

Home Page

Title Page



Page 1 of 13

Go Back

Full Screen

Close

Quit

Linux as Forensic platform of choice

Jonathan C. Busey

busey@cs.fsu.edu

April 29, 2003

Overview

- advantages
- common tools
- command concatenation
- specialty software

Home Page

Title Page



Page 2 of 13

Go Back

Full Screen

Close

Quit

Advantages of Linux for forensic investigation

- freely available
- runs on nearly every platform
- forensic examination thrives in open source environment
 - easily controlled environment
 - simply made into a bootable cdrom kit
 - security holes widely published (e.g. NTFS partitions)
- over 30 supported filesystem types:

Advantages (II)

- - Extended Filesystems - ext, ext2, ext3
- Reiser Filesystem - reiserfs
- Amiga Fast Filesystem - affs
- High Performance Filesystem - hpfs (OS/2)
- ISO 9660 Filesystem - iso9660
- Minix Filesystem - Minix
- FAT 16 bit - msdos
- Virtual Fat Filesystem - vfat
- Network Filesystem - NFS
- Novell Filesystem - NCPFS (Novell)
- System V Filesystem - sysv (System V Unix variants)
- Uniform Filesystem - ufs (BSD, Solaris, NeXTStep)
- UMSDOS Filesystem - umsdos (Unix filesystem on DOS)
- linuxswap, adfs, autofs, coherent, cramfs, devpts, efs, hfs, jfs, ntfs, proc, qnx4, romfs, smbfs, tmpfs, udf, xenix, xfs, xiafs, loopback and
- RAID, LVM, “distributed filesystems” (exported over network, e.g.Coda, OpenAFS)

Home Page

Title Page



Page 3 of 13

Go Back

Full Screen

Close

Quit

Home Page

Title Page



Page 4 of 13

Go Back

Full Screen

Close

Quit

Standard tools

- `find`
- `strings`
- `stat`
- `dd (fsgrab)`
- `debugfs`
- `md5sum`

Home Page

Title Page



Page 5 of 13

Go Back

Full Screen

Close

Quit

Examples-mounted `/dev/mem` image

Home Page

Title Page



Page 6 of 13

Go Back

Full Screen

Close

Quit

Examples-strings

Home Page

Title Page



Page 7 of 13

Go Back

Full Screen

Close

Quit

concatenating commands: `ls`, `stat`, and `find`

Home Page

Title Page



Page 8 of 13

Go Back

Full Screen

Close

Quit

Specialty software

TASK • Linux

- Mac OS X
- Open & FreeBSD
- Solaris

Autopsy

chkrootkit <http://www.chkrootkit.org/>

TCT The Coroner's Toolkit

Home Page

Title Page



Page 9 of 13

Go Back

Full Screen

Close

Quit

Autopsy screenshot

Home Page

Title Page



Page 10 of 13

Go Back

Full Screen

Close

Quit

Autopsy screenshot

Home Page

Title Page



Page 11 of 13

Go Back

Full Screen

Close

Quit

Autopsy screenshot

Home Page

Title Page



Page 12 of 13

Go Back

Full Screen

Close

Quit

Autopsy screenshot

Home Page

Title Page



Page 13 of 13

Go Back

Full Screen

Close

Quit

Links to forensics with Linux

- <http://www.atstake.com>
- <http://www.linux-sec.net/Tracking>
- <http://cert.uni-stuttgart.de/forensics>
- <http://www.cerias.purdue.edu/homes/carrier/forensics>