Basic Linux

Original slides from GTFO Security

outline

- Linux
  - What it is?
  - Commands
  - Filesystem / Shell
  - Package Management

Services run on Linux

- mail
- dns
- web
- central authentication
- router
- database
- virtual machines
- voip
- anything

Linux

- The core of many computers and devices
  - Android
  - Ubuntu Desktop
  - Red Hat / Fedora
- Linux is a term to describe a set of tools
  - Command line programs
  - Programs such as email and websites
  - Shell scripts
  - Free and Open Source approach
  - Layout of filesystem

Linux

- Linux has distributions/variants
  - Debian/RedHat/SUSE
    - Ubuntu - Debian based
    - Mint - Debian based
    - Fedora - RedHat based
    - CentOS - RedHat based
    - Trisquel - Debian based

basic commands

man
pwd
cd, ls, cp, mv, rm
mkdir
cat, less
vi, nano, emacs
grep, lsof
sudo, su
passwd

top
chmod, chown, chgrp
ps
netstat
who
which

cat

```
$cat filename      #write the file to the screen

$cat > filename    #write input to a file

$echo hi | cat     #take input from a bash pipe

$echo hi | cat | cat
```

grep

$cat filename | grep "hello"

$cat filename | grep -v "hello"

$cat /usr/share/dict/words | grep -B 5 base

$cat /usr/share/dict/words | grep -A 5 base

grep

$head

prints out the top of a file

$tail

prints out the bottom of a file

$more

shows a file a page at a time

$less

same as more but lets to scroll up

moving files

$mv filename1 filename2

same renaming

$cp filename1 filename2

two files exist now

$cat filename1 > filename2

directories

$mkdir directory1

creates a folder

$cd directory1

moves into a new folder

$cd ..

moves out of a folder

$pwd

prints the path from the root

processes

$ps

lists the processes that are running

$top

shows processes using the most cpu

editing files

$vi filename

$nano filename

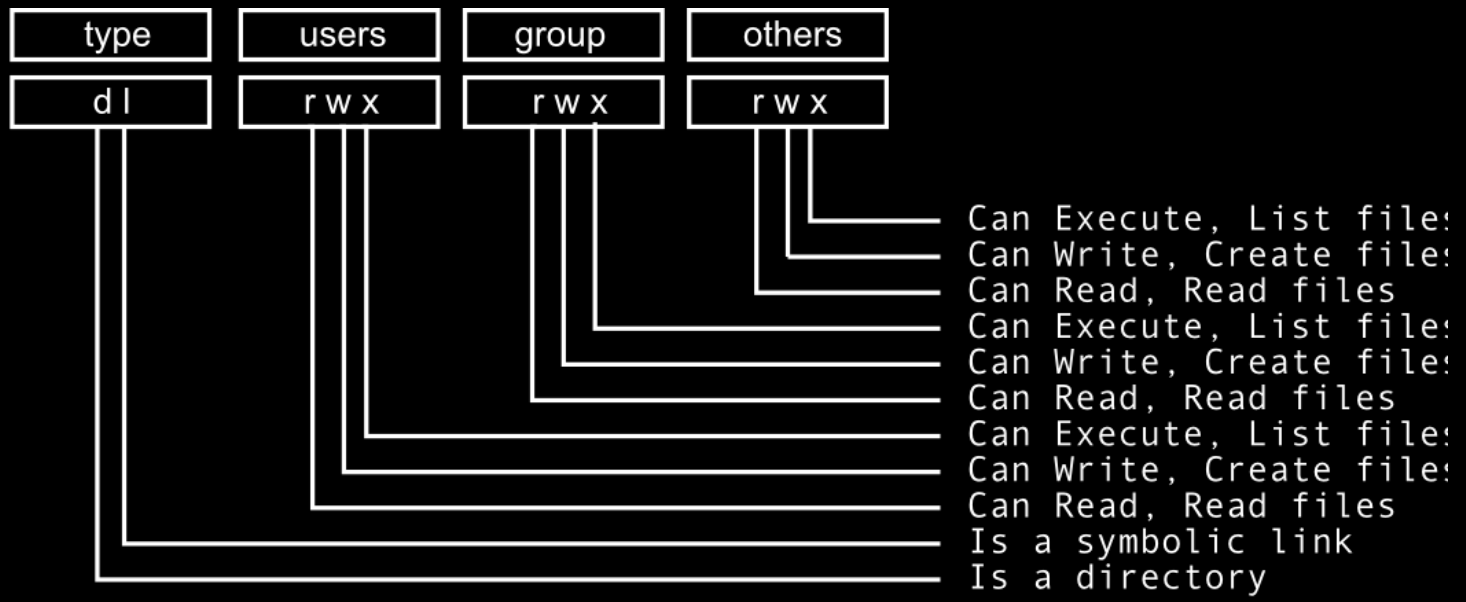
$nano filename

cat filename1 | grep -v hello > filename2

permissions

- files and directories have permissions
- two dimensions:
  - users, group, others
  - read, write, execute
- every file is owned by a user and a group
- user has several groups

permissions



- example:

```
drwxr-xr-x   2 root root      bin
-rw-r-----   1 root shadow    shadow
```

filesystem

- executables (programs):
  - /usr/local/bin
  - /usr/bin
  - /bin
- configuration files:
  - /etc
- logs:
  - /var/logs
- user files:
  - /home
- devices:
  - /dev

package management system

- what is it?:
  - a tool that automates the process of installing, upgrading, configuring and removing software
  - other purposes
  - Verifying file checksums for correct and complete packages.
- Verifying digital signatures to authenticate origin.
- Applying file archivers to manage encapsulated files.
- Upgrading software with latest versions.
- Grouping of packages by function to reduce user confusion.
- Managing dependencies to ensure a package is installed with all packages it requires.

package

- what's a package?:
  - packages, are distributions of software, application and data.
  - they typically contain meta such as information about what it is, purpose, name, checksum, and a list of dependencies.

package mangers

- different flavors of linux = different package managers

Common Terminal Management Apps	Extension
apt-get	.deb
aptitude	.deb / ported to .rpm
dpkg	.deb
rpm	.rpm
yum	.rpm

Other common tools
wget

apt-get

- configuring apt-get
  - /etc/apt/sources.list: Locations to fetch packages from.
  - /etc/apt/sources.list.d/: Additional source list fragments.
  - /etc/apt/apt.conf: APT configuration file.
  - /etc/apt/apt.conf.d/: APT configuration file fragments.
  - /etc/apt/preferences: version preferences file.
  - /var/cache/apt/archives/: storage area for retrieved package files.
  - /var/cache/apt/archives/partial/: storage area for package files in transit.
  - /var/lib/apt/lists/: storage area for state information for each package
  - /var/lib/apt/lists/partial/: storage area for state information in transit.

Quick Commands

apt-get install <PKG>
apt-get remove --purge <PKG>
apt-get autoremove <PKG>
apt-get -s <PKG>
apt-get -u install <PKG>
apt-get -u upgrade
apt-get clean & apt-get autoclean
apt-get dist-upgrade
apt-file search <FILE>
apt-file update

Quick Commands 2

apt-file list <PKG>
apt-file search "libsupp.a"
apt-cache showpkg <PKG>
apt-cache search "Intrusion Detection"
apt-cache pkgnames | sort
apt-cache show <PKG>
apt-key
sha1sum / md5sum <FILE>
dpkg -l | grep
dpkg -L
dpkg -S /bin/netstat
dpkg -s <PKG> | grep Status

Debian package management cheat sheet

quick reference for apt-get and dpkg commands and tricks
http://www.cyberciti.biz/tips/linux-debian-package-management-cheat-sheet.html

quick Package Manager cheat sheet (rpm, dpkg, yum, apt, solaris, aix)
http://nakedape.cc/wiki/PackageManagerCheatsheet
https://wiki.archlinux.org/index.php/Pacman_Rosetta