Linux Core Features

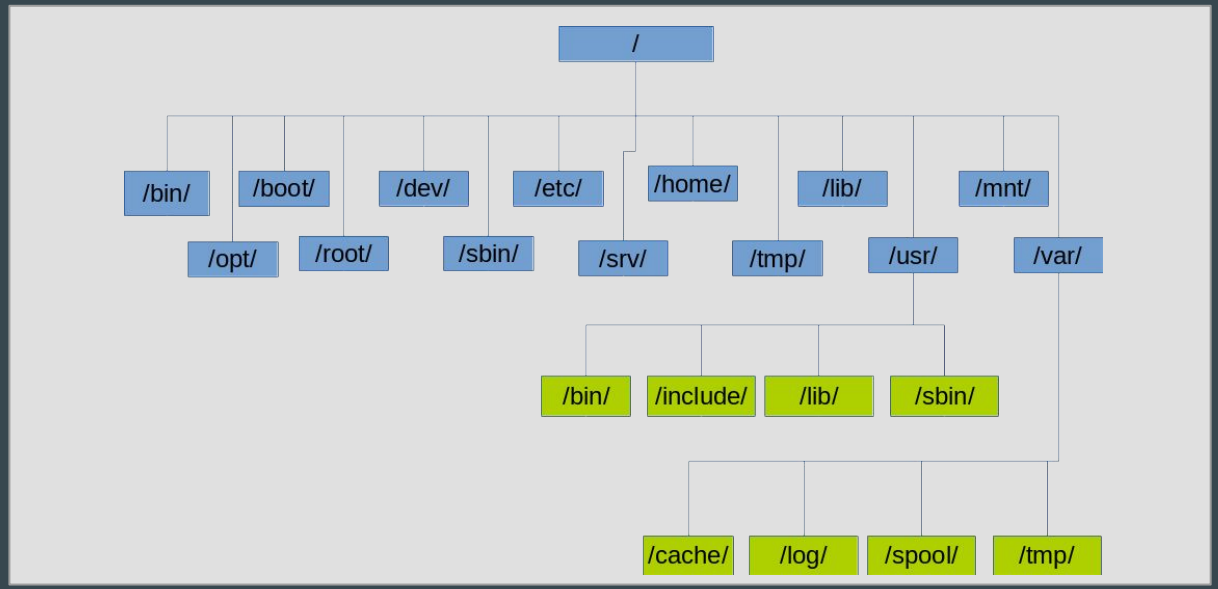
...

DAY 3

Files n' REGEX

Linux Filesystems (1)

Most distros follow the Linux Filesystem Hierarchy Standard



http://refspecs.linuxfoundation.org/fhs.shtml

Linux Filesystems (2)

ext3/4

Hard drive partitioning format

Tmpfs

Appears as a mounted volume, but is actually stored in volatile memory

Sysfs

Pseudo file system providing information about kernel, hardware, device drivers

Linux Filesystems (3)

Demos

1. Mount
2. Df
3. File system hierarchy

Pseudo Filesystems

/proc – information about processes, connections, and some hardware

/sys – information about the system (hardware)

Dynamic Filesystems

/tmp – temporary directory, cleaned at every reboot and system day change

/dev – device directory that is dynamically populated by udev

Ownership

Demos

1. Ls -la
2. Chown
3. Chgrp

File Properties

```
-          # regular file
d          # directory
l          # link (symbolic or hard)
b          # block special file
c          # character special file
s          # socket
p          # named pipe (mknod, mkfifo)
```

File Attributes

Demo

1. Chattr
2. Lsattr

File Permissions

Octal permissions

R W X

4 2 1

File Permissions

Suid - program set with SUID runs under the security context of the user (owner) of the program

SGID - program set with SGID runs under the security context of the group of the program

Sticky bit - when set on a directory only the owner of the file can delete or rename files in that directory

File Permissions

SUID - displays as lowercase s, uppercase means not set, chmod 4755 *file*

SGID - displays as lowercase s, uppercase means not set, chmod 2755 *file*

Sticky bit - displays as lowercase t in octal perms, uppercase means not set

- set with chmod 1755 *file*

File Permissions

Dangers of suid/sgid

- Can exploit vulnerable binaries and run arbitrary code as owner

Replacement for suid/sgid

- Capabilities
- https://www.theurbanpenguin.com/using-posix-capabilities/

File Permissions

Demo

1. Chmod

Timestamps (1)

EXT3

mtime: modified time - time file content was last modified

atime: access time - time file was last accessed (persistent for 24 hrs)

ctime: change time - time of inode record change (file attribute changes: size, location, type, etc.)

EXT4*

crtime: creation time

Timestamps (2)

Demo

1. Finding timestamp info

REGEX Primer

[ ]

{ } {,} + * ?

\d, etc

\

\t, etc

^ $

rexegg.com/regex-quickstart.html || Regex101.com || Regexer.com ||
https://www.regular-expressions.info/numericranges.html

REGEX Demo

Demo

Grep w/ regex - IPv4 address

REGEX Challenges

As a class:

Social Security Number

US Phone Numbers