Infrastructure Security Using Linux

Computer science / Cybersecurity

01

Introduction

Course Project:

- **Deploying a Real Open-Source Web App on an Apache Web Server**
- Project Overview
  - Students will deploy a real open-source web application on an Apache web server running on an Ubuntu server. The project involves configuring, securing, and testing the deployment to ensure a stable and secure web application.

Project Requirements

1. **Web App Selection**
    1. Choose a real open-source web application for deployment
    2. **Get approval** for the selected web app during office hours (ASK ME!).
2. **Server Setup and Configuration**
    1. Install and configure an Ubuntu server.
    2. Set up the Apache web server and deploy the selected web app.
    3. Configure local domain settings to use the host web browser on a Virtual Network.
3. **Security Implementation**
    1. Secure the Ubuntu server and Apache web server (e.g., firewall rules, SSH hardening).
    2. Apply best security practices to protect the web app (e.g., secure configurations), Here **HTTP** is allowed due to static IP limitation.

Project Requirements

4. Penetration Testing

1. Use 3 well-known penetration testing tools to assess the security of both the server and the web app.
2. Document vulnerabilities found and provide mitigation strategies.

5. Documentation and Submission

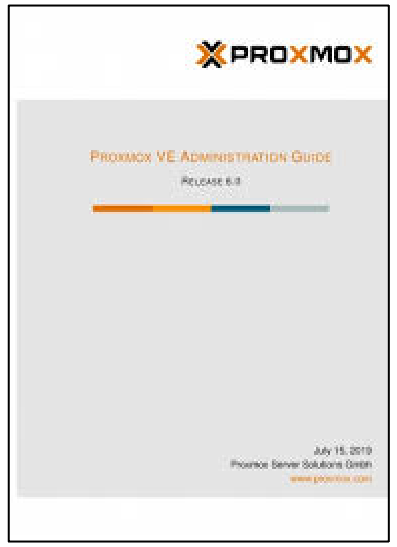
1. Submit a detailed report covering:
   - Web app selection and rationale
   - Deployment steps and configurations
   - Security measures implemented
   - Penetration testing results and mitigation strategies
2. Upload the report to LMS before the submission deadline (08/05/2025).
3. Late submissions will not be accepted.

Project Presentation

- **Presentation**
  - The presentation schedule will be announced after submission.
  - Students will demonstrate their deployment, security measures, and testing process.
- This project evaluates students' ability to deploy, secure, and assess the security of web applications in a Virtual environment.

Books

- **Note:** The course books are required for the exam. Students are expected to study:
  1. *UNIX and Linux System Administration Handbook* (5th Edition) (2017). Evi Nemeth, Garth Snyder, and Trent Hein. Addison-Wesley Professional.
  2. *Proxmox VE Administration Guide* (2024). Proxmox Server Solutions GmbH.
- Ensure you have access to these books for exam preparation.

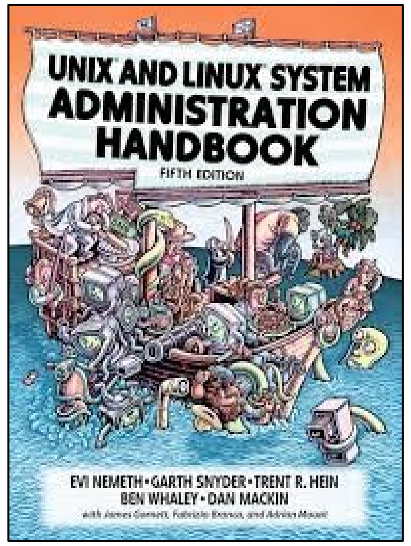


PROXMOX

Proxmox VE Administration Guide

Release 6.0

July 15, 2019
Proxmox Server Solutions GmbH
www.proxmox.com


UNIX AND LINUX SYSTEM
ADMINISTRATION
HANDBOOK
FIFTH EDITION
EVI NEMETH • GARTH SNYDER • TRENT R. HEIN
BEN WHALEY • DAN MACKIN
with James Garnett, Fabrizio Branca, and Adrian Mouat

Overview …………

- Overview of infrastructure security principles
- Introduction to Linux

Overview of Infrastructure Security Principles

Infrastructure Security Principles

- Infrastructure security involves protecting systems, networks, and data across physical and virtual environments.
- By understanding foundational principles, administrators can correctly manage IT Infrastructure and build defenses tailored to organizational needs.

Core Security Concepts

- CIA Triad: Confidentiality, Integrity, Availability
  - **Confidentiality** ensures that sensitive information remains accessible only to authorized users.
  - **Integrity** means data and systems remain accurate and unmodified by unauthorized actions.
  - **Availability** emphasizes continuous accessibility of resources.
- Together, these pillars guide security measures and risk assessments.

The Threat Landscape

- Modern infrastructures face diverse attacks from a variety of sources.
- Malware can compromise systems, phishing tricks users into divulging secrets, and insider threats exploit privileges.
- Distributed Denial of Service (DDoS) floods networks, crippling service availability.
- Recognizing these threats shapes effective defensive strategies.

Risk Assessment & Management

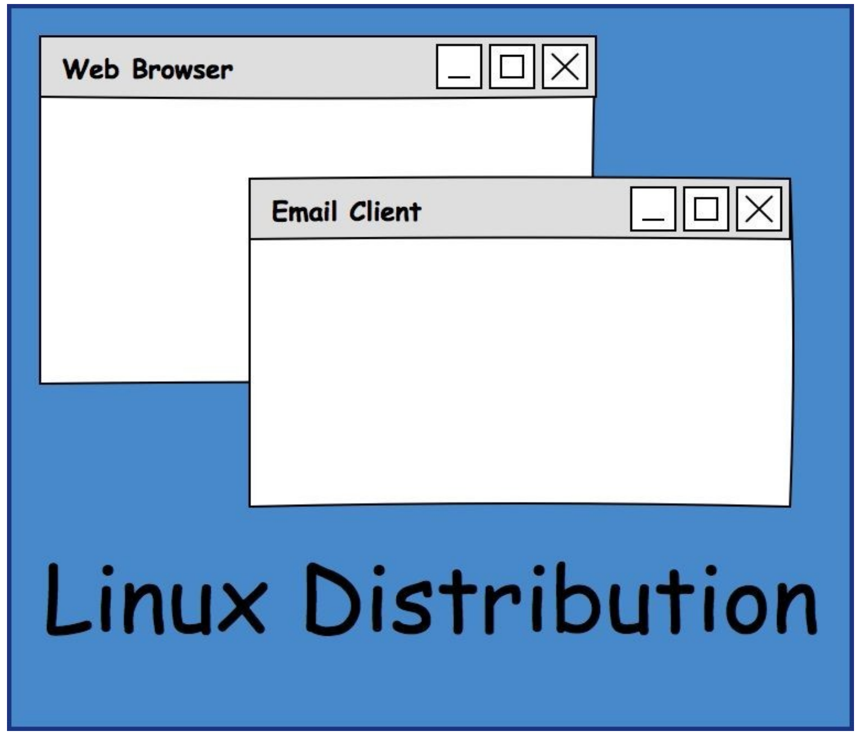
- Security begins by identifying key assets (data, hardware, applications).
- Pinpoint possible vulnerabilities, then measure the likelihood and severity of risks.
- Addressing the greatest risks first ensures efficient use of security resources. This cyclical process enables continuous improvement.

Risk Assessment & Management

- Defense in depth combines multiple protective measures so that if one fails, additional layers remain.
- Layers may include physical security, network segmentation, firewalls, and access controls.
- This overlapping strategy makes unauthorized access more difficult and costly for attackers.

Linux

Linux Distributions

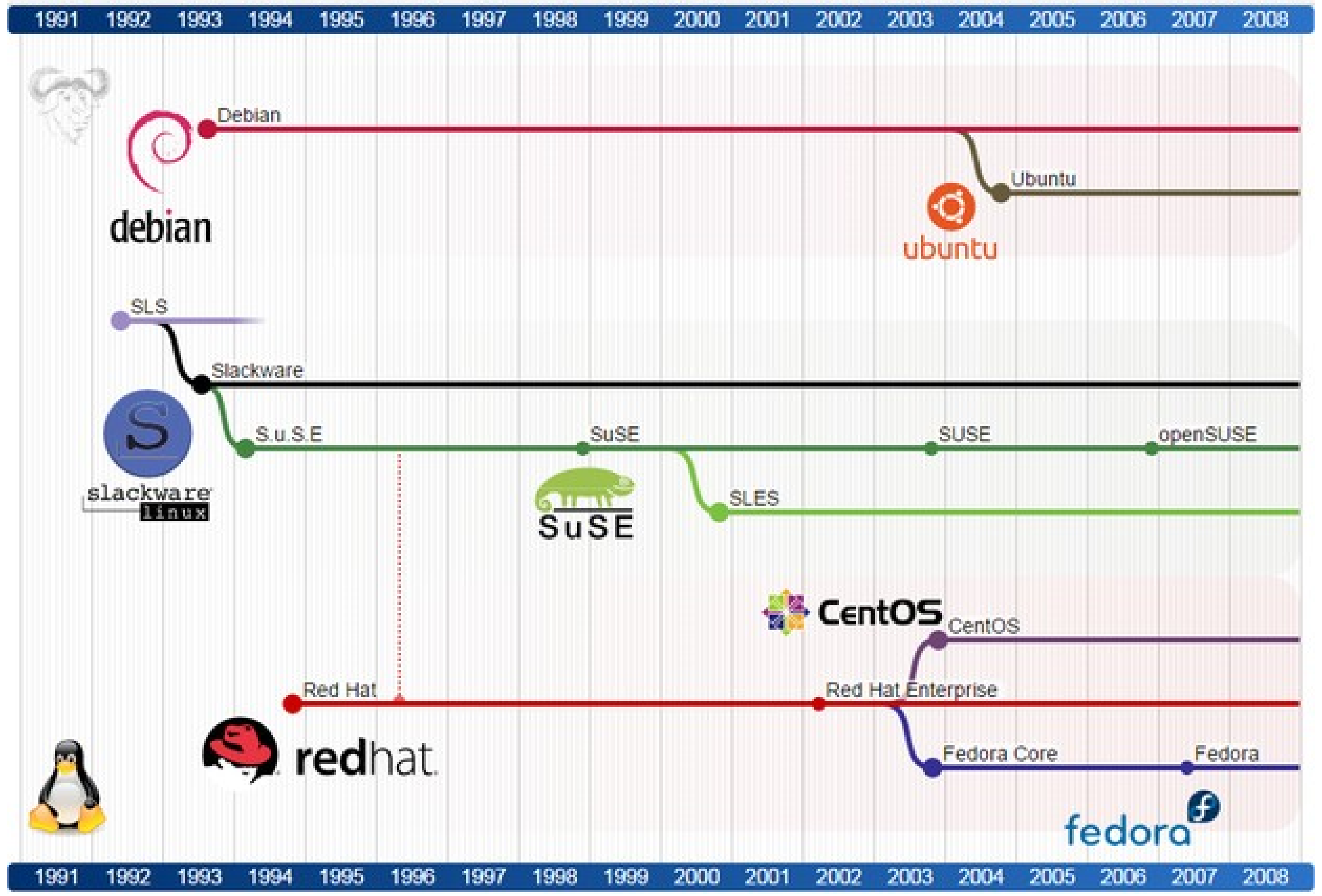


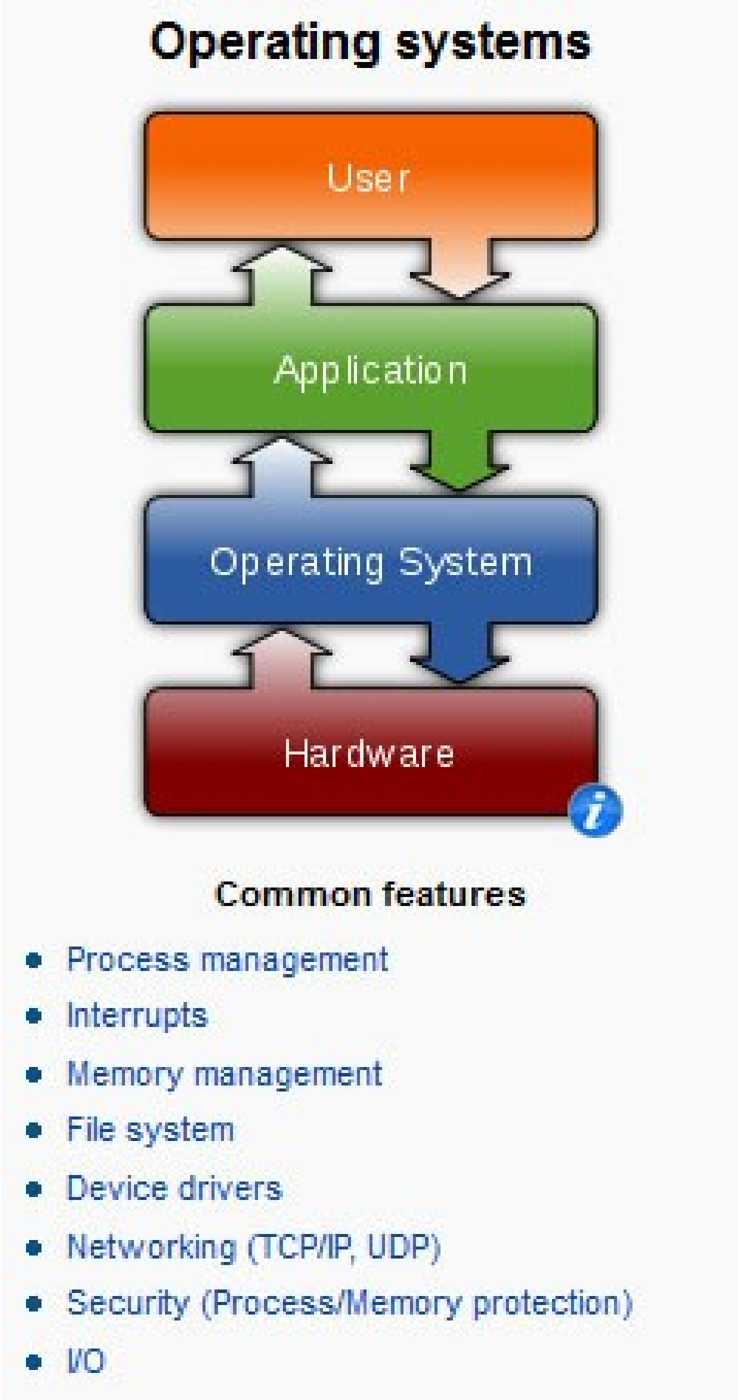
What is Linux?

- Linux is an Operating System

- Linux OS = Linux Distribution
  - **With flavor software's**

- Distro / Flavor = Distribution





Operating systems

Common features

- Process management
- Interrupts
- Memory management
- File system
- Device drivers
- Networking (TCP/IP, UDP)
- Security (Process/Memory protection)
- I/O

What is Linux?

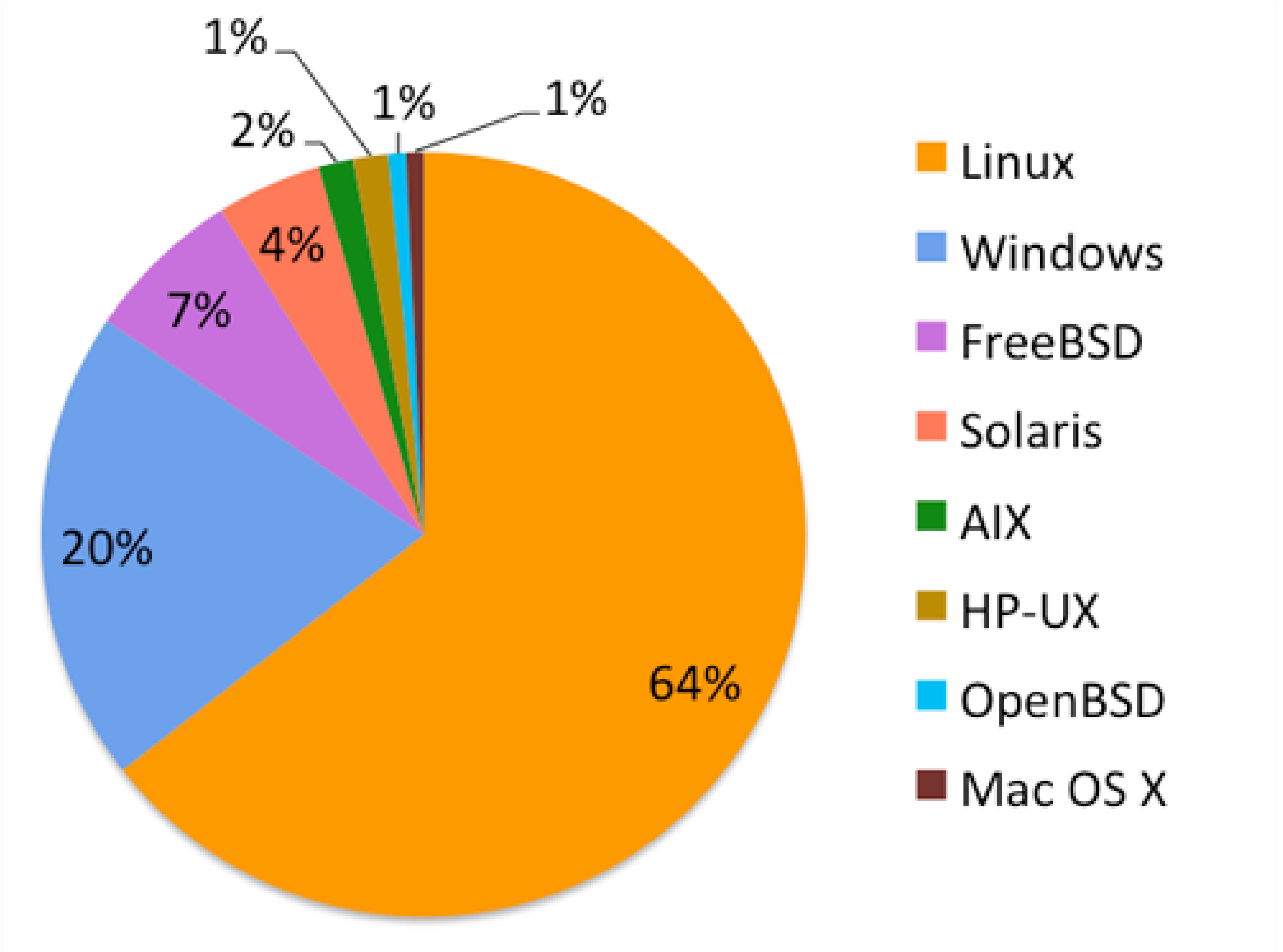
- **Linux** is a **Unix** *clone* written from scratch by **Linus Torvalds** with assistance from a loosely-knit team.
- Unix is a multitasking, multi-user computer operating system originally developed in 1969 by a group of AT&T employees at Bell Labs.
- Linux and Unix strive to be POSIX (Portable Operating System Interface IEEE) compliant.
- 64% of the **world’s servers** run some variant of Unix or Linux.

Where can you find it?

- Smartphones (Android phone)
- Kindle run Linux.
- 96% of 500 top supercomputers
- TVs
- Military applications
- Self-driving cars

Why Linux?

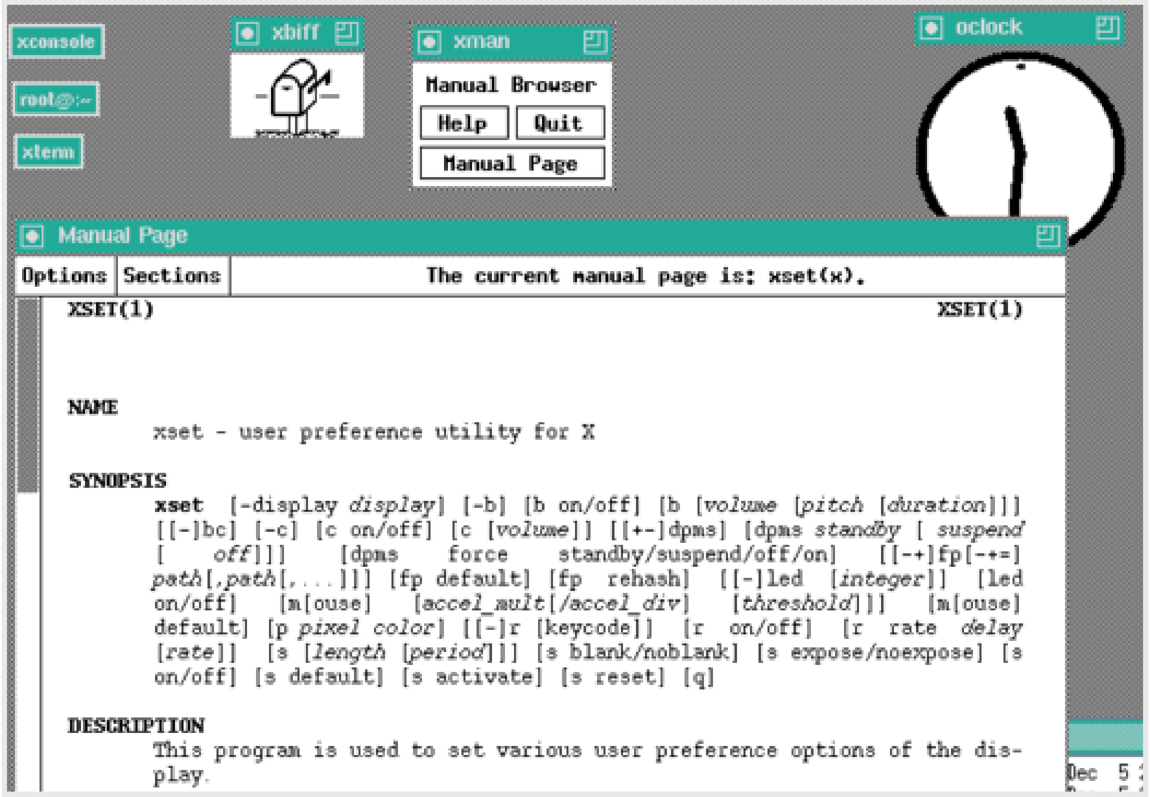
- Free
- Open Source
- Choose your own flavor
- Community support
- It’s a foundation for jobs



Apache HTTP server usage research

Unix

- brief history:
  - Multics (1964) for mainframes
  - Unix (1969)
  - K&R
  - Linus Torvalds and Linux (1992)



```
The current manual page is: xset(x).

XSET(1)                                                    XSET(1)


NAME
       xset - user preference utility for X

SYNOPSIS
       xset  [-display display] [-b] [b on/off] [b [volume [pitch [duration]]]
       [[-]bc] [-c] [c on/off] [c [volume]] [[+-]dpms] [dpms standby [ suspend
       [    off]]]     [dpms     force     standby/suspend/off/on]    [[-+]fp[-+=]
       path[,path[,...]]] [fp default] [fp  rehash]  [[-]led  [integer]]  [led
       on/off]    [m[ouse]    [accel_mult[/accel_div]    [threshold]]]    [m[ouse]
       default] [p pixel color] [[-]r [keycode]]  [r  on/off]  [r  rate  delay
       [rate]]  [s [length [period]]] [s blank/noblank] [s expose/noexpose] [s
       on/off] [s default] [s activate] [s reset] [q]

DESCRIPTION
       This program is used to set various user preference options of the dis-
       play.
```

- key Unix ideas:
  - written in a high-level language (C)
  - virtual memory
  - hierarchical file system; "everything" is a file
  - lots of small programs that work together to solve larger problems
  - security, users, access, and groups
  - human-readable documentation included

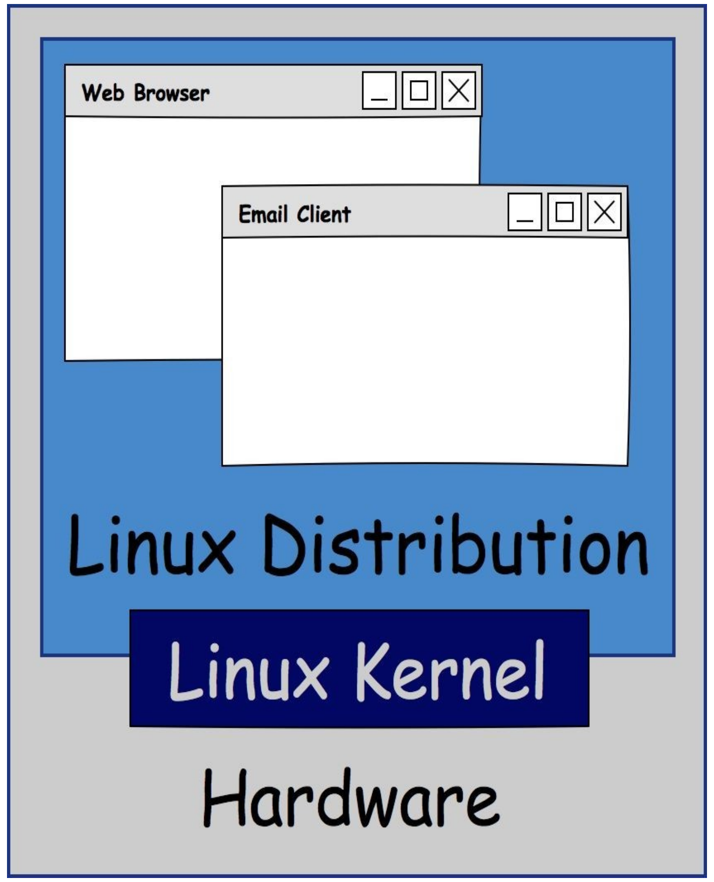
The Linux Philosophy

The *Nix Philosophy of Doug McIlroy

- (i) Make each program do one thing well. To do a new job, build afresh rather than complicate old programs by adding new features.
- (ii) Expect the output of every program to become the input to another, as yet unknown, program. Don't clutter output with extraneous information. Avoid stringently columnar or binary input formats. Don't insist on interactive input.
- (iii) Use tools in preference to unskilled help to lighten a programming task, even if you have to detour to build the tools and expect to throw some of them out after you've finished using them.

Linux Kernel

- The kernel is the core.
- Linux Kernel + Apps = Distro
- **kernel**: The lowest-level core of an operating system.
- Features provided by an operating system:
  - ability to execute programs (and multi-tasking)
  - memory management (and virtual memory)
  - file systems, disk and network access
  - an interface to communicate with hardware
  - a user interface (often graphical)



What is Linux?

- Linux + GNU Utilities = Free Unix

Linux is an O/S core written by Linus Torvalds and others

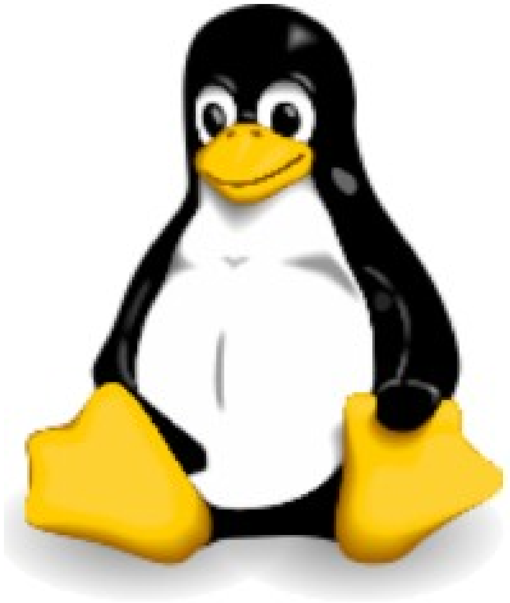
GNU: a set of small programs written by Richard Stallman and others.

They are the GNU utilities.

http://www.gnu.org/

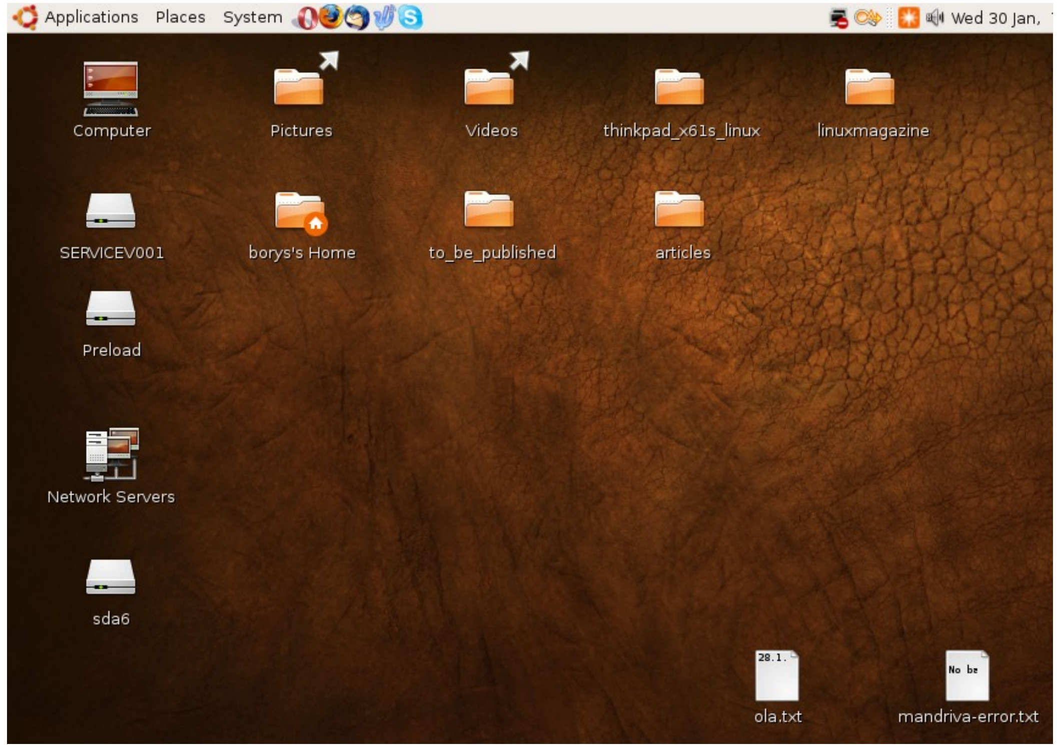
Linux

- **Linux**: A kernel for a Unix-like operating system.
  - commonly seen/used today in servers, mobile/embedded devices, ...
- **GNU**: A "free software" implementation of many Unix-like tools
  - many GNU tools are distributed with the Linux kernel
- **distribution**: A pre-packaged set of Linux software.
  - examples: Ubuntu, Fedora
- **key features of Linux**:
  - **open-source software**: source can be downloaded
  - free to use
  - constantly being improved/updated by the community



Linux Desktop

- X-windows: Display Server using a X protocol (Client and server communicate)
- Window managers
- The desktop environments can be roughly classified into the following categories:
  - Similar to MS Windows **Cinnamon**, **Mate** or **KDE Plasma**
  - Easy to use **Gnome**, **XFCE** or **LXDE/LXQT**
  - Flexible and adaptable **KDE Plasma**, **Cinnamon**, **XFCE**
  - Low hardware requirements **LXQT**, **XFCE**



- How can I try out Linux?
  - Virtual machine
  - labs
  - OnWorks

Shell

- **Shell**: An interactive program that uses user input to manage the execution of other programs.
  - A command processor, typically runs in a text window.
  - User types commands, the shell runs the commands
  - Several different shell programs exist:
    - **Bash** : the default shell program on most Linux/Unix systems
    - We will use bash (x-terminal)
    - Other shells: Bourne, csh, tsch
- Why should I learn to use a shell when GUIs exist?

Why use a shell?

- Why should I learn to use a shell when GUIs exist?
  - Faster
  - Work Remotely vary well (using SSH, and SFTP protocols)
  - Programmable
  - Customizable
  - Repeatable

Small programs that do one thing well

- **Network:** ssh, scp, ping, telnet, nslookup, wget
- **Shells:** BASH, TCSH, alias, watch, clear, history, chsh, echo, set, setenv, xargs
- **System Information:** w, whoami, man, info, which, free, echo, date, cal, df, free, info
- **Command Information:** man, info, help (h)
- **Symbols:** |, >, >>, <, &, >&, 2>&1, ;, ~, ., .., $!, !:<n>, !<n>
- **Filters:** grep, egrep, more, less, head, tail
- **Hotkeys:** <ctrl><c>, <ctrl><d>
- **File System:** ls, mkdir, cd, pwd, mv, ln, touch, cat, file, find, diff, cmp, /net/<hostname>/<path>, mount, du, df, chmod, find
- **Line Editors:** awk, sed
- **File Editors:** nano, vim, gvim, emacs –nw, emacs, touch, vscode

Linux Has Many Distributions

redhat
MEPIS
turbolinux
LUNAR
EvilEntity
debian
Vine Linux
cAos/CentOS
MiniKazit
UTUTO
archlinux
m0n0wall
jamd LINUX
Knoppix STD
gentoo linux
DeLi Linux
Hiweed
amlug
slackware linux
yellow dog linux
Fedora
LPG
PLD
SLAX
COREL LINUX
Progeny
GEEXBOX
BIGLINUX
FREEDUC
Lycoris
EnGarde
Mandrakelinux
BeatrIX
Linspire
SuSE
中文延伸套件
YOPER
BearOps
ASPLINUX
kalango
Slackintosh
Frugalware
Foresight
Mint
PCLinuxOS
Haydar Linux
sabayon
ubuntu
JULEX
blag

There are over 600 **active** Linux distros (Linux Statistics – 2024)

Linux distribution family

sorted by base distro with derivatives

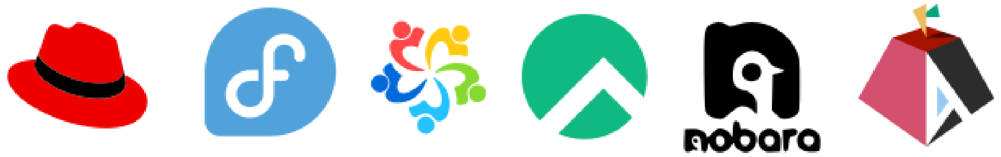
Debian / Ubuntu

KALI
Tails
Pop!_OS

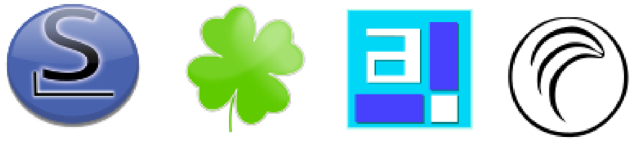
Arch Linux

ENDEAVOUROS

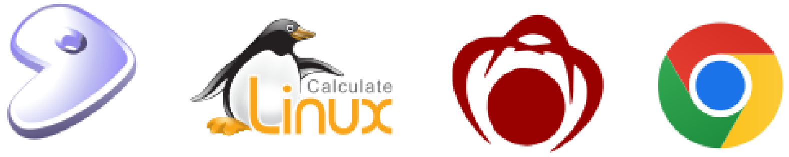
RH Fedora



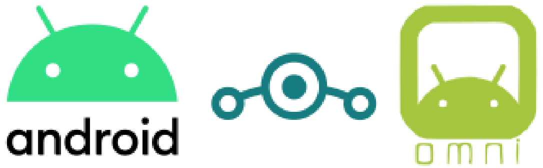
Slackware



Gentoo



Android



SUSE

Alpine

Indie

VOID
ROSA
KNOPPIX

Most popular Linux distributions

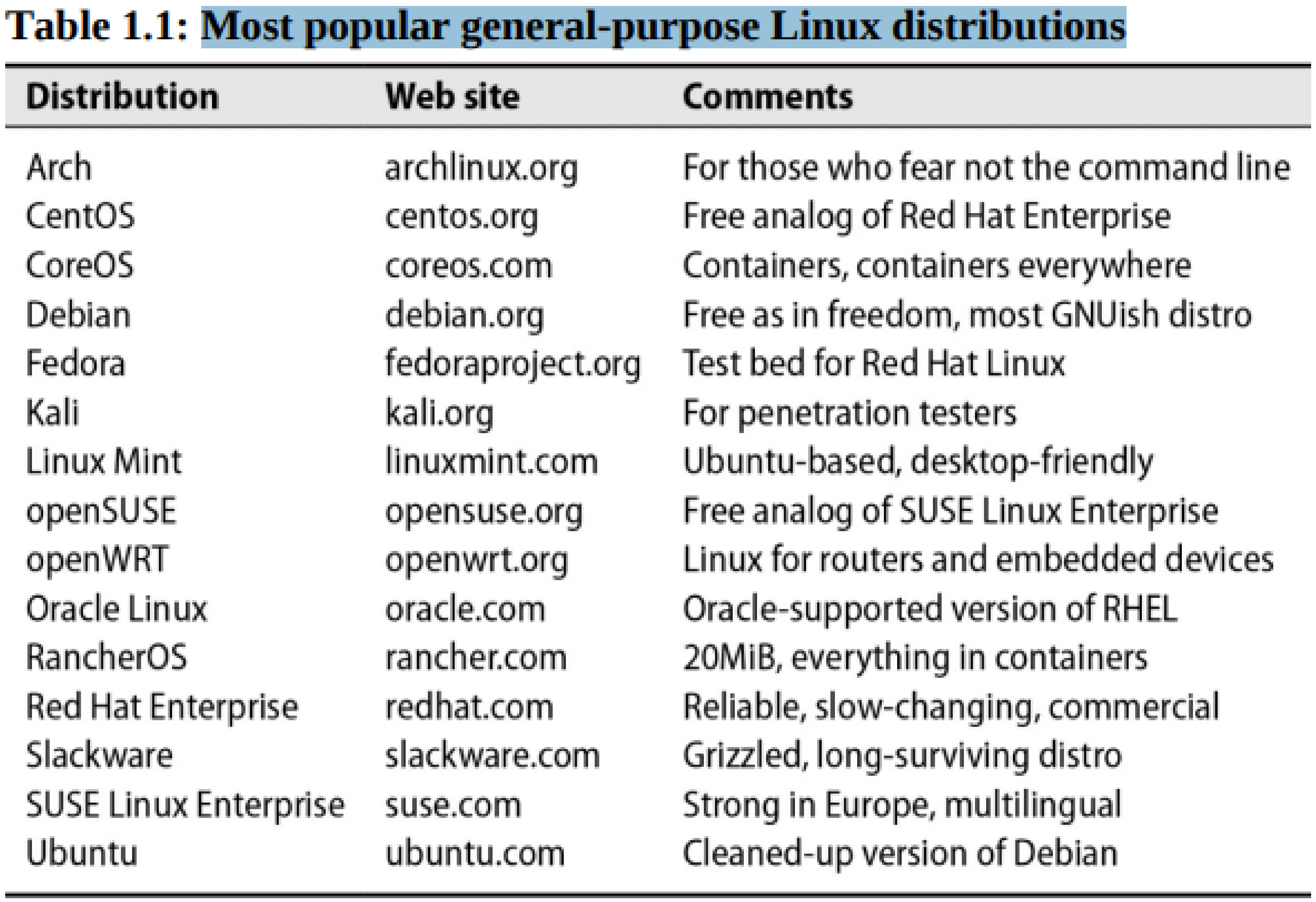


Table 1.1: Most popular general-purpose Linux distributions

Distribution	Web site	Comments
Arch	archlinux.org	For those who fear not the command line
CentOS	centos.org	Free analog of Red Hat Enterprise
CoreOS	coreos.com	Containers, containers everywhere
Debian	debian.org	Free as in freedom, most GNUish distro
Fedora	fedoraproject.org	Test bed for Red Hat Linux
Kali	kali.org	For penetration testers
Linux Mint	linuxmint.com	Ubuntu-based, desktop-friendly
openSUSE	opensuse.org	Free analog of SUSE Linux Enterprise
openWRT	openwrt.org	Linux for routers and embedded devices
Oracle Linux	oracle.com	Oracle-supported version of RHEL
RancherOS	rancher.com	20MiB, everything in containers
Red Hat Enterprise	redhat.com	Reliable, slow-changing, commercial
Slackware	slackware.com	Grizzled, long-surviving distro
SUSE Linux Enterprise	suse.com	Strong in Europe, multilingual
Ubuntu	ubuntu.com	Cleaned-up version of Debian

redhat

CentOS

debian

ubuntu

fedora

Linux distributions

Popular in:

- Banks
- Airlines
- Telecoms
- Healthcare

The most viable distributions are not necessarily the most corporate. For example, we expect Debian GNU/Linux to remain viable for a long time despite the fact that Debian is not a company, doesn't sell anything, and offers no enterprise-level support.

Debian benefits from a committed group of contributors and from the enormous popularity of the Ubuntu distribution, which is based on it.

Example of a Linux distribution

Debian (pronounced deb-ian, named after Debra and Ian Murdock) is one of the oldest and most well-regarded distributions. It is a noncommercial project with more than a thousand contributors worldwide.

Debian maintains an ideological commitment to community development and open access, so there's never any question about which parts of the distribution are free or redistributable.

Debian defines three release that are maintained simultaneously:

- **stable**: targeting the production servers,
- **unstable**: with current packages that may have bugs and security vulnerabilities
- **testing**: a mix of stable and unstable.

Example of a Linux distribution

Ubuntu: is based on Debian and maintains Debian's commitment to free and open-source software. Ubuntu is a commercial distribution, and it is backed by a company called Canonical.

Ubuntu version numbers derive from the year and month of release, so 18.04 was released in April 2018. Each release also has a code name, such as Bionic Beaver for 18.04 or Focal Fossa for 20.04.

Two versions of Ubuntu are released every year, one in April and one in October. The April release is a long-term support (LTS) release, which is supported for five years. The October release is supported for nine months.

Popular in:

- Startups
- SaaS
- Social Networks
- Cloud Based

Example of a Linux distribution

Red Hat has been a dominant force in the Linux world for more than two decades, and its distributions are widely used in North America and beyond. By the numbers, Red Hat, Inc., is the most successful open-source software company in the world.

Red Hat Enterprise Linux, often shortened to **RHEL**, targets production environments at large enterprises that require support and consulting services to keep their systems running smoothly.

Somewhat paradoxically, RHEL is open source but requires a license. If you’re not willing to pay for the license, you’re not going to be running Red Hat.

Red Hat also sponsors **Fedora**, a community-driven distribution that is a proving ground for new technologies that may eventually be included in RHEL. Fedora is a good choice for developers and enthusiasts who want to stay on the cutting edge of Linux. s

Example of a Linux distribution

CentOS is a free, open source, community-driven distribution that is functionally compatible with RHEL.

The CentOS distribution lacks the RHEL branding and logos, but it is otherwise identical to RHEL. CentOS is a good choice for organizations that want the benefits of RHEL without the cost.

TTU uses CentOS in its web services Linux cluster which is a free version of RedHat Enterprise Linux with the trademarks removed.

Rocky Linux, AlmaLinux, Oracle Linux or Ubuntu

On June 30, 2024 reached end of life (EOL), and the CentOS Project discontinued updates and releases at that time. If you’re still running CentOS Linux, you’re at risk of exposing your organization to unpatched vulnerabilities and potential security breaches. **But, EOL is changed to 2030 (Contingent on end of full support phase of based on RHEL 10)**

Example of a Linux distribution

SUSE Linux Enterprise Server (SLES) is a commercial distribution that is popular in Europe. SLES is developed and maintained by the German company SUSE.

SUSE also sponsors openSUSE, a community-driven distribution that is a proving ground for new technologies that may eventually be included in SLES.

Example of a Linux distribution

FreeBSD, first release in late 1993, is the most widely used of the BSD derivatives.

Unlike Linux, FreeBSD is a complete operating system, not just a kernel.

Both the kernel and userland software are licensed under the permissive BSD License, a fact that encourages development by and additions from the business community.

Linux isn't just for business:

- Linux Mint
- Debian
- Mageia
- Fedora
- Arch Linux
- Slackware
- Ubuntu
- SuSE

Connecting to a Linux Host

- You need a “xterm” emulation – software that emulates an “X” terminal and that connects using the “SSH” Secure Shell protocol.
  - Windows
    - If you don’t need windowing, “putty” is good: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
    - If you need windowing, use StarNet “X-Win32:” or “Bitvise SSH Client”

You can also connect to a Linux machine by using VNC to get a whole desktop if it’s supported by the server.

Connecting to a Linux Host – Mac OS X Client Software

- Mac OS X
  - “Terminal” is already installed
  - Why? Darwin, the system on which Apple's Mac OS X is built, is a derivative of 4.4 BSD-Lite2 and FreeBSD. In other words, the Mac is a Unix system!

Specialization and adjacent disciplines

- **DevOps:** DevOps is not so much a specific function as a culture or operational philosophy. It aims to improve the efficiency of building and delivering software, especially at large sites that have many interrelated services and teams.
- Organizations with a DevOps practice promote integration among engineering teams and may draw little or no distinction between development and operations.
- Experts who work in this area seek out inefficient processes and replace them with small shell scripts or large and unwieldy Chef repositories.

Specialization and adjacent disciplines

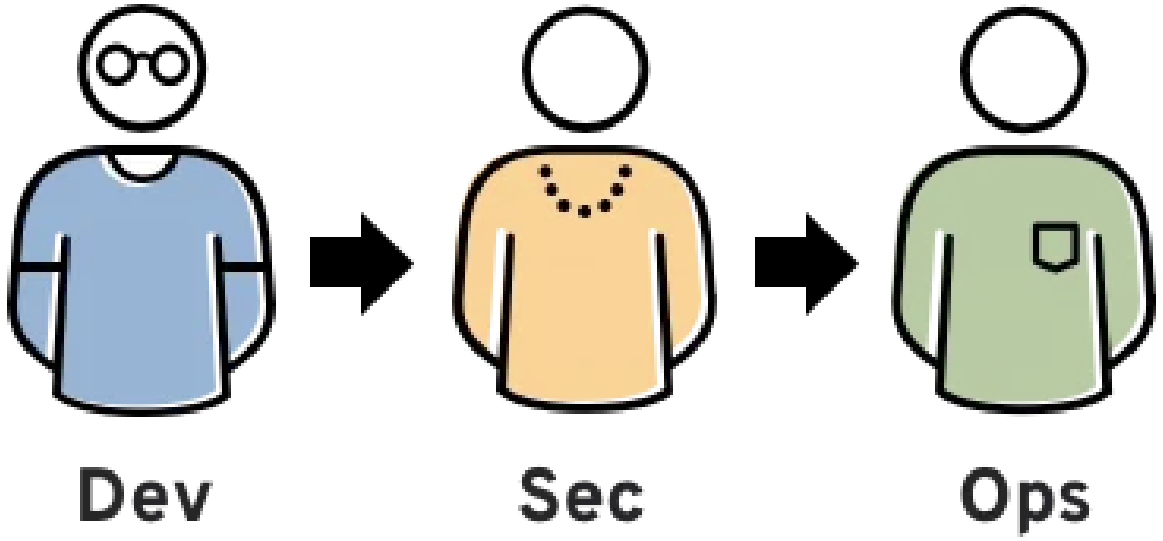
- **Site Reliability Engineering (SRE):** Site reliability engineers value uptime and correctness above all else. Monitoring networks, deploying production software, taking pager duty, planning future expansion, and debugging outages all lie within the realm of these availability crusaders.
- Single points of failure are site reliability engineers’ nemeses.

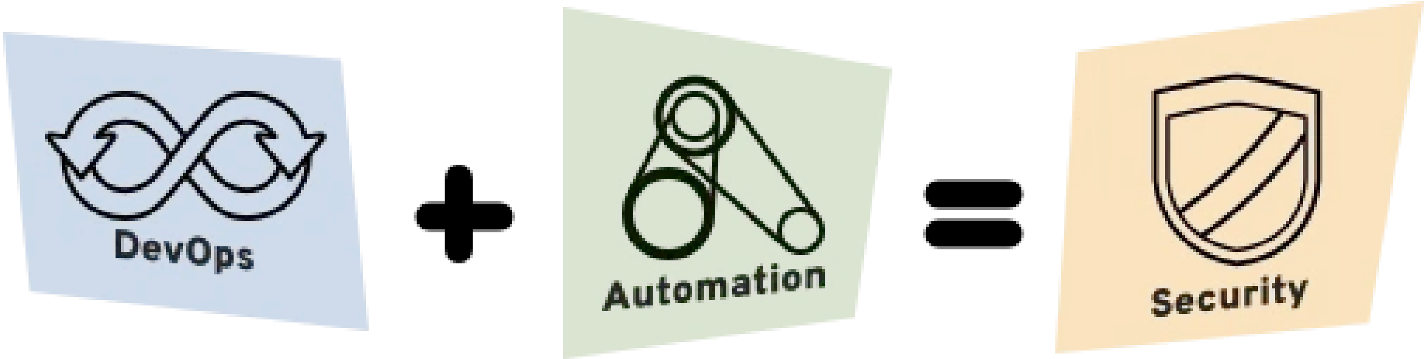
Specialization and adjacent disciplines

- **Architects:** Systems architects have deep expertise in more than one area. They use their experience to design distributed systems.
- Their job descriptions may include defining security zones and segmentation, eliminating single points of failure, planning for future growth, ensuring connectivity among multiple networks and third parties, and other site-wide decision making.
- Good architects are technically proficient and generally prefer to implement and test their own designs.

Specialization and adjacent disciplines

- **DevSecOps** stands for **development**, **security**, and **operations**. It's an approach to culture, automation, and platform design that integrates security as a shared responsibility throughout the entire IT lifecycle.





5-minute read
https://www.redhat.com/en/topics/devops/what-is-devsecops

Basic Linux Commands

- **ls** - Lists directory contents, -l Option long listing format
- **cd** - Changes the current directory.
- **pwd** - Displays the present working directory.
- **cat** - Concatenates and displays files.
- **echo** - Displays arguments to the screen.
- **man** - Displays the online manual.
- **exit -** Exits the shell or your current session.
- **clear** - Clears the screen
- **which -** Locate a command
- Ask commands for help with **--help** or **-h**.

The **MAN** pages

- Man pages are concise descriptions of commands, drivers; file formats, or library routines. They do not address more general topics such as "How do I install a new device?" or "WHy is this system so damn slow?"
- On Linux systems, you can find out the current default search path with the *manpath* command. If necessary, you can set the MANPATH environment variable to override the default search path.

```
$ export MANPATH=/home/share/localman:/usr/share/man
```

System Information

- After you connect to Lunix, type
  - **whoami**
  - **hostname**
  - **date**
  - **cal**
  - **free**
- Commands have three parts; *command*, *options* and *parameters*. Example: **cal –j 3 1999**. “cal” is the command, “-j” is an option (or switch), “3” and “1999” are parameters.
- Options have long and short forms. Example:
  - **date –u**
  - **data --universal**

What is the nature of the prompt?
What was the system’s response to the command?

Help with Commands

- Type
  - **hostname –-help**
  - **man hostname**
  - **info hostname** (gives the same or most information, but must be paged)
- And “**Yes**,” **you can always Google it**

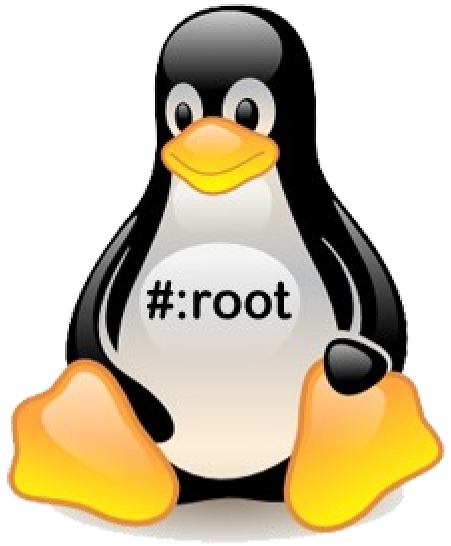
Editing the Command Line with Emacs Keys

- **<Ctrl-a>** go to beginning
- **<Ctrl-e>** go to end
- **<Alt-f>** forward one word
- **<Alt-b>** back one word
- **<Ctrl-f>** forward one character
- **<Ctrl-b>** back one character
- **<Ctrl-d>** delete character
- **<Alt-d>** delete word
- **<Ctrl-u>** delete from cursor to beginning of line
- **<Ctrl-k>** delete from cursor to end of line

See emacs-editing-mode.pdf and emacs-editing-mode-short.pdf

Go to through command history in shell and practice editing.

root



The root user is the master

Linux Directory Structure

The Filesystem Hierarchy “**Google it for now**”

# Linux is ?

- Linux concepts are universal.
- Each distro is slightly different.
- You can accomplish the same goals on most Linux distros.
- You can't make a "wrong" choice!
- Linux Distro = kernel + software
- For Enterprise use what you recommending RHEL **Or** Ubuntu ????
- CentOS = RHEL - branding/logos

Other Sources

- Linux : The Linux Foundation's official website.
- Linux Foundation : Employer of Linus Torvalds and steward of the Linux kernel.
- LWN : A weekly publication that covers the Linux kernel and other open-source software.
- Servers for hackers : High-quality videos, forums, and articles on administration

https://serversforhackers.com/s/fresh-server-security-setup