    |    pmppc, prep, sandpoint, sbmips,     |
    |     sgimips, shark, sparc[32,64],      |
    |  sun[2,3], vax, x68k                   |
    +----------------------------------------+
    See our website at http://www.NetBSD.org/
     We log all FTP transfers and commands.                       (FL)
230-
    EXPORT NOTICE

    Please note that portions of this FTP site contain cryptographic
    software controlled under the Export Administration Regulations (EAR).
```

NetBSD Update in Action (4)



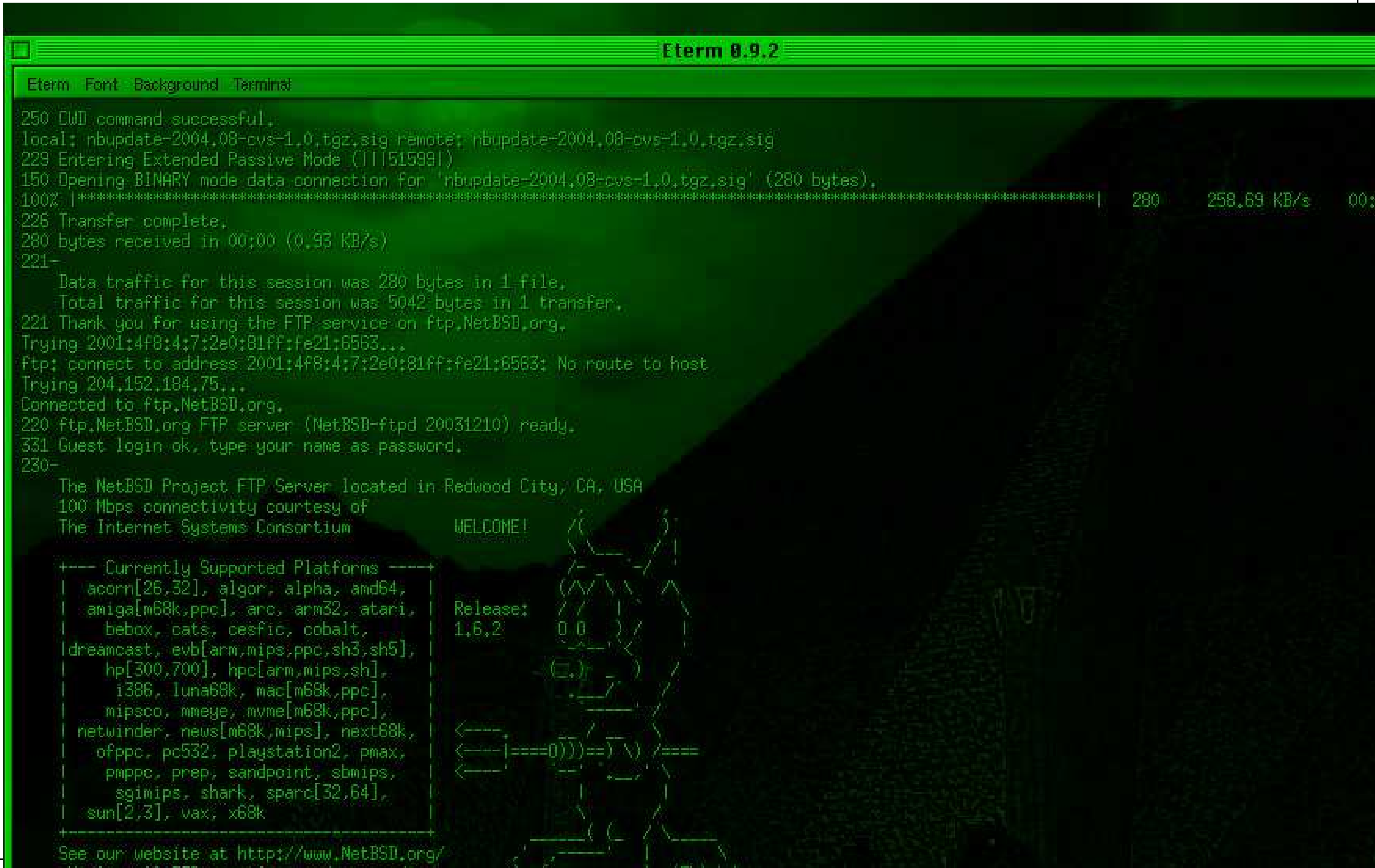
```
    U.S. has embargoed goods.

    By downloading or using said software, you are agreeing to the
    foregoing and you are representing and warranting that you are not
    located in, under the control of, or a national or resident of any
    such country or on any such list.
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
200 Type set to I.
250 CWD command successful.
250-
    EXPORT NOTICE

    Please note that portions of this FTP site contain cryptographic
    software controlled under the Export Administration Regulations (EAR).

    None of this software may be downloaded or otherwise exported or
    re-exported into (or to a national or resident of) Cuba, Iraq, Libya,
    Sudan, North Korea, Iran, Syria or any other country to which the
    U.S. has embargoed goods.

    By downloading or using said software, you are agreeing to the
    foregoing and you are representing and warranting that you are not
    located in, under the control of, or a national or resident of any
    such country or on any such list.
250-
    Please read the file README
      it was last modified on Sat Mar 13 07:47:59 2004 - 108 days ago
    Please read the file README.export-control
      it was last modified on Wed Jun  7 04:38:56 2000 - 1482 days ago
    Please read the file README.sup
      it was last modified on Thu May  1 10:02:29 2003 - 425 days ago
250 CWD command successful.
250 CWD command successful.
250 CWD command successful.
250 CWD command successful.
```

NetBSD Update in Action (5)



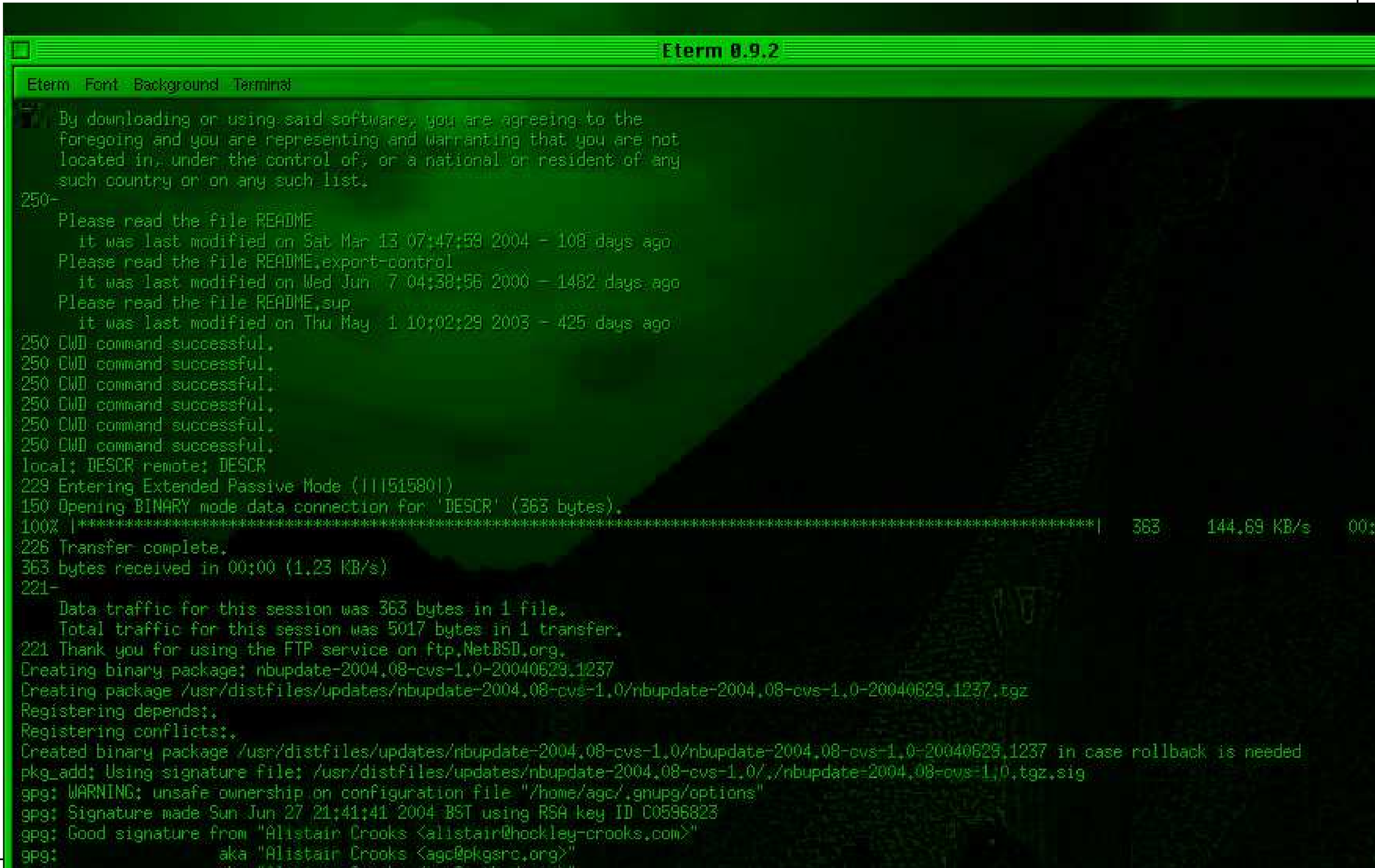
```
150 Opening BINARY mode data connection for 'nbupdate-2004.08-cvs-1.0.tgz' (512717 bytes).
100% |************************************************************************************************************|   500 KB  159.00 KB/s    00:
226 Transfer complete.
512717 bytes received in 00:03 (158.97 KB/s)
221-
    Data traffic for this session was 512717 bytes in 1 file.
    Total traffic for this session was 517472 bytes in 1 transfer.
221 Thank you for using the FTP service on ftp.NetBSD.org.
Trying 2001:4f8:4:7:2e0:81ff:fe21:6563...
ftp: connect to address 2001:4f8:4:7:2e0:81ff:fe21:6563: No route to host
Trying 204.152.184.75...
Connected to ftp.NetBSD.org.
220 ftp.NetBSD.org FTP server (NetBSD-ftpd 20031210) ready.
331 Guest login ok, type your name as password.
230-
    The NetBSD Project FTP Server located in Redwood City, CA, USA
    100 Mbps connectivity courtesy of                      ,        ,
    The Internet Systems Consortium           WELCOME!    /(        )`
                                                          \ \___   / |
    +---- Currently Supported Platforms ----+             /- _  `-/  '
    |  acorn[26,32], algor, alpha, amd64,   |            (/\/ \ \   /\
    |  amiga[m68k,ppc], arc, arm32, atari,  | Release:   / /   | `    \
    |    bebox, cats, cesfic, cobalt,       | 1.6.2      O O   ) /    |
    |dreamcast, evb[arm,mips,ppc,sh3,sh5], |            `-^--'`<     '
    |    hp[300,700], hpc[arm,mips,sh],     |           (_.)  _  )   /
    |     i386, luna68k, mac[m68k,ppc],     |            `.___/`    /
    |    mipsco, mmeye, mvme[m68k,ppc],     |              `-----' /
    | netwinder, news[m68k,mips], next68k,  | <----.     __ / __   \
    |   ofppc, pc532, playstation2, pmax,   | <----|====O)))==) \) /====
    |    pmppc, prep, sandpoint, sbmips,    | <----'    `--' `.__,' \
    |     sgimips, shark, sparc[32,64],     |              |        |
    |  sun[2,3], vax, x68k                  |               \       /
    +---------------------------------------+         ______( (_  / \______
    See our website at http://www.NetBSD.org/       ,'  ,-----'   |        \
     We log all FTP transfers and commands.         `--{__________)  (FL) \/
230-
    EXPORT NOTICE
```

NetBSD Update in Action (6)



```
250 CWD command successful.
local: nbupdate-2004.08-cvs-1.0.tgz.sig remote: nbupdate-2004.08-cvs-1.0.tgz.sig
229 Entering Extended Passive Mode (|||51599|)
150 Opening BINARY mode data connection for 'nbupdate-2004.08-cvs-1.0.tgz.sig' (280 bytes).
100% |***************************************************************************************|   280     258.69 KB/s    00:
226 Transfer complete.
280 bytes received in 00:00 (0.93 KB/s)
221-
    Data traffic for this session was 280 bytes in 1 file.
    Total traffic for this session was 5042 bytes in 1 transfer.
221 Thank you for using the FTP service on ftp.NetBSD.org.
Trying 2001:4f8:4:7:2e0:81ff:fe21:6563...
ftp: connect to address 2001:4f8:4:7:2e0:81ff:fe21:6563: No route to host
Trying 204.152.184.75...
Connected to ftp.NetBSD.org.
220 ftp.NetBSD.org FTP server (NetBSD-ftpd 20031210) ready.
331 Guest login ok, type your name as password.
230-
    The NetBSD Project FTP Server located in Redwood City, CA, USA
    100 Mbps connectivity courtesy of
    The Internet Systems Consortium             WELCOME!

    +--- Currently Supported Platforms -----+
    |  acorn[26,32], algor, alpha, amd64,   |
    |  amiga[m68k,ppc], arc, arm32, atari,  |  Release:
    |    bebox, cats, cesfic, cobalt,       |  1.6.2
    |dreamcast, evb[arm,mips,ppc,sh3,sh5],  |
    |    hp[300,700], hpc[arm,mips,sh],     |
    |     i386, luna68k, mac[m68k,ppc],     |
    |    mipsco, mmeye, mvme[m68k,ppc],     |
    | netwinder, news[m68k,mips], next68k,  |
    |   ofppc, pc532, playstation2, pmax,   |
    |    pmppc, prep, sandpoint, sbmips,    |
    |     sgimips, shark, sparc[32,64],     |
    |  sun[2,3], vax, x68k                  |
    +---------------------------------------+
    See our website at http://www.NetBSD.org/
```

NetBSD Update in Action (7)



```
    By downloading or using said software, you are agreeing to the
    foregoing and you are representing and warranting that you are not
    located in, under the control of, or a national or resident of any
    such country or on any such list.
250-
    Please read the file README
      it was last modified on Sat Mar 13 07:47:59 2004 - 108 days ago
    Please read the file README.export-control
      it was last modified on Wed Jun  7 04:38:56 2000 - 1482 days ago
    Please read the file README.sup
      it was last modified on Thu May  1 10:02:29 2003 - 425 days ago
250 CWD command successful.
250 CWD command successful.
250 CWD command successful.
250 CWD command successful.
250 CWD command successful.
250 CWD command successful.
local: DESCR remote: DESCR
229 Entering Extended Passive Mode (|||51580|)
150 Opening BINARY mode data connection for 'DESCR' (363 bytes).
100% |************************************************************************************************************|   363     144.69 KB/s    00:
226 Transfer complete.
363 bytes received in 00:00 (1.23 KB/s)
221-
    Data traffic for this session was 363 bytes in 1 file.
    Total traffic for this session was 5017 bytes in 1 transfer.
221 Thank you for using the FTP service on ftp.NetBSD.org.
Creating binary package: nbupdate-2004.08-cvs-1.0-20040629.1237
Creating package /usr/distfiles/updates/nbupdate-2004.08-cvs-1.0/nbupdate-2004.08-cvs-1.0-20040629.1237.tgz
Registering depends:.
Registering conflicts:.
Created binary package /usr/distfiles/updates/nbupdate-2004.08-cvs-1.0/nbupdate-2004.08-cvs-1.0-20040629.1237 in case rollback is needed
pkg_add: Using signature file: /usr/distfiles/updates/nbupdate-2004.08-cvs-1.0/./nbupdate-2004.08-cvs-1.0.tgz.sig
gpg: WARNING: unsafe ownership on configuration file "/home/agc/.gnupg/options"
gpg: Signature made Sun Jun 27 21:41:41 2004 BST using RSA key ID C0596823
gpg: Good signature from "Alistair Crooks <alistair@hockley-crooks.com>"
gpg:                 aka "Alistair Crooks <agc@pkgsrc.org>"
```

Future Work

- replace gpg with BSD-licensed tool
- new pkg tools can use an internal digital signature
- bundle downloaded components together per-update?

Status of Work

- □Infrastructure is installed on ftp.NetBSD.org
- □NetBSD pkgsrc entry for netbsd-update
- □NetBSD pkgsrc entry for building a new update package

The End

Any Questions?

Alistair G. Crooks
agc@netbsd.org

agc@pkgsrc.org

The NetBSD Project

Personal
self@alistaircrooks.com

D415 9DEB 336D E4CC CDFA 00CD 1B68 DCFC C059 6823

Mon Jul 5 22:42:58 BST 2004

Contact details

Alistair G. Crooks
agc@netbsd.org

agc@pkgsrc.org

The NetBSD Project

Personal
self@alistaircrooks.com

D415 9DEB 336D E4CC CDFA 00CD 1B68 DCFC C059 6823

Mon Jul 5 22:42:58 BST 2004