LEARNING EXPERIENCE KNOWLEDGE

التعلم الخبرة المعرفة

المؤسسة العامة للتدريب التقني والمهني

Technical and Vocational Training Corporation

معهد ميثاق للتدريب

HAQ TRAINING INSTITUT

الهاكر الاخلاقي

أ.هيله الحارثي

Day 2:Introduction to kali Linux

Objective :

- Understanding the concept of virtual environment
- Understanding kali linux basic command
- Kali-linux file Permission
- Kali-linux feature
- Common Applications of Linux

What is Linux ?

- just like Windows, iOS, and Mac OS, Linux is an operating system.
- In fact, one of the most popular platforms on the planet, Android, is powered by the Linux operating system.
- An operating system is software that manages all of the hardware resources associated with your desktop or laptop. To put it simply, the operating system manages the communication between your software and your hardware. Without the operating system (OS), the software wouldn?t function.

```
irror_mod = modifier_ob
t mirror object to mirror
irror_mod.mirror_object
operation == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
_operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
_operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

election at the end -add
_ob.select= 1
ier_ob.select=1
ntext.scene.objects.activ
("Selected" + str(modifier
irror_ob.select = 0
bpy.context.selected_obj
ata.objects[one.name].se

int("please select exactl

- OPERATOR CLASSES ----

types.Operator):
X mirror to the selected
ject.mirror_mirror_x"
rror X"

ontext):
xt.active_object is not
```

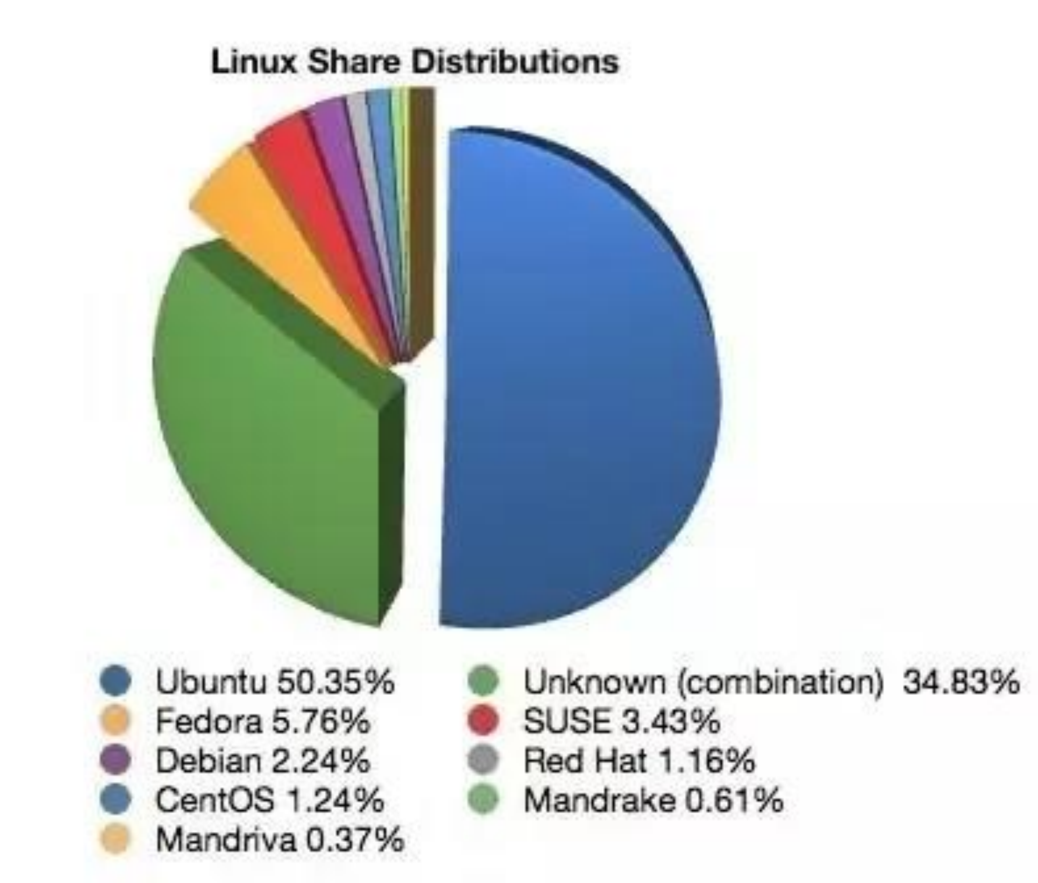
Linux Basics

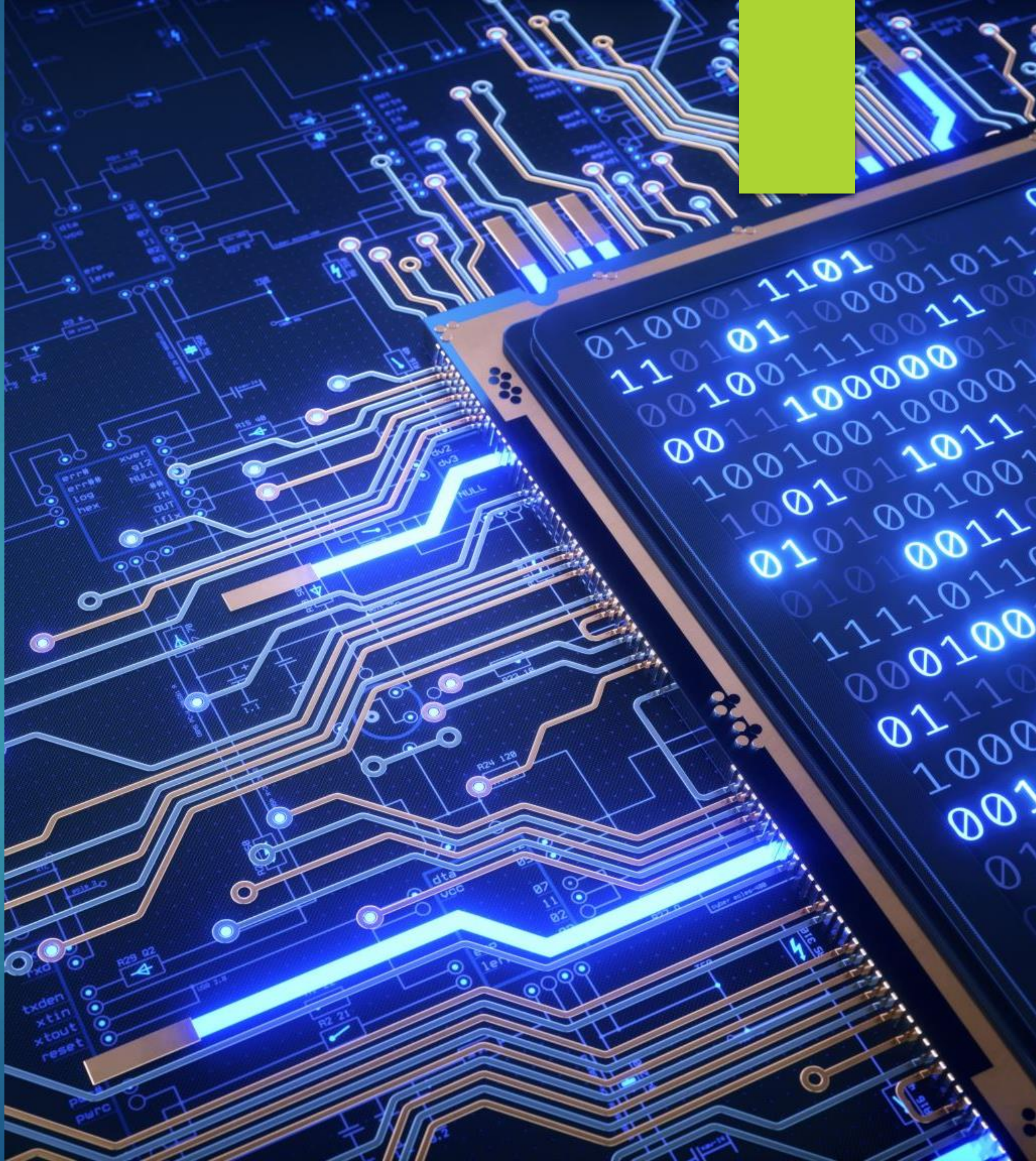
- Linux is one of popular version of UNIX operating System.
- It is open source as its source code is freely available.
- It is free to use.

Major Linux Operating Systems

- *Redhat Linux*—Used mostly for administration purpose.
- *Debian Linux*—Designed for using only in open source software.
- *Ubuntu Linux*—Designed mostly for personal use.
- *Mac OS X*—Used in all Apple computers.
- *Solaris*—Used in many commercial environments.
- *kali Linux*—Used mostly for penetration testing.

Popular Linux distributions





06:09 PM
Trash
File System
Home
KALI
BY OFFENSIVE SECURITY

ما هو كالي لينكس؟

- Kali Linuxهو توزيعة Linux مبنية على Debian تهدف إلى اختبار الاختراق المتقدم والتدقيق الأمني.
-

يحتوي Kali Linuxعلى عدة أدوات لاستخدامات مختلفه في أمن المعلومات ، مثل:

  - اختبار الاختراق .Penetration Testing
  - أبحاث الأمان ,Security research
  - الهندسة العكسية Computer Forensics, and Reverse Engineering
- تم تطوير Kali Linux وتمويله وصيانته بواسطة Offensive Security، وهي شركة رائدة في التدريب على أمن المعلومات.
  كان يُعرف سابقًا باسم Backtrack
- UNIX > Linux > BackTrack > Kali

مزايا الكالي

Information Gathering

Vulnerability Analysis

Wireless Attacks

Web Applications

Exploitation Tools

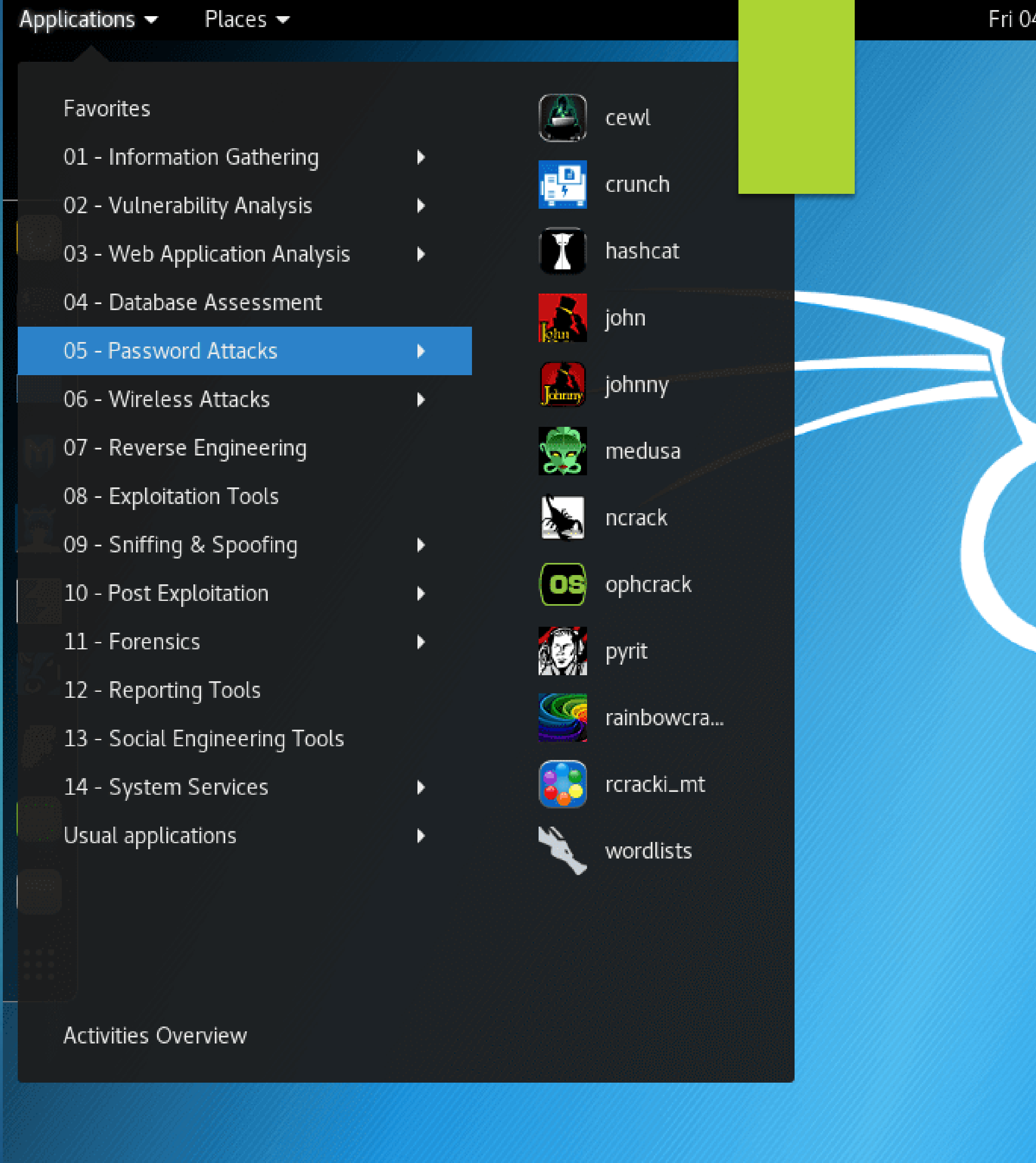
Forensics Tools

Sniffing & Spoofing

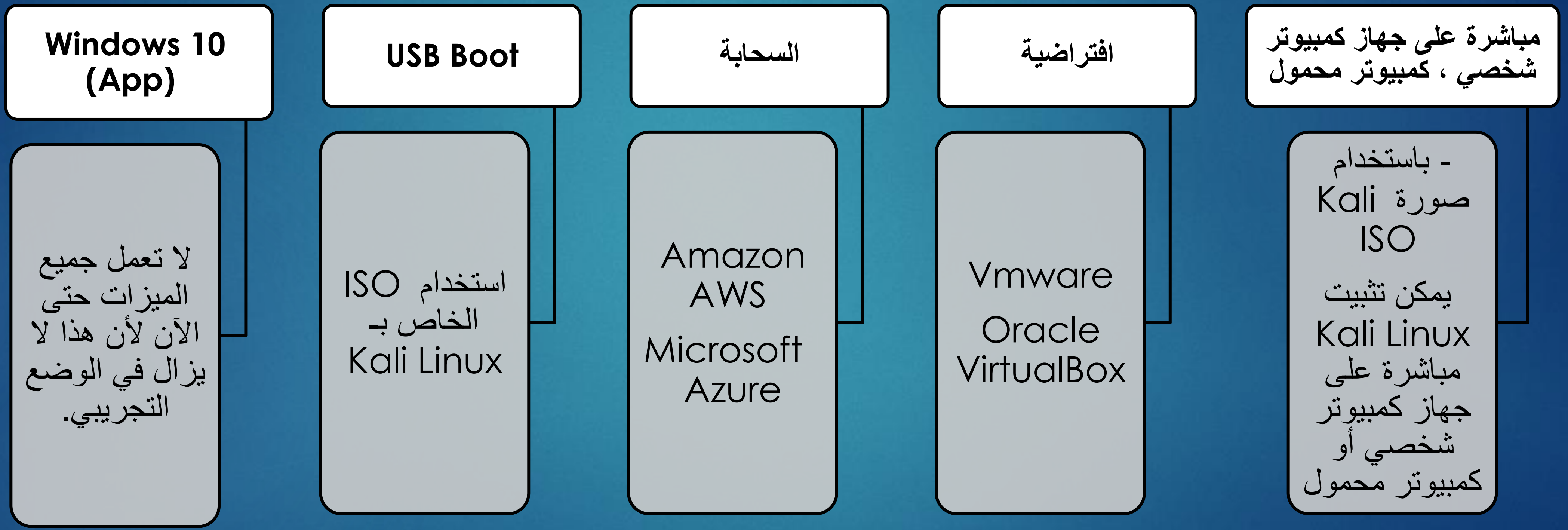
Password Attacks

Reverse Engineering

Reporting Tools



طرق تشغيل Kali Linux



مباشرة على جهاز كمبيوتر شخصي ، كمبيوتر محمول

- باستخدام صورة Kali ISO

يمكن تثبيت Kali Linux مباشرة على جهاز كمبيوتر شخصي أو كمبيوتر محمول

افتراضية

Vmware

Oracle VirtualBox

السحابة

Amazon AWS

Microsoft Azure

USB Boot

استخدام ISO الخاص بـ Kali Linux

Windows 10 (App)

لا تعمل جميع الميزات حتى الآن لأن هذا لا يزال في الوضع التجريبي.

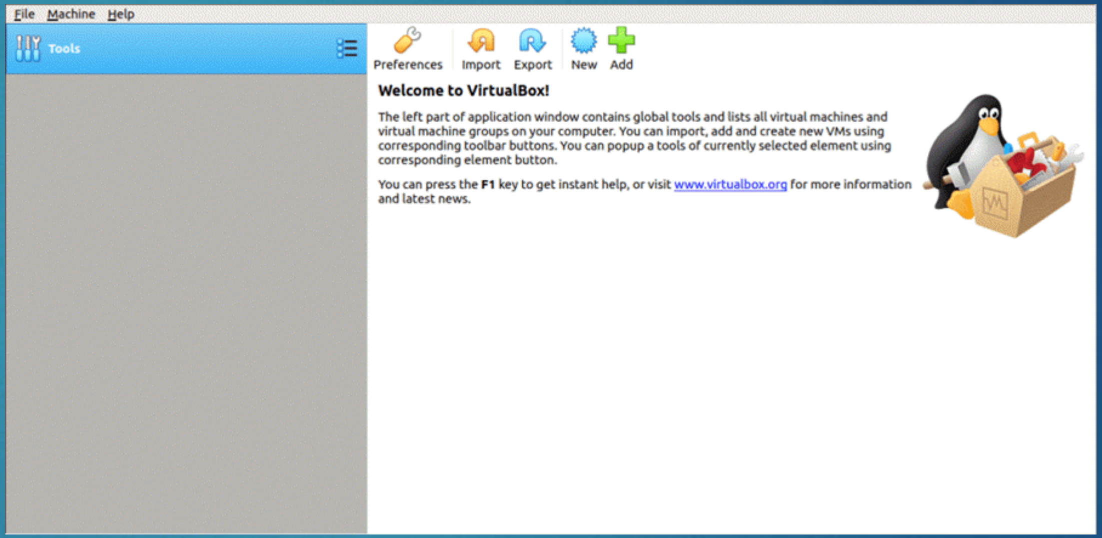
Take
A Break

تحميل kali on Virtual Box

الخطوة ١) نحميل كلا من :

[VirtualBox]

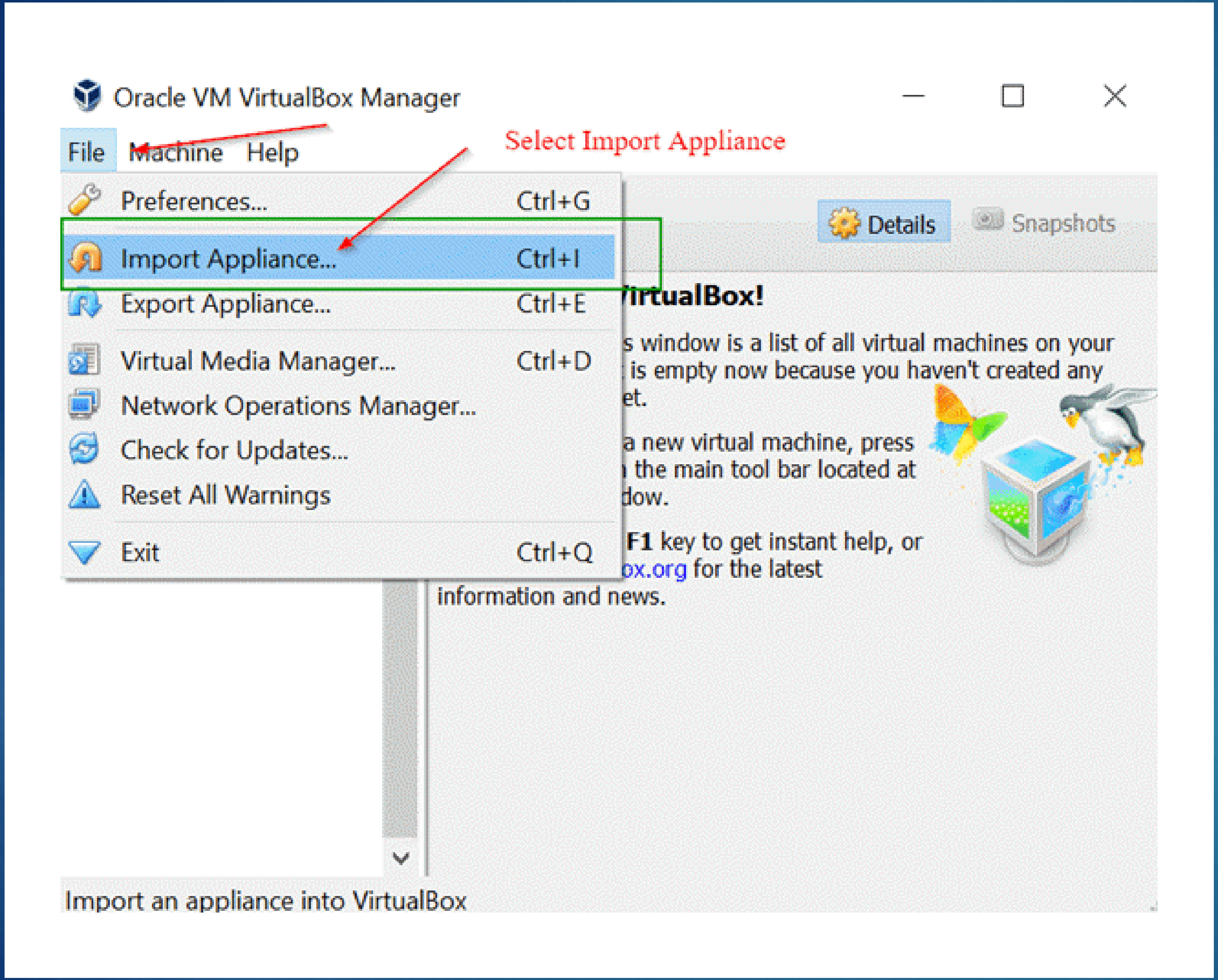
[Kali linux]



Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.


Oracle VM VirtualBox Manager
File
Machine
Help
Select Import Appliance
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
Virtual Media Manager... Ctrl+D
Network Operations Manager...
Check for Updates...
Reset All Warnings
Exit Ctrl+Q
Details
Snapshots

irtualBox!

s window is a list of all virtual machines on your
is empty now because you haven't created any
et.

a new virtual machine, press
the main tool bar located at
dow.

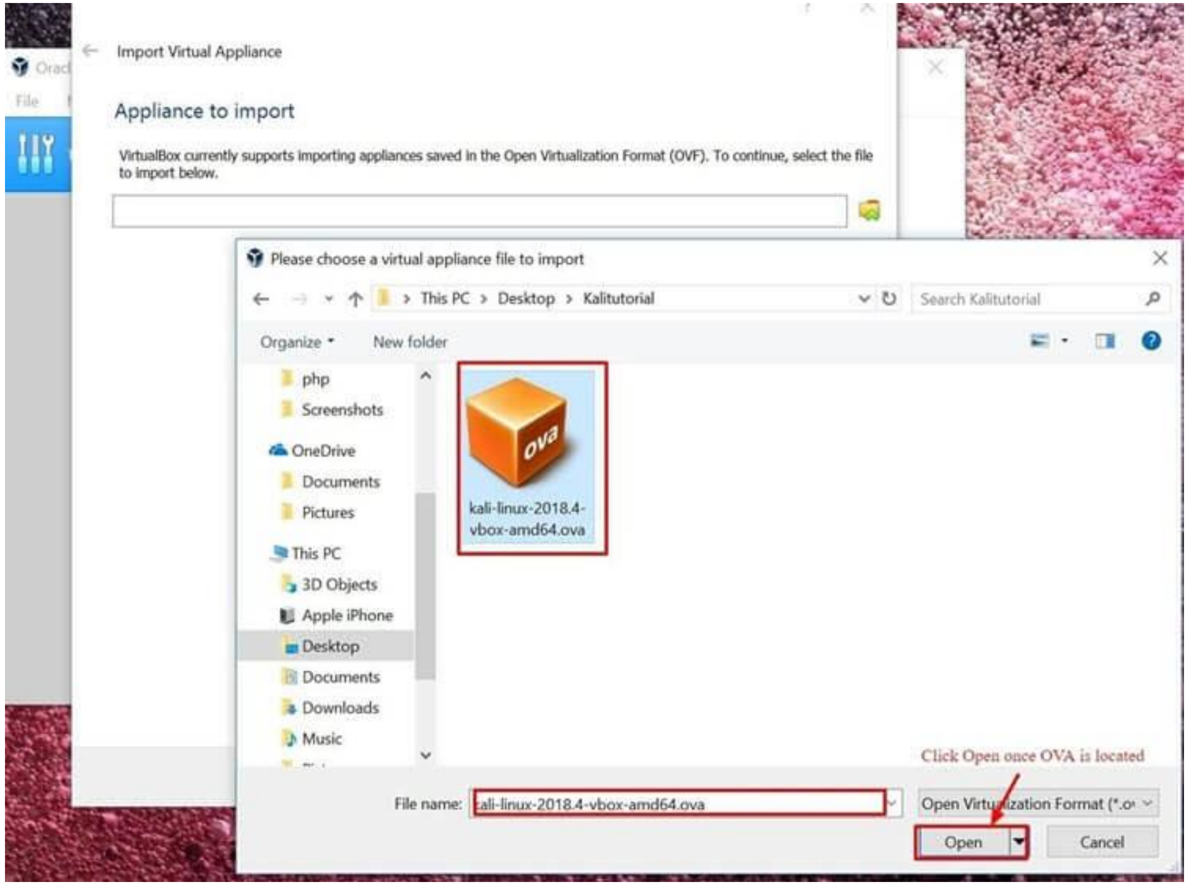
F1 key to get instant help, or
ox.org for the latest
information and news.

Import an appliance into VirtualBox

الخطوة2) افتح تطبيقOracle
VirtualBox ومن القائمة ،
"ملف" حدد ،"استيراد جهاز“

File Menu -> Import Appliance

- الخطوة (3في الشاشة التالية "جهاز
للاستيراد "، تصفح إلى موقع ملف OVA
الذي تم تنزيله وانقر فوق فتح



Import Virtual Appliance

Appliance to import

VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

Please choose a virtual appliance file to import

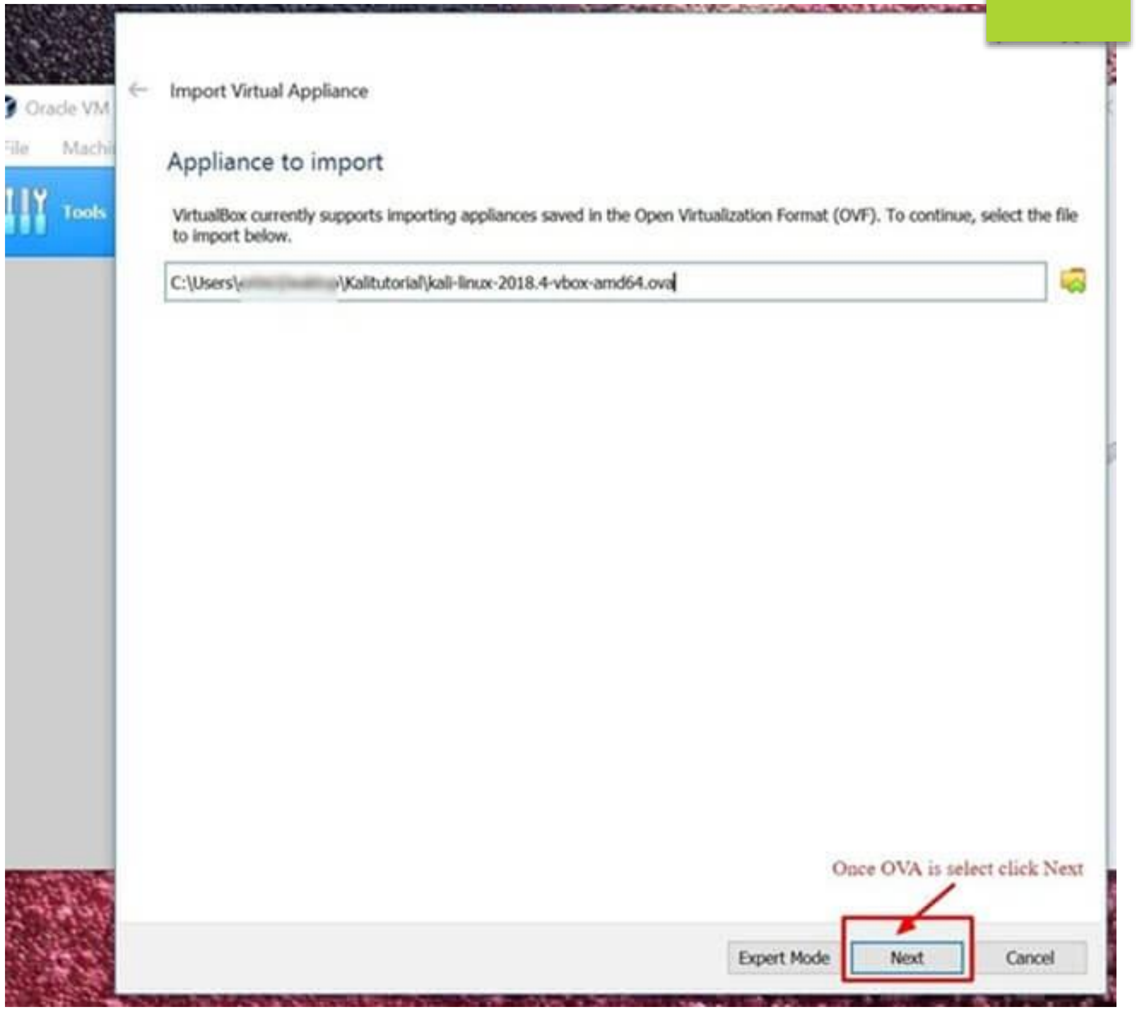
This PC › Desktop › Kalitutorial

File name: kali-linux-2018.4-vbox-amd64.ova

Open Virtualization Format (*.o

Click Open once OVA is located

- بمجرد النقر فوق فتح ، سيتم (4الخطوة
"جهاز للاستيراد"نقلك مرة أخرى إلى
ببساطة انقر فوق التالي



Import Virtual Appliance

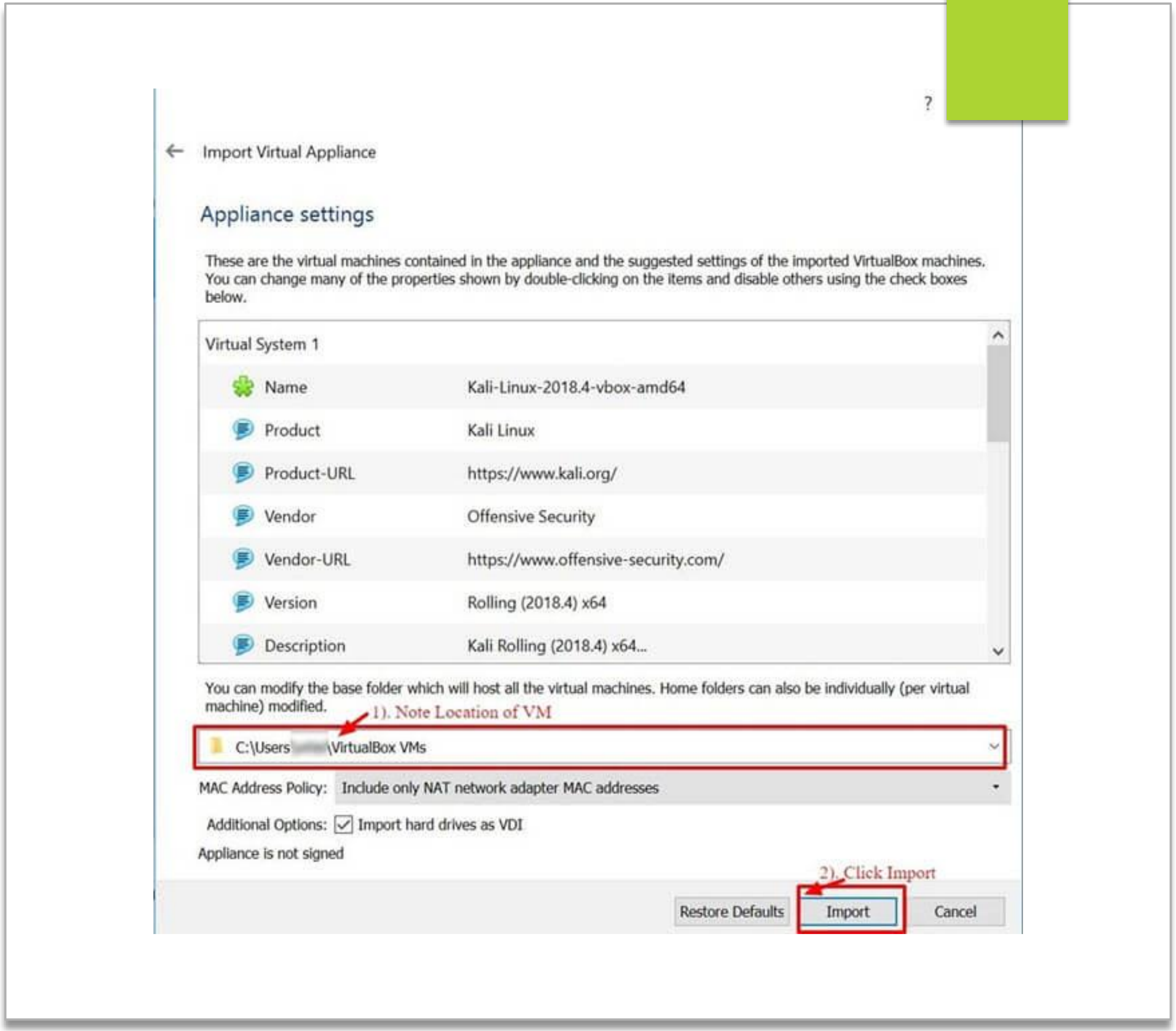
Appliance to import

VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

C:\Users\[redacted]\Kalitutorial\kali-linux-2018.4-vbox-amd64.ova

Once OVA is select click Next

- الخطوة (5)تعرض الشاشة التالية "إعدادات الجهاز "ملخصًا لإعدادات الأنظمة ، مع ترك الإعدادات الافتراضية على ما يرام .كما هو موضح في لقطة الشاشة أدناه ، قم بتدوين مكان وجود الجهاز الظاهري ثم انقر فوق استيراد.



← Import Virtual Appliance

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1

Name	Kali-Linux-2018.4-vbox-amd64
Product	Kali Linux
Product-URL	https://www.kali.org/
Vendor	Offensive Security
Vendor-URL	https://www.offensive-security.com/
Version	Rolling (2018.4) x64
Description	Kali Rolling (2018.4) x64...

You can modify the base folder which will host all the virtual machines. Home folders can also be individually (per virtual machine) modified.

1). Note Location of VM

C:\Users\[redacted]\VirtualBox VMs

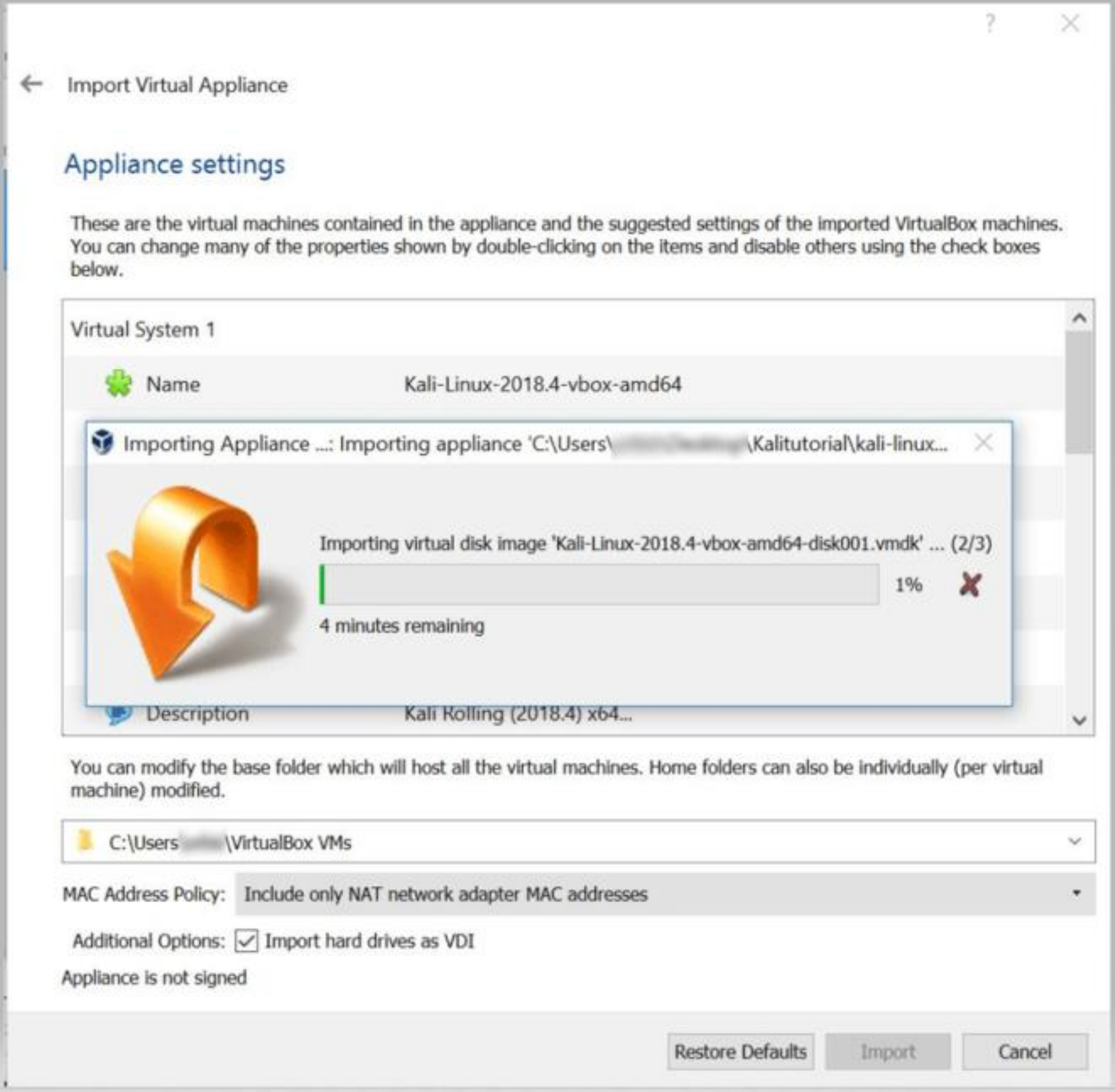
MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: ☑ Import hard drives as VDI

Appliance is not signed

2). Click Import

الخطوة ٦) سيقوم برنامج VirtualBoxالآن
باستيراد جهاز .Kali Linux OVA قد تستغرق هذه
العملية من ٥ إلى ١٠ دقائق حتى تكتمل.



Import Virtual Appliance

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1

Name Kali-Linux-2018.4-vbox-amd64

Importing Appliance ...: Importing appliance 'C:\Users\[redacted]\Kalitutorial\kali-linux...

Importing virtual disk image 'Kali-Linux-2018.4-vbox-amd64-disk001.vmdk' ... (2/3)

1%

4 minutes remaining

Description Kali Rolling (2018.4) x64...

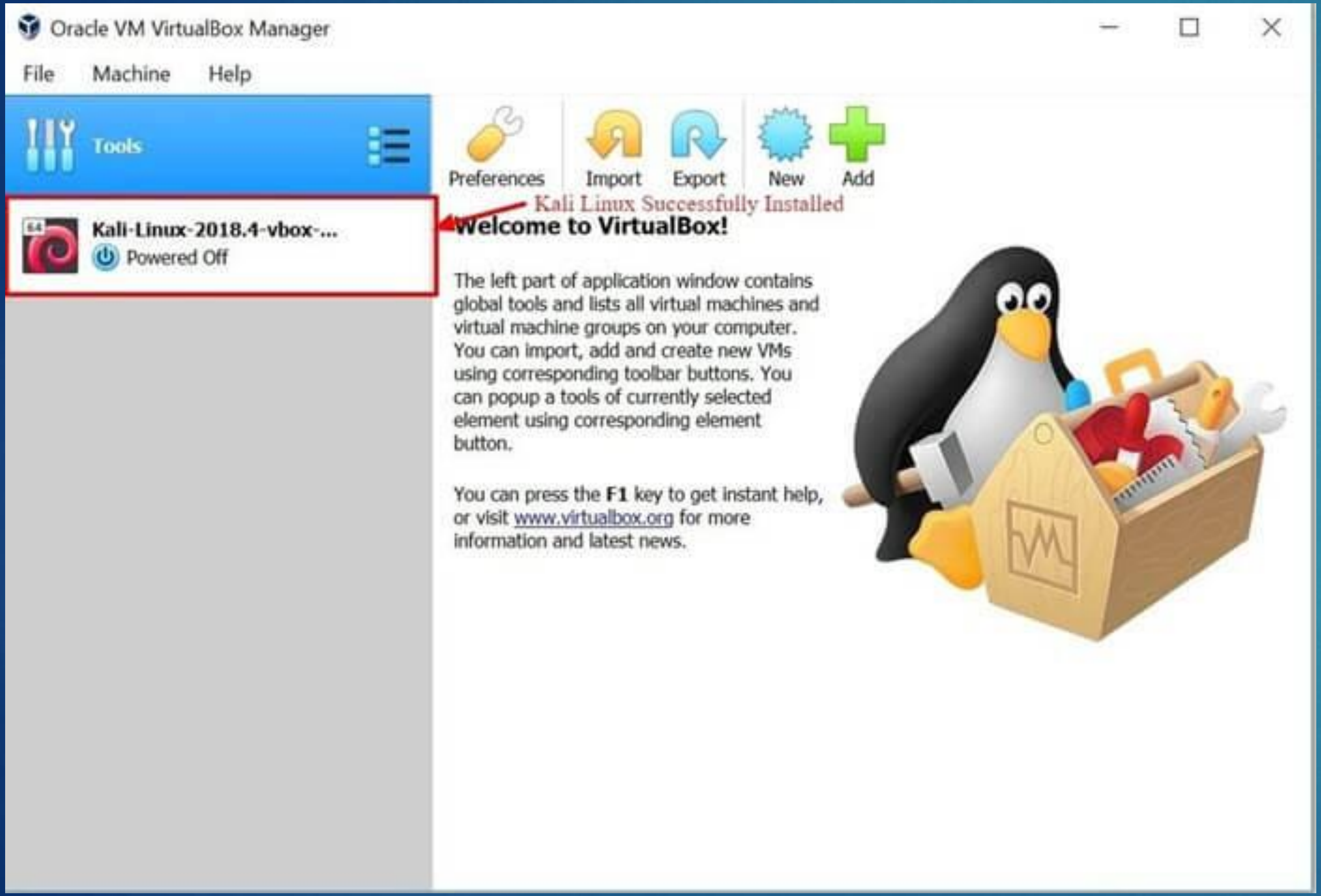
You can modify the base folder which will host all the virtual machines. Home folders can also be individually (per virtual machine) modified.

C:\Users[redacted]\VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: ☑ Import hard drives as VDI

Appliance is not signed

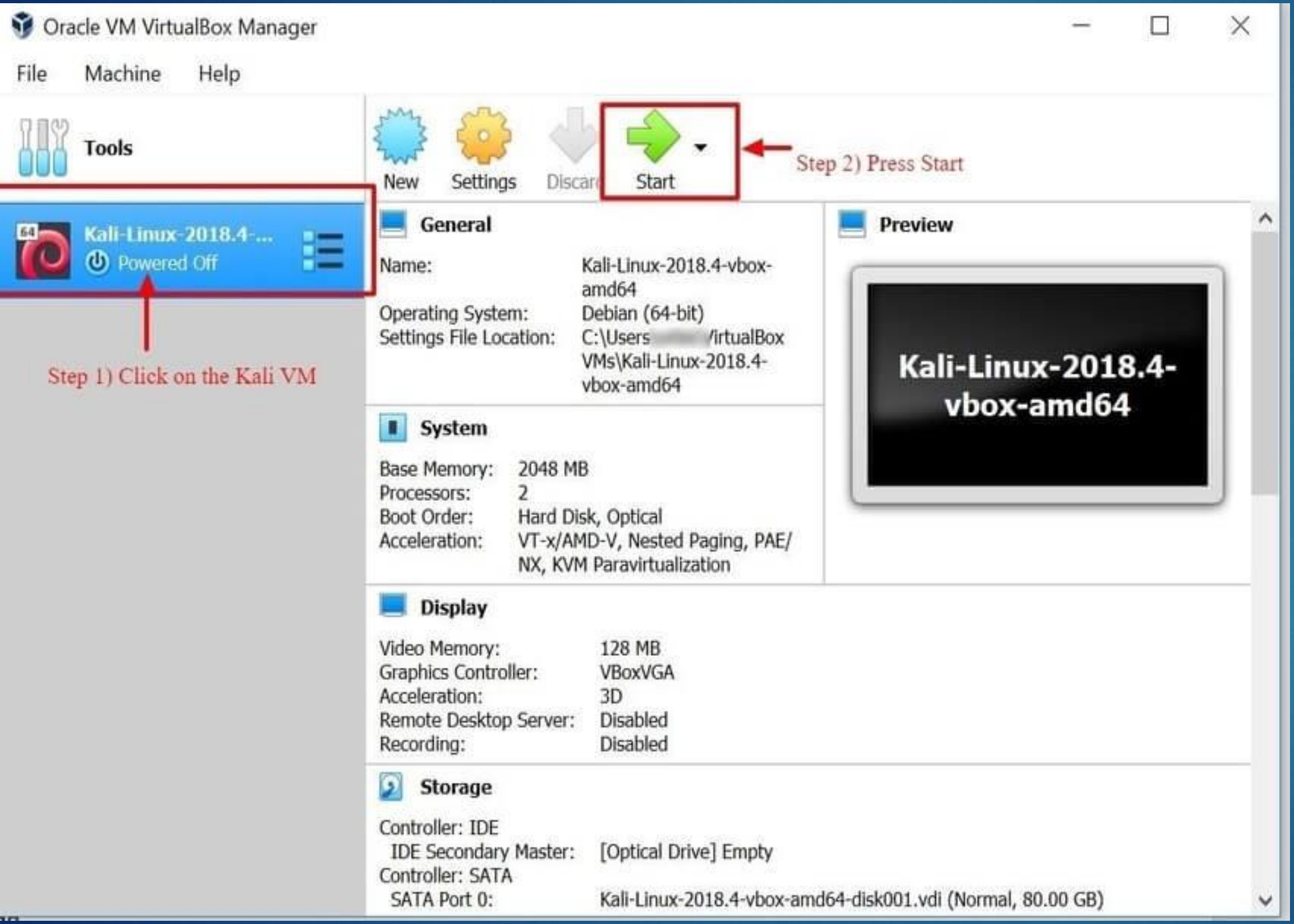

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
Preferences
Import
Export
New
Add
Kali Linux Successfully Installed
Kali-Linux-2018.4-vbox-...
Powered Off

Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

الخطوة ٧) تهانينا ، تم تثبيت Kali Linux
بنجاح على .VirtualBoxيجب أن تشاهد الآن
Kali Linux VMفي VirtualBox
Console.بعد ذلك ، سنلقي نظرة على Kali
Linuxوبعض الخطوات الأولية التي يجب
تنفيذها.



Step 1) Click on the Kali VM

Step 2) Press Start

General

Name: Kali-Linux-2018.4-vbox-amd64
Operating System: Debian (64-bit)
Settings File Location: C:\Users[redacted]irtualBox VMs\Kali-Linux-2018.4-vbox-amd64

System

Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

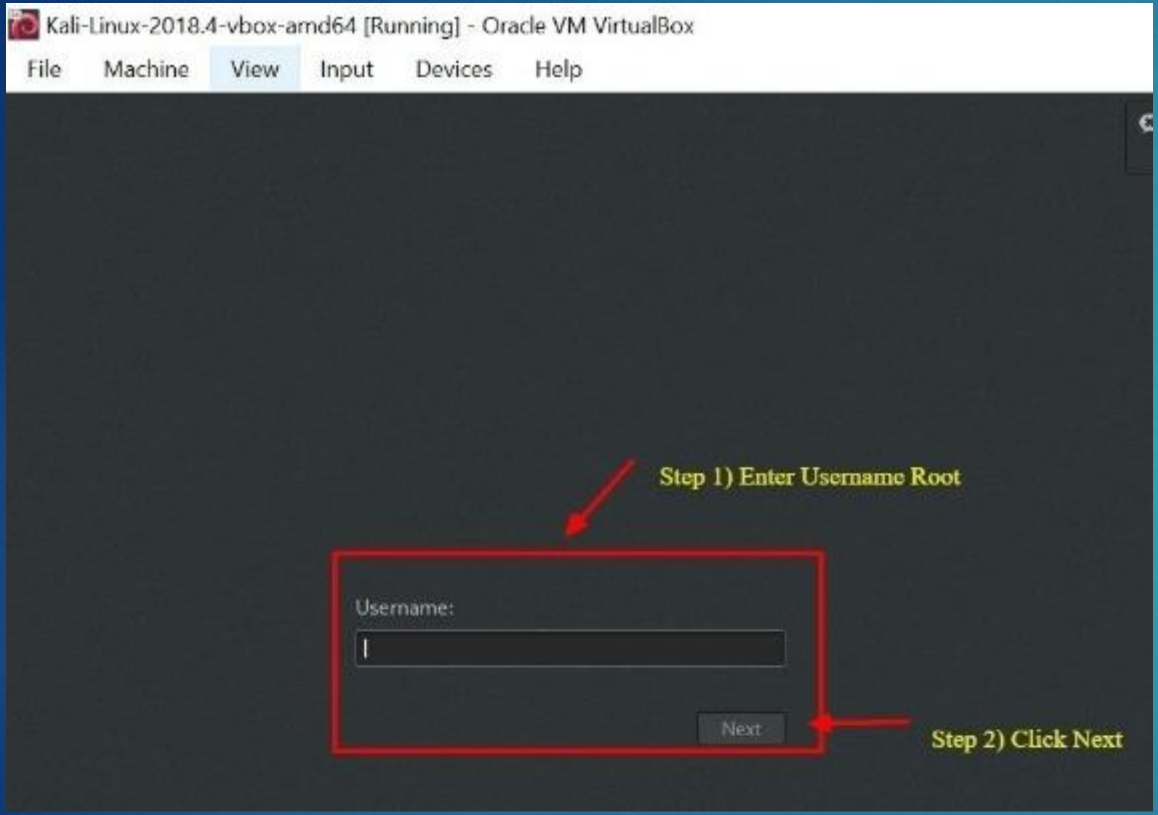
Video Memory: 128 MB
Graphics Controller: VBoxVGA
Acceleration: 3D
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
  IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
  SATA Port 0: Kali-Linux-2018.4-vbox-amd64-disk001.vdi (Normal, 80.00 GB)

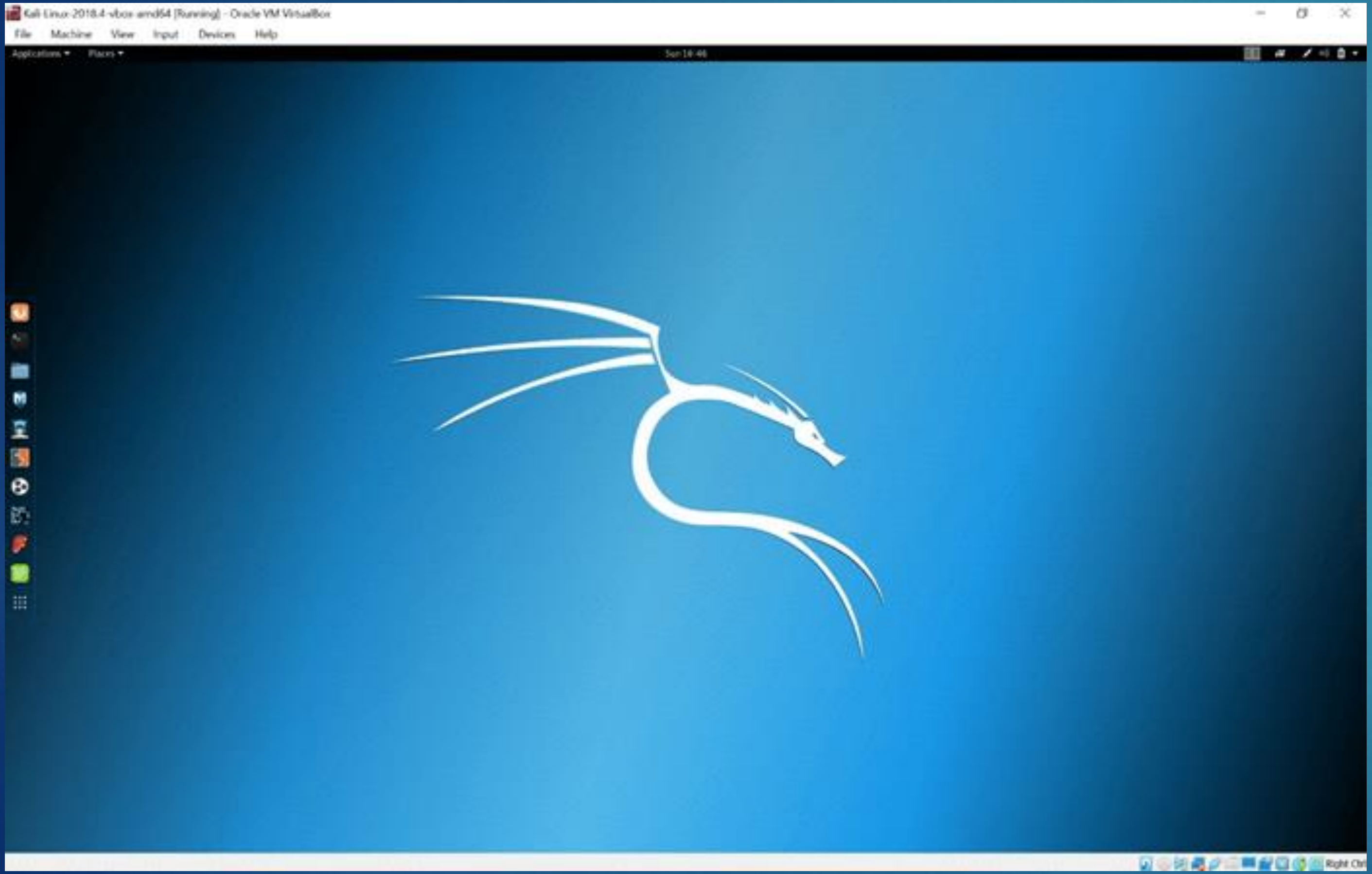
الخطوة ٨) انقر فوق Kali Linux VMداخل لوحة
معلومات VirtualBoxوانقر فوق ابدأ ، سيؤدي
ذلك إلى تشغيل نظام التشغيل .Kali Linux

الخطوة ٩) في شاشة تسجيل الدخول ، أدخل “root" كاسم مستخدم
وانقر فوق "التالي".

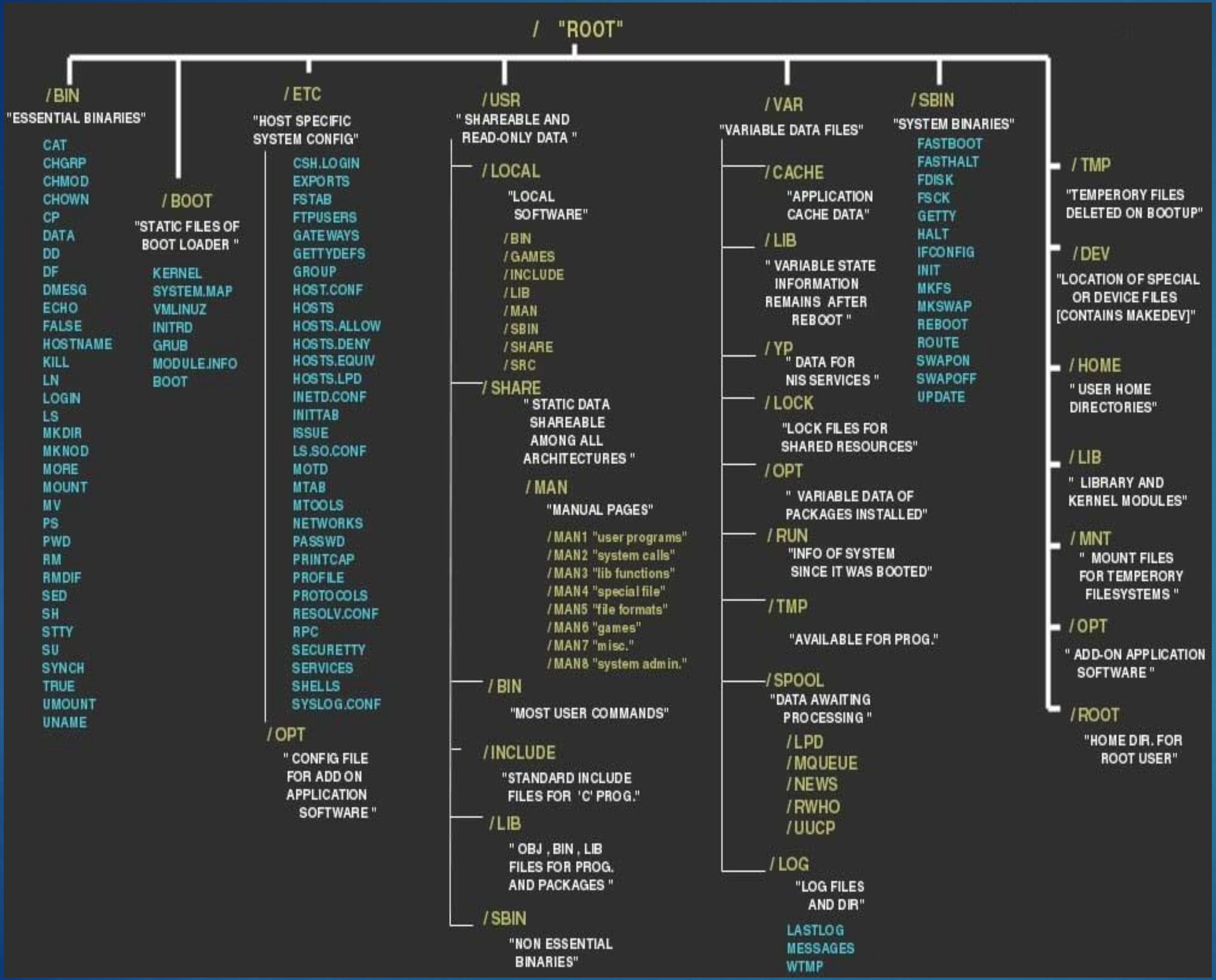

Kali-Linux-2018.4-vbox-amd64 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Username:
Next

Step 1) Enter Username Root

Step 2) Click Next



الخطوة ١٠) كما ذكرنا سابقًا ، أدخل "toor" ككلمة
مرور وانقر فوق تسجيل الدخول. ستكون الآن حاضرًا مع
Kali Linux GUI Desktop. تهانينا ، لقد قمت بتسجيل
الدخول بنجاح إلى Kali Linux.

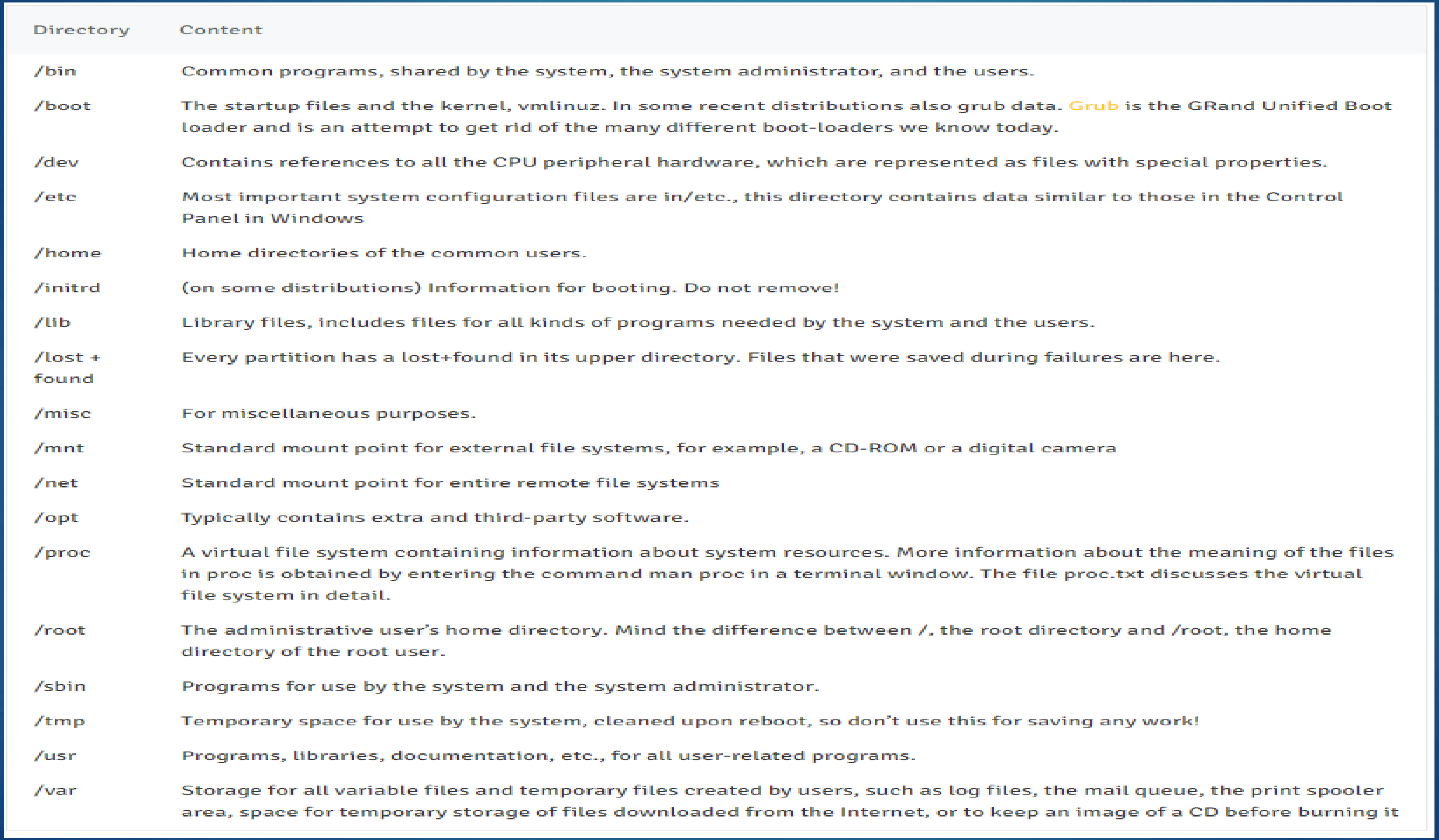


/ "ROOT"

- /BIN "ESSENTIAL BINARIES"
  - CAT
  - CHGRP
  - CHMOD
  - CHOWN
  - CP
  - DATA
  - DD
  - DF
  - DMESG
  - ECHO
  - FALSE
  - HOSTNAME
  - KILL
  - LN
  - LOGIN
  - LS
  - MKDIR
  - MKNOD
  - MORE
  - MOUNT
  - MV
  - PS
  - PWD
  - RM
  - RMDIF
  - SED
  - SH
  - STTY
  - SU
  - SYNCH
  - TRUE
  - UMOUNT
  - UNAME
- /BOOT "STATIC FILES OF BOOT LOADER "
  - KERNEL
  - SYSTEM.MAP
  - VMLINUZ
  - INITRD
  - GRUB
  - MODULE.INFO
  - BOOT
- /ETC "HOST SPECIFIC SYSTEM CONFIG"
  - CSH.LOGIN
  - EXPORTS
  - FSTAB
  - FTPUSERS
  - GATEWAYS
  - GETTYDEFS
  - GROUP
  - HOST.CONF
  - HOSTS
  - HOSTS.ALLOW
  - HOSTS.DENY
  - HOSTS.EQUIV
  - HOSTS.LPD
  - INETD.CONF
  - INITTAB
  - ISSUE
  - LS.SO.CONF
  - MOTD
  - MTAB
  - MTOOLS
  - NETWORKS
  - PASSWD
  - PRINTCAP
  - PROFILE
  - PROTOCOLS
  - RESOLV.CONF
  - RPC
  - SECURETTY
  - SERVICES
  - SHELLS
  - SYSLOG.CONF
  - /OPT " CONFIG FILE FOR ADD ON APPLICATION SOFTWARE "
- /USR " SHAREABLE AND READ-ONLY DATA "
  - /LOCAL "LOCAL SOFTWARE"
    - /BIN
    - /GAMES
    - /INCLUDE
    - /LIB
    - /MAN
    - /SBIN
    - /SHARE
    - /SRC
  - /SHARE " STATIC DATA SHAREABLE AMONG ALL ARCHITECTURES "
    - /MAN "MANUAL PAGES"
      - /MAN1 "user programs"
      - /MAN2 "system calls"
      - /MAN3 "lib functions"
      - /MAN4 "special file"
      - /MAN5 "file formats"
      - /MAN6 "games"
      - /MAN7 "misc."
      - /MAN8 "system admin."
  - /BIN "MOST USER COMMANDS"
  - /INCLUDE "STANDARD INCLUDE FILES FOR 'C' PROG."
  - /LIB " OBJ , BIN , LIB FILES FOR PROG. AND PACKAGES "
  - /SBIN "NON ESSENTIAL BINARIES"
- /VAR "VARIABLE DATA FILES"
  - /CACHE "APPLICATION CACHE DATA"
  - /LIB " VARIABLE STATE INFORMATION REMAINS AFTER REBOOT "
  - /YP " DATA FOR NIS SERVICES "
  - /LOCK "LOCK FILES FOR SHARED RESOURCES"
  - /OPT " VARIABLE DATA OF PACKAGES INSTALLED"
  - /RUN "INFO OF SYSTEM SINCE IT WAS BOOTED"
  - /TMP "AVAILABLE FOR PROG."
  - /SPOOL "DATA AWAITING PROCESSING "
    - /LPD
    - /MQUEUE
    - /NEWS
    - /RWHO
    - /UUCP
  - /LOG "LOG FILES AND DIR"
    - LASTLOG
    - MESSAGES
    - WTMP
- /SBIN "SYSTEM BINARIES"
  - FASTBOOT
  - FASTHALT
  - FDISK
  - FSCK
  - GETTY
  - HALT
  - IFCONFIG
  - INIT
  - MKFS
  - MKSWAP
  - REBOOT
  - ROUTE
  - SWAPON
  - SWAPOFF
  - UPDATE
- /TMP "TEMPERORY FILES DELETED ON BOOTUP"
- /DEV "LOCATION OF SPECIAL OR DEVICE FILES [CONTAINS MAKEDEV]"
- /HOME " USER HOME DIRECTORIES"
- /LIB " LIBRARY AND KERNEL MODULES"
- /MNT " MOUNT FILES FOR TEMPERORY FILESYSTEMS "
- /OPT " ADD-ON APPLICATION SOFTWARE "
- /ROOT "HOME DIR. FOR ROOT USER"

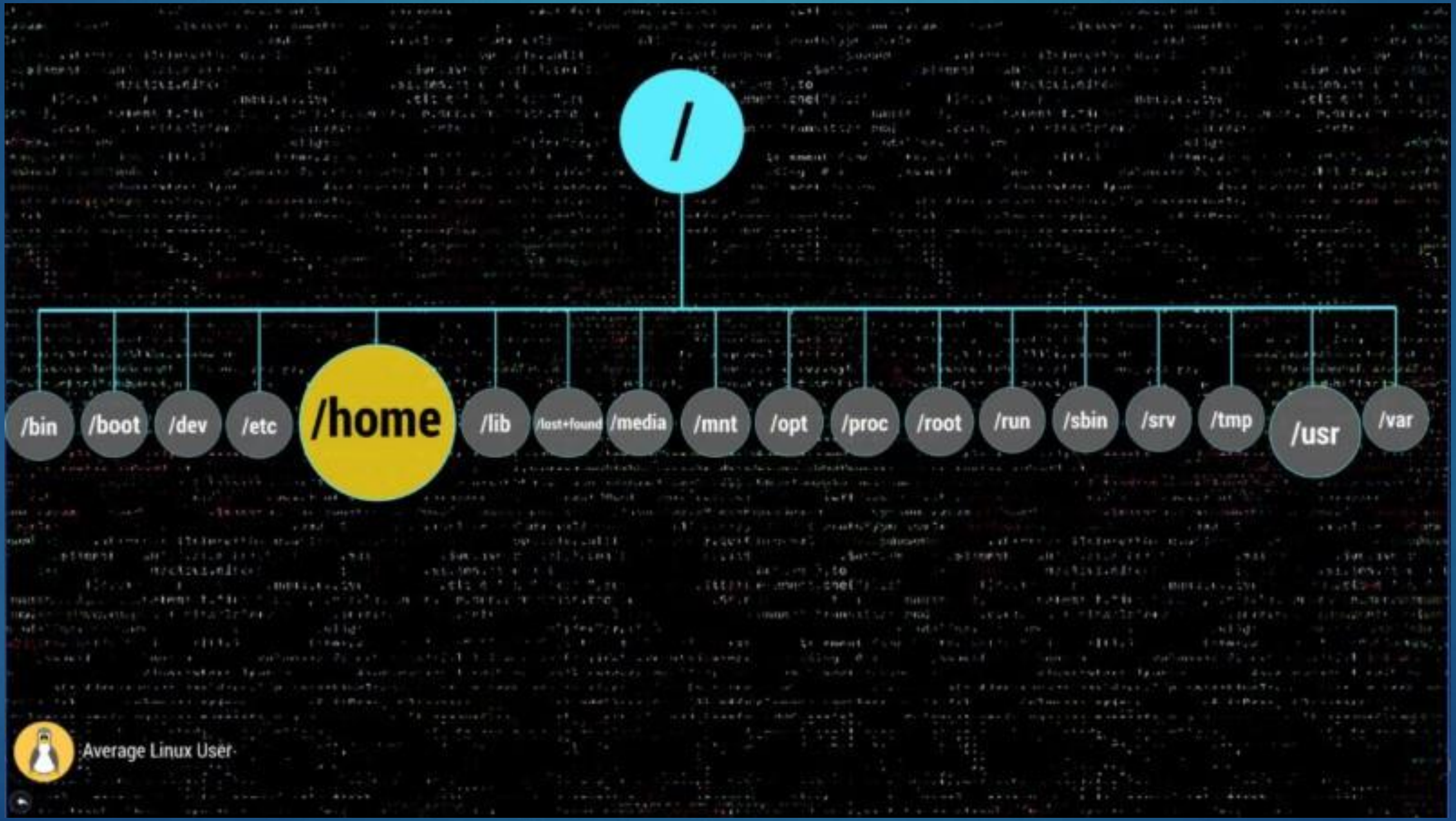
On a Linux system , most everything is files, and if is not a file , then it is a process

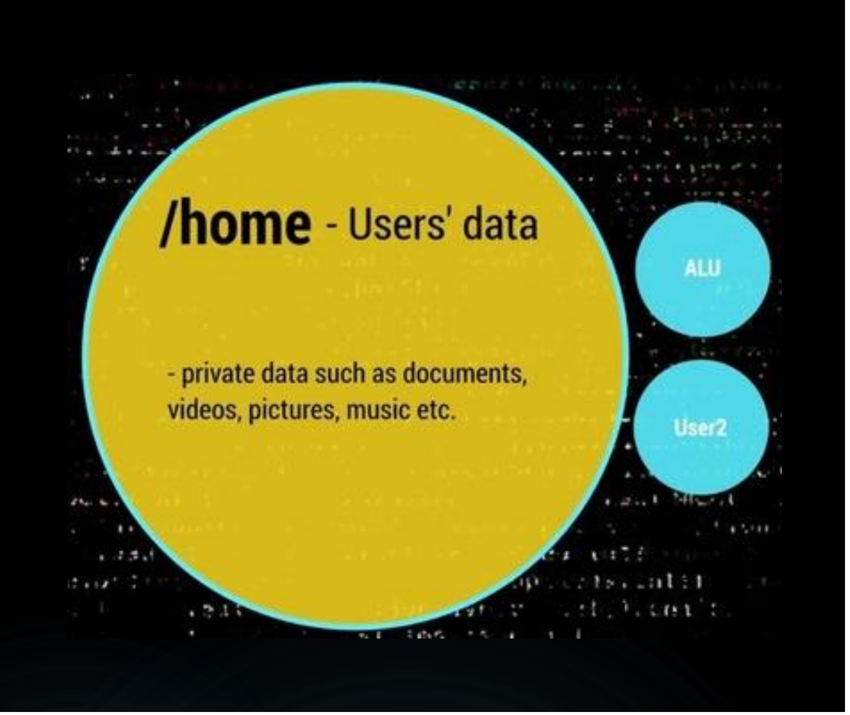
Subdirectories of the root directory



Directory	Content
/bin	Common programs, shared by the system, the system administrator, and the users.
/boot	The startup files and the kernel, vmlinuz. In some recent distributions also grub data. Grub is the GRand Unified Boot loader and is an attempt to get rid of the many different boot-loaders we know today.
/dev	Contains references to all the CPU peripheral hardware, which are represented as files with special properties.
/etc	Most important system configuration files are in/etc., this directory contains data similar to those in the Control Panel in Windows
/home	Home directories of the common users.
/initrd	(on some distributions) Information for booting. Do not remove!
/lib	Library files, includes files for all kinds of programs needed by the system and the users.
/lost + found	Every partition has a lost+found in its upper directory. Files that were saved during failures are here.
/misc	For miscellaneous purposes.
/mnt	Standard mount point for external file systems, for example, a CD-ROM or a digital camera
/net	Standard mount point for entire remote file systems
/opt	Typically contains extra and third-party software.
/proc	A virtual file system containing information about system resources. More information about the meaning of the files in proc is obtained by entering the command man proc in a terminal window. The file proc.txt discusses the virtual file system in detail.
/root	The administrative user's home directory. Mind the difference between /, the root directory and /root, the home directory of the root user.
/sbin	Programs for use by the system and the system administrator.
/tmp	Temporary space for use by the system, cleaned upon reboot, so don't use this for saving any work!
/usr	Programs, libraries, documentation, etc., for all user-related programs.
/var	Storage for all variable files and temporary files created by users, such as log files, the mail queue, the print spooler area, space for temporary storage of files downloaded from the Internet, or to keep an image of a CD before burning it

Linux Root Folders Explained



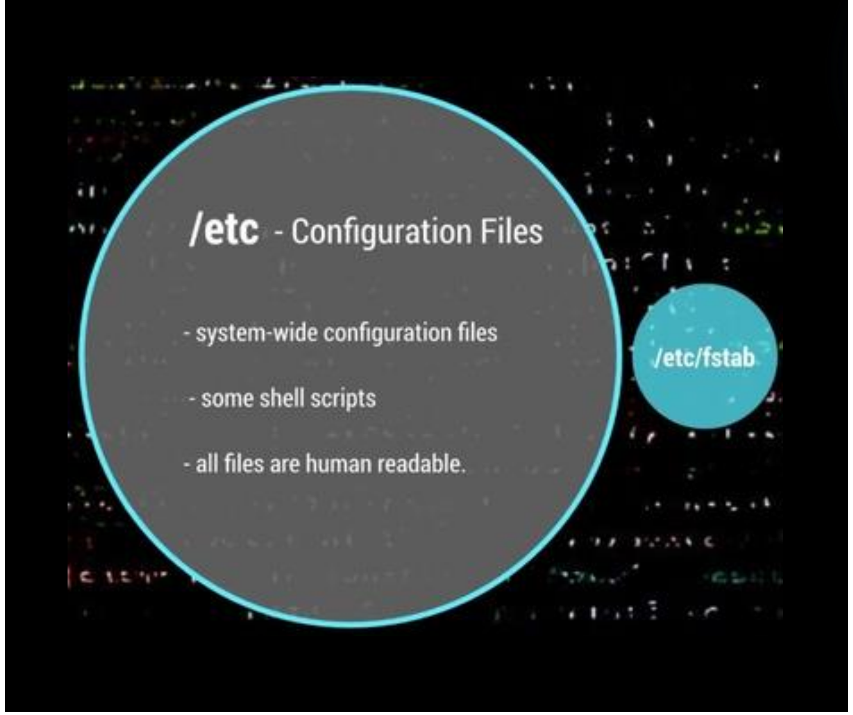


/home - Users' data

- private data such as documents, videos, pictures, music etc.

ALU

User2



/etc - Configuration Files

- system-wide configuration files
- some shell scripts
- all files are human readable.

/etc/fstab

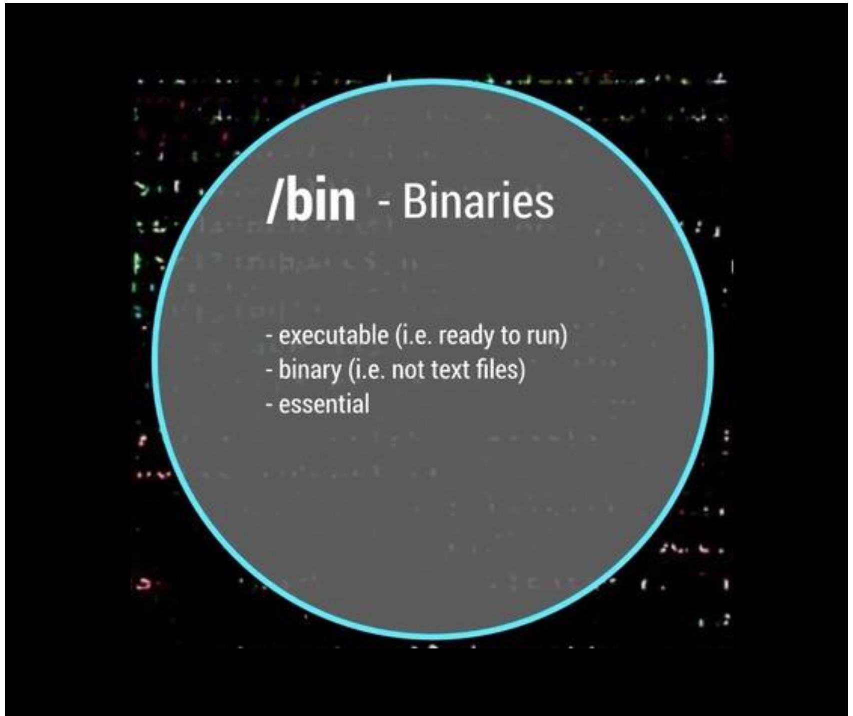
/lib – Libraries

- libraries required by programs in /bin

A library is a set of functions that are shared between programs.

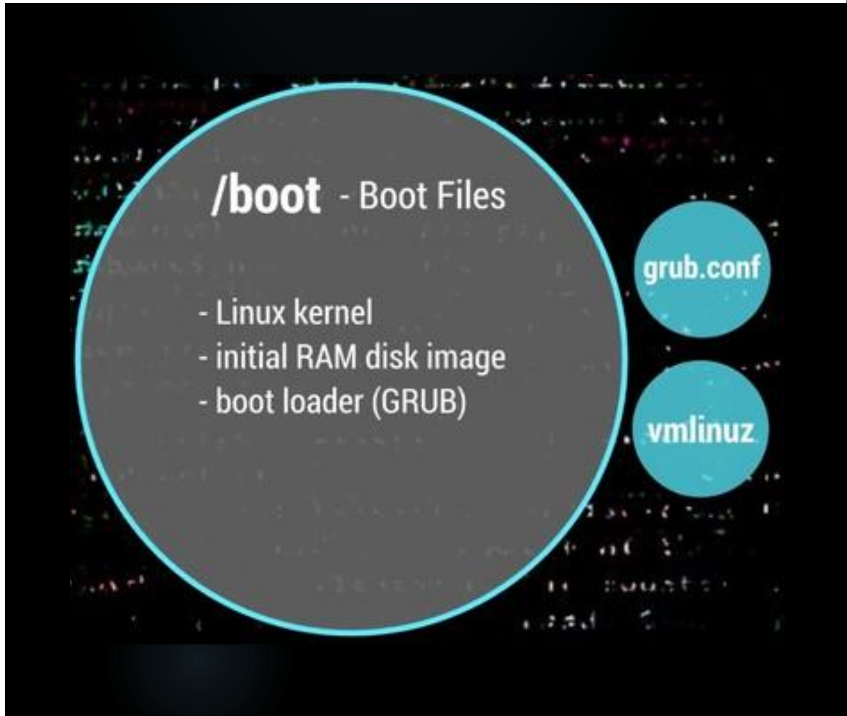
/dev - Device Nodes

- all devices represented here as files
- /dev/sda1 (sda - name of a disk)
- USB devices, cpu etc



/bin - Binaries

- executable (i.e. ready to run)
- binary (i.e. not text files)
- essential

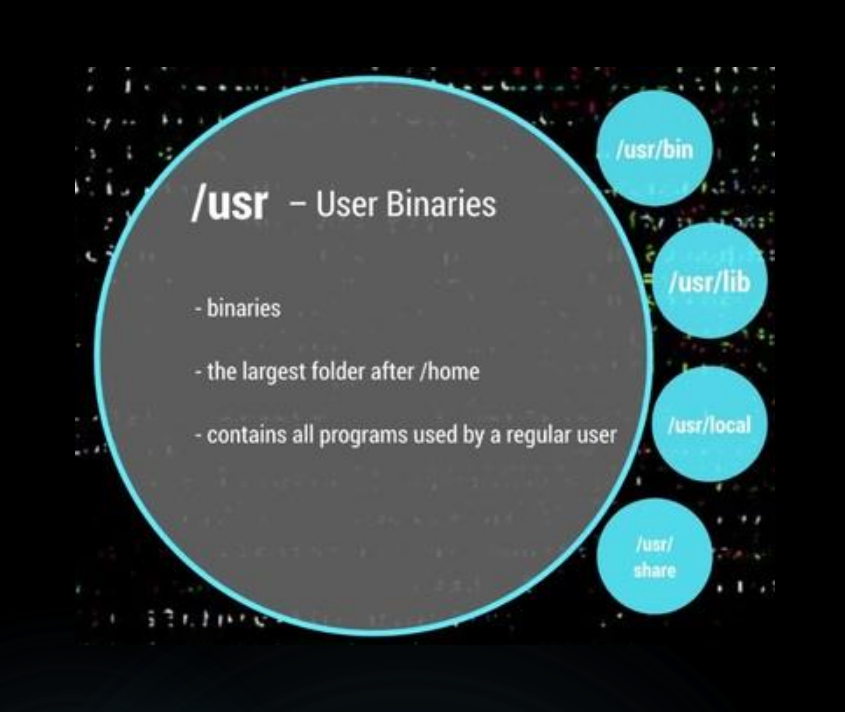


/boot - Boot Files

- Linux kernel
- initial RAM disk image
- boot loader (GRUB)

grub.conf

vmlinuz



/usr – User Binaries

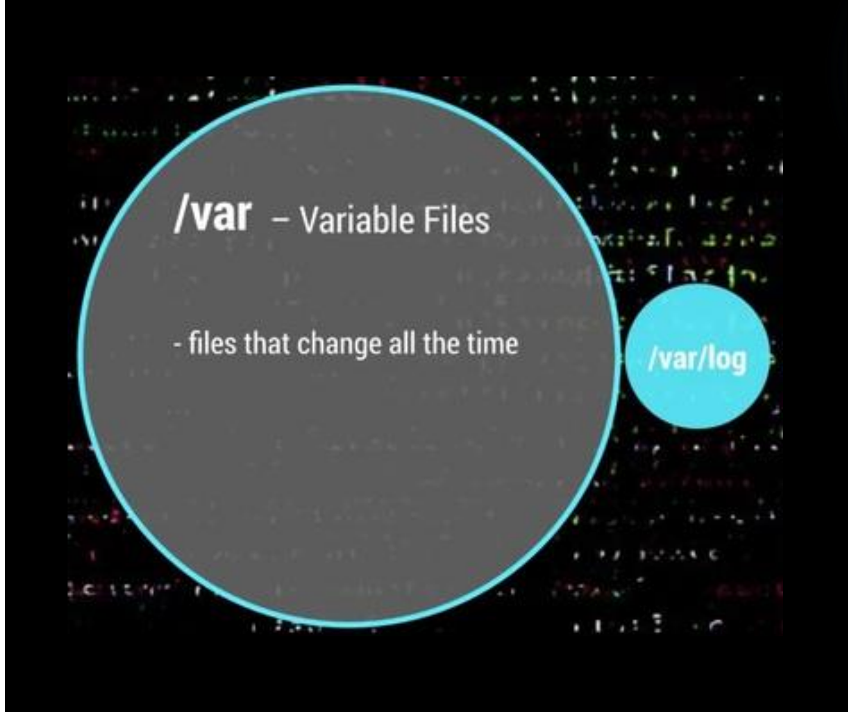
- binaries
- the largest folder after /home
- contains all programs used by a regular user

/usr/bin

/usr/lib

/usr/local

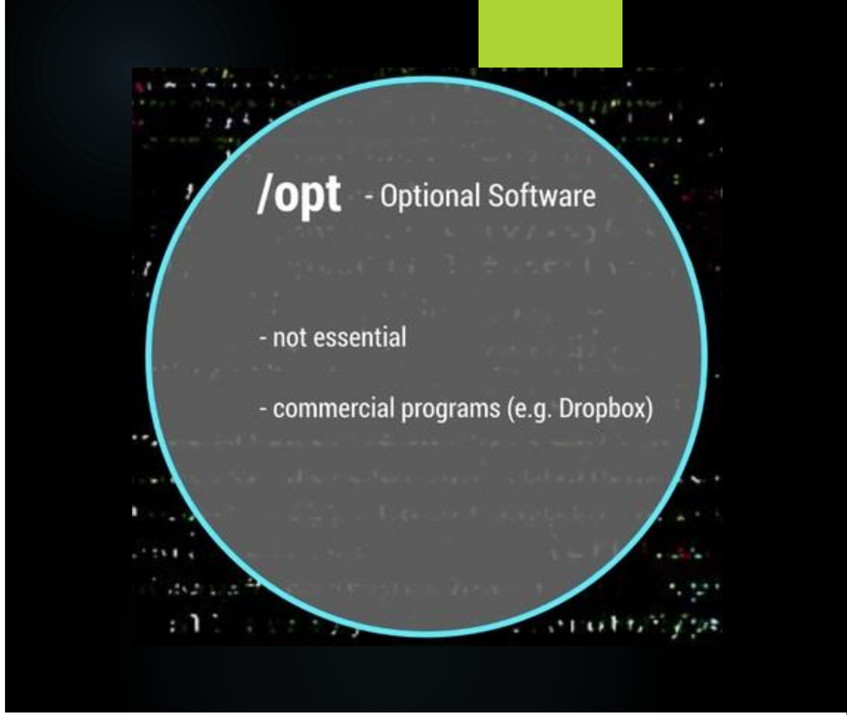
/usr/share



/var – Variable Files

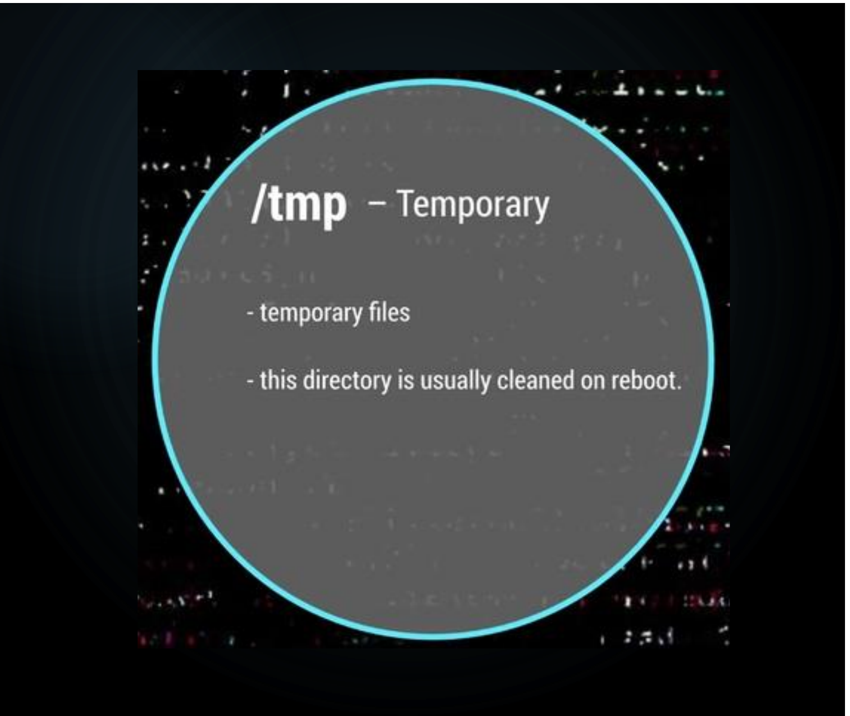
- files that change all the time

/var/log



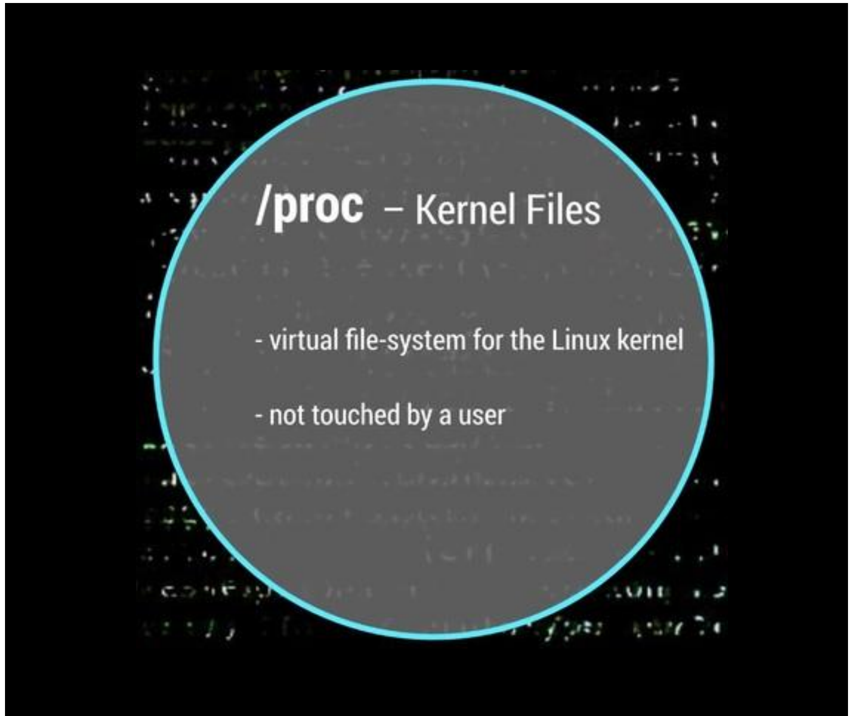
/opt - Optional Software

- not essential
- commercial programs (e.g. Dropbox)



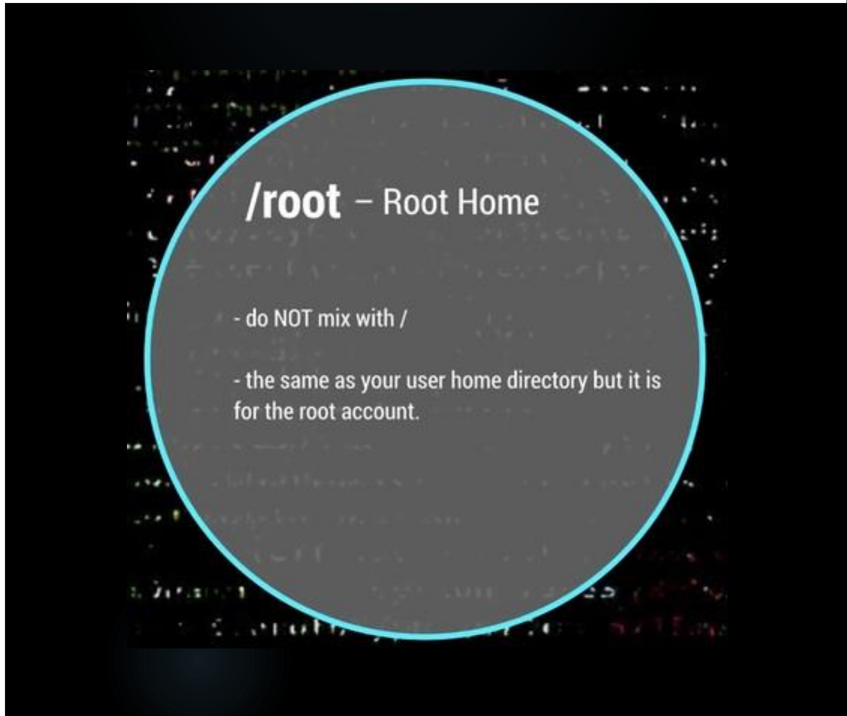
/tmp – Temporary

- temporary files
- this directory is usually cleaned on reboot.



/proc – Kernel Files

- virtual file-system for the Linux kernel
- not touched by a user



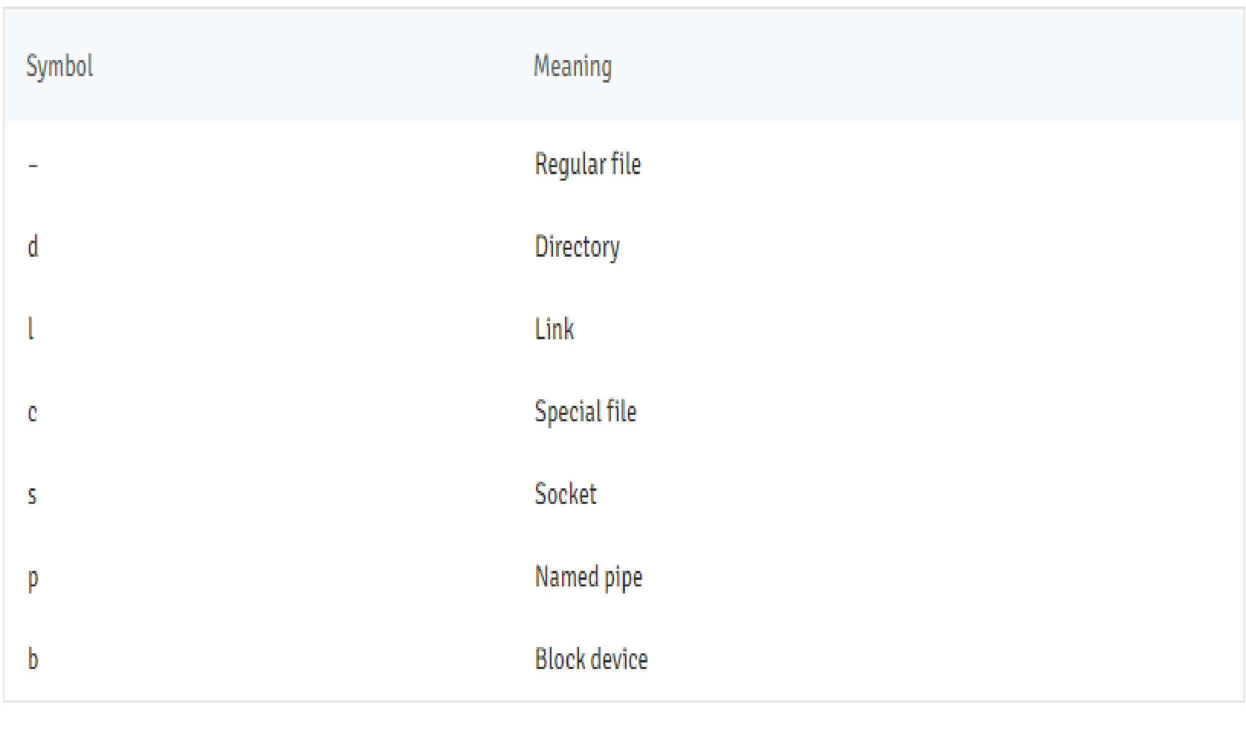
/root – Root Home

- do NOT mix with /
- the same as your user home directory but it is for the root account.

Linux file system

There are certain exceptions in a Linux file system

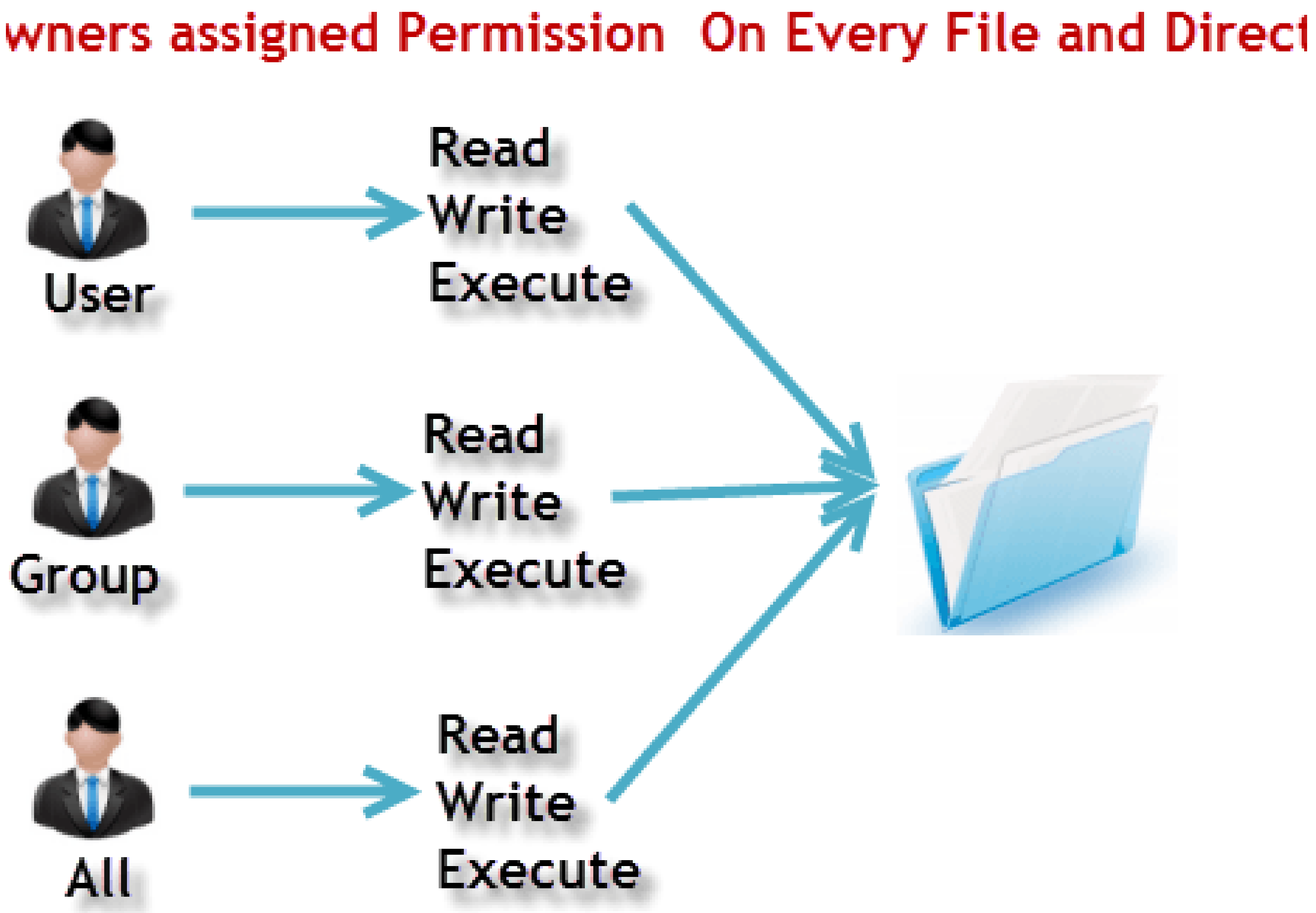
- Directories: Files that are lists of other files.
- Special file: The mechanism used for inout and output. /dev are special files.
- Links: A system to make file or directory visible in multiple parts of the systems.
- Sockets:A special file type, similar to TCP/IP sockets providing inter-process networking.
- Pipes:More or less like sockets; they form a way for process to communicate with each other with out using network socket.



Symbol	Meaning
-	Regular file
d	Directory
l	Link
c	Special file
s	Socket
p	Named pipe
b	Block device

Take
A Break

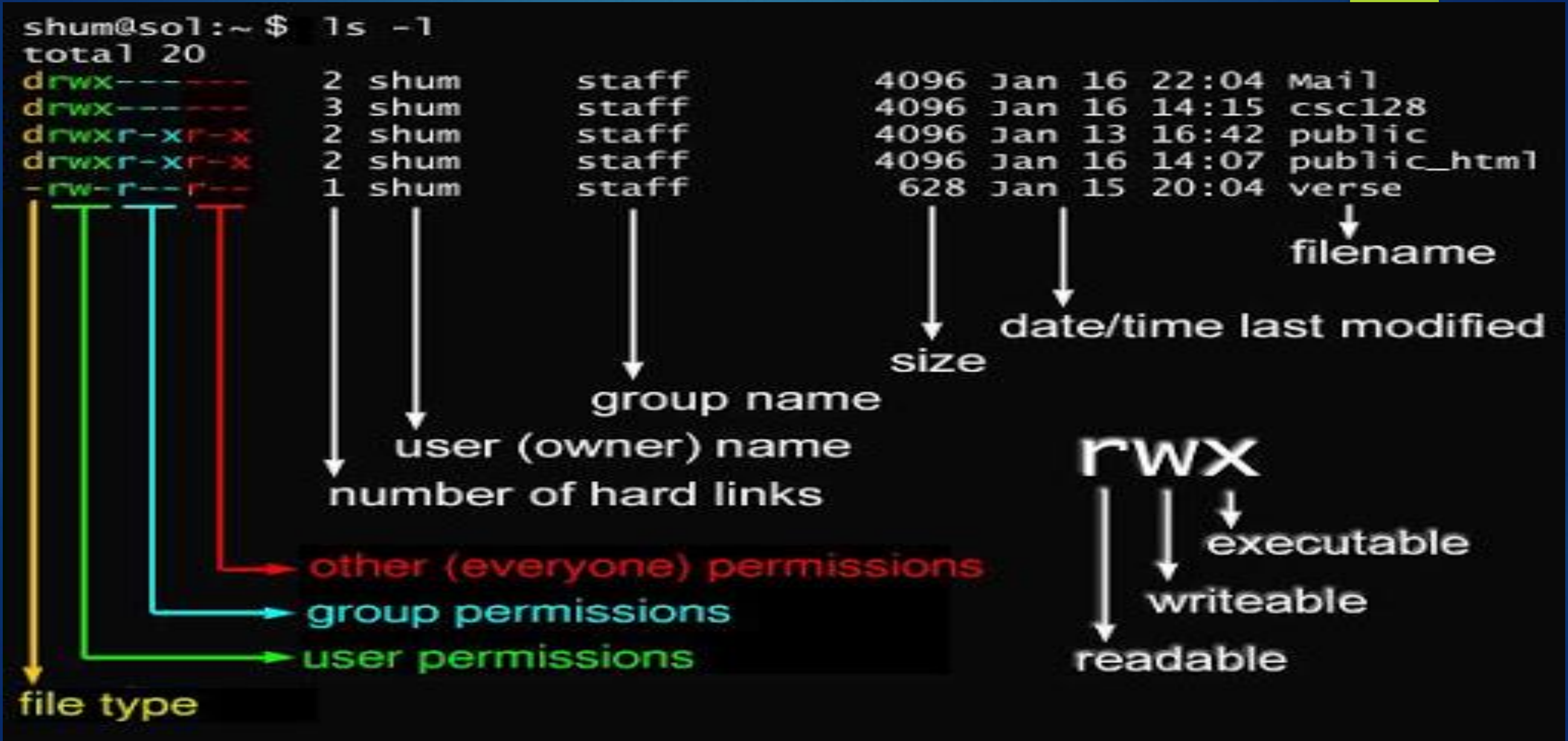
Group Permission



File Permission in Linux

- *Group Permission*
  - ***Owner***—The Owner permissions apply only the owner of the file or directory; they will not impact the actions of other users.
  - ***Group***—The Group permissions apply only to the group that has been assigned to the file or directory; they will not affect the actions of other users.
  - ***All User/Other***—The All Users permissions apply to all other users on the system; this is the permission group that you want to watch the most.
- ***Each file or directory has three basic permission types:***
  - *Read*—The Read permission refers to a user's capability to read the contents of the file.
  - *Write*—The Write permissions refer to a user's capability to write or modify a file or directory.
  - *Execute*—The Execute permission affects a user's capability to execute a file or view the contents of a directory.

Permission



```
shum@sol:~$ ls -l
total 20
drwx------   2 shum     staff        4096 Jan 16 22:04 Mail
drwx------   3 shum     staff        4096 Jan 16 14:15 csc128
drwxr-xr-x   2 shum     staff        4096 Jan 13 16:42 public
drwxr-xr-x   2 shum     staff        4096 Jan 16 14:07 public_html
-rw-r--r--   1 shum     staff         628 Jan 15 20:04 verse
```

Linux Advance/Special Permission

L: The file or directory is a symbolic link [ارتباط رمزي]

S : This indicated the setuid/setgid permissions. Represented as a s in the read portion of the owner or group permissions.

T:This indicates the sticky bit permissions. Represented as a t in the executable portion of the all users permissions

i—chatter Making file unchangeable

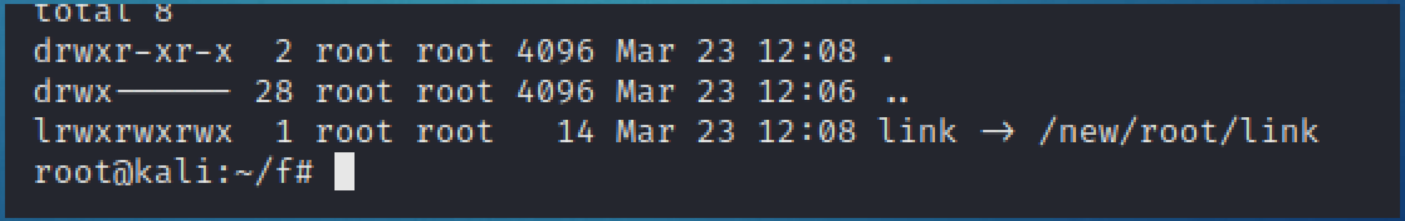
There are two more which mostly used by devices. (تستخدم مع الاجهزة)

c—Character device -

b—Block device (i.e., hdd)

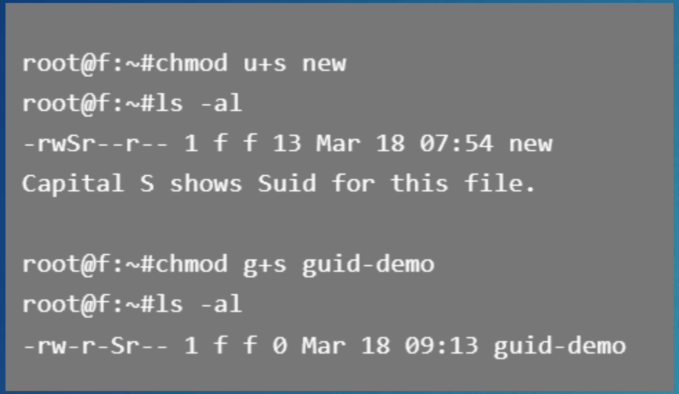
Link Permission

root@f:~#ln -s new /root/link
root@f:~#ls -al
lrwxrwxrwx 1 f roof 3 Mar 18 08:09 link -> new
link is created for a file name called new (link is symbolic for file name new)



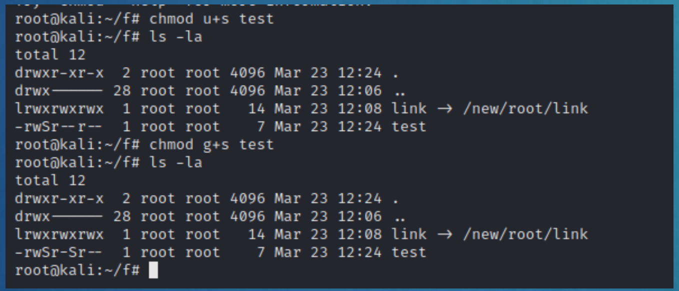
```
total 8
drwxr-xr-x  2 root root 4096 Mar 23 12:08 .
drwx------ 28 root root 4096 Mar 23 12:06 ..
lrwxrwxrwx  1 root root   14 Mar 23 12:08 link -> /new/root/link
root@kali:~/f# 
```

Suid & Guid Permission



```
root@f:~#chmod u+s new
root@f:~#ls -al
-rwSr--r-- 1 f f 13 Mar 18 07:54 new
Capital S shows Suid for this file.

root@f:~#chmod g+s guid-demo
root@f:~#ls -al
-rw-r-Sr-- 1 f f 0 Mar 18 09:13 guid-demo
```



```
root@kali:~/f# chmod u+s test
root@kali:~/f# ls -la
total 12
drwxr-xr-x  2 root root 4096 Mar 23 12:24 .
drwx------ 28 root root 4096 Mar 23 12:06 ..
lrwxrwxrwx  1 root root   14 Mar 23 12:08 link → /new/root/link
-rwSr--r--  1 root root    7 Mar 23 12:24 test
root@kali:~/f# chmod g+s test
root@kali:~/f# ls -la
total 12
drwxr-xr-x  2 root root 4096 Mar 23 12:24 .
drwx------ 28 root root 4096 Mar 23 12:06 ..
lrwxrwxrwx  1 root root   14 Mar 23 12:08 link → /new/root/link
-rwSr-Sr--  1 root root    7 Mar 23 12:24 test
root@kali:~/f# █
```

setuid (SUID):

This is used to grant root level access or permissions to users
When an executable is given setuid permissions, **normal users **can execute the file with root level or owner privileges. **Setuid** is commonly used to assign temporarily privileges to a user to accomplish a certain task.

For example, changing a user's password would require higher privileges, and in this case, setuid can be used.

setgid (SGID)

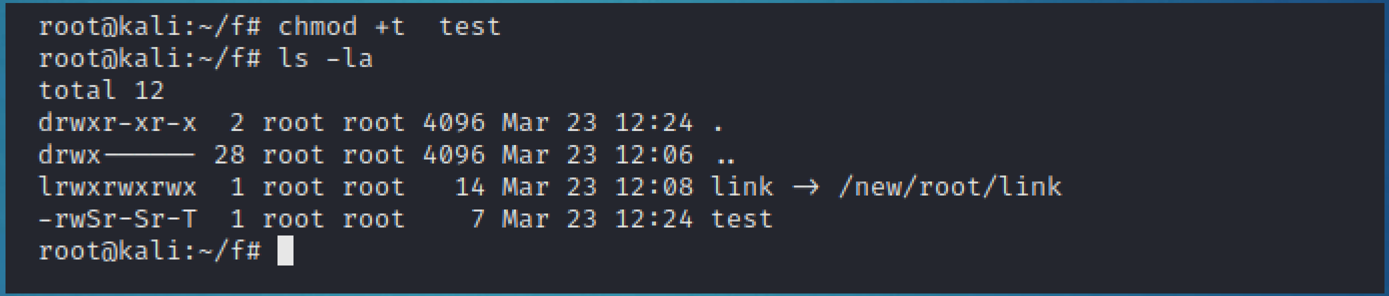
This is similar to setuid, the only difference being that it's used in the context of a group, whereas setuid is used in the context of a user.

Capital S shows Guid for guid-demo file and

capital S is in group section

Stickybit Permission

* **Stickybit** Permission
This is another type of permission; it is mostly used on directories to prevent anyone other than the “root” or the “owner” from deleting the contents.

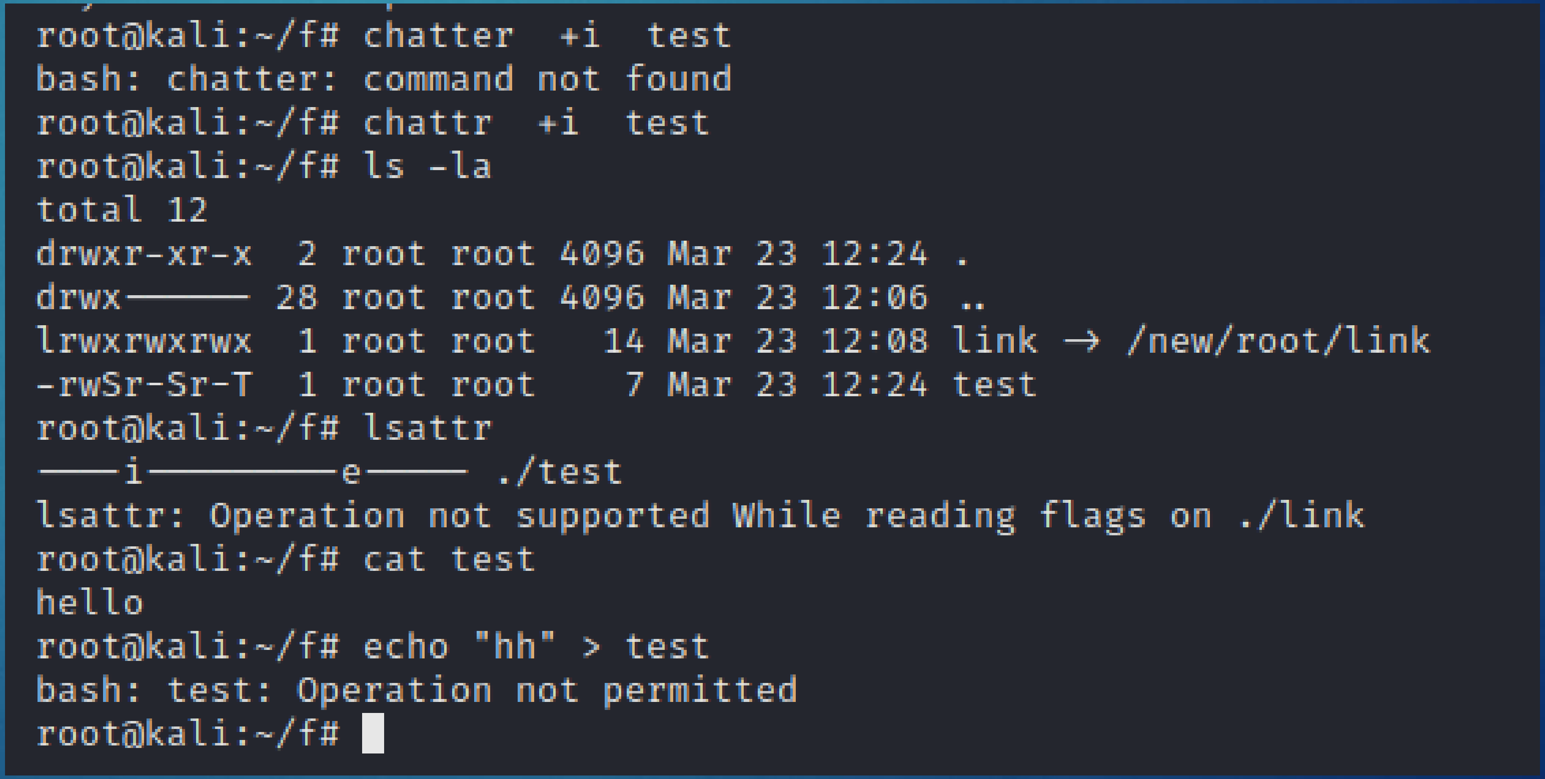


```
root@kali:~/f# chmod +t  test
root@kali:~/f# ls -la
total 12
drwxr-xr-x  2 root root 4096 Mar 23 12:24 .
drwx------ 28 root root 4096 Mar 23 12:06 ..
lrwxrwxrwx  1 root root   14 Mar 23 12:08 link → /new/root/link
-rwSr-Sr-T  1 root root    7 Mar 23 12:24 test
root@kali:~/f# █
```

Capital **T **shows that stickybit has been set for other user (only owner or root user can delete files)

Permission

* Chatter Permission



```
root@kali:~/f# chatter  +i  test
bash: chatter: command not found
root@kali:~/f# chattr  +i  test
root@kali:~/f# ls -la
total 12
drwxr-xr-x  2 root root 4096 Mar 23 12:24 .
drwx------ 28 root root 4096 Mar 23 12:06 ..
lrwxrwxrwx  1 root root   14 Mar 23 12:08 link -> /new/root/link
-rwSr-Sr-T  1 root root    7 Mar 23 12:24 test
root@kali:~/f# lsattr
----i---------e----- ./test
lsattr: Operation not supported While reading flags on ./link
root@kali:~/f# cat test
hello
root@kali:~/f# echo "hh" > test
bash: test: Operation not permitted
root@kali:~/f# 
```

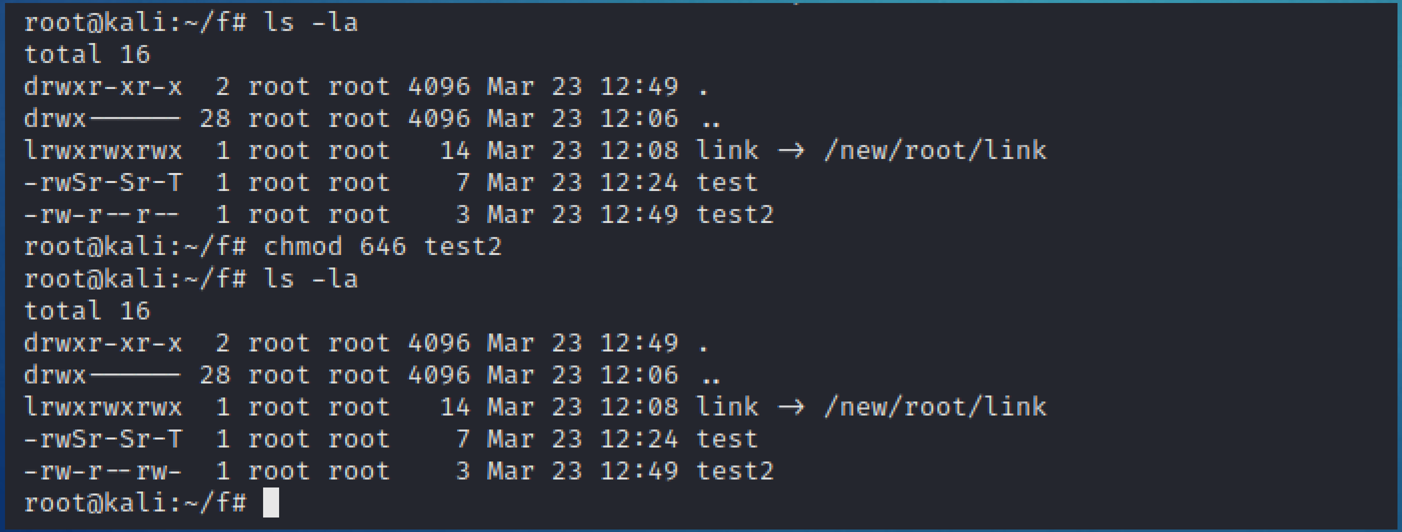
let’s have little look about numerical file permission

r = 4

w = 2

x = 1

Here other user only having “read” permission so what we are going to do is to change it into read and write but not execute.

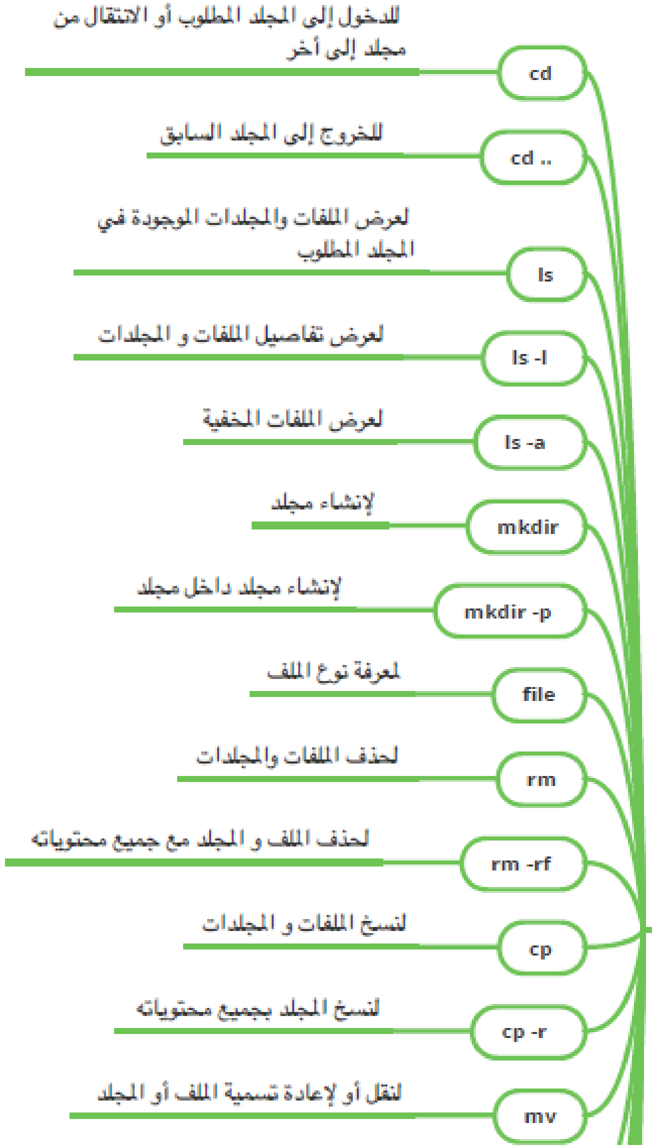


```
root@kali:~/f# ls -la
total 16
drwxr-xr-x  2 root root 4096 Mar 23 12:49 .
drwx------ 28 root root 4096 Mar 23 12:06 ..
lrwxrwxrwx  1 root root   14 Mar 23 12:08 link → /new/root/link
-rwSr-Sr-T  1 root root    7 Mar 23 12:24 test
-rw-r--r--  1 root root    3 Mar 23 12:49 test2
root@kali:~/f# chmod 646 test2
root@kali:~/f# ls -la
total 16
drwxr-xr-x  2 root root 4096 Mar 23 12:49 .
drwx------ 28 root root 4096 Mar 23 12:06 ..
lrwxrwxrwx  1 root root   14 Mar 23 12:08 link → /new/root/link
-rwSr-Sr-T  1 root root    7 Mar 23 12:24 test
-rw-r--rw-  1 root root    3 Mar 23 12:49 test2
root@kali:~/f# 
```

Let’s explore a bit more into it, we want read + write permission so 4 + 2 = 6 that’s mean read and write.

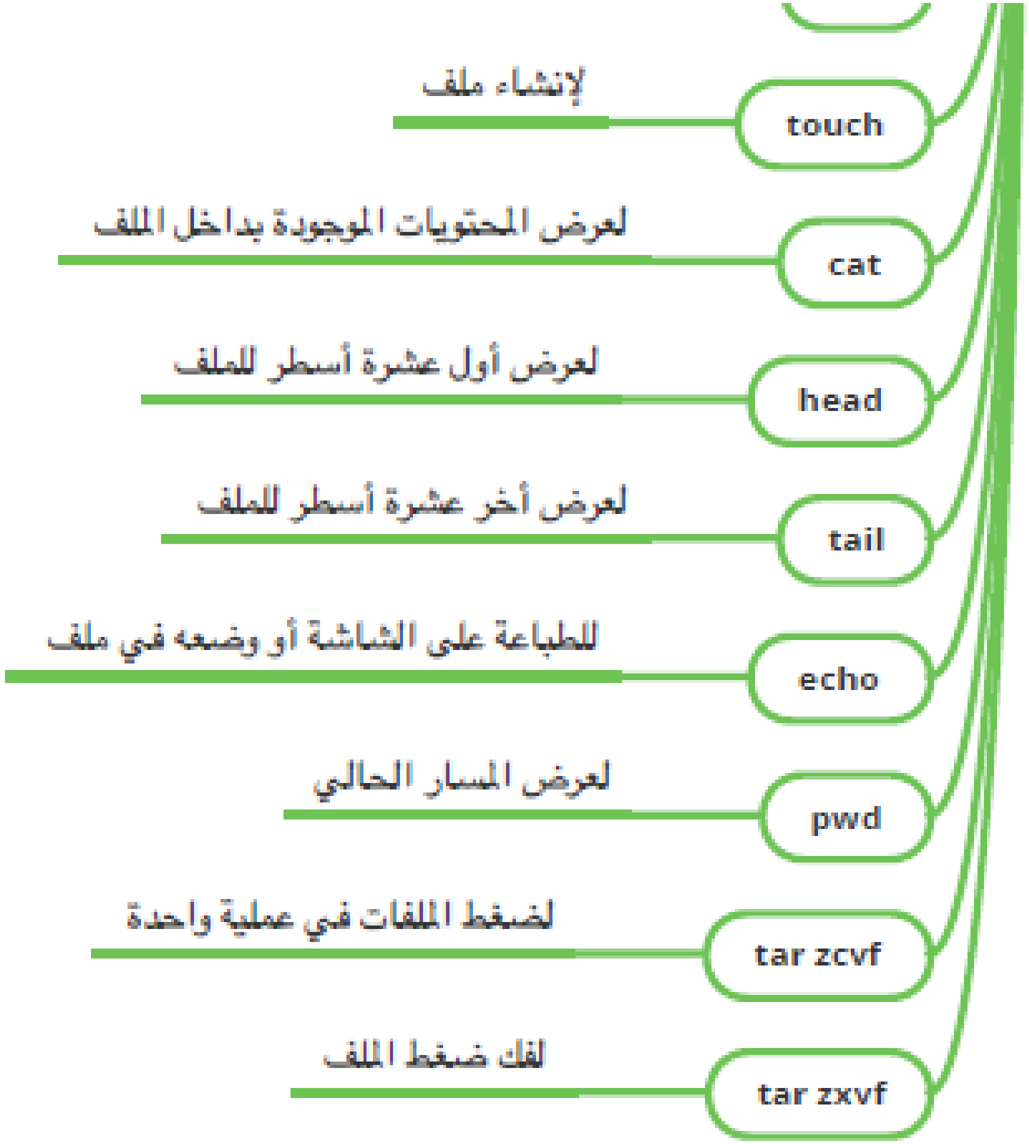
Hope it is clear now how to set permission on a file and what it does.

Most Common and Important Commands



cd	للدخول إلى المجلد المطلوب أو الانتقال من مجلد إلى أخر
cd ..	للخروج إلى المجلد السابق
ls	لعرض الملفات والمجلدات الموجودة في المجلد المطلوب
ls -l	لعرض تفاصيل الملفات و المجلدات
ls -a	لعرض الملفات المخفية
mkdir	لإنشاء مجلد
mkdir -p	لإنشاء مجلد داخل مجلد
file	لمعرفة نوع الملف
rm	لحذف الملفات والمجلدات
rm -rf	لحذف الملف و المجلد مع جميع محتوياته
cp	لنسخ الملفات و المجلدات
cp -r	لنسخ المجلد بجميع محتوياته
mv	لنقل أو لإعادة تسمية الملف أو المجلد

Most Common and Important Commands



لإنشاء ملف
touch

لعرض المحتويات الموجودة بداخل الملف
cat

لعرض أول عشرة أسطر للملف
head

لعرض أخر عشرة أسطر للملف
tail

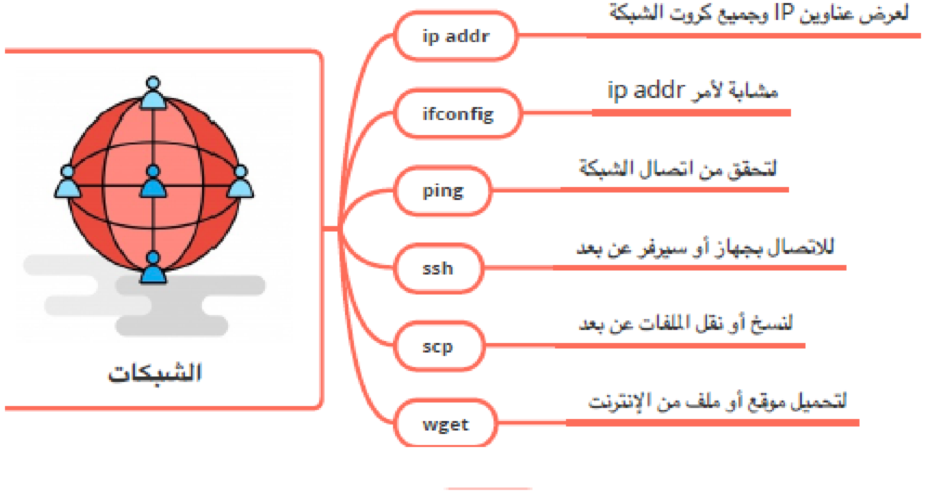
للطباعة على الشاشة أو وضعه في ملف
echo

لعرض المسار الحالي
pwd

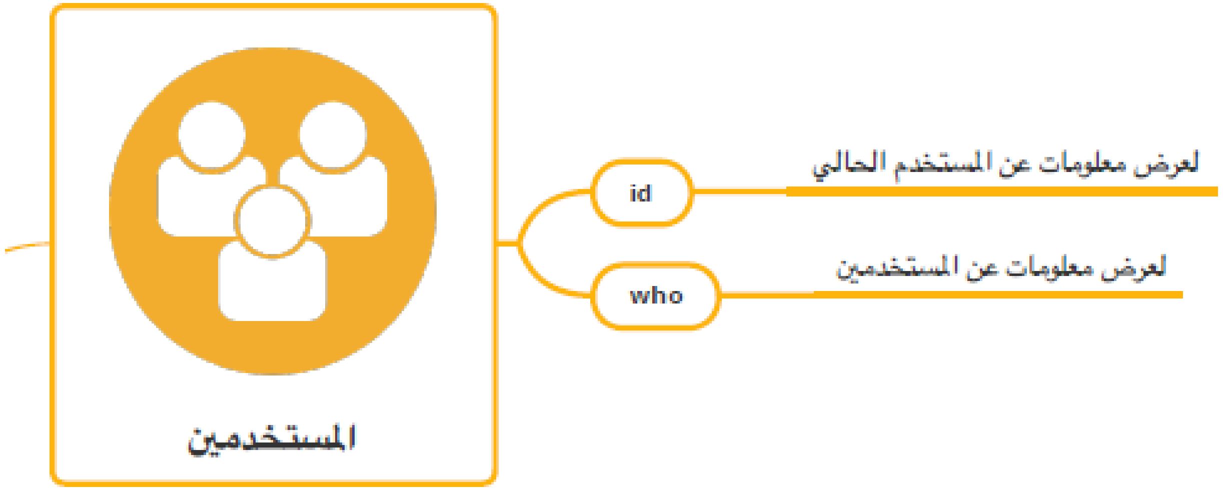
لضغط الملفات في عملية واحدة
tar zcvf

لفك ضغط الملف
tar zxvf

Most Common and Important Commands

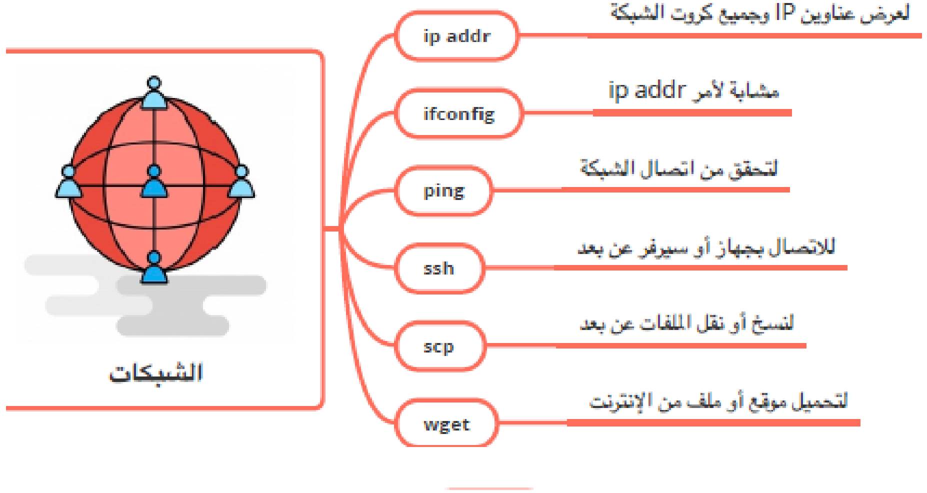


ip addr	لعرض عناوين IP وجميع كروت الشبكة
ifconfig	مشابة لأمر ip addr
ping	لتحقق من اتصال الشبكة
ssh	للاتصال بجهاز أو سيرفر عن بعد
scp	لنسخ أو نقل الملفات عن بعد
wget	لتحميل موقع أو ملف من الإنترنت



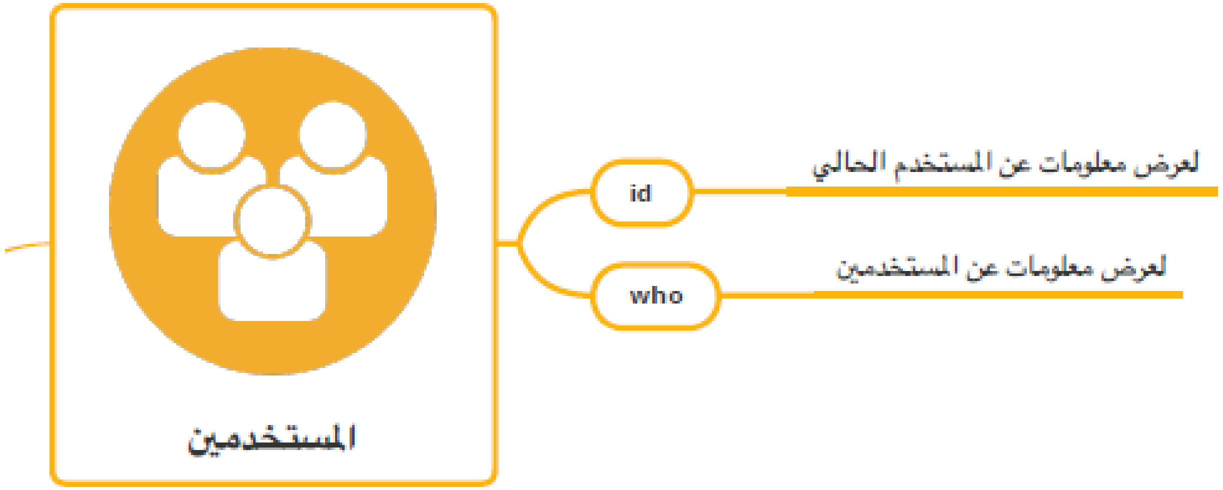
id	لعرض معلومات عن المستخدم الحالي
who	لعرض معلومات عن المستخدمين

Most Common and Important Commands



الشبكات

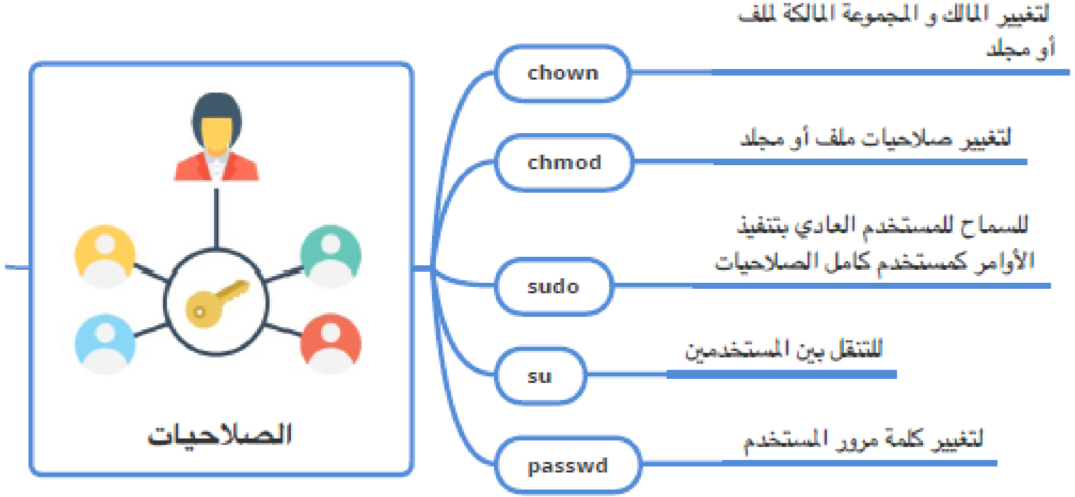
- ip addr — لعرض عناوين IP وجميع كروت الشبكة
- ifconfig — مشابة لأمر ip addr
- ping — لتحقق من اتصال الشبكة
- ssh — للاتصال بجهاز أو سيرفر عن بعد
- scp — لنسخ أو نقل الملفات عن بعد
- wget — لتحميل موقع أو ملف من الإنترنت



المستخدمين

- id — لعرض معلومات عن المستخدم الحالي
- who — لعرض معلومات عن المستخدمين

Most Common and Important Commands



الصلاحيات

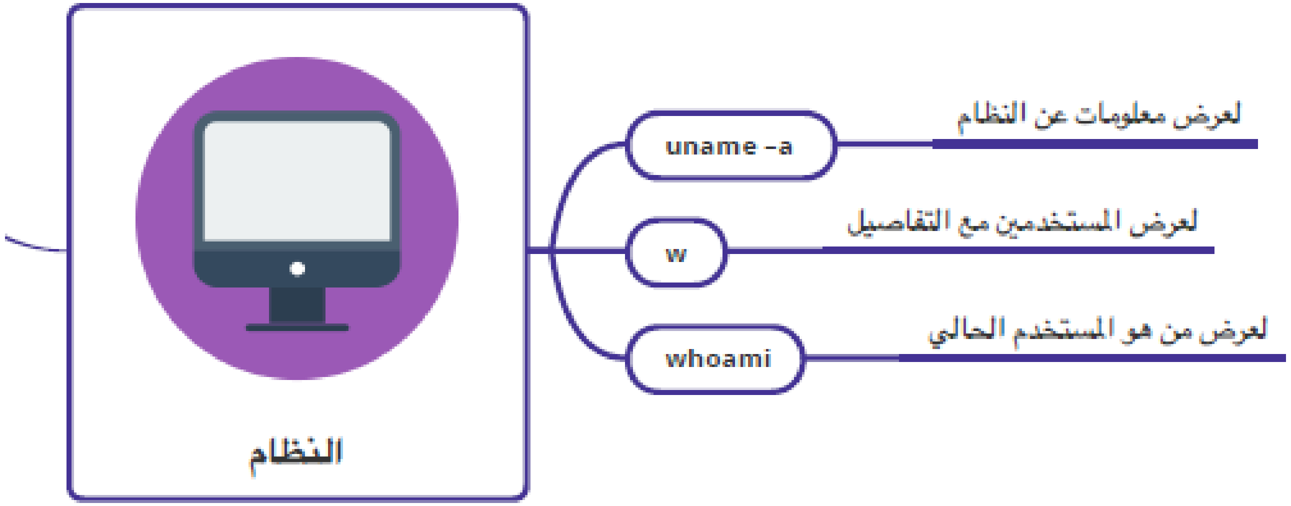
chown — لتغيير المالك و المجموعة المالكة لملف أو مجلد

chmod — لتغيير صلاحيات ملف أو مجلد

sudo — للسماح للمستخدم العادي بتنفيذ الأوامر كمستخدم كامل الصلاحيات

su — للتنقل بين المستخدمين

passwd — لتغيير كلمة مرور المستخدم



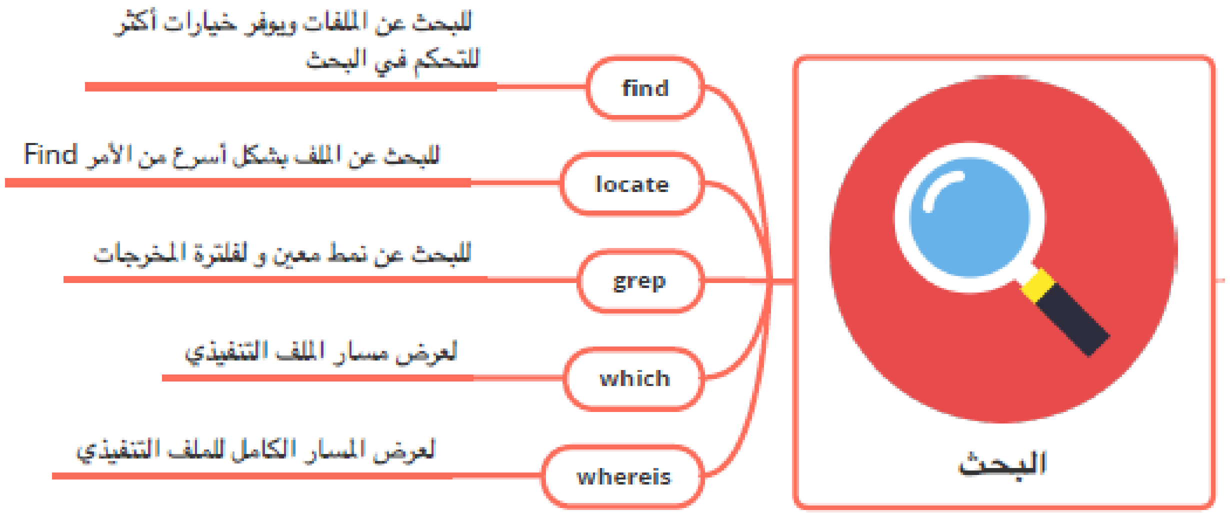
النظام

uname -a — لعرض معلومات عن النظام

w — لعرض المستخدمين مع التفاصيل

whoami — لعرض من هو المستخدم الحالي

Most Common and Important Commands



البحث

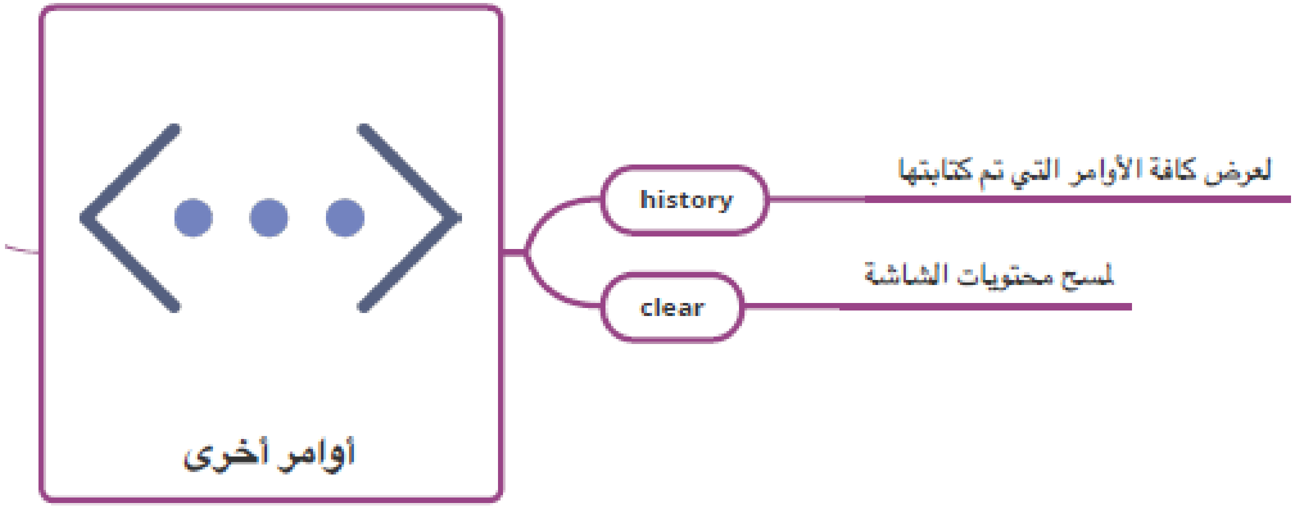
find
للبحث عن الملفات ويوفر خيارات أكثر للتحكم في البحث

locate
للبحث عن الملف بشكل أسرع من الأمر Find

grep
للبحث عن نمط معين و لفلترة المخرجات

which
لعرض مسار الملف التنفيذي

whereis
لعرض المسار الكامل للملف التنفيذي

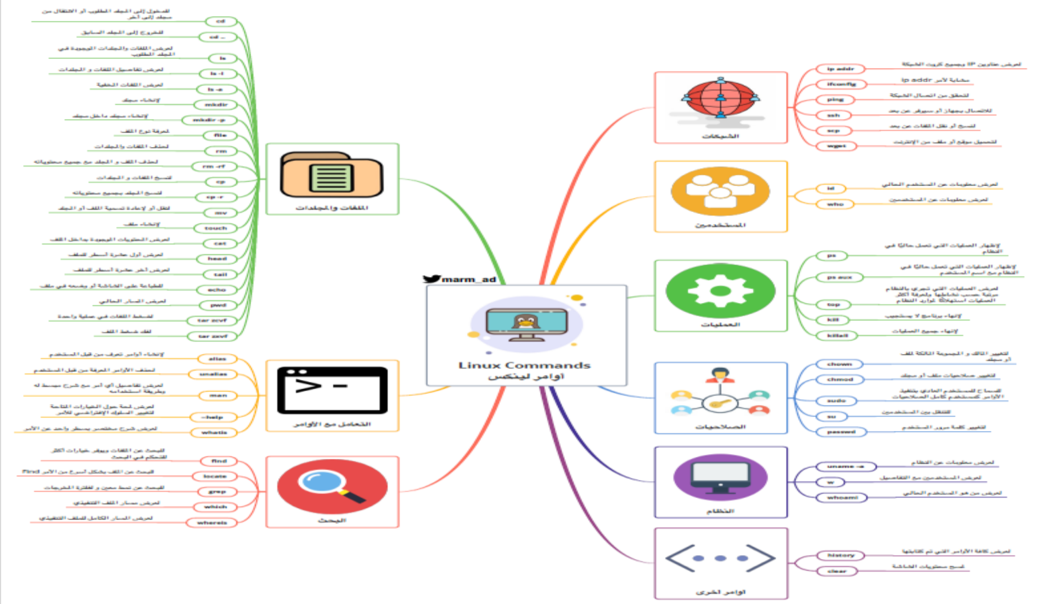


أوامر أخرى

history
لعرض كافة الأوامر التي تم كتابتها

clear
لمسح محتويات الشاشة

Most Common and Important Commands



marm_ad

Linux Commands
أوامر لينكس

الملفات والمجلدات

cd للدخول إلى المجلد المطلوب أو الانتقال من مجلد إلى آخر
cd .. للخروج إلى المجلد السابق
ls لعرض الملفات والمجلدات الموجودة في المجلد المطلوب
ls -l لعرض تفاصيل الملفات و المجلدات
ls -a لعرض الملفات المخفية
mkdir لإنشاء مجلد
mkdir -p لإنشاء مجلد داخل مجلد
file لمعرفة نوع الملف
rm لحذف الملفات والمجلدات
rm -rf لحذف الملف و المجلد مع جميع محتوياته
cp لنسخ الملفات و المجلدات
cp -r لنسخ المجلد بجميع محتوياته
mv لنقل أو إعادة تسمية الملف أو المجلد
touch لإنشاء ملف
cat لعرض المحتويات الموجودة بداخل الملف
head لعرض أول عشرة أسطر للملف
tail لعرض آخر عشرة أسطر للملف
echo للطباعة على الشاشة أو وضعه في ملف
pwd لعرض المسار الحالي
tar zcvf لضغط الملفات في عملية واحدة
tar zxvf لفك ضغط الملف

التعامل مع الأوامر

alias لإنشاء أوامر تعرف من قبل المستخدم
unalias لحذف الأوامر المعرفة من قبل المستخدم
man لعرض تفاصيل أي أمر مع شرح مبسط له وطريقة استخدامه
--help لعرض لمحة حول الخيارات المتاحة لتغيير السلوك الإفتراضي للأمر
whatis لعرض شرح مختصر بسطر واحد عن الأمر

البحث

find للبحث عن الملفات ويوفر خيارات أكثر للتحكم في البحث
locate البحث عن الملف بشكل أسرع من الأمر Find
grep للبحث عن نمط معين و لفلترة المخرجات
which لعرض مسار الملف التنفيذي
whereis لعرض المسار الكامل للملف التنفيذي

الشبكات

ip addr لعرض عناوين IP وجميع كروت الشبكة
ifconfig مشابه لأمر ip addr
ping لتحقق من اتصال الشبكة
ssh للاتصال بجهاز أو سيرفر عن بعد
scp لنسخ أو نقل الملفات عن بعد
wget لتحميل موقع أو ملف من الإنترنت

المستخدمين

id لعرض معلومات عن المستخدم الحالي
who لعرض معلومات عن المستخدمين

العمليات

ps لإظهار العمليات التي تعمل حاليًا في النظام
ps aux لإظهار العمليات التي تعمل حاليًا في النظام مع اسم المستخدم
top لعرض العمليات التي تجري بالنظام مرتبة حسب نشاطها ولمعرفة أكثر العمليات استهلاكًا لموارد النظام
kill لإنهاء برنامج لا يستجيب
killall لإنهاء جميع العمليات

الصلاحيات

chown لتغيير المالك و المجموعة المالكة لملف أو مجلد
chmod لتغيير صلاحيات ملف أو مجلد
sudo للسماح للمستخدم العادي بتنفيذ الأوامر كمستخدم كامل الصلاحيات
su للتنقل بين المستخدمين
passwd لتغيير كلمة مرور المستخدم

النظام

uname -a لعرض معلومات عن النظام
w لعرض المستخدمين مع التفاصيل
whoami لعرض من هو المستخدم الحالي

اوامر اخرى

history لعرض كافة الأوامر التي تم كتابتها
clear لمسح محتويات الشاشة

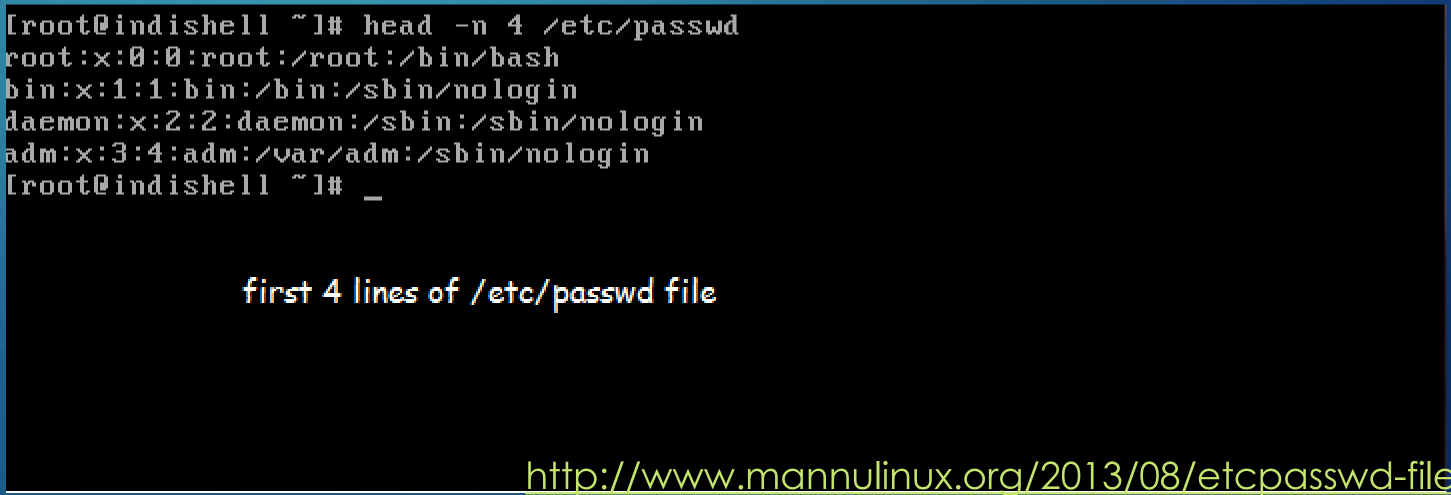
Take
A Break

Users inside of Linux

يتم تخزين المستخدمين داخل Linux داخل ملف : / etc / passwd

إذن هذا ما تبدو عليه محتويات ملف / etc / passwd

1.user name
2.user id
3.user group id
4.user home directory
5.user login shell
etc etc ;)

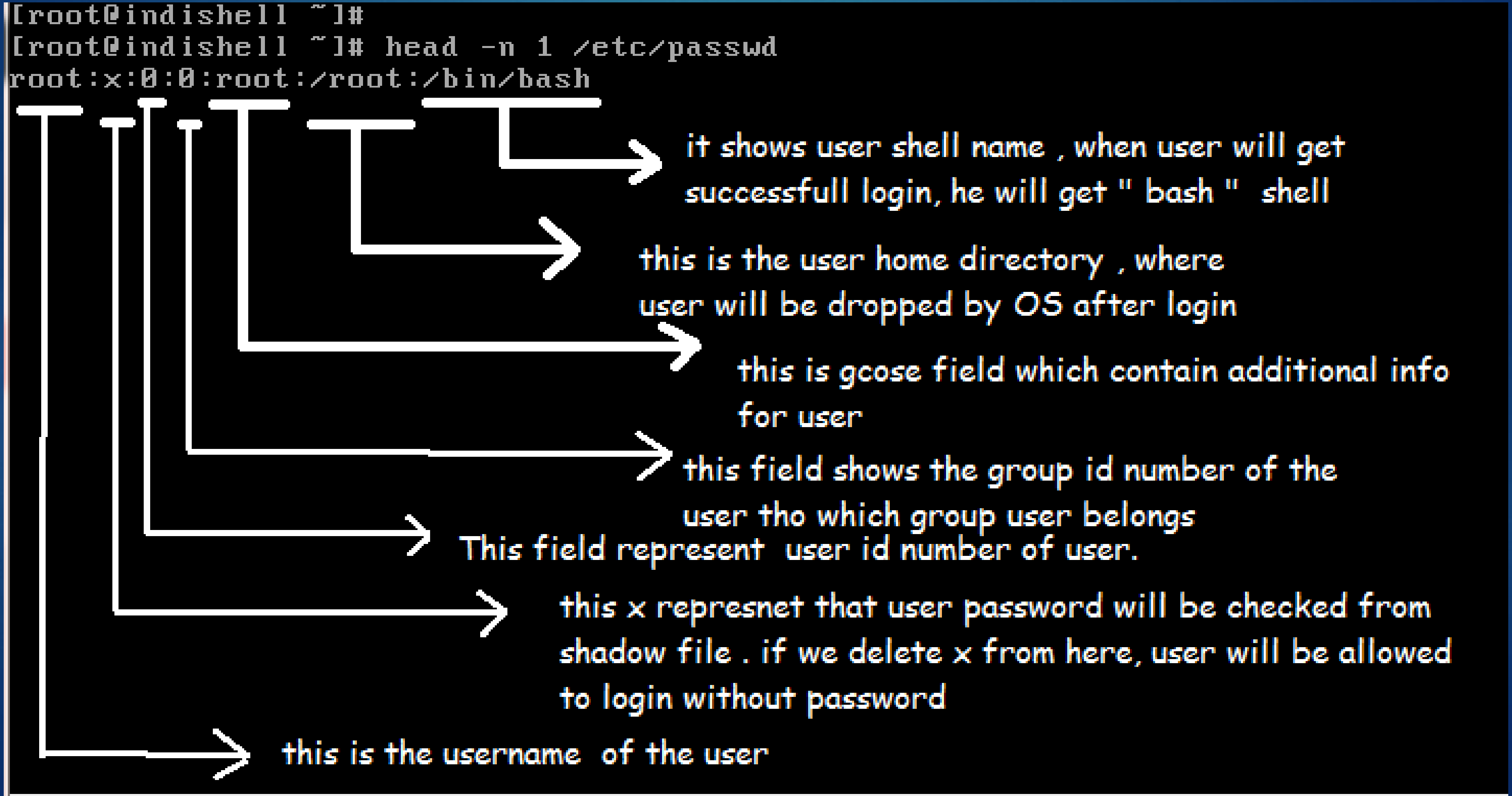


```
[root@indishell ~]# head -n 4 /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
[root@indishell ~]# _
```

first 4 lines of /etc/passwd file

http://www.mannulinux.org/2013/08/etcpasswd-file.html

root:x:0:0:root:/root:/bin/bash



```
[root@indishell ~]#
[root@indishell ~]# head -n 1 /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

it shows user shell name , when user will get successfull login, he will get " bash " shell

this is the user home directory , where user will be dropped by OS after login

this is gcose field which contain additional info for user

this field shows the group id number of the user tho which group user belongs

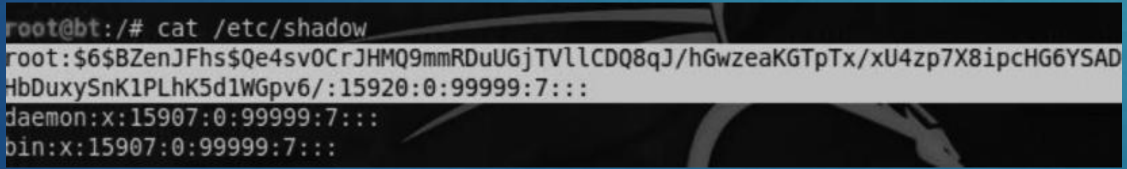
This field represent user id number of user.

this x represnet that user password will be checked from shadow file . if we delete x from here, user will be allowed to login without password

this is the username of the user

Linux Password Storage

- يتم تخزين كلمة المرور الخاصة بـ Linux / Unix داخل ملف / etc / passwd أو / / etc / shadow.
- تخزن الأنظمة الحديثة المبنية على Unix كلمات المرور فقط في ملف / etc / shadow ولا يمكن قراءتها إلا بواسطة الروت.
- في إصدارات Unix الأقدم ، قد تجد كلمات مرور مخزنة في ملف / etc / passwd. هذا ما يبدو عليه ملف / etc / shadow:



```
root@bt:/# cat /etc/shadow
root:$6$BZenJFhs$Qe4svOCrJHMQ9mmRDuUGjTVllCDQ8qJ/hGwzeaKGTpTx/xU4zp7X8ipcHG6YSAD
HbDuxySnK1PLhK5d1WGpv6/:15920:0:99999:7:::
daemon:x:15907:0:99999:7:::
bin:x:15907:0:99999:7:::
```

Common Applications of Linux

فيما يلي بعض التطبيقات الشائعة التي قد تواجهها على الأرجح مع أي نكهة Linux تستخدمها:

■■ Apache —هذا خادم ويب مفتوح المصدر. تعمل معظم مواقع الويب على خادم الويب Apache.

■■ MySQL - هذه هي قاعدة البيانات الأكثر شيوعًا المستخدمة في الأنظمة المستندة إلى Unix.

■■ Sendmail - خادم بريد مجاني يعمل بنظام Linux. وهي متوفرة داخل كل من الإصدارات مفتوحة المصدر والتجارية.

■■ Postfix - يمكن استخدام هذا كبديل لإرسال البريد الإلكتروني.

■■ PureFTP - هذا هو خادم بروتوكول نقل الملفات الافتراضي المستخدم تقريبًا لجميع الأنظمة القائمة على نظام يونكس.

■■ Samba - يوفر هذا خدمات مشاركة الملفات والطابعات. أفضل جزء هو أنه يمكن أن يتكامل بسهولة مع الأنظمة المستندة إلى Windows.

Online website for practice

- Try hack me
- Hackthe box
- Cyberhub
- hackerenv
- Vulnweb.php http://testphp.vulnweb.com/login.php
- https://dst.com.ng/15-vulnerable-sites-legally-practice-hacking-skills/

Ejpt course

- شركة eLearnSecurity وفرت كورس PTS مجاناً بشكل كامل بما في ذلك الفيديوهات والابات الخاصه بالكورس
- وكل اللي عليك ساعتها بعد التطبيق للكورس انك تدفع تمن الامتحان بس ٢٠٠$ (غير اجباري)
- ادخل عاللينك وتسجل
  https://lnkd.in/gCuDiDA
- بعد متسجل هتدخل عاللينك دا وتبدا الكورس
  https://lnkd.in/gW2KQmN
  موجود السلايدات والفيديوهات وتفاصيل الدخول عالابات

Notebook

https://github.com/d3m0n4l3x/eJPT

- https://github.com/zAbuQasem/eJPT-Notes
- رابط فيه جميع الأنظمة :
- https://mega.nz/folder/STRVnKaR#6qeWpSkF1gSZAzBp5ebLNw