Intro to Linux

@LegendaryPatMan

Paddy@legendary.industries

Topics Covered

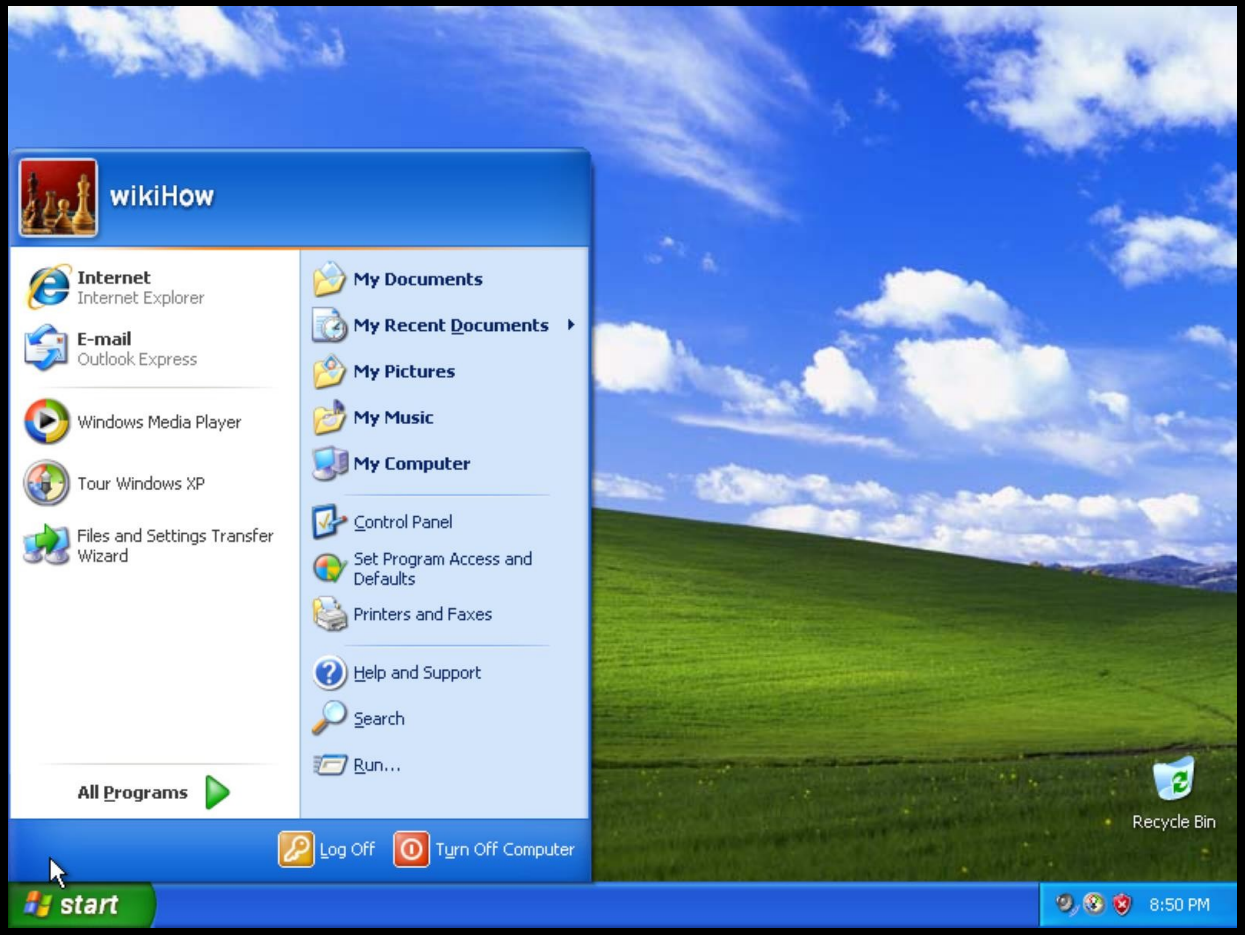
- What is Linux?
- Linux Concepts
- The Cli
- Why should you get used to Linux?
- Sources & Resources
- Q&A

What is Linux?

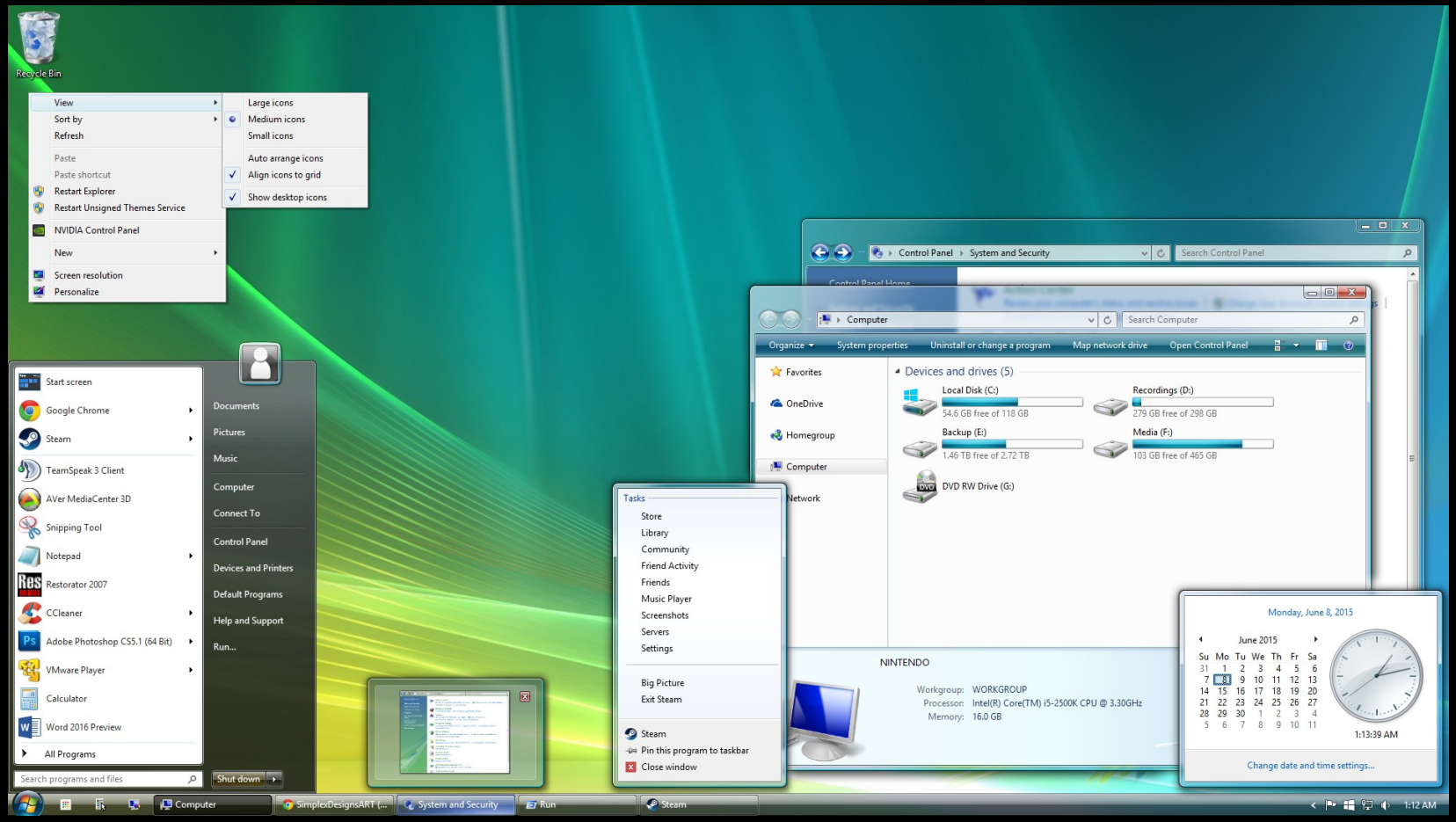
Windows

- Windows is a family of operating systems built around the Windows kernel
- Windows comes in different forms known as Versions
- Each Version has a Series which change it’s feature set
  - Enterprise, Pro, Home etc

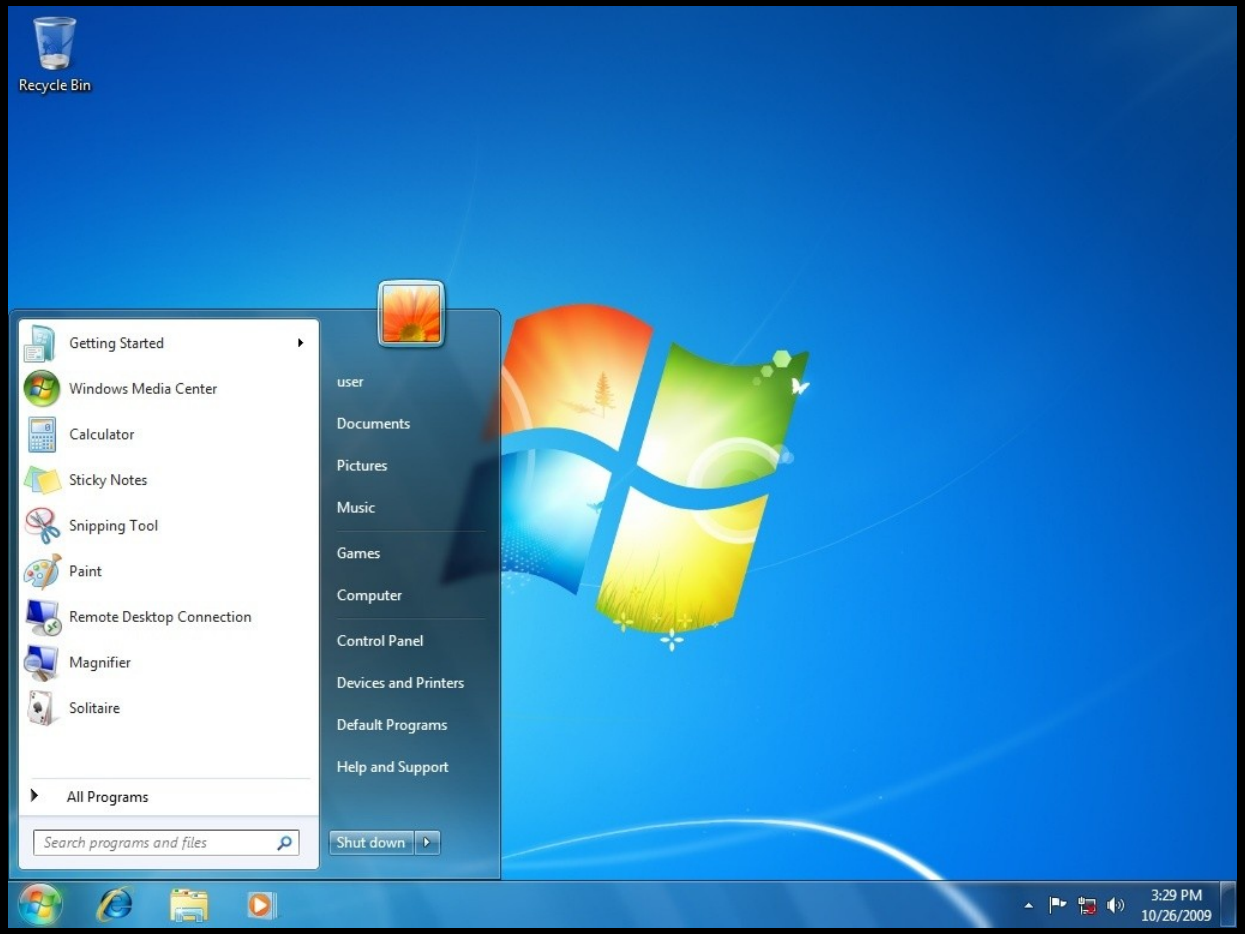
Windows XP


wikiHow
Internet
Internet Explorer
E-mail
Outlook Express
Windows Media Player
Tour Windows XP
Files and Settings Transfer Wizard
All Programs
My Documents
My Recent Documents
My Pictures
My Music
My Computer
Control Panel
Set Program Access and Defaults
Printers and Faxes
Help and Support
Search
Run...
Log Off
Turn Off Computer
Recycle Bin
start
8:50 PM

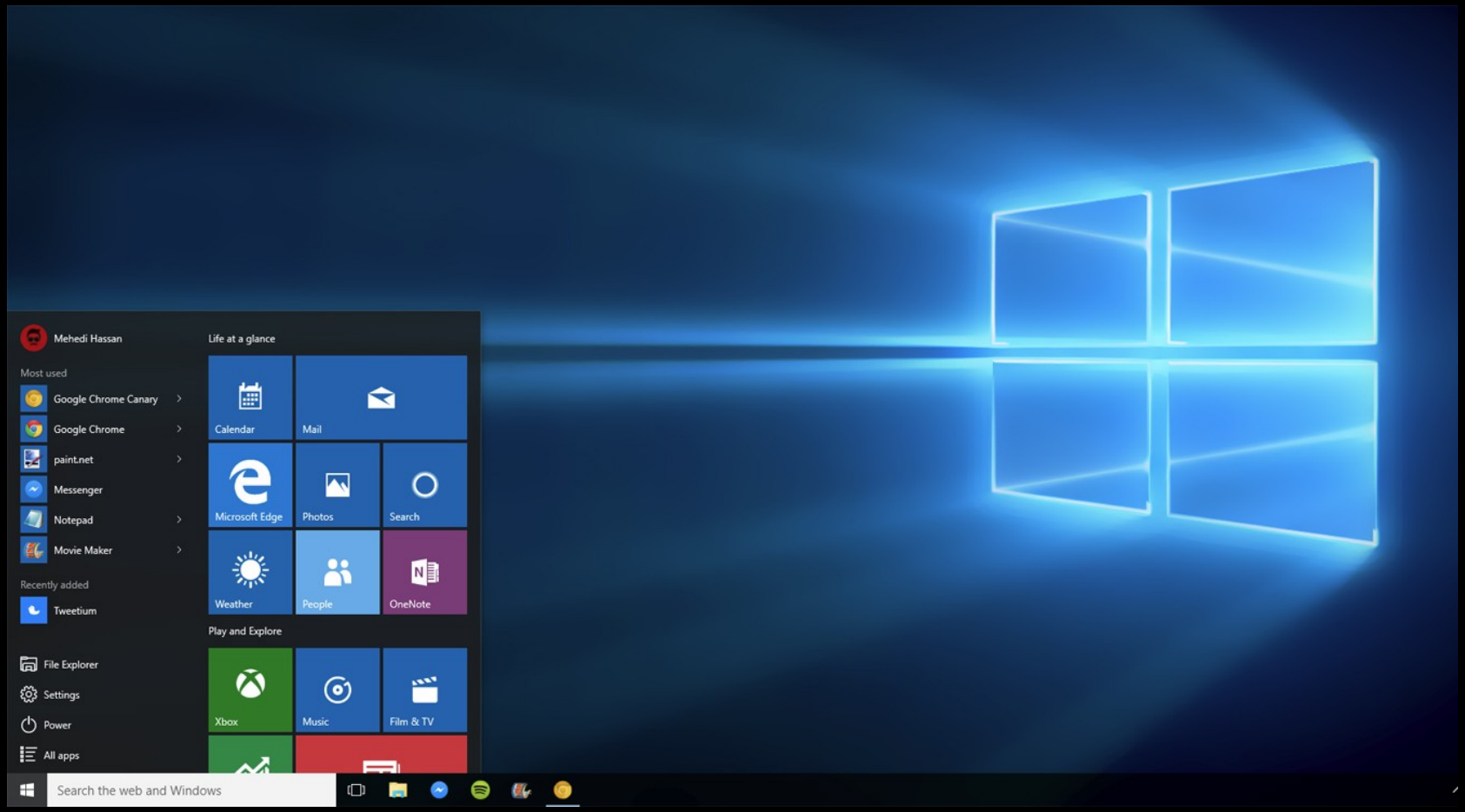
Windows Vista



Windows 7


Recycle Bin
Getting Started
Windows Media Center
Calculator
Sticky Notes
Snipping Tool
Paint
Remote Desktop Connection
Magnifier
Solitaire
All Programs
Search programs and files
user
Documents
Pictures
Music
Games
Computer
Control Panel
Devices and Printers
Default Programs
Help and Support
Shut down
3:29 PM
10/26/2009

Windows 10

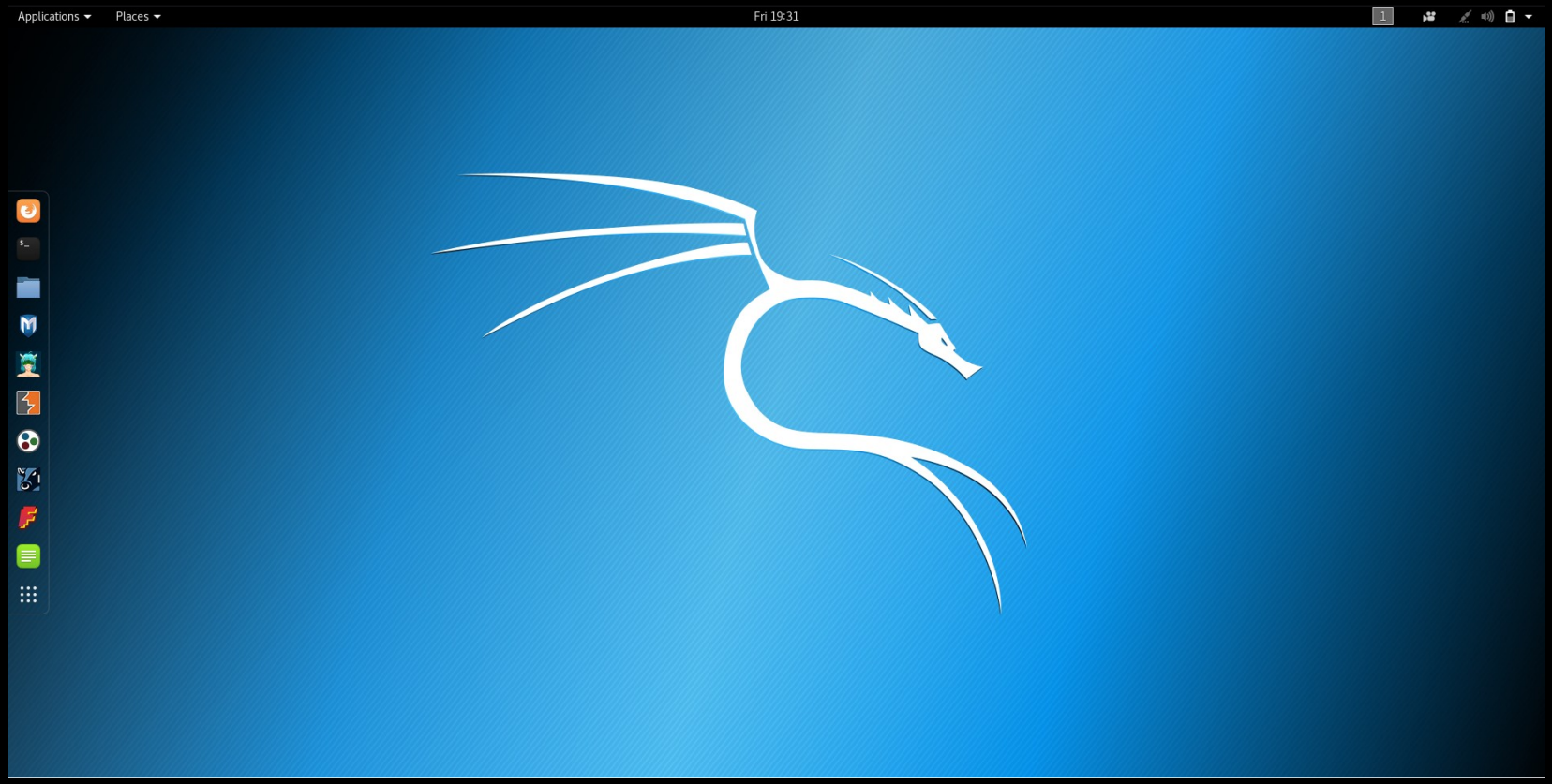

Mehedi Hassan
Most used
Google Chrome Canary
Google Chrome
paint.net
Messenger
Notepad
Movie Maker
Recently added
Tweetium
File Explorer
Settings
Power
All apps
Life at a glance
Calendar
Mail
Microsoft Edge
Photos
Search
Weather
People
OneNote
Play and Explore
Xbox
Music
Film & TV
Search the web and Windows

So how does this compare to Linux?

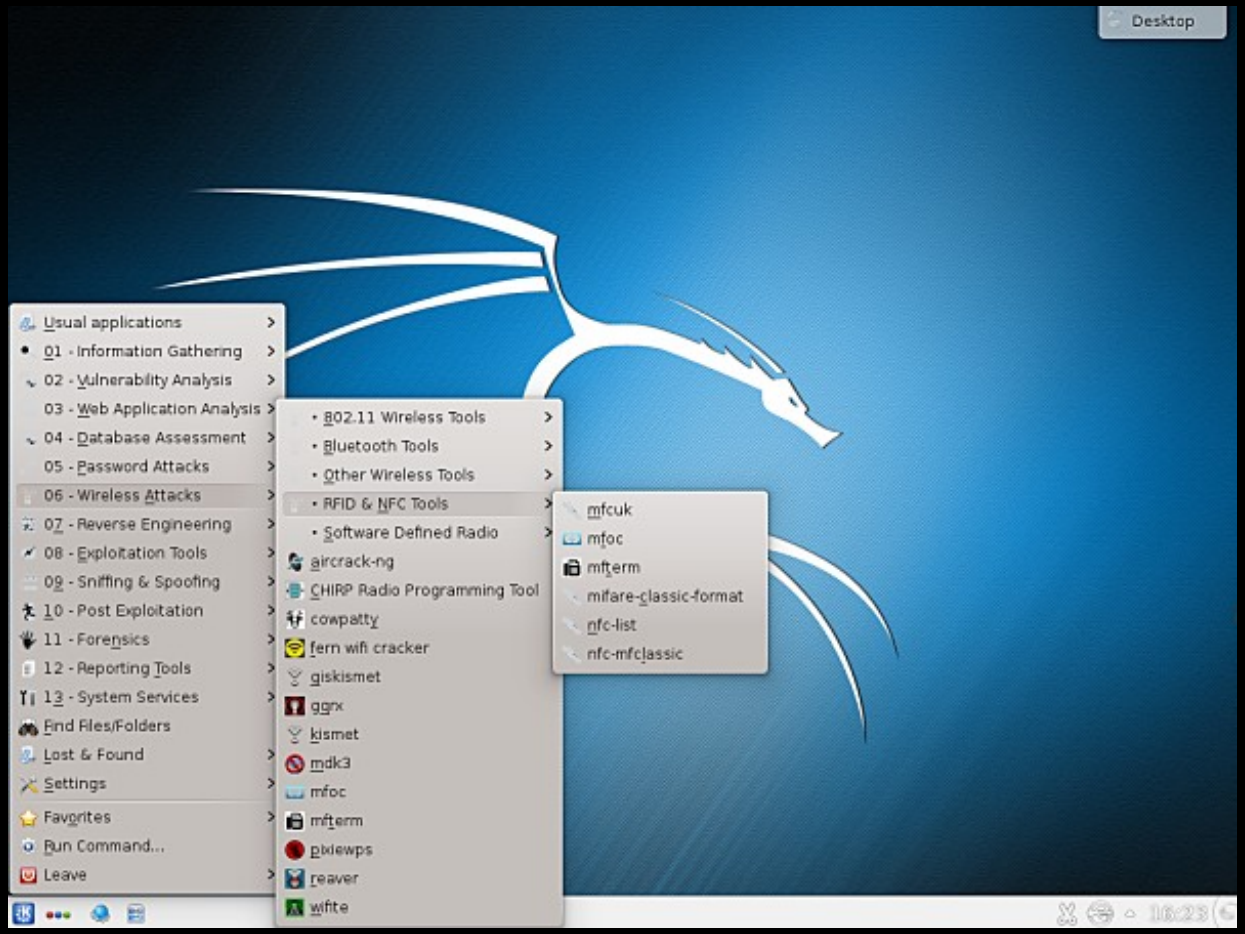
What is Linux?

- Linux is a family of free and open-source software operating systems built around the Linux kernel
- Linux comes in different forms known as Distro’s
- Each Distro has flavours which change how it looks

Kali Distro



KDE Flavor


Desktop
Usual applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - System Services
Find Files/Folders
Lost & Found
Settings
Favorites
Run Command...
Leave
802.11 Wireless Tools
Bluetooth Tools
Other Wireless Tools
RFID & NFC Tools
Software Defined Radio
aircrack-ng
CHIRP Radio Programming Tool
cowpatty
fern wifi cracker
giskismet
gqrx
kismet
mdk3
mfoc
mfterm
pixiewps
reaver
wifite
mfcuk
mfoc
mfterm
mifare-classic-format
nfc-list
nfc-mfclassic

LXDE Flavor


Accessories
Electronics
Graphics
Internet
Kali Linux
Office
Other
Programming
Sound & Video
System Tools
Universal Access
Wine
Preferences
Run
Logout
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
Reporting Tools
System Services
aircrack-ng
burpsuite
hydra
john
maltego
metasploit framework
nmap
owasp-zap
sqlmap
wireshark
KALI LINUX
The quieter you become, the more you are able to hear.
00:30

MATE Flavor


Applications
Places
System
Mon Dec 28, 18:42
Kali Linux Extra Tools
Usual applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - System Services
GoyscriptWPS
GoyscriptWEP
GoyscriptWPA
Airvengers
Handshakeharvest
Her0xDa
Wifi-Eye
Wifite-AUTO
Kali Linux
Kali Linux 2.0 Mate
www.kali-linux.net

XFCE Flavor

Linux Concepts and Comparisons to Windows

Free and Open Source

Free as in no cost

AND/OR

Free as in Freedom

AND

Source Code is shared

Free Software's Four Freedoms

1. The unlimited use for any purpose
2. The right to study how the program works and understand it
3. The right to share copies of the software
4. The freedom to improve the program and to distribute the improvements to the program

https://fsfe.org/freesoftware/basics/4freedoms.en.html

udev

- Device Manager
- Provides a set of generic open source drivers to makes any hardware work with your install
- Ensures that hardware just works when you plug it in

Hardware Support

Works on anything

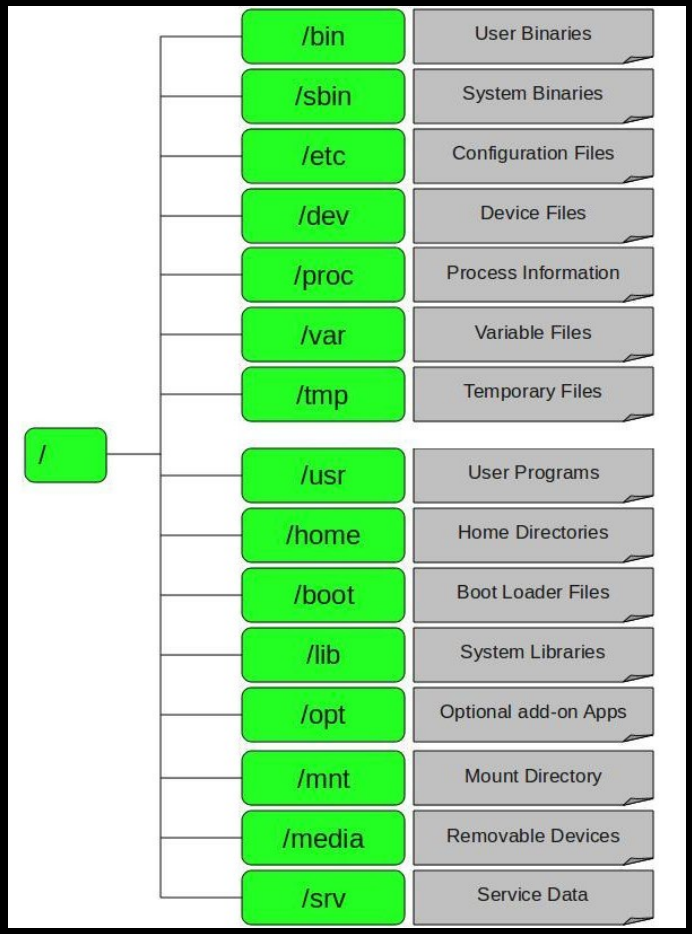
- Support on nearly every device from 1991 to now, and older even stuff you've never heard of like Itanium, RISC-V and Sparc

FHS

Logical layout of files in Linux

Done so;

- Software knows where other software is
- So the user can find files in the system



Data Mobility

You can copy paste your home folder to a new linux install and everything just works

You can even install /home as a partition and change your Linux install without issues

All thank’s to the FHS

Choice of Run Level

The mode of operation

- 0-6 depending on what you need
  - 0 is shutdown/ halt 6 is reboot
  - 1 is rescue, no reboot required
  - 2 and 3 are CLi only
  - 5 is GUI

Security

- Being open, everyone knows how a give piece of software works
- Patches are written, tested deployed in hours to users

Privacy

The Linux platform does not collect user data. Period.

The CLi

Why?!

- A lot of tools you'll use over time are Cli only
  - `airmon-ng`, `aircrack-ng`, `recon-ng`, `r2`
- Some things in courses are CLi only
- In the real world, a lot of work is done in the Cli, espescially on servers even on Windwos
- Get used to it now rather than later

A note on $ and

`$` == regular user

`#` == root/superuser

root/superuser is the admin

`sudo <cmd>` to run commands as root

`su root` to swtch user to root

Getting Help

```
ls --help
man ls
info ls
```

Creating and modifying files

- `touch` - Create a file
- `rm` - Delete a file with a warning
  - `rm -rf` - Delete a file without warning

Text Editors

`nano` - A simple text editor

`vim` - A a black hole from which you will never emerge

- `:q` to quit

`emacs` - A whole operating system

Getting around the file system

`pwd` == list the current directory

`ls` == list files in a directory

`cd` == change directory

`pwd`

`touch abc.txt`

`nano abc.txt`

type a

b

c

d

e

`Ctrl-X` to save and `y` to overwrite the file

`ls` to verify it’s there

Looking at files

`cat` - Print a file to the CLi

`less` - Print a file to the CLi in a human readable format

`tail` - Print the first and last lines of a file

`file` - Identifies what type of file something is

Searching For Stuff

`locate` - Locates a file on the system

`grep` - Search in side files for a particular pattern

```
cat abc.txt
less abc.txt
q to exit less
tail abc.txt
file abc.txt
cd /
pwd
ls
locate abc.txt
```

Manipulating files

`mkdir` - make a directory ie folder

- May require admin permissions so `sudo` it

`cp` - Copy file

`mv` - Move or rename a file

- `mv abc.txt abcde.txt` to rename
- `mv abcde <location>` to move

File Permissions

`chmod` - change file permissions

- `chmod -x <filename>`
  - To make it executable
- `chmod 600 ~/.ssh/authorized_keys`
  - To make sure that only you can read your SSH keys

Archives and tarballs

`.zip`, `.7z`, `.rar` etc. Generally `.tar`, sometimes `.tgz` on Linux systems

`tar` or `.tar.gz` – tar is archived gz is compressed

`gzip` and `gunzip` can do the same but easier, though it not always installed

`tar cvf abcde.txt`

- To archive

`tar xvf abcde.tar`

- To unarchive

`tar czvf abcde.txt`

- To archive and compress

`tar xzvf abcde.tar.gz`

- To unarchive and decompress

`gzip abcde.txt` - To archive and compress

`gunzip abcde.gz` - To unarchive and compress

Installing Software

- `dpkg`, `apt`, `aptitude` and `apt-get` installed on Kali
- `apt-get` is the most commonly used

```
sudo apt-get udpate
```
- To update the cache with updates

```
sudo apt-get upgrade -y
```
- To install said updates and bypass warning (-y)

```
sudo apt-cache search gzip gunzip
```
- Search for gzip gunzip

```
sudo apt-get install gzip gunzip
```
- Install gzip gunzip

```
apt-get moo
```

```
sudo dpkg -i <filename.deb>
```
- Install .deb files found elsewhere

User Managment

- `useradd` - Add a user
- `passwd` – Change password
  - `passwd <username>` to change someone elses passsord
- `userdel` - Delete a user
- `usermod` - modify a user
  - `usermod -aG sudo <username>` - make user sudo

Doing More

`top` - displays a task manager

`kill` - kill a process

- `kill <PID>`

`netstat` - display all open network connections

Useful commands

`echo` - allow you to print strings and variables

`&&` string two commands together and execute

- `sudo apt-get update && sudo apt-get upgrade -y`

`|` - allow you to add an output to a new command

- `sudo apt-get --help | grep -i cow`

Aliases allow you to shorten commands you use regularly

- `alias <ud>='sudo apt-get update && sudo apt-get upgrade -y'`

Being Lazy

1. Use text editors to create files rather than using `touch`
2. Use tab to finish commands
3. Aliases can be handy to reuse often used commands

Run Levels

`runlevel` - to show the last and current run levels

`init 0` - to shutdown can be `poweroff`

`init 1` - to enter rescue mode

`init 3` - to switch to CLi only mode

`init 5` - to enter GUI mode

`init 6` - to reboot or `reboot`

Why should you get used to Linux?

It’s part of some courses here

Entire courses in this college are built on it
You’ll have to learn to use it sooner or later

Operating Systems and Professional Penetration Testing

The world is built on it

60% of web servers

66% of games consoles

80% of mobile phones

99% of super computers

99% of start ups

100% of IoT devices; even microsoft

Governments

- Brazil, Russia, China and North Korea are built on Linux
- India, France, Germany and Spain have taken huge steps to build on Linux
- The European Commission is working to ensure Europe is built on Linux and FOSS

Sources & Resources

Sources

- Ten Steps to Linux Survival
  - https://www.oreilly.com/learning/ten-steps-to-linux-survival
- Practical LPIC-1 Linux Certification Study Guide by David Clinton
  - https://cloud.legendary.industries/index.php/s/CYPAf7PRtfdnyRX

Good reading

- Introducing Linux Distros by Jose Dieguez Castro
  - https://www.apress.com/us/book/9781484213933
  - https://cloud.legendary.industries/index.php/s/3zsGCybCCmqt4b4
- Linux Pocket Guide by Daniel J. Barrett
  - https://linuxpocketguide.com/
  - https://cloud.legendary.industries/index.php/s/8PFWoQN4ordLz5y

CTF’s

- CTF with 34 challenges to teach you the Linux CLI envioment
  - http://overthewire.org/wargames/bandit/

Q&A