LINUX PULIYA

ANANT SHRIVASTAVA

- Information Security Consultant
- Admin - Dev - Security
- null + OWASP + G4H
- http://anantshri.info and @anantshri
- Trainer : Blackhat, RuxCon, NullCon, g0s, c0c0n
- Speaker : Nullcon, c0c0n, ClubHack, RootConf

Android Tamer Code Vigilant

WHAT ARE WE COVERING

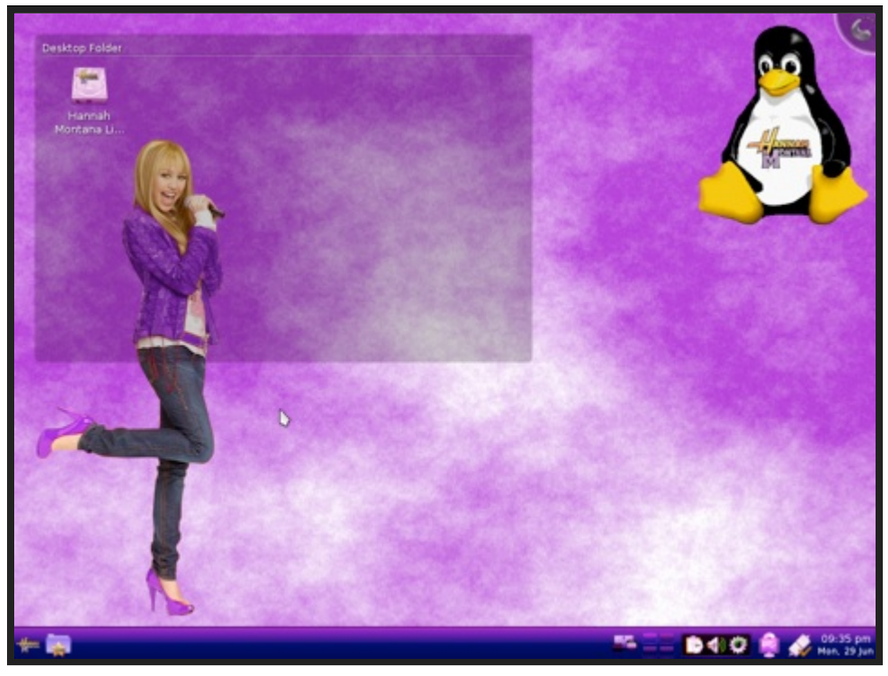
1. Understanding *nix
2. File System Basics
3. Understanding I/O
4. Basic Commands
5. How to Exit VIM
6. Shell Script basics
7. Automation

NIX

1. Family of OS ranging from Unix, Linux, *BSD (FreeBSD, OpenBSD etc)
2. Follow same standards in terms of file systems, directory layout etc

LINUX

1. Free as in free speech not free beer
2. Everyone can create there own Distro
3. Hanna Montanna Linux



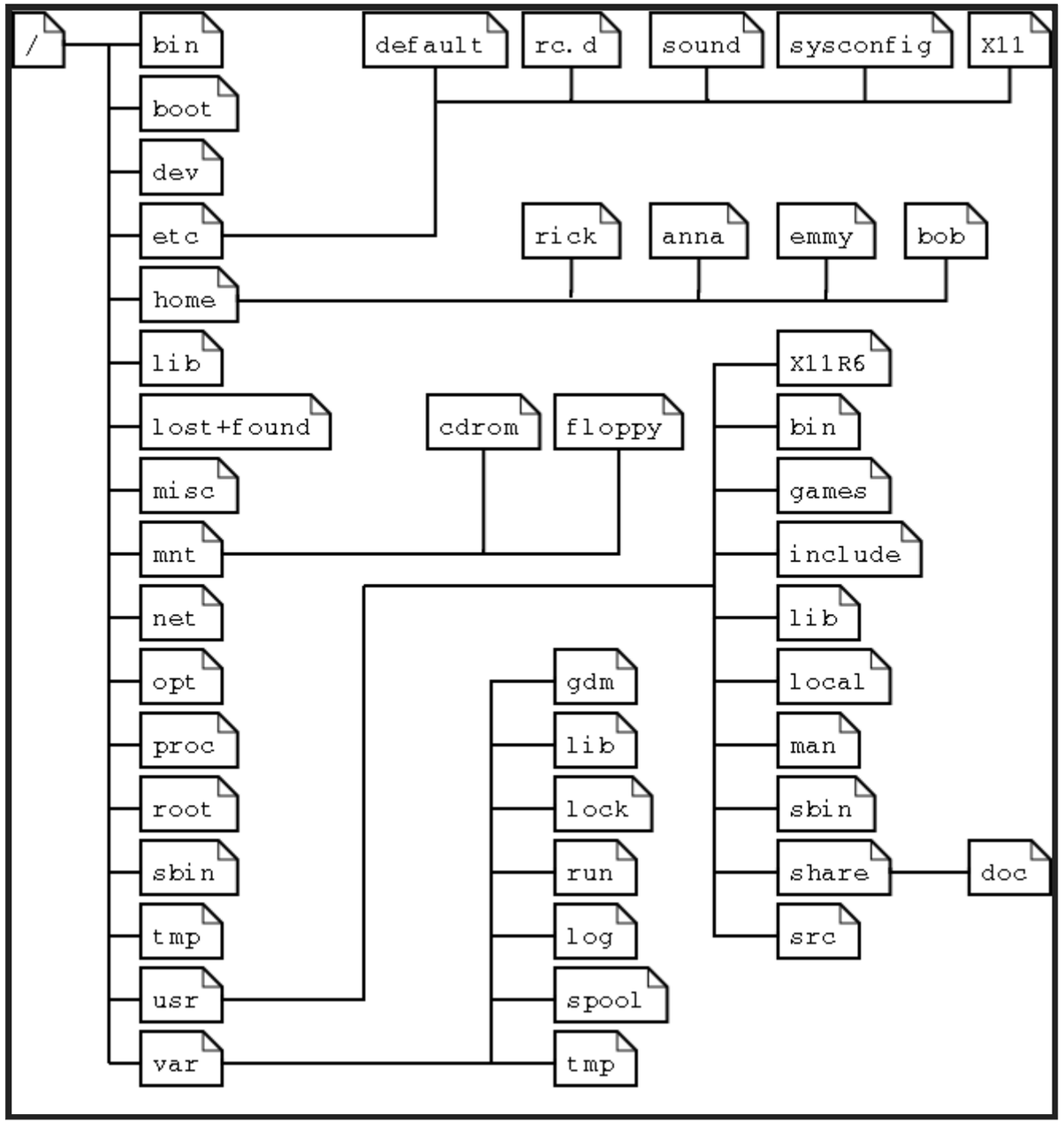
and more

LINUX DISTRIBUTIONS

1. Various Linux Distributions
2. Debian Based (apt-get / dpkg)
3. RedHat based (yum / rpm)
4. LTS or not

FILE SYSTEM BASICS

1. Everything is a file
2. File System Layout
3. Standard File system layout
    1. / as highest level
    2. /etc for all configuration
    3. /home : users home folder


/
bin
boot
dev
etc
home
lib
lost+found
misc
mnt
net
opt
proc
root
sbin
tmp
usr
var
default
rc.d
sound
sysconfig
X11
rick
anna
emmy
bob
cdrom
floppy
gdm
lib
lock
run
log
spool
tmp
X11R6
bin
games
include
lib
local
man
sbin
share
doc
src

FILE SYSTEM TYPES

- ext2
  - Maximum file size = 16 GB to 2 TB
  - File system size = 2 TB to 32 TB
- ext3
  1. Journaling (Linux Kernel 2.4.15)
  2. Maximum file size = 16 GB to 2 TB
  3. File system size = 2 TB to 32 TB
- ext4
  1. Starting from Linux Kernel 2.6.19 ext4
  2. Maximum file size = 16 GB to 16 TB
  3. File system size = 1 EB
     1. 1 EB = 1024 PB
     2. 1 PB = 1024 TB

MORE FILE SYSTEM BASIC

1. File System Permissions

   -rwxrwxrwx

2. Suid bits

   -rwsrwxrwx

3. sgid bit

   -rwxrwsrwx

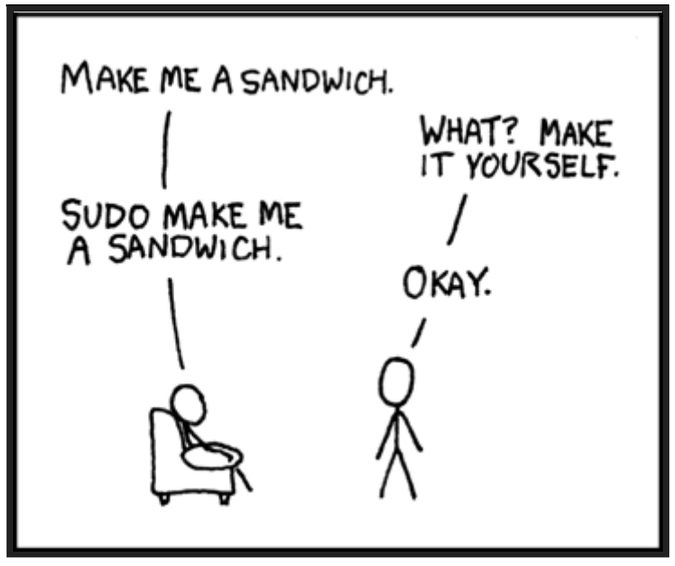
4. sticky bit

   -rwxrwxrwt

5. First bit can be l,c,b,d,-

SUDO

1. id 0 is omnipotent
2. its suggested not to use root access
3. So how do we do high privilege actions



STANDARD I/O

1. Input (<)
2. Output (>)
3. Error (2>)

USEFUL COMMANDS

1. ls, cd, mkdir
2. cut
3. grep
4. sed
5. sort
6. uniq
7. xargs
8. find
9. tr
10. ps
11. screen
12. netstat -lntp
13. file

EDITOR

1. Vim
2. Nano
3. EMACS

INSTALLING SOFTWARES

1. Debian apt-get install
2. Redhat yum install
3. python pip install
4. ruby gem install
5. npm / nodejs npm install

MORE USEFUL COMMANDS

1. python -m SimpleHTTPServer Port
2. !!
3. cd ~
4. cd -
5. mtr
6. mount and format
7. setting environment Variables

CRONTAB

1. Automate periodic execution

```
* * * * * * CMD
| | | | | |
| | | | | +-- Year              (range: 1900-3000)
| | | | +---- Day of the Week   (range: 1-7, 1 standing for Monday)
| | | +------ Month of the Year (range: 1-12)
| | +-------- Day of the Month  (range: 1-31)
| +---------- Hour              (range: 0-23)
+------------ Minute            (range: 0-59)
```

CONFIGURING SERVICES

SSH

Configuration file : /etc/ssh/sshd_config

USING SSH

1. SSH Authentication
    1. Password
    2. SSH Key
2. How to Configure SSH Login via Key
3. ~/.ssh/authorized_keys

SHELL SCRIPT BASICS

1. Shebang
2. $1 $2, $* $@ $0
3. read
4. echo
5. cat
6. Conditions
7. Loop
8. Expansion {}

WRITING CUSTOM SCRIPTS

1. Write a shell script to calculate simple interest
2. Write a shell script to check whether no is even or odd
3. Print prime numbers from 1 to 5000

OVERLOAD COMMANDS

1. alias
2. Why alias and why not
3. find location add path before everything else and then overload

EXAMPLE

QUESTIONS

THANK YOU