José L. Quiñones-Borrero, BS

MCP, MCSA, MCT, CEH, CEI, GCIH, GPEN

LINUX INTRO FOR SECURITY PROFESSIONALS

Got Linux?

- Linux is a free Unix-type operating system (kernel) originally created by **Linus Torvalds** with the assistance of developers around the world. Developed under the GNU General Public License , the source code for Linux is freely available to everyone.
- All freely available tools under Linux where developed under the Free Software Foundation, founded and still run by **Richard Stallman**.
- GNU/Linux consists of the kernel, drivers, programs, shell and a GUI (X + Gnome, KDE, Unity)

Boot Stuff

- /boot
  - vmlinuz.*
  - initramfs*
- GRUB (boot manager)
  - /boot/grub/grub.conf
  - Pass arguments to kernel
- Single user mode
- Rescue/Recovery mode (boot DVD/CD)

Init process (pid 1)

- init
  - init is the father of all processes. Its primary role is to create processes. Uses a scripts stored in /etc/init.d
- System V (Uses runlevels)
  - `/etc/inittab` – this is where the initialization level is set.
    - **`id:x:initdefault:`**
  - `/etc/rc.d` – init scripts directory
  - `rc.sysinit` – runs at startup
- Upstart (Does not keep track of runlevels, they are implemented by the userspace tools.
  - `/etc/init/` - configuration files
  - `/etc/init.d/` - init scripts directory
- Common
  - `/etc/{rc1.d,rc2.d,rc3.d,rc4.d,rc5.d,rc6.d}`
  - `rc.local` – runs after startup

Directory Structure

- /: root directory
- /etc: configuration files
- /boot: kernel & boot loader
- /root: root's home dir
- /bin: common shared commands
- /sbin: super user commands (root only)
- /dev: devices
- /home: user's home dir
- /lib: support & lib files
- /proc: runtime system info (not a dir)
- /tmp: temporary files
- /usr: home dir for apps
- /var: variable data (logs, print spools, …)
- /mnt: old dir for mount points
- /media: automatic mount points (usb, cd-rom, …)
- /opt: optional structure

Interesting Directories

- /tmp : gets cleaned every time the system is rebooted
- /var/log : All log files are stored here
- /dev/null: null (black hole)
- /dev/zero: zero data
- /dev/urandom: random data
- /dev/shm: ram disk, files written here never touch the file system.
- /dev/mem: RAM
- /proc: it's a psudo directory with sysinfo/sysstate
- .ssh: holds the ssh keys and know hosts for the ssh
- .gnupg: holds the gpg keys for the system

Installing from binaries

- rpm [options] <filename.rpm>
  - `-i  install`
  - `-v  verbose`
  - `-U  upgrade`
  - `-e  erase`
  - `-h  hash`
  - `-q  query`
- dpkg [options] <filename.deb>
  - `-i : install`
  - `-r : remove`
  - `-l : list`

Installing using package managers

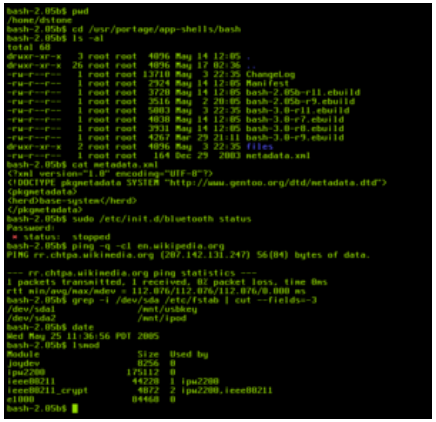
- PMs will download needed packages and install them with all dependencies.
- RPM Based systems use *yum*
  - `yum [options] <commands> package`
    - `-y`
    - `install`
    - `update`
    - `checkupdate`
  - `yum –y install package1 package2 package3`
  - `yum groupinstall "group_name"`
- DEB based systems use apt-get/aptitude
  - `apt-get`
    - `apt-get install <package>`
  - `aptitude`

Installing from source files

- Tarballs
  - `tar –vzf <tarball.tar>` - this will extract files from tarball to a directory with the same name. remember to use –z (.gz) or –j (.bz2) depending on the compression used
  - `configure` – this script will search for libraries, paths, and other information needed for compiling the software. It will create .makefile to be used by make.
  - `make` – this is the actual compilation command
  - `make install` – this will copy the files to the appropriate directories (/bin, sbin, etc …)
- Source file
  - `gcc <source.c> -o <compiled_file>`

Using the command line

- bash – born again shell
  - `.bash_history`
  - `.bashrc`
  - `/etc/bashrc` (global options)
  - `root@host#` (logged in as superuser/root UID=0)
  - `user@host$` (logged in as non-privilege user)
- Commands
  - exit
  - clear
  - reset
  - history



Help System

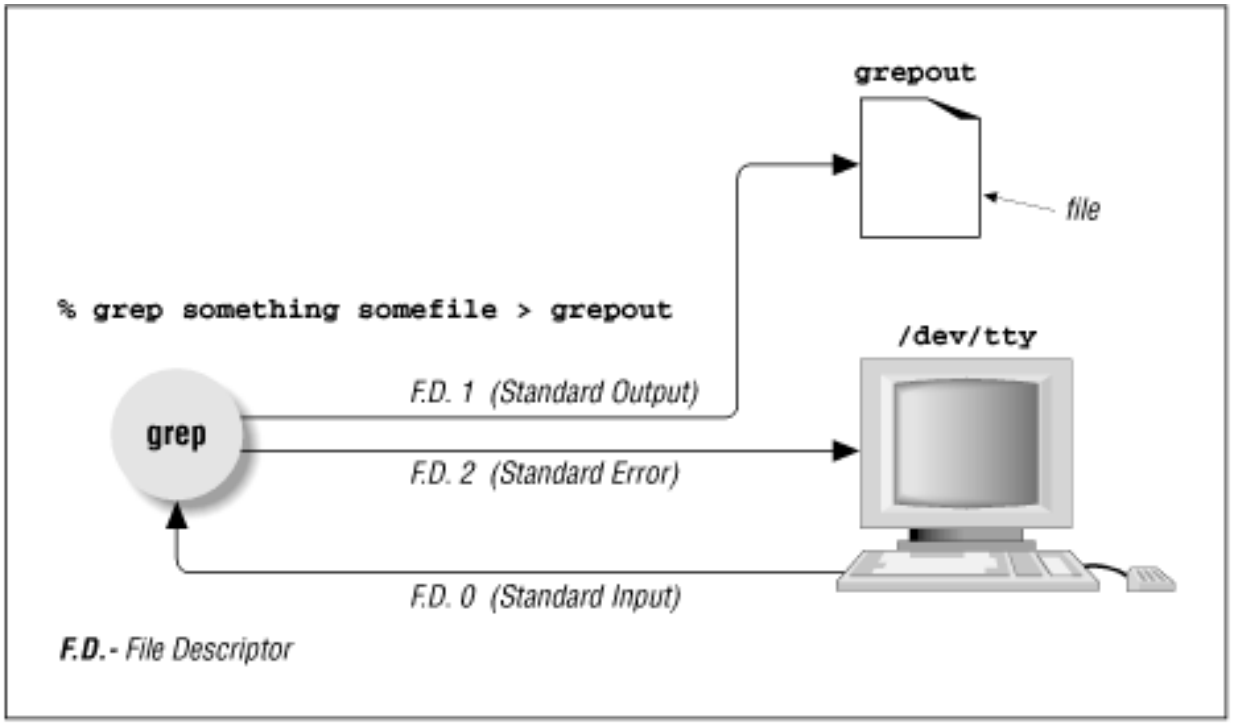
- Once you have Linux installed and running, the most important piece of information you need is how to get help.
- What are my options?
  - `(-h or --help)`
  - `whatis <command>`
  - `man`
    - `man -k <keywords>`
    - `man <section> <command>`
  - `info <command>`
- Local docs
  - `/usr/share/doc`
- The Linux Documentation Project
  - http://tldp.org/

Text File Editing

- A text editor is just like a word processor without a lot of features.
- The main use of a text editor is for writing something in plain text with no formatting so that another program can read it.
- vi – this is the universal text editor in Linux.
  - Common commands:
    - insert/replace – insert key toggle
    - :w – write
    - :q – quit
    - :! – do nothing
    - :/ - search
    - :n – search next
- Other more poweful text editors are:
  - nano, vim, gedit, kedit

Working the CLI

- stdin, stdout(1), stderr(2) and redirection
  - |
  - ||
  - &
  - &&
  - >
  - <
- Job control
  - CTRL+C
  - CTRL+Z
  - jobs
  - fg



Searching

- Search for text (strings)
  - grep {regex}
    - ^string: strictly starts with string
    - *string*: anything with string
    - string$: strictly ends with string
    - [abc]string: has a, b or c before string
    - [^abc]string: anything but a, b, or c before string
    - \.string: take it literal (escape .)
- Search for commands
  - whereis <command>
- Indexed Search (updatedb)
  - locate <file>
- Iterative search
  - find / -name string

Recon

- Memory
  - `free -m`
- Disk space usage
  - `df -h <directory>`
  - `du -sh <directory>`
- Environment
  - `set`
  - `set | grep OSTYPE`
  - `echo $PATH`
- Date & time
  - `date`
  - `ntpdate`

Recon (cont.)

- What processes are running?
  - `ps -aux`
  - `top`
  - `lsof`
  - `pstree`
- Which kernel I'm running & what modules are loaded?
  - `uname -a`
  - `lsmod`
- Hardware
  - `dmidecode`
  - `lspci`
  - `lsusb`

Recon (cont.)

- System Uptime
  - `uptime`
- SE Linux policy
  - `sestatus`
  - `genforce`
- Mount points
  - `mount [options] <device> <mount dir>`
  - `cat /etc/fstab`
  - `fdisk -l`
- Installed packages
  - `rpm -qa`
  - `yum list installed`
  - `dpkg -l`

Working with Identity

- Identity
  - `who`
  - `w`
  - `last [tty_ |<username>]`
  - `id <username>`
- Impersonate
  - `su [-, -l|-c <command>|`
  - `sudo <command>`

Managage Users & Groups

- Users
  - `useradd -m -o -u <uid> -g <groupX> -G <groupY> <username>`
  - `userdel -r <username>`
  - `usermod [options] <username>`
- Groups
  - `groupadd -g <gid> <groupname>`
  - `groupdel <groupname>`
  - `groupmod [options] <groupname>`

File Permissions

- Standard Permissions

	owner	group	others
letter	**rwx**	**rwx**	**rwx**
bin	**111**	**111**	**111**
weight	**421**	**421**	**421**
dec	**7**	**7**	**7**

- Commands
  - `chmod <permissions> <filename/directory>`
  - `chown <user> <group> <filename/directory>`
  - `chgrp <group> <filename/directory>`
- Access Control Lists
  - `getfacl`
- Umas
  - `umask -S`

Working with files/directories

- Identify file types
  - `file <filename>`
- Touching files
  - `touch <filename>`
  - `touch [-m|-a|-d] -t <STAMP> <filename>`
- View contents of a file
  - `strings`
  - `cat`
  - `tail`
  - `head`
  - `less`
  - `more`
  - `wc`

Working with files/directories (cont.)

- list files or directories
  - `ls -al`
- Manage files
  - `cp <source> <target>`
  - `mv <source< <target>`
  - `rm -rf <target>`
- Mangage directories
  - `mkdir <dir_name>`
  - `rmdir <dir_name>`
- Other
  - `pwd`
  - `~`
  - `.`
  - `..`

Strings (Text)

- Cutting text from files
  - `cut -d <delim> [-f <field#>|--fields=x,y,z …]`
- Replacing strings
  - `sed 's/string_to_find/replace_with/g'`
- sorting
  - `sort <list>`
- Echo a string to stdin
  - `echo "string"`

Cyphers

- Hashing
  - *sum family utils
    - `sha[1,256,512]sum`
    - `md5sum`
    - `cksum`
  - openssl
    - `openssl dgst -[md5|sha1|sha256|sha512] <file>`
- Encrypting
  - `openssl enc -aes256 -in <source> -out <target>`
  - `openssl enc -d -aes256 -in <source> -out echo<target>`
  - `openssl passwd <password>`

Working with processes

- Signals
  - KILL (9)
  - HUP (1)
  - TERM (15)
- Sending signals to processes
  - kill –signal <PID>
  - killall – signal <process name>
- Priority
  - nice –n # pid
  - renice –n # pid
- Other
  - lsof –p <pid>

Password File

- /etc/passwd
  - `user:salt:userid:groupid:name:homedir:defaultshell`
- saltkey + password = password hash
- Prevent login
  - `Defaultshell=/sbin/nologin or /sbin/false`
  - `usermod -L <username>`
- /etc/shadow
  - `user:$hash_algorythm$hash_value: … :`
  - Hash algorithms
    - No $#$ - DES or crypt()
    - 1 - MD5
    - 2 - Blowfish
    - 5 - SHA256
    - 6 - SHA-512

Networking

- Connectivity
  - ifconfig
    - ifconfig –a (show all interfaces)
    - ifconfig <int> <ipaddress> (assign ip address)
    - ifconfig <int> add <ipaddress> (assign secondary address)
  - ifup / ifdown scripts
  - netstat –nap (show all connections with process associated to it)
  - ping –c X <ipaddress>
- Routing
  - route add default gw <gw_ipaddress>
  - traceroute [-T|-U|-I|-p] <target>
- ARP
  - arp –a
  - arping <ip address>

Networking (cont.)

- Network connections
  - `netstat [options]`
    - `-a: all`
    - `-n: do not resolve`
    - `-p: show process`
    - `-t: show only tcp`
    - `-u: sho wonly udp`
- Firewall
  - `iptables [-L|-F]`
- CLI internet
  - `wget http://site.com/file`
  - `ftp user:password@ftp.site.com`
  - `ssh -i rsa_key user@host.domain.com -p <port>`
  - `telnet host.domian.com`

Name Resolution

- Name Resolution
  - /etc/resolv.conf
    - `nameserver <dns_ip>`
  - dig
    - `dig @<dns_ip> <domain_name> -t AXFR`
    - `dig @<dns_ip> <domain_name> -t <type_of_record>`
  - nslookup
    - `nslookup -query=<record_type> <host|domain> <dns_server>`
  - host
    - `host -t <record_type> <host/domain> <dns_ip>`

Next Time!

- Pivoting Techniques
  - ssh
  - netcat
  - bash
  - metasploit
  - routing (linux)
  - windows routing
  - proxychains

Gracias!

josequinones@codefidelio.org