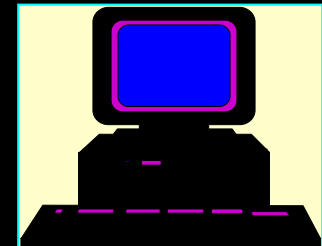


Linux Os, Networking and Forensics

**Rockland County Sheriff Dept
55 New Hempstead Rd
New City NY 10956
Computer Crime Unit
Sheriff James Kralik
Shlomo Koenig CFCE SCERS CFE
Tel 914-638-5415
Depshlomo@fcc.net**



Linux



- A Operating System
- A Networking System
- A Forensics Tool

Parts of the System



- Hardware
- Kernel
- Modules
- Devices
- Shell

Run Levels And Permissions

- Rights and Permissions
- Absolute `rwx rwx rwx s`
- Relative `4777`
- `umask`
- `#` Root Command Prompt
- `$` User Command Prompt
- Run Levels
- `0 -5` Text `6` Gui

Path



- The path is set in the `/etc/profile`
 - and every user can have there `/profile`
 - absolute vs relative
 - `/` .

passwd,



- User list, passwords, and group and user memberships Rights UID and GUID
- File Application and User Rights
- Shadow password file
- located in /etc

File Types



- d Directory
- Data and Text files
- Binary Files
- dev files
- block
- l Symbolik Links
- case sensitive very important
- Makefile makefile

File types



- `.c` or `cc` source file
- `.o` object the output of a compiled `.c` exe
- `.H` header
- `.L` or `.a` library
- `.d` daemons
- block
- character
- link

mtab fstab, vfstab mnttab

- File system mount configuration information
- Local / remote mounts and where data is stored
- mtab
- The list of current mounted Devices
- mnttab vfstab for solaris
- current mounted and auto mount

Logs



- `/VAR/LOG`
- `dmesg dmesg |more`
- Messages
 - Has Start up info
- `/var/log/wtmp` has login in info
- last command to see
 - - 10 for last 10 - userid for his logins
- `/var/run/utmp` has the current users

LOGS



- **SYSLOG**
 - logins , errors, emrg, and different
 - notices that are set up thru `syslog.conf`
 - are stored here
- **history** has the last 500 typed lines
 - `history` to see

Mounting Files



- Mount
- Umount
- mount to Showmount
- Switches
 - -r
 - -w
- Mount Points

Device Files



- **Linux**
 - `hd /dev/hda-b` for physical
 - `hd /dev/hda1` for logical
 - `scsi /dev/sda`
 - `tape /dev/sta nsta` for no rewind
- **Solaris**
- `c0t0d0s0` in `dev/rsdk` directory

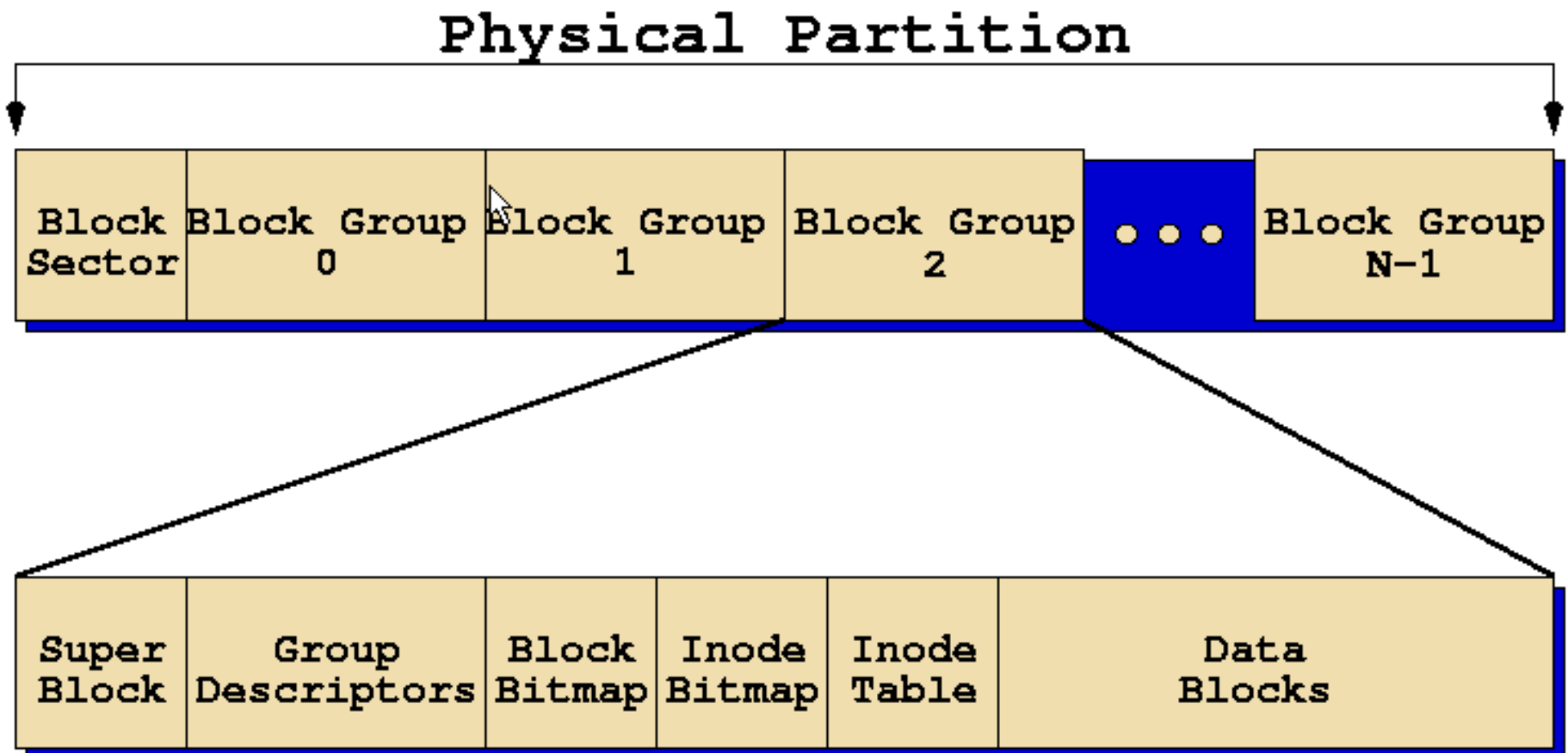
The File system



- Uses Inodes
- Super Blocks
- Direct and Indirect Inodes
- Inode Bit Maps
- Inode blocks
- Data Blocks



The *ext2* Physical Structure





Super Block	Group Descriptors	Block Bitmap	Inode Bitmap	Inode Table	Data Blocks
--------------------	--------------------------	---------------------	---------------------	--------------------	--------------------

Magic Number
Revision Level
Mount Count & Maximum Mount Count
Block Group Number
Block Size
Blocks per Group
Free Blocks
Free Inodes
First Inode

An Example Of An Inode

```
lde v2.4.pre1 : ext2fs : /dev/hda2  
Inode:          2 (0x00000002)  Block:          0 (0x00000000)  012345678910
```

```
drwxr-xr-x  25 root      root          1024  Thu Jan  7 08:46:58 1999
```

```
TYPE: directory      LINKS: 25          DIRECT BLOCKS= 0x00000107  
MODE: \0755          FLAGS: \04  
UID: 00000(root)     GID: 00000(root)  
SIZE: 1024           SIZE(BLKS): 2
```

```
ACCESS TIME:         Wed Feb  3 10:23:58 1999  
CREATION TIME:       Thu Jan  7 08:46:58 1999  
MODIFICATION TIME:  Thu Jan  7 08:46:58 1999  
DELETION TIME:       Wed Dec 31 19:00:00 1969
```

```
INDIRECT BLOCK=  
2x INDIRECT BLOCK=  
3x INDIRECT BLOCK=
```

```
F1/? for help. F2/^0 for menu. Q to quit
```

Data BLOCK:

How Directory Entries Are Stored

```
lde v2.4.pre1 : ext2fs : /dev/hda2
Inode:          2 (0x00000002)  Block:          263 (0x00000107)  0123456789!
00041C00  02 00 00 00 0C 00 01 00 : 2E 00 00 00 02 00 00 00  .....
00041C10  0C 00 02 00 2E 2E 00 00 : 0B 00 00 00 14 00 0A 00  .....
00041C20  6C 6F 73 74 2B 66 6F 75 : 6E 64 00 00 F9 07 00 00  lost+found.
00041C30  0C 00 04 00 68 6F 6D 65 : F1 0F 00 00 0C 00 03 00  ....home...
00041C40  75 73 72 00 E9 17 00 00 : 0C 00 03 00 76 61 72 00  usr.....
00041C50  E1 1F 00 00 10 00 05 00 : 77 69 6E 39 38 00 00 00  .....win
00041C60  D9 27 00 00 0C 00 03 00 : 64 65 76 00 D1 2F 00 00  .`.....dev
00041C70  0C 00 03 00 65 74 63 00 : C9 37 00 00 0C 00 03 00  ....etc..7.
00041C80  74 6D 70 00 E9 47 00 00 : 0C 00 03 00 62 69 6E 00  tmp..G....
00041C90  B1 4F 00 00 0C 00 04 00 : 62 6F 6F 74 A1 5F 00 00  .0.....boo
00041CA0  0C 00 03 00 6C 69 62 00 : 91 6F 00 00 0C 00 03 00  ....lib..o.
00041CB0  6D 6E 74 00 79 87 00 00 : 0C 00 04 00 70 72 6F 63  mnt.y.....
00041CC0  71 8F 00 00 0C 00 04 00 : 72 6F 6F 74 69 97 00 00  q.....roo
00041CD0  0C 00 04 00 73 62 69 6E : 11 EF 00 00 14 00 0A 00  ....sbin...
```

*Directory
Entry
Length*

*Name
Length*

*Filename
(in ASCII)*

*Inode of
Filename*

Fdisk



- Types of Files that it can Mount include
- Dos 16
- Dos 32
- Ntfs
- Hpfs Hfs
- Novell
- EXT2FS the liunx system by default
- Mkfs the Liunx Format

Modules



- Lsmmod
- Insmod
- Rmmmod
- Modprobe depmode
- IE. card.o card=0x140,1
- Installing Modules
- Configuration
- Loadable modules VS Kernel services

Inode tools and commands

- Lsdel
- r2recover
- midnight commander
- fstgrab
- xxd

Important Directories

- Mnt Lib
- proc Virtual
- etc
- sbin and /bin
- var
- root
- tmp
- usr/src

Daemons



- Runs process and programs
- starts the init
 - some include
- `init.d`
- `profile.`, `rc.d`, 1 - 6
- `inetd.d`,
- `nsswitch.d` for remote authentication for secure net

Environments

- `.Profile` for env information in `/etc`
- `set` to display
- `.bashrc` for alias's IE.
- `alias ls="ls -aF --color`
- `alias dir="bin/ls -af "`
- `.rc` run command
- `echo $PATH` to see path
- `echo $SHELL` to see shell version

Profiles



- `.profile`
- profile scripts I.e. logon sign and home dir
- `etc/shells` list allowable shells
- `profile.d` demaon
- `/etc/skel` template file

Inittab



- Configures the init daemons
- `etc/inittab` to set default init levels
- and can restrict init 1
- is called by the `init.d` demaon

inetd.conf



- A Network Demaon
- Gives list of what programs are listening on the net
- Where the binaries are located
- in /etc

rc.local



- . Programs started on boot
- May need to examine carefully
 - To eliminate normal programs
 - To find abnormal programs in rc.local (syslog)
- What the . Does
- /etc/rc.d
- the run script files
- numbering and sa ,k types

Starup and ShutDown



- Lilo
- Loadlin
- Bootdisk
- Partition magic
- Shutdown - * now
 - h -r -9

Meta Characters

- Pipe
- tee
- >
- >>
- <
- ~
- {}

Useful Commands

- Man Howto Pwd uname
- which Locate whereis
- Stat ls file
- more less cat
- cp dd md5sum
- find grep Sort
- mv ps kill
- wc head / tail diff
- du df chmod Strings

PWD



- `pwd` to see current directory

WHICH



- which “ls”
- shows where the ls command is located
 - it searches the path
 - it won't show if not in the path

Stat



- `stat file`

- gives the inode information for a file

LS



- `ls` is a directory listing like `dir`
 - some switches
 - `-R` recursive
 - `-a` all including hidden
 - `-l` long name
 - `-i` inode
 - `-f` uses the file command

LS



- *ls -Lran*
- *L* long file
- *R* recurse
- *A* Hidden
- *n* number for uid name

- *ls -la [a-g] or B-G b-g]*

Sort



- Sorts files
 - -m merges the sorted file
 - -I ignores case
 - -k pos1 to sort on field 2 or pos2
 - -o output file
 - sort +4 -n for numerical order
 - -r reverse order

file



- Tries to identify a file's contents
 - `file /bin/ls`
 - Use the file header
 - searches the magic file

More and Less

- Displays files one page at a time
 - Useful as the end of a "pipe"

CHMOD



- Changes file permissions
 - `chmod 660 foo.txt`
 - `-r` for recursive
 - Chown
 - `uid gid and ~ directory`

Cat



- `Cat` prints a file to the screen
- `cat foo.txt`
 - the output can be piped to a second
 - command

ps kill



- Gives a list of processes currently running
 - `ps -aux`
 - `ps -delf`

 - Kill to stop Process

/PROC



- Cpuinfo
- mounts
- Scsi

- A virtual file system

UNAME



- `uname -a` to see system info

DU



- Gives you used disk space of a file
 - -a files
 - -k in kilobytes
 - -sm sum in megs
- `du /dev/had1 -sm >hdausage.txt`

df



- Gives a list of disks and how much of their space is free
- -k kilobyte size
- -h human readable
- -T file system type -t msdos for only dos
- `df /dev/hdb1`

MD5SUM



- A hash program
- `md5sum /dev/hda1 > hda1hash.txt`

DD



- Disk dump
 - a disk bit dump
 - can be used as a imaging tool
- `dd if=/home/foo.txt of=/dev/fd0`
 - `-bs` gives the block size
 - and can use the count command
 - `count 1`
 - 2 gig limit on logical but not physical level

find



- `find`- Find files by name and / or other attributes
- `find /etc -name '*.cf' -print`
- `-name` `-type`
- `-mtime` `f` `file`
- `-ctime`
- `-atime`
- `-exec`

Find



- `Find / -name >file`
- `find -type f -exec grep "hello" >file`
- `find -type f -exec grep -ilf /listfile { } \; >file`
- `find / -mtime -90 \(-name "*.ps" -o -name "*.doc" -o -name "*.DOC" -o -name "*.xls" -o -name "*.XLS" -o -name "*.pdf" -o -name "*.PDF" -o -name "*.ppt" -o -name "*.PPT" \) -exec ls -l { } \; >f.res 2>/dev/null`
- for files in the last 90 days

grep

- Displays all lines of a file that match the given pattern
 - Good for searching large files
 - `grep string list_of_files`
 - `-f` file list
 - `-l` prints file name
 - `-v` verbose
 - `-i` ignore case
 - `-ab` physical level binary
 - `-A2 -B2` gives you 2 lines above and below

Grep



Grep

```
Gerp "lde" /dev/hda6>file
```

```
grep -i "hello" -A1 -B2 /dev/hda6>file
```

```
grep -abi "hello /dev/hda6>file
```

```
grep abif /filelist /dev/hda6>file
```

Grep



```
find / -type f -exec grep -ilf url.txt {} \; > outp.txt
```

I ignore case

F use file

L trim header and give file name

{ } put here

\end

; next command

```
find / -type f -name *.url -exec grep abc {} \; > url.txt
```

```
find / -type f \(-name *.url -o -name *.lnk\) -exec grep abc {} \; > url.txt
```

-o other variable

Strings



```
Strings /dev/hda |grep "hello" > file
```

```
Strings /dev/hda |grep -if /filelist > file
```

```
strings /dev/hdb |grep "[1-254]\.[0-255]\.[0-255]\.[1-254]" >file
```

CHMOD



- Changes file permissions
 - `chmod 660 foo.txt`
 - `-r` for recursive
 - Chown
 - `uid gid and ~ directory`

ps kill



- Gives a list of processes currently running
 - `ps -aux`
 - `ps -delf`

 - Kill to stop Process

Compression Tools



- Tar
- Gzip
- Cpio

Tar



- A archive program
- `Tar - cvf /dev/file name .`
 - `-c` create
 - `-v` verbose
 - `-f` file
 - `.` This directory
 - `-z` to zip

untar



- To unarchive
- `tar -xvzf file name`
 - `-x` to extract
 - it will put it in the current directory

Gzip



- `Gzip -rv filename`
- `gzip -v file` to see
- `gunzip -f file`

cpio

- `Find . -print | cpio -o > dev/file`
 - it needs a input
 - or `-f` for a file name to use as input
- to unzip
- `cpio -ivt <filename`
 - `<` where to get the input
- will handle some zips tar won't

Rpm install

- Rpm -q and the package name
- -ql
- -verify
- read the README
- configure
- make ,all ,install
- make modules

Compiling a Kernel

- Cd /usr/src/linux or source
- make menuconfig
- make install
- make clean some versions
- make modules
- make modules_install
- make pcmcia if needed
- make bzImage or zImage
- cp /arch/i386/boot/bzimage /boot/vmlinuz?
- edit etc/lilo.conf run lilo

Mtools



- Dos tools
- mcopy
- mdel
- mmd
- mdir
- mcd
- Vfat Msdos

netstat



- netstat gives information about network connections
- netstat -an

last



- Gives last login times and usernames
 - `last -10 username`
 - `last -10`

Rootkit



- Very popular set of tools
- A set of backdoors, a sniffer, and system program
Tools are usually fragile
- Don't require understanding of the flaw exploited
- Can't trust programs on a compromised system
- to hide the intruder's tracks

Resources



- www.rootshell.com
- www.geek-girl.com/bugtraq
- packetstorm.securify.com