

Università degli Studi di Salerno



Dipartimento di Informatica

# Penetration Testing & Ethical Hacking

Distribuzioni Linux per il PenTesting e  
Fondamenti di Linux

Arcangelo Castiglione  
[arcastiglione@unisa.it](mailto:arcastiglione@unisa.it)

# Outline

---

- Kali Linux
- Altre Distribuzioni per il Pentesting
- Fondamenti di Linux
  - Struttura del File System
  - Comandi di Base

# Outline

---

- Kali Linux
- Altre Distribuzioni per il Pentesting
- Fondamenti di Linux
  - Struttura del File System
  - Comandi di Base

# Kali Linux

## Storia

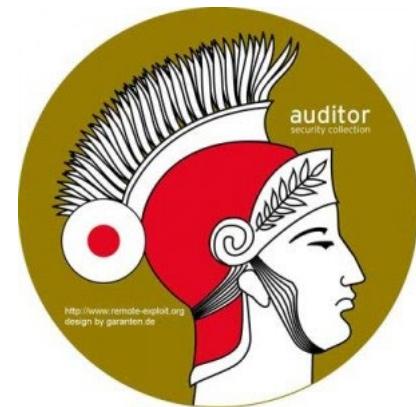
- Distribuzione Linux sviluppata appositamente per il penetration testing
- Kali Linux 1.0
  - È stata rilasciata il 12 marzo 2013
  - Prima era distribuita con il nome di BackTrack



# Kali Linux

## Storia

- BackTrack deriva a sua volta dalla fusione di varie distribuzioni Linux Live sviluppate per il penetration testing



# Kali Linux

## Diffusione

- Kali è tra le distribuzioni Linux più popolari comunemente usate

Classifica pagine visitate		
Periodo dati:		
Class.	Distribuzione	HPD*
1	<a href="#">Mint</a>	2826▲
2	<a href="#">MX Linux</a>	2056▼
3	<a href="#">EndeavourOS</a>	1778▼
4	<a href="#">CachyOS</a>	1761▲
5	<a href="#">Debian</a>	1407▲
6	<a href="#">Pop!_OS</a>	1249▼
7	<a href="#">Manjaro</a>	1152▲
8	<a href="#">Ubuntu</a>	1071▲
9	<a href="#">Fedora</a>	1007-
10	<a href="#">openSUSE</a>	741▲
11	<a href="#">Zorin</a>	721▲
12	<a href="#">elementary</a>	670▲
13	<a href="#">Nobara</a>	660▲
14	<a href="#">antiX</a>	528-
15	<a href="#">KDE neon</a>	521▼
16	<a href="#">TUXEDO</a>	503-
17	<a href="#">NixOS</a>	442▲
18	<a href="#">Solus</a>	419▲
19	<a href="#">Kali</a>	410-

<https://distrowatch.com/>



# Kali Linux

## Diffusione

➤ <https://distrowatch.com/table.php?distribution=kali>



## Kali Linux

Ultimo aggiornamento: 2025-03-19 18:14 UTC

- **Tipo:** [Linux](#)
- Basata su: [Debian \(Testing\)](#)
- Provenienza: [Gibraltar](#)
- Architettura: [aarch64, Apple M1, armel, x86\\_64](#)
- Desktop: [GNOME, KDE Plasma, Xfce](#)
- Categorie: [Data Rescue, Forensics, Live Medium, Raspberry Pi, Security](#)
- Stato: [Attiva](#)
- Popolarità: [19 \(410 visite al giorno\)](#)

Kali Linux (formerly known as BackTrack) is a Debian-based distribution with a collection of security and forensics tools. It features timely security updates, support for the ARM architecture, a choice of four popular desktop environments, and seamless upgrades to newer versions.

**Popolarità (visite al giorno):** 12 mesi: **19** (379), 6 mesi: **19** (410), 3 mesi: **20** (440), 4 settimane: **18** (488), 1 settimana: **28** (426)

**Average visitor rating:** 9.13/10 from 16 [review\(s\)](#).



# Kali Linux

## Caratteristiche Principali

---

- Si basa sulla distribuzione Debian Linux
- Ha un vasto supporto per le schede Wi-Fi
  - Ha un kernel personalizzato, con patch per *Packet Injection*
- Gli utenti possono personalizzare Kali Linux in base alle proprie esigenze
- Supporta (ed è supportata da) sistemi ARM-based

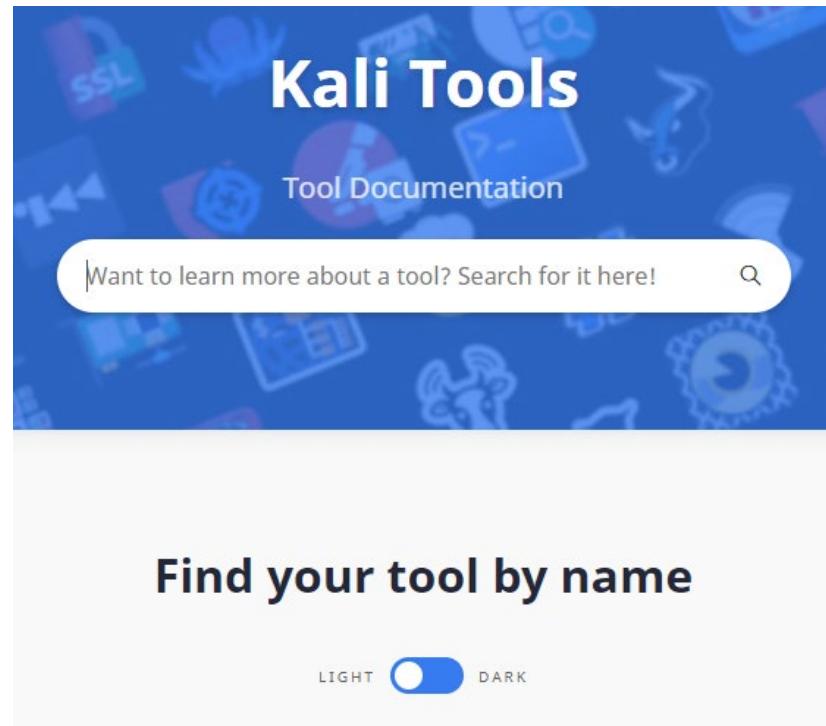


# Kali Linux

## Strumenti

---

- Ha più di 600 applicazioni per il penetration testing
- <https://tools.kali.org/tools-listing>



# Kali Linux

## Installazione

---

- Esistono varie modalità di utilizzo per Kali Linux
  - Eseguire Kali Linux direttamente da un CD/DVD Live
    - Senza installazione
  - Installare Kali Linux sull'Hard Disk
  - Installare Kali Linux su Penna USB
  - Installare Kali Linux in Virtual Machine
  - **Importare una pre-esistente immagine della Virtual Machine di Kali Linux**

# Kali Linux

## Installazione e Configurazione

---

- Nell'ambito del corso utilizzeremo Kali Linux in VirtualBox
  
- Per il download di VirtualBox
  - <https://www.virtualbox.org/wiki/Downloads>

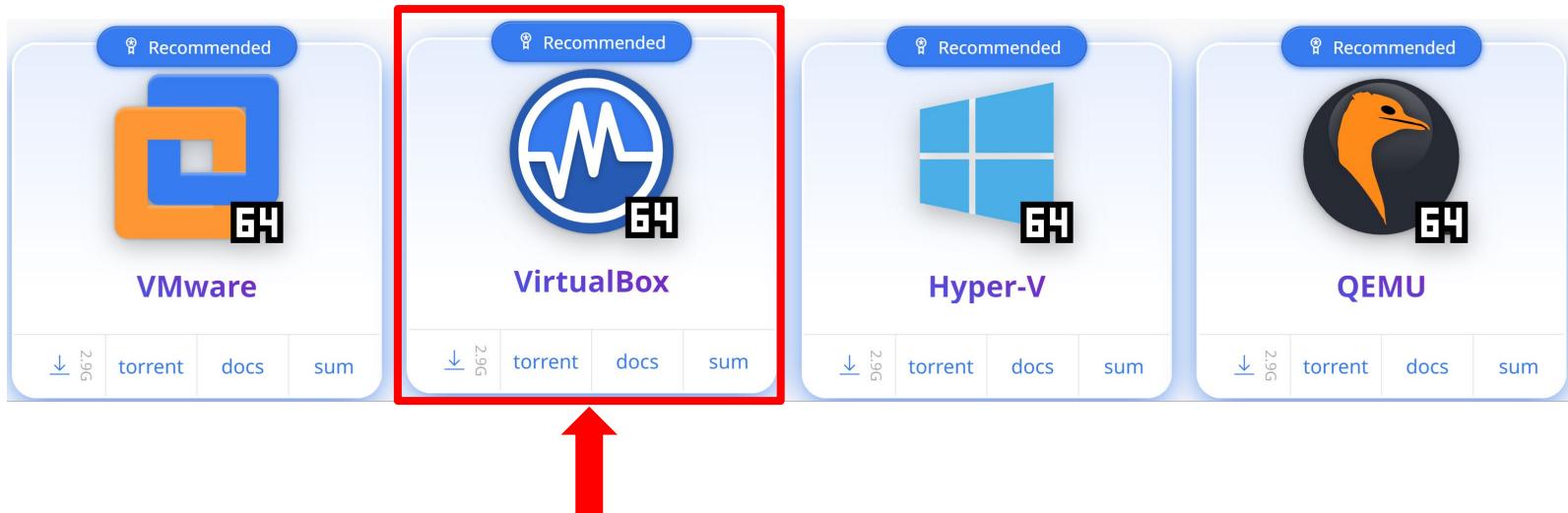
**«VirtualBox is a general-purpose full virtualizer for x86 hardware, targeted at server, desktop and embedded use»**



# Kali Linux

## Installazione e Configurazione

- Download ed installazione di un'immagine Kali Linux
- <https://www.kali.org/get-kali/#kali-virtual-machines>



# Kali Linux

## Installazione e Configurazione

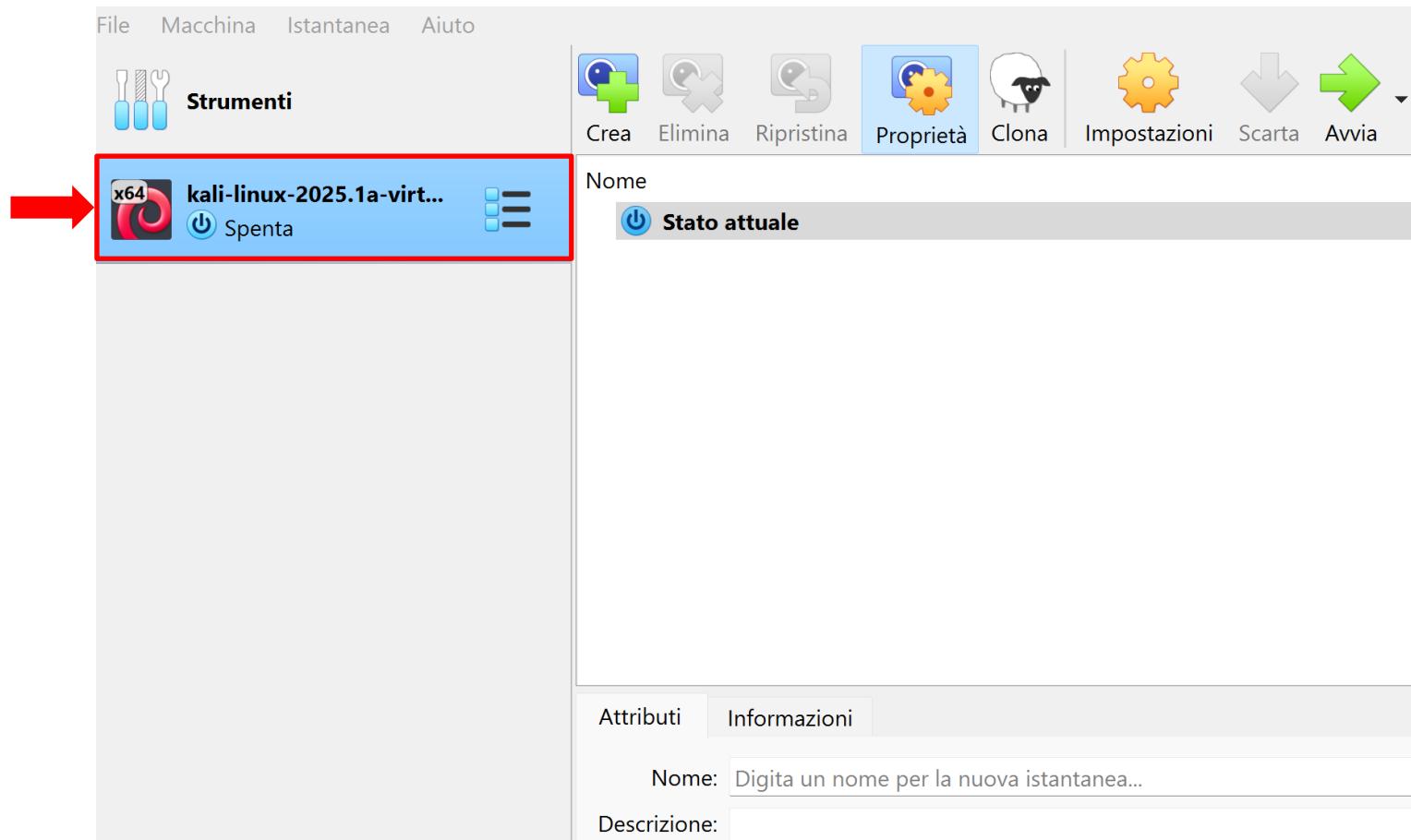
---

- Dopo aver scaricato il file **kali-linux-2025.1a-virtualbox-amd64.7z**, decomprimerlo e fare doppio click sul file **kali-linux-2025.1a-virtualbox-amd64.vbox**

 kali-linux-2025.1a-virtualbox-amd64.vbox	VirtualBox Machine Defini...	3 KB	07/03/2025 15:21
 kali-linux-2025.1a-virtualbox-amd64.vdi	Virtual Disk Image	14.685.505 KB	07/03/2025 15:21

# Kali Linux

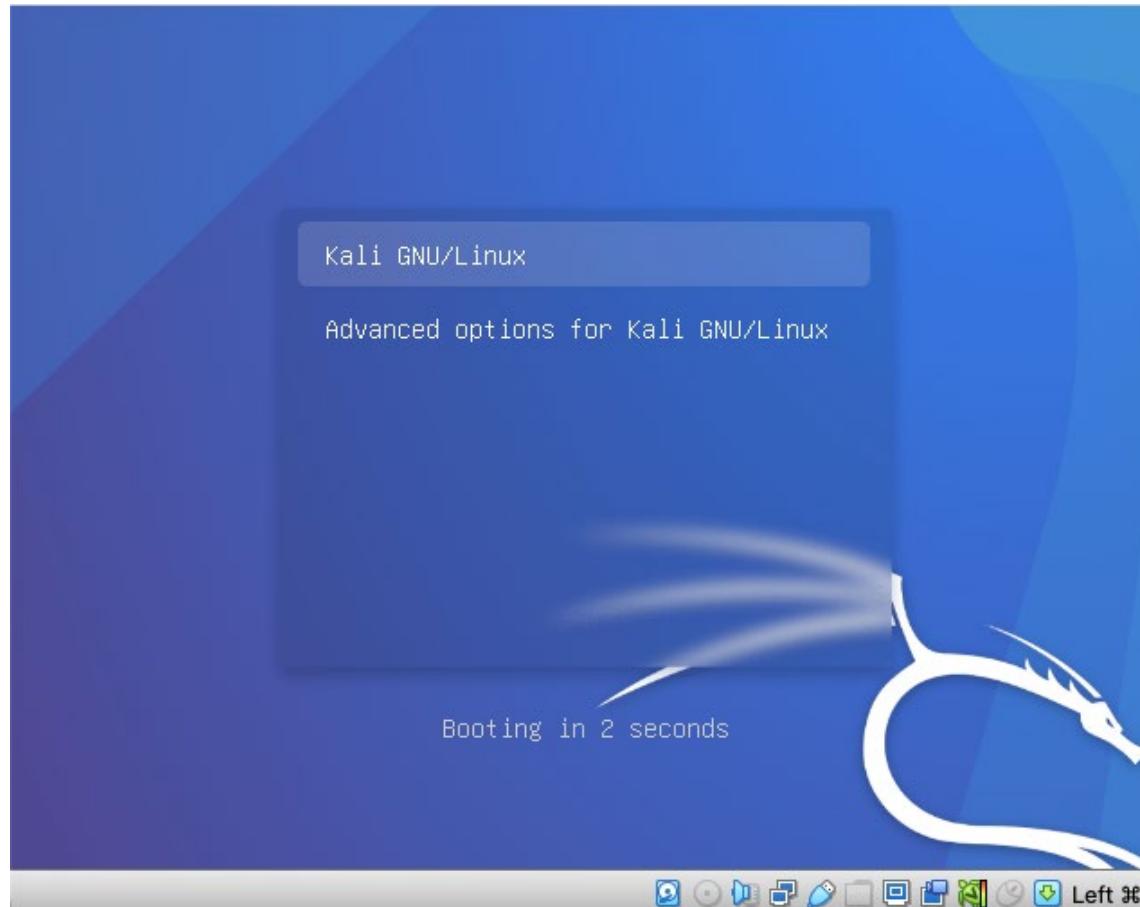
## Installazione e Configurazione



# Kali Linux

## Installazione e Configurazione

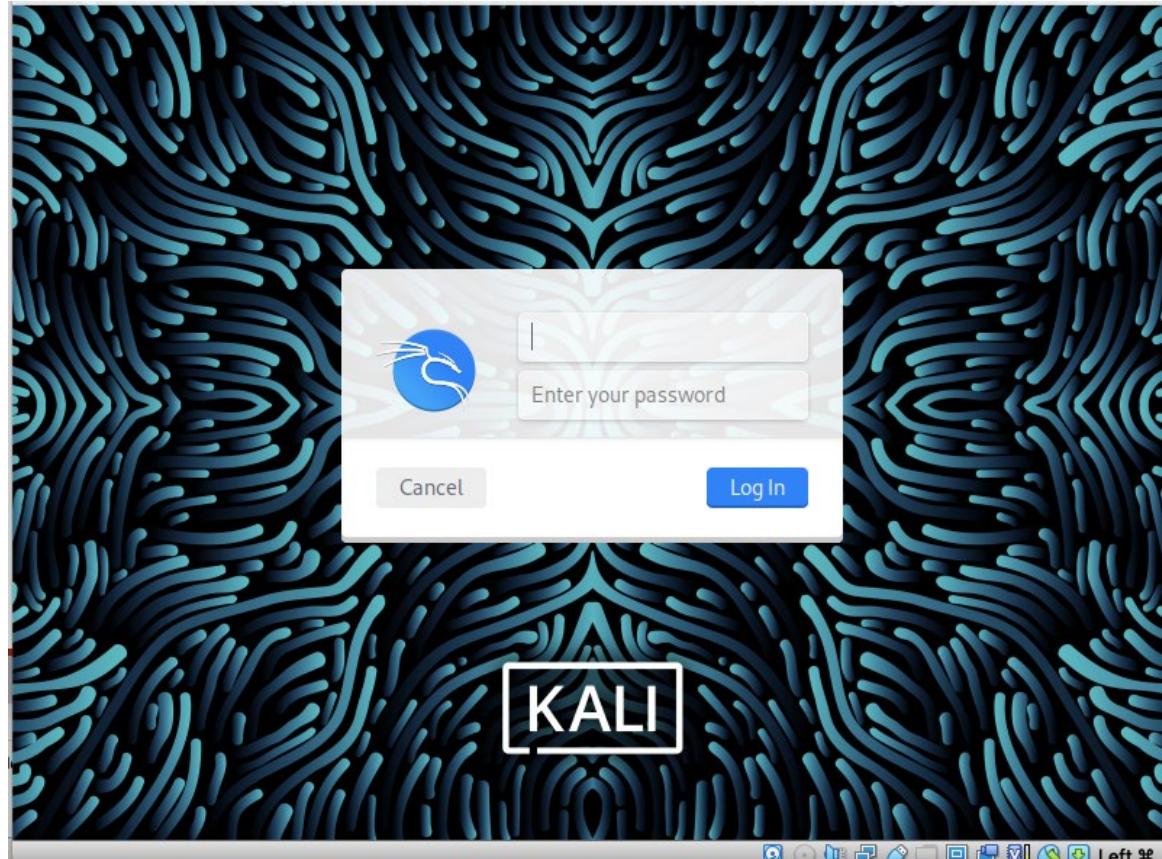
---



# Kali Linux

## Login

---

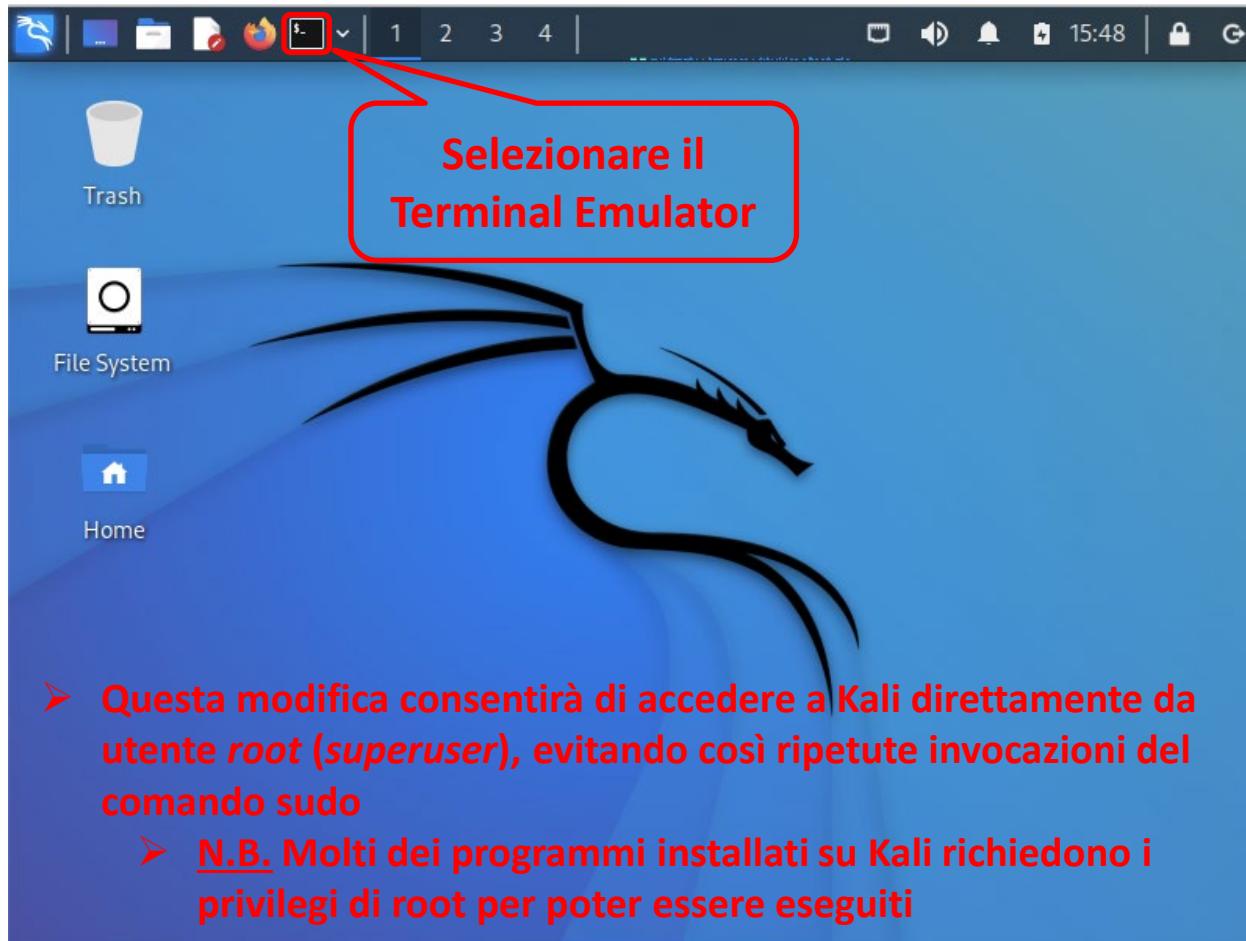


Username: **kali**

Password: **kali**

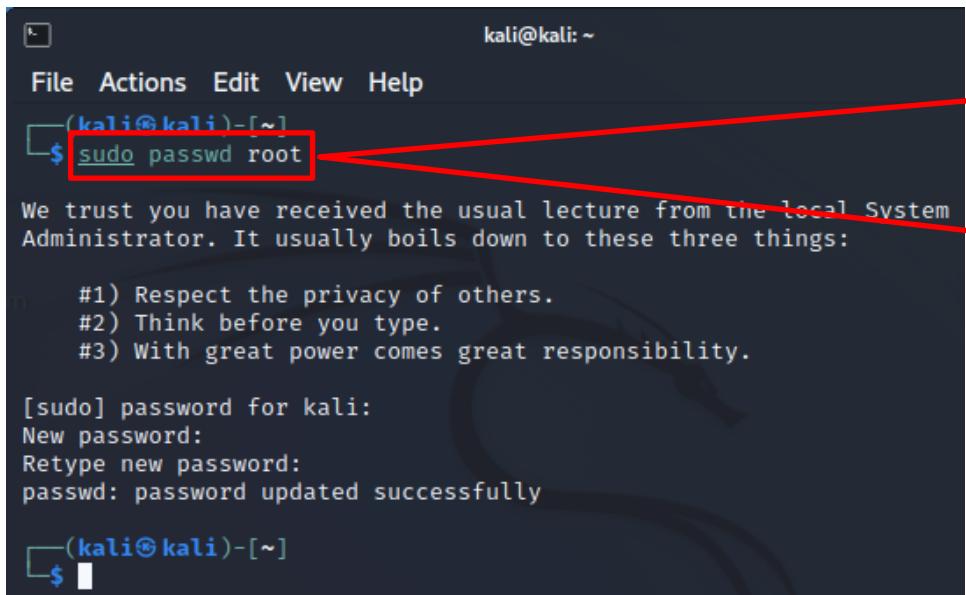
# Kali Linux

## Abilitare Login Utente Root



# Kali Linux

## Abilitare Login Utente Root



```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo passwd root
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for kali:
New password:
Retype new password:
passwd: password updated successfully

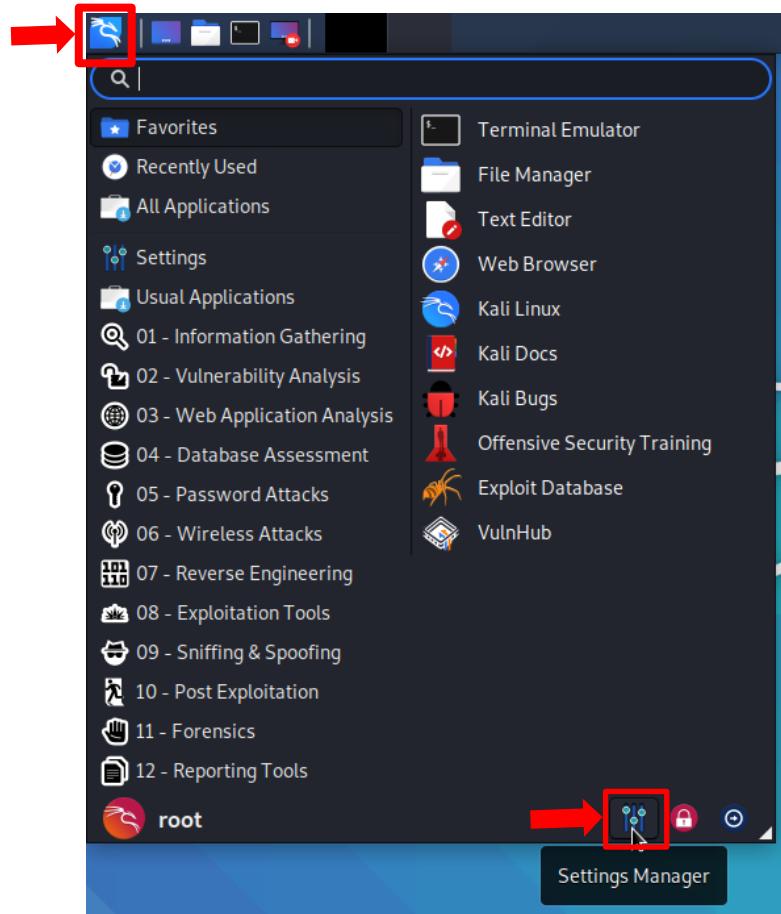
(kali㉿kali)-[~]
$
```

A red box highlights the command `sudo passwd root` in the terminal. A red curved arrow points from this highlighted command to the first point of the explanatory text on the right.

- Tramite il comando «`sudo passwd root`» imposto la password per l'utente root
- Va innanzitutto inserita la password per l'utente **kali**: **kali**
- Poi va scelta la password per l'utente **root**

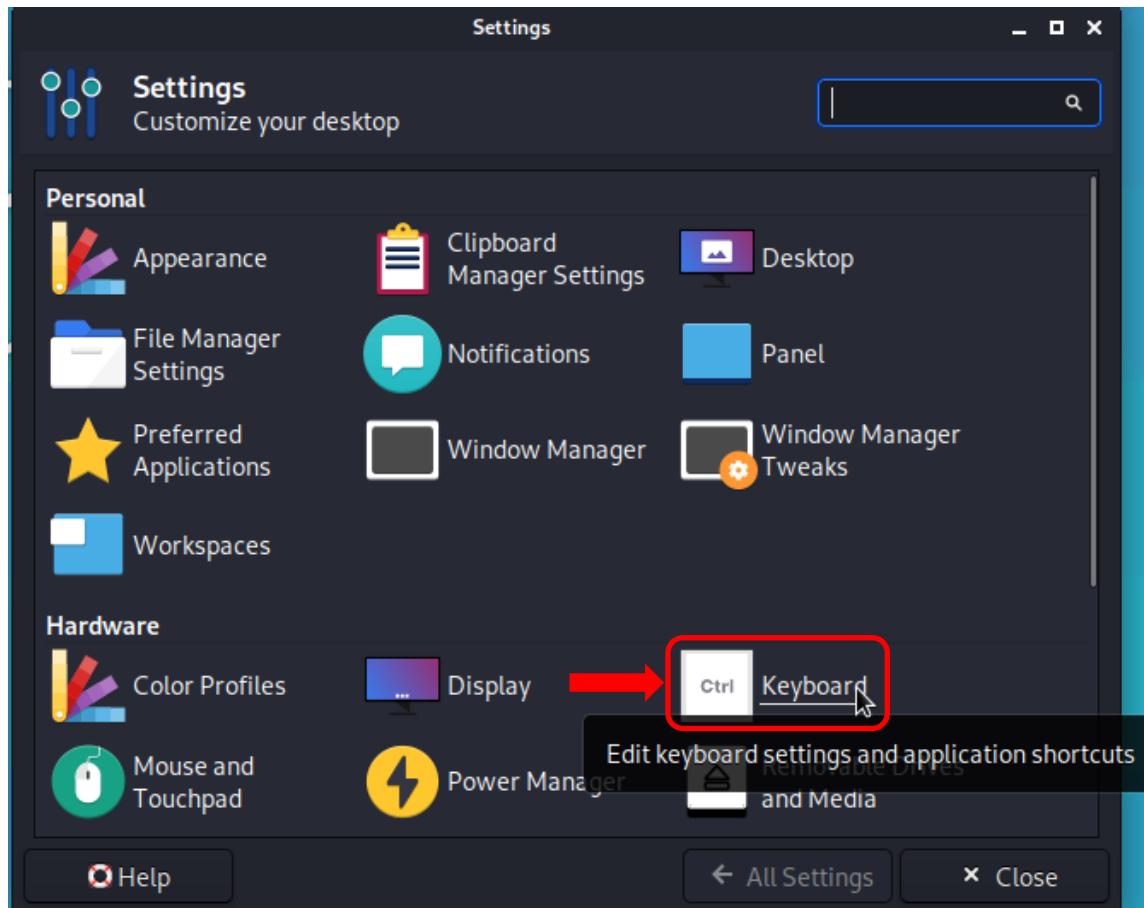
# Kali Linux

## Impostare Tastiera Italiana



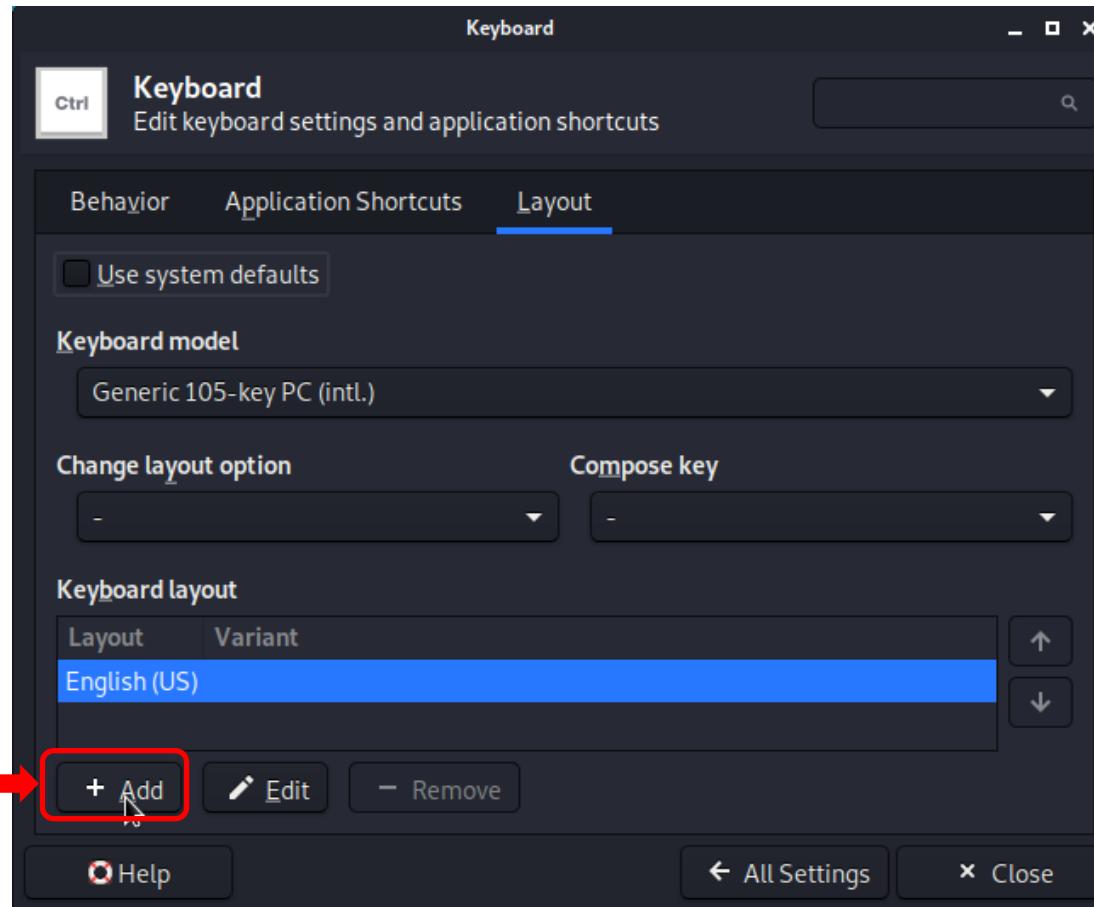
# Kali Linux

## Impostare Tastiera Italiana



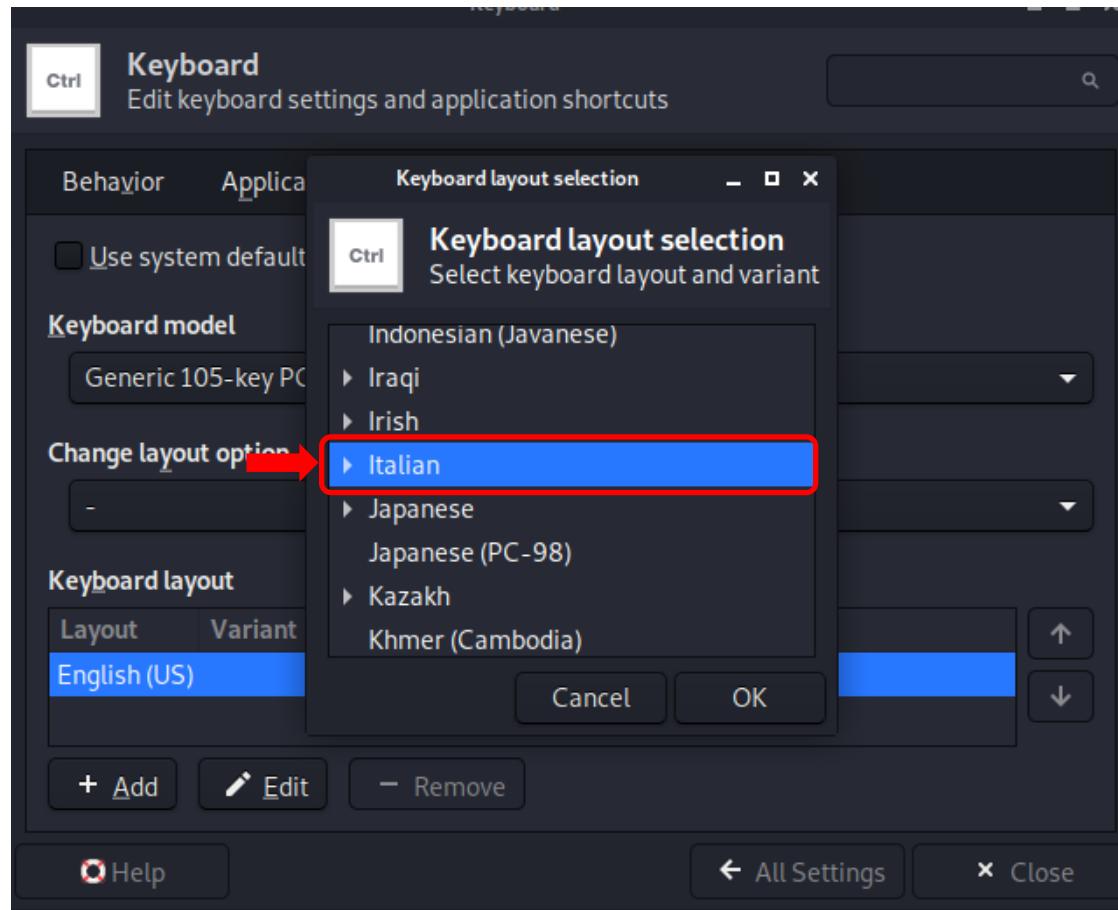
# Kali Linux

## Impostare Tastiera Italiana



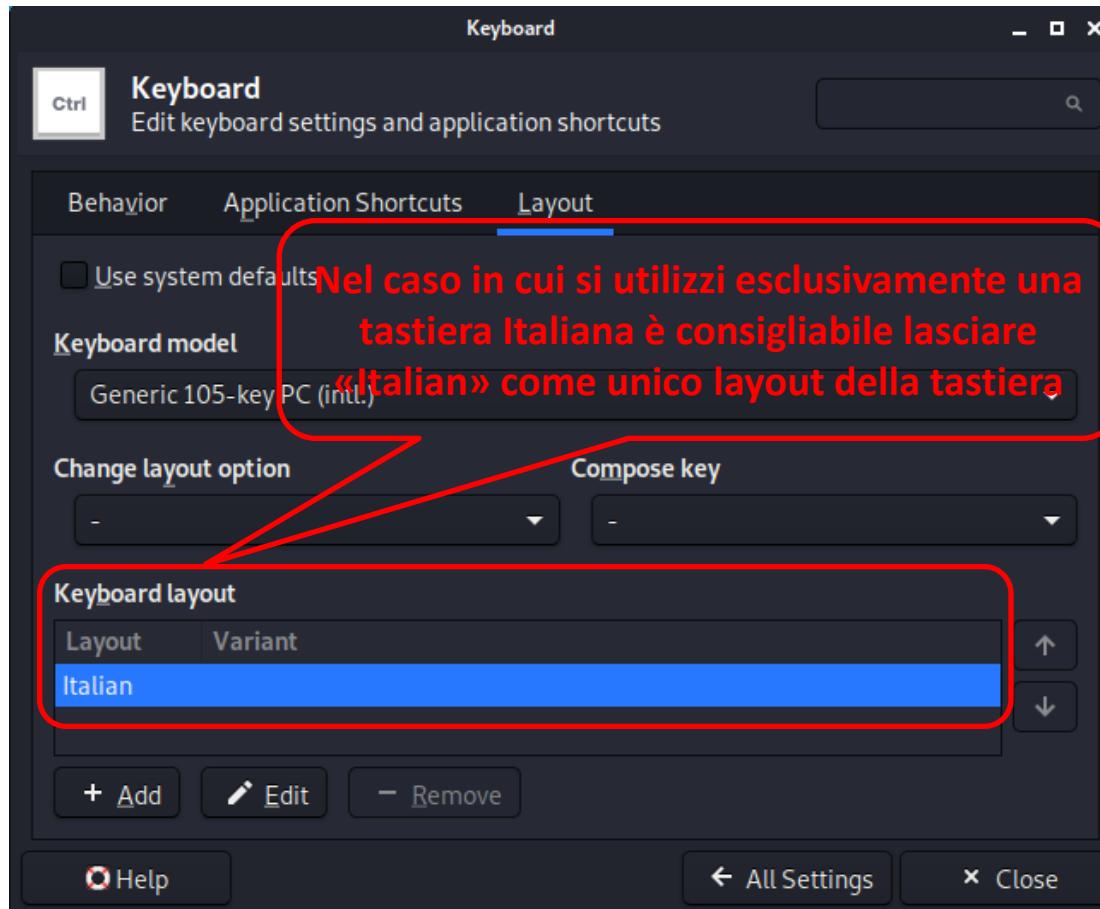
# Kali Linux

## Impostare Tastiera Italiana



# Kali Linux

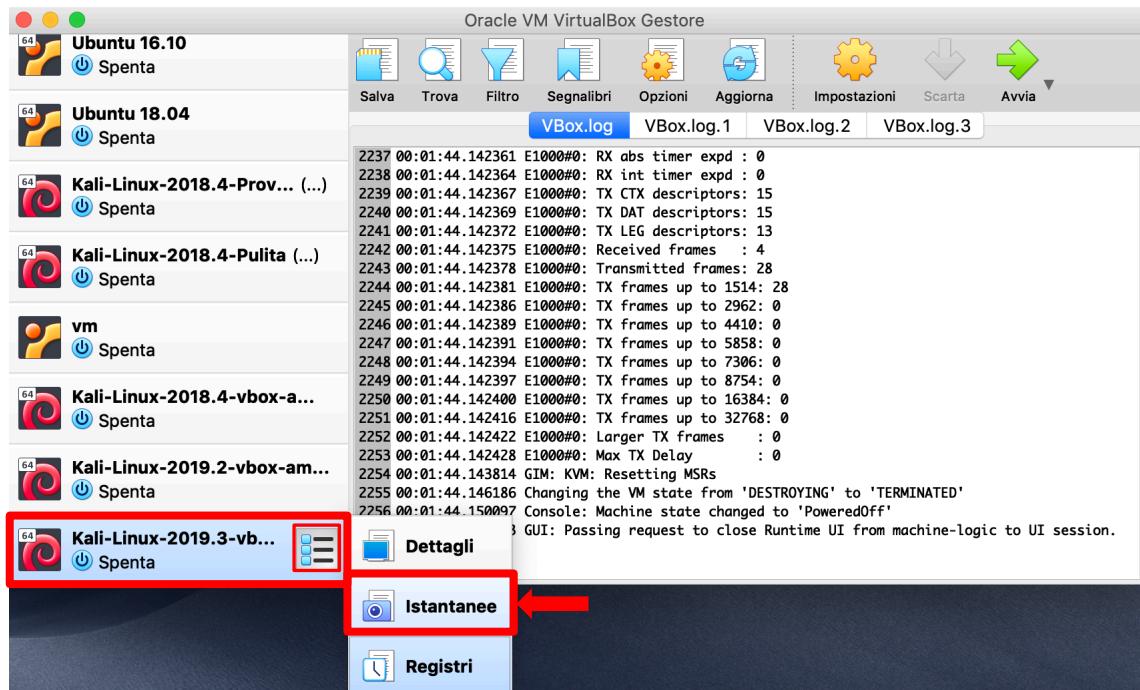
## Impostare Tastiera Italiana



# Kali Linux

## Istantanee Virtual Box

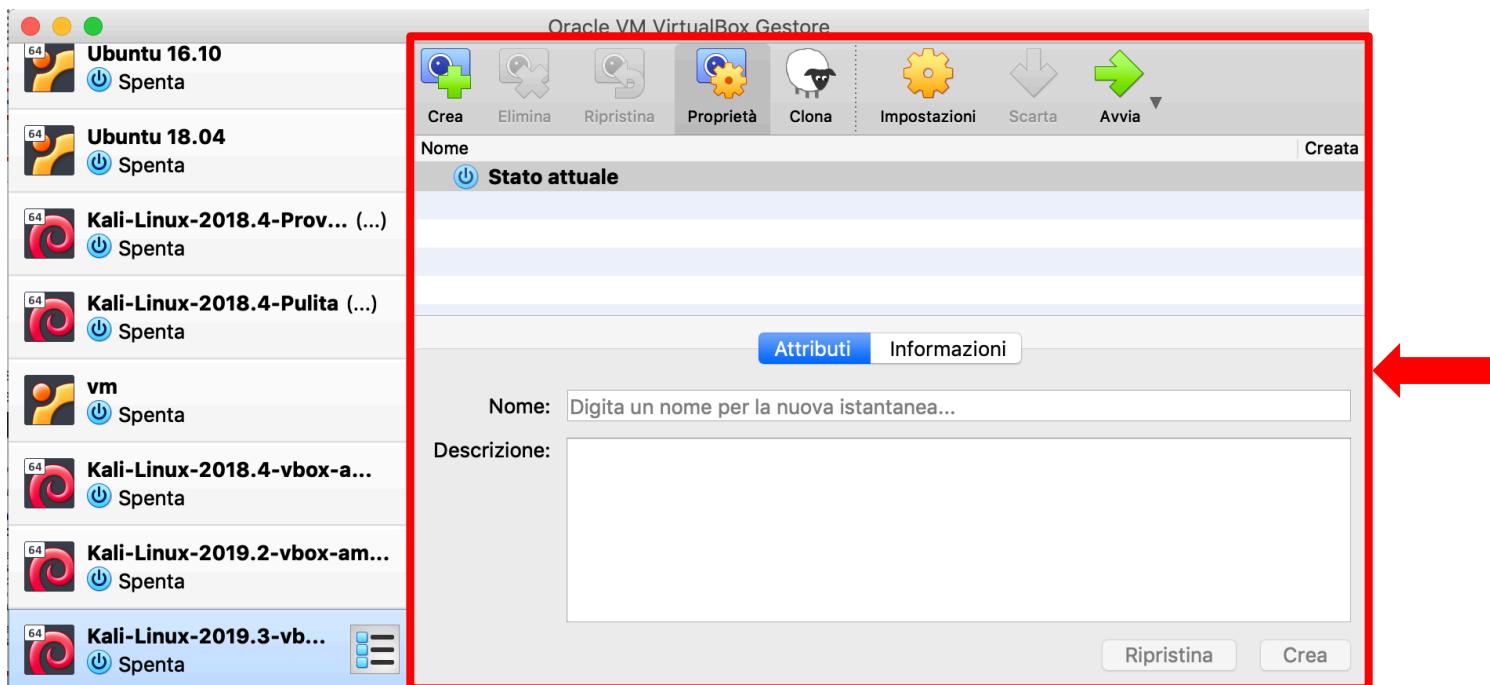
- Dette anche snapshot
- Permettono di «salvare» lo stato di una macchina virtuale in un dato momento e di ripristinarlo successivamente



# Kali Linux

## Istantanee Virtual Box

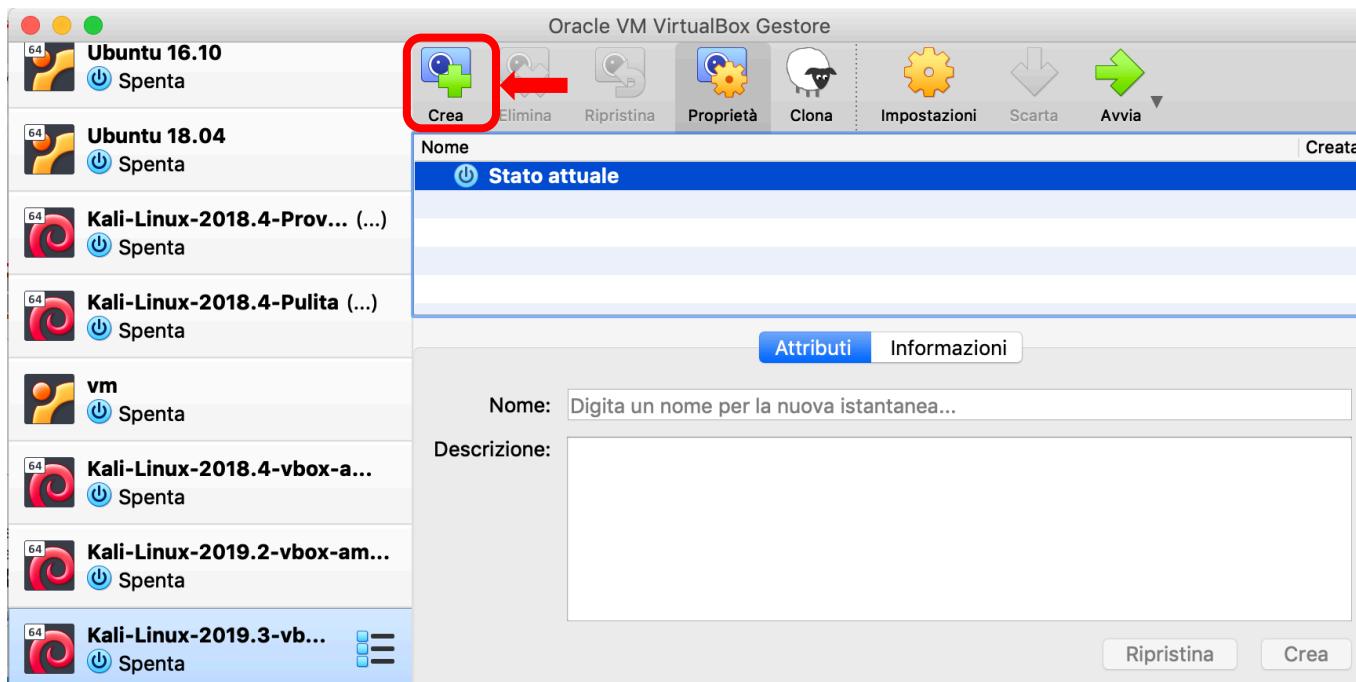
- Dette anche snapshot
- Permettono di «salvare» lo stato di una macchina virtuale in un dato momento e di ripristinarlo successivamente



# Kali Linux

## Istantanee Virtual Box

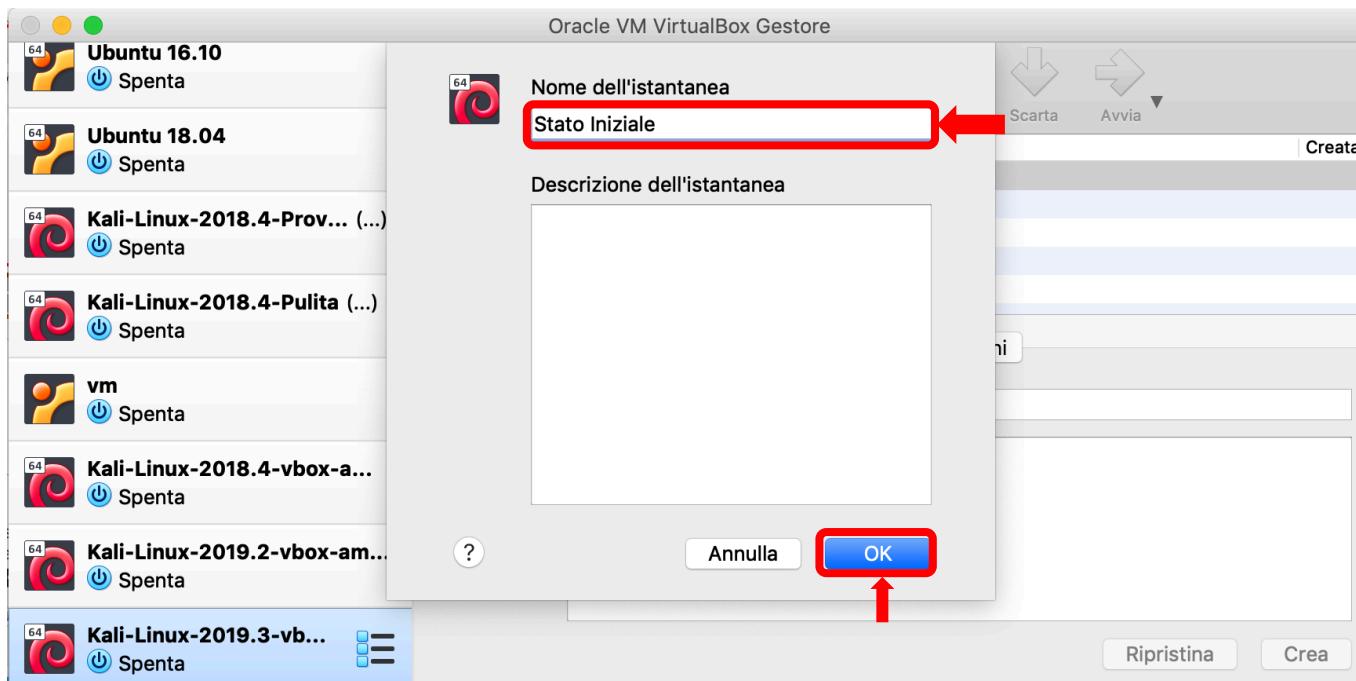
- Dette anche snapshot
- Permettono di «salvare» lo stato di una macchina virtuale in un dato momento e di ripristinarlo successivamente



# Kali Linux

## Istantanee Virtual Box

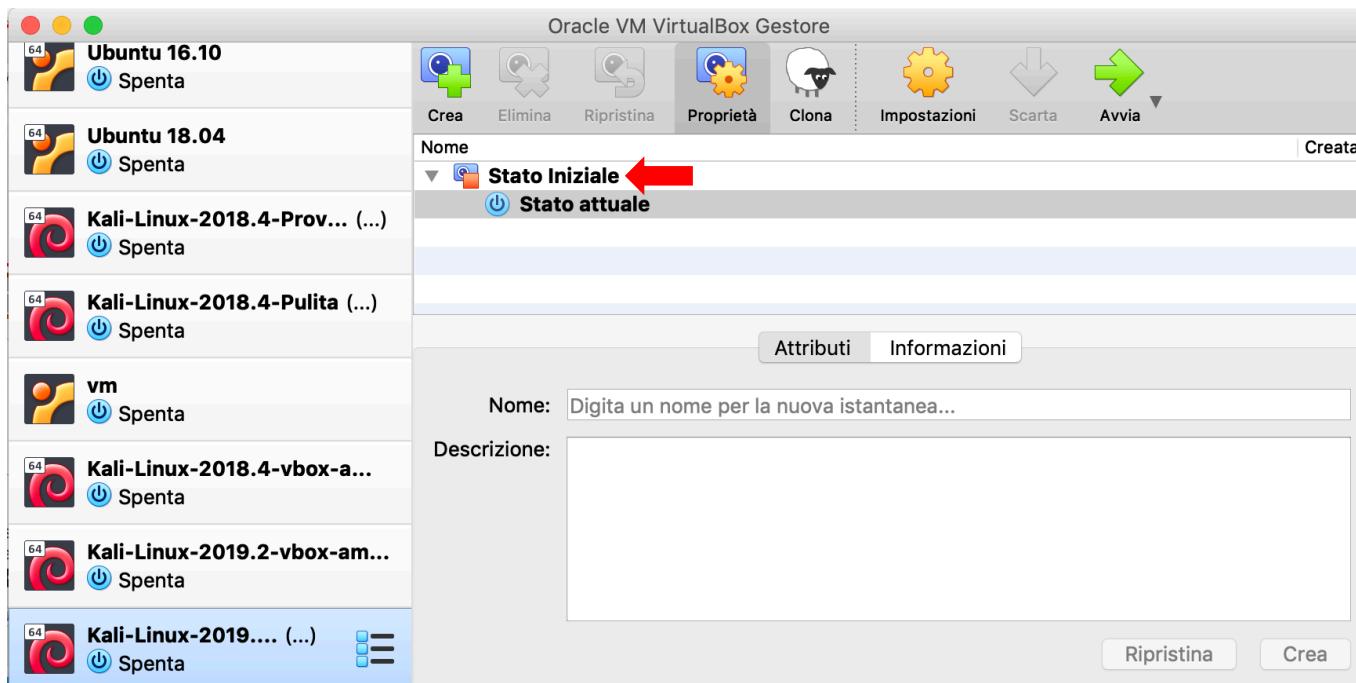
- Dette anche snapshot
- Permettono di «salvare» lo stato di una macchina virtuale in un dato momento e di ripristinarlo successivamente



# Kali Linux

## Istantanee Virtual Box

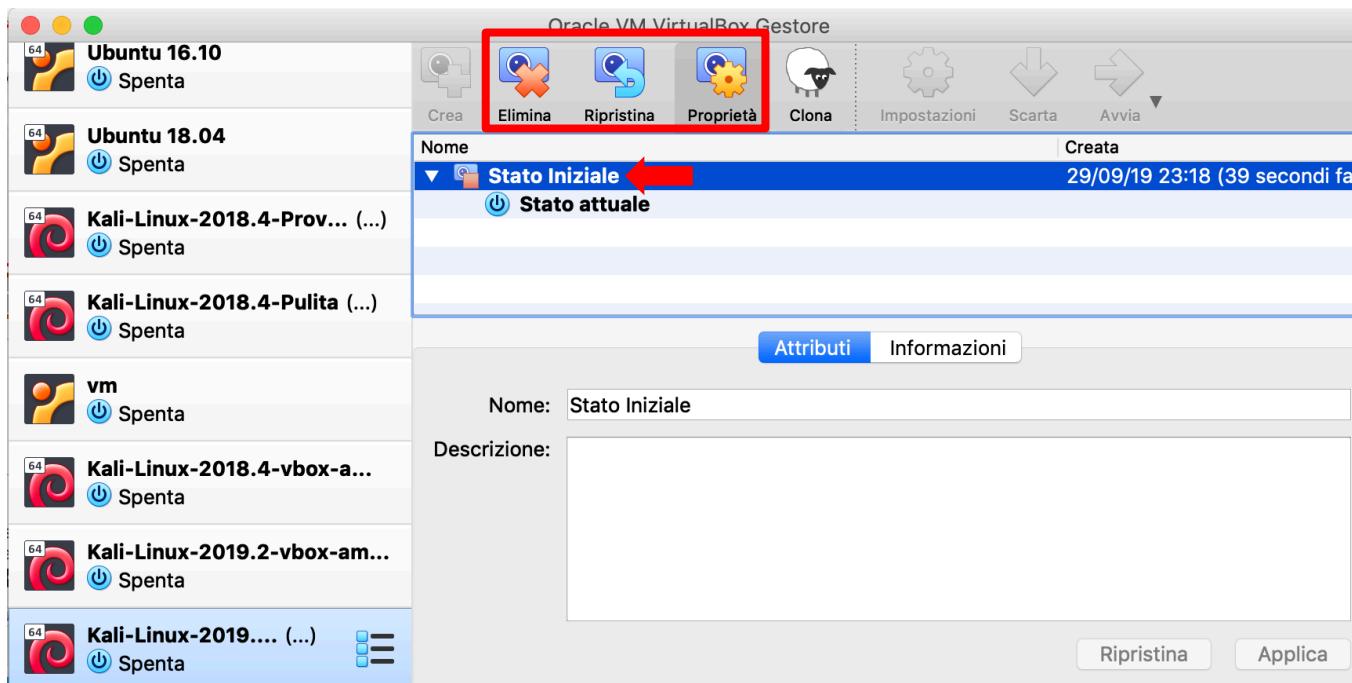
- Dette anche snapshot
- Permettono di «salvare» lo stato di una macchina virtuale in un dato momento e di ripristinarlo successivamente



# Kali Linux

## Istantanee Virtual Box

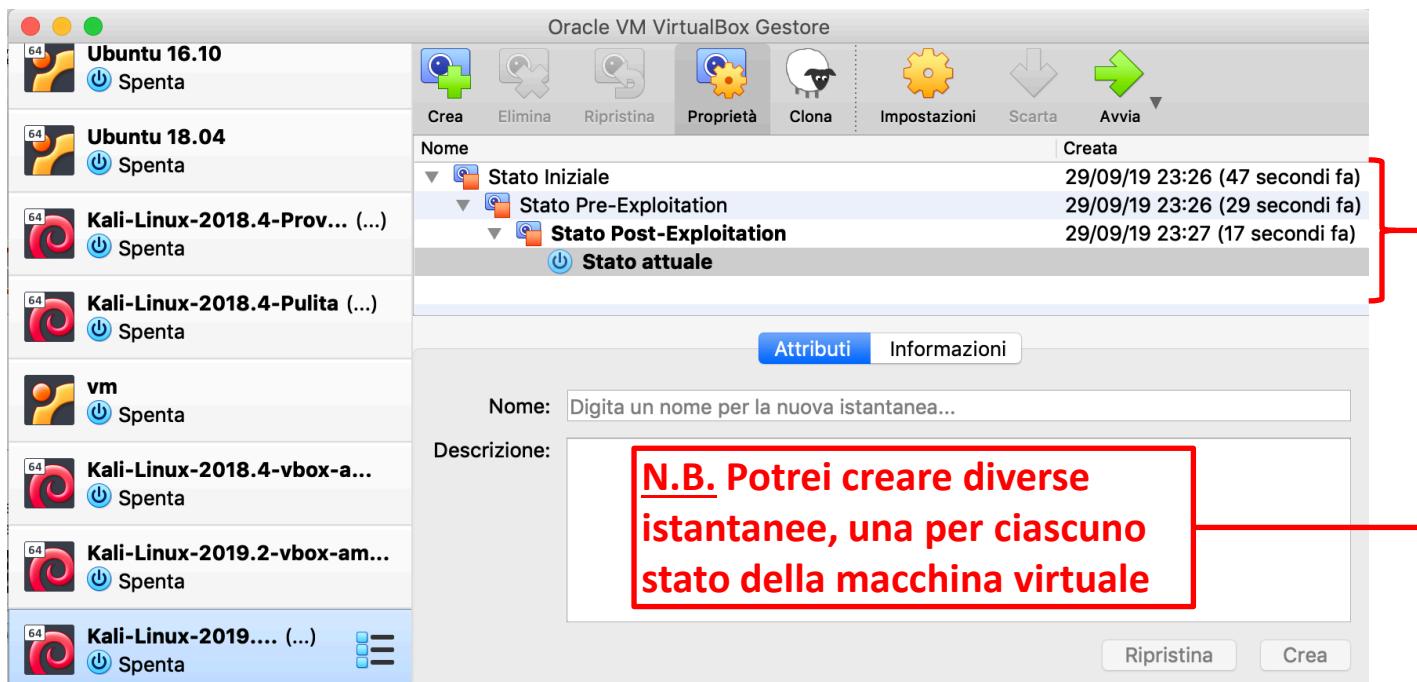
- Dette anche snapshot
- Permettono di «salvare» lo stato di una macchina virtuale in un dato momento e di ripristinarlo successivamente



# Kali Linux

## Istantanee Virtual Box

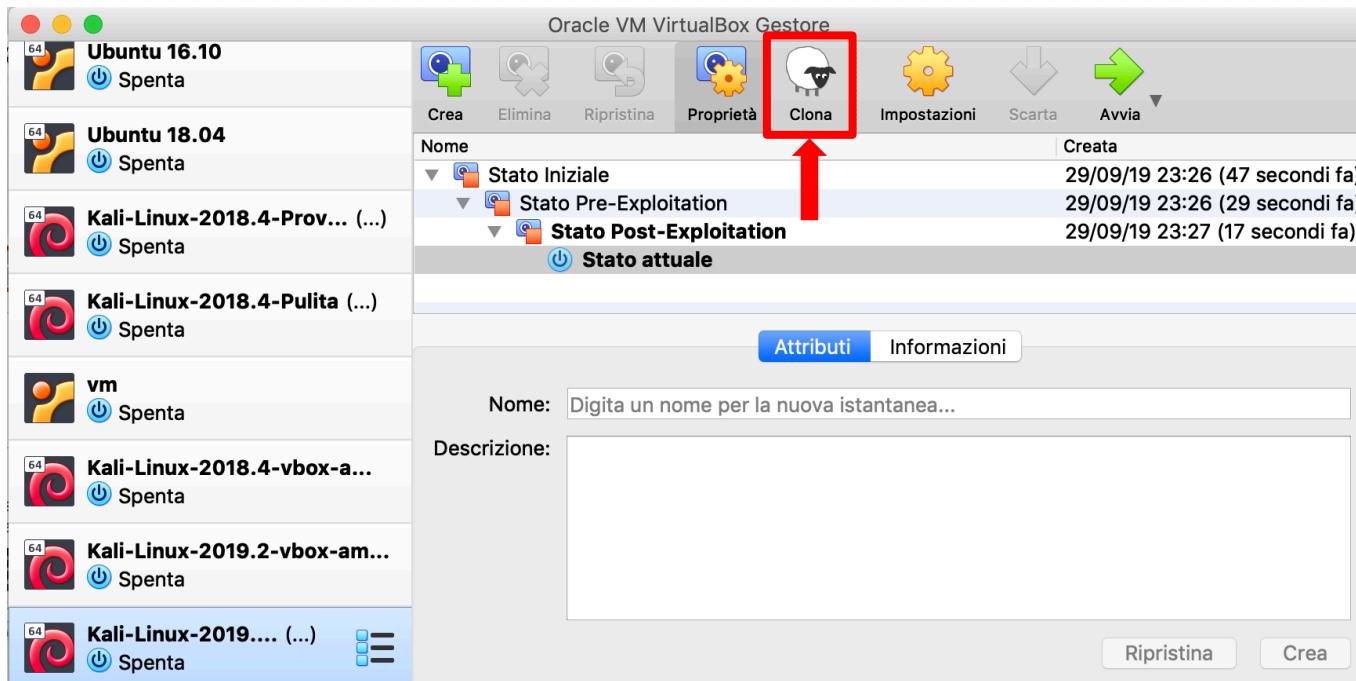
- Dette anche snapshot
- Permettono di «salvare» lo stato di una macchina virtuale in un dato momento e di ripristinarlo successivamente



# Kali Linux

## Istantanee Virtual Box

- Dette anche snapshot
- Permettono anche di clonare l'intera macchina virtuale



# Kali Linux

## Istantanee Virtual Box

- Dette anche snapshot
- Permettono anche di clonare l'intera macchina virtuale



# Kali Linux

## Comandi

---

- Vengono eseguiti nel Terminale (o **shell**)
- Un comando può anche essere seguito da parametri



# Kali Linux

## Comandi

---

- In generale è possibile ottenere informazioni su un determinato comando (**nomeComando**) nei modi seguenti
  - `man nomeComando`
  - `nomeComando -help`
  - `nomeComando --help`
- È possibile completare il nome di un comando usando il tasto Tab

# Kali Linux

## Comandi

### ➤ Esempio: **man ls**

```
LS(1)                               User Commands                               LS(1)

NAME
ls - list directory contents

SYNOPSIS
ls [OPTION]... [FILE]...

DESCRIPTION
List information about the FILEs (the current directory by default). Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.

Mandatory arguments to long options are mandatory for short options too.

-a, --all
      do not ignore entries starting with .

-A, --almost-all
      do not list implied . and ..

--author
      with -l, print the author of each file

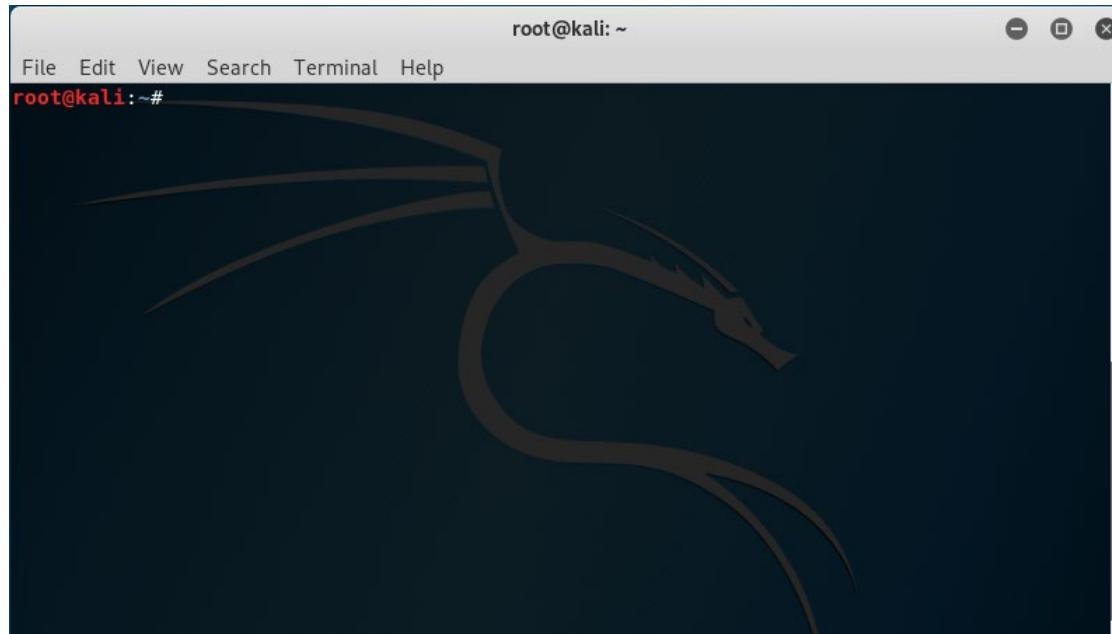
-b, --escape
      print C-style escapes for nongraphic characters

--block-size=SIZE
      with -l, scale sizes by SIZE when printing them; e.g., '--block-size=M';
      see SIZE format below
```

# Kali Linux

## Aggiornare il Sistema

- Per aggiornare il sistema è necessario eseguire il terminale (Terminal) e digitare in sequenza i seguenti due comandi
  - **sudo apt-get update** (oppure **apt update**)
  - **sudo apt-get dist-upgrade** (oppure **apt dist-upgrade**)



# Kali Linux

## Aggiornare il Sistema

---

➤ **apt-get update**

```
root@kali:~# apt-get update
Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
root@kali:~#
```

# Kali Linux

## Aggiornare il Sistema

---

➤ **apt-get dist-upgrade**

```
root@kali:~# apt-get dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
```

```
1356 upgraded, 155 newly installed, 5 to remove and 0 not upgraded.
Need to get 1.778 MB/1.823 MB of archives.
After this operation, 1.899 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

# Kali Linux

## Aggiornare il Sistema

➤ **apt-get dist-upgrade**

```
root@kali:~# apt-get dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
```

```
1356 upgraded, 155 newly installed, 5 to remove and 0 not upgraded.
Need to get 1.778 MB/1.823 MB of archives.
After this operation, 1.899 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

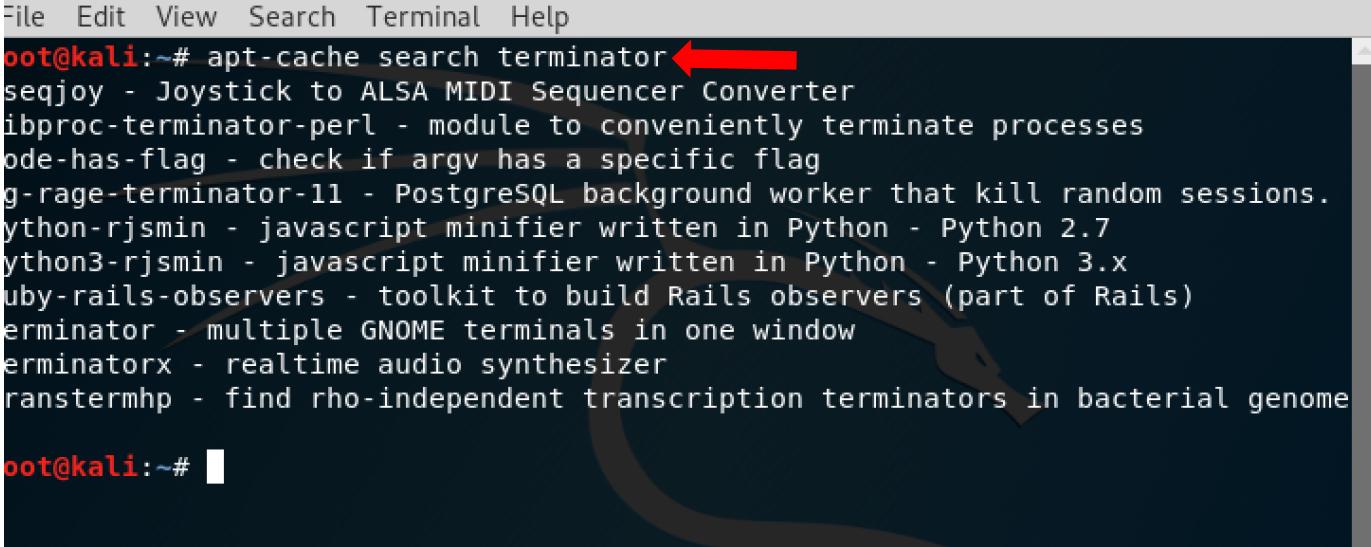
**N.B. Il processo di aggiornamento richiede un tempo variabile a seconda della quantità di dati da scaricare e della velocità della connessione Internet di cui si dispone**

# Kali Linux

## Ricerca ed Installazione di Applicativi

### ➤ Ricerca Applicativi

➤ **apt-cache search NomeApplicativo\***



```
File Edit View Search Terminal Help
oot@kali:~# apt-cache search terminator←
seqjoy - Joystick to ALSA MIDI Sequencer Converter
ibproc-terminator-perl - module to conveniently terminate processes
ode-has-flag - check if argv has a specific flag
g-rage-terminator-11 - PostgreSQL background worker that kill random sessions.
python-rjsmin - javascript minifier written in Python - Python 2.7
python3-rjsmin - javascript minifier written in Python - Python 3.x
uby-rails-observers - toolkit to build Rails observers (part of Rails)
erminator - multiple GNOME terminals in one window
erminatorx - realtime audio synthesizer
ranstermh - find rho-independent transcription terminators in bacterial genome

oot@kali:~# █
```

# Kali Linux

## Ricerca ed Installazione di Applicativi

### ➤ Ricerca Applicativi

➤ `apt-cache search NomeApplicativo*`

```
File Edit View Search Terminal Help
root@kali:~# apt-cache search terminator
seqjoy - Joystick to ALSA MIDI Sequencer Converter
ibproc-terminator-perl - module to conveniently terminate
ode-has-flag - check if argv has a specific flag
g-rage-terminator-11 - PostgreSQL background worker
python-rjsmin - javascript minifier written in Python
python3-rjsmin - javascript minifier written in Python
uby-rails-observers - toolkit to build Rails observers
terminator - multiple GNOME terminals in one window
terminatorx - realtime audio synthesizer
ranstermh - find rho-independent transcription factors
```

root@kali:~# █

Facendo terminare con il simbolo \* il nome del comando da cercare, verranno individuati tutti gli applicativi il cui nome comincia per la stringa cercata

# Kali Linux

## Ricerca ed Installazione di Applicativi

### ➤ Installazione Applicativi

➤ `apt-get install NomeApplicativo`

```
File Edit View Search Terminal Help
root@kali:~# apt-get install terminator
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  glusterfs-common guile-2.0-libs ibverbs-providers libacl1-dev libattr1-dev
  libbind9-160 libboost-atomic1.62.0 libboost-chrono1.62.0
  libboost-date-time1.62.0 libboost-filesystem1.62.0 libboost-iostreams1.62.0
  libboost-program-options1.62.0 libboost-program-options1.67.0
  libboost-python1.62.0 libboost-random1.62.0 libboost-serialization1.62.0
  libboost-serialization1.67.0 libboost-system1.62.0 libboost-test1.62.0
  libboost-test1.67.0 libboost-thread1.62.0 libboost-timer1.62.0
  libboost-timer1.67.0 libcephfs1 libcgal13 libcharls1 libdee-1.0-4 libdns1102
  libenca0 libexempi3 libfcgi-bin libfcgioldbl libgeos-3.7.0 libgfchangelog0
  libgfdb0 libglusterfs-dev libgmime-3.0-0 libgtk2-perl libhunspell-1.6-0
  libibverbs1 libirs160 libisc169 libisccc160 libiscfg160 libjemalloc1
  liblouis16 liblvm2app2.2 liblvm2cmd2.02 liblwgeom-2.5-0 liblwgeom-dev
  liblwres160 libmozjs-52-0 libnfs11 libntfs-3g88 libomp5 libopencv-core3.2
  libopencv-imgproc3.2 libpango-perl libperl5.26 libpoppler74 libpoppler80
  libprotobuf-lite10 libprotobuf10 libpside1.2 libpython3.6 libpython3.6-dev
```

Oltre all'applicativo vengono installate anche tutte le dipendenze necessarie al suo funzionamento

# Kali Linux

## Gestione Pacchetti

- Per maggiori informazioni sulla gestione dei pacchetti in Kali Linux digitare il comando
- **man apt**

```
root@kali: ~
File Edit View Search Terminal Help
APT(8) APT APT(8)

NAME
apt - command-line interface

SYNOPSIS
apt [-h] [-o=config_string] [-c=config_file] [-t=target_release]
[-a=architecture] {list | search | show | update |
install pkg [=pkg_version_number | /target_release]... | |
remove pkg... | upgrade | full-upgrade | edit-sources |
{-v | --version} | {-h | --help} }

DESCRIPTION
apt provides a high-level commandline interface for the package
management system. It is intended as an end user interface and enables
some options better suited for interactive usage by default compared to
more specialized APT tools like apt-get(8) and apt-cache(8).

Much like apt itself, its manpage is intended as an end user interface
and as such only mentions the most used commands and options partly to
not duplicate information in multiple places and partly to avoid
overwhelming readers with a cornucopia of options and details.

Dis Man page apt(8) line 1 (press h for help or q to quit) ux
```

# Kali Linux

## VirtualBox Guest Additions

---

- Forniscono alla Virtual Machine (VM) funzionalità aggiuntive
- Consentono di ottenere una migliore interazione tra la **macchina host** (dove è eseguita la VM) e la **macchina guest** (VM in esecuzione)
  - Copia e incolla, drag and drop di file, etc
- Per maggiori informazioni
  - <https://www.virtualbox.org/manual/ch04.html>

# Kali Linux

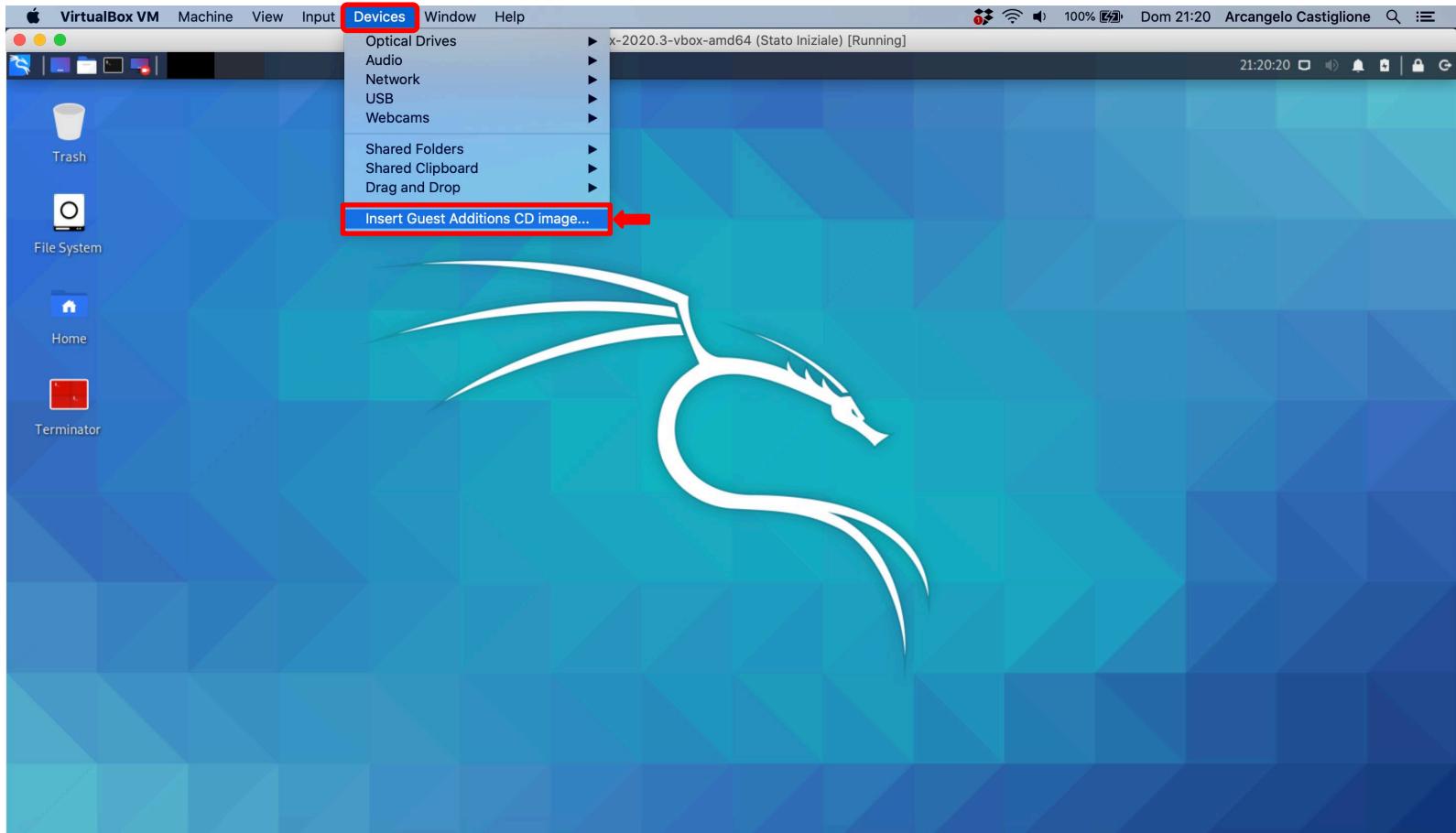
## VirtualBox Guest Additions

---

- Prima dell'installazione delle Guest Additions è necessario installare determinati moduli del kernel
  - **sudo apt-get install build-essential linux-headers-\$(uname -r) dkms**
  - **sudo apt-get install virtualbox-ext-pack virtualbox-guest-utils virtualbox-guest-x11**

# Kali Linux

## VirtualBox Guest Additions – Installazione (1/4)



# Kali Linux

## VirtualBox Guest Additions – Installazione (2/4)

```
cd /media/kali/VBox_GAs_7.0.6
```

```
(root@kali)-[/media/kali/VBox_GAs_7.0.6]
ls
ORUN.INF          VBoxDarwinAdditionsUninstall.i
orun.sh           VBoxLinuxAdditions.run
t                 VBoxSolarisAdditions.pkg
x                 VBoxWindowsAdditions-amd64.exe
asroot.sh         VBoxWindowsAdditions.exe
NS.TBL           VBoxWindowsAdditions-x86.exe
xDarwinAdditions.pkg windows11-bypass.reg
```

Entrare nella Directory **/media/kali/VBox\_GAs\_7.0.6** usando il comando **cd**

# Kali Linux

## VirtualBox Guest Additions – Installazione (2/4)

```
(root@kali)-[/media/kali/VBox_GAs_7.0.6]
# ls
AUTORUN.INF          VBoxDarwinAdditionsUninstall.tool
autorun.sh            VBoxLinuxAdditions.run
cert                  VBoxSolarisAdditions.pkg
NT3x                  VBoxWindowsAdditions-amd64.exe
OS2                   VBoxWindowsAdditions.exe
runasroot.sh          VBoxWindowsAdditions-x86.exe
TRANS.TBL             windows11-bypass.reg
VBoxDarwinAdditions.pkg
```

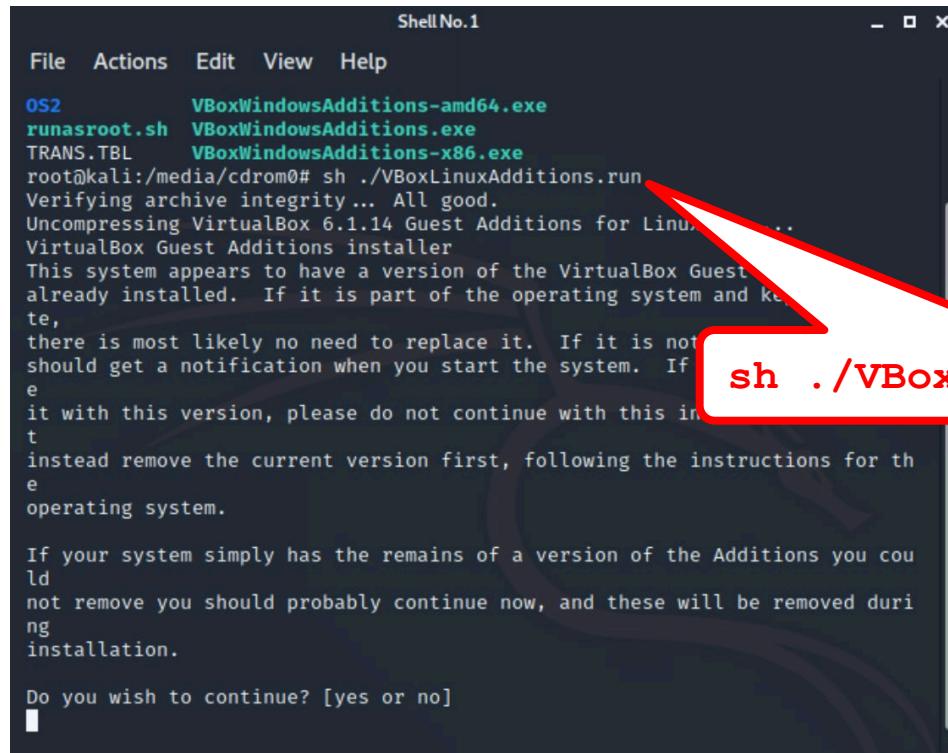
A red callout box labeled "ls" points to the command in the terminal window.

A red rectangle highlights the file "VBoxLinuxAdditions.run". A red arrow points from this rectangle to the file name.

Visualizzare il contenuto della Directory **/media/kali/VBox\_GAs\_7.0.6** usando il comando **ls**

# Kali Linux

## VirtualBox Guest Additions – Installazione (3/4)



```
File Actions Edit View Help
OS2      VBoxWindowsAdditions-amd64.exe
runasroot.sh VBoxWindowsAdditions.exe
TRANS.TBL   VBoxWindowsAdditions-x86.exe
root@kali:/media/cdrom0# sh ./VBoxLinuxAdditions.run
Verifying archive integrity ... All good.
Uncompressing VirtualBox 6.1.14 Guest Additions for Linux... .
VirtualBox Guest Additions installer
This system appears to have a version of the VirtualBox Guest
already installed. If it is part of the operating system and ke
te,
there is most likely no need to replace it. If it is not
should get a notification when you start the system. If
e
it with this version, please do not continue with this in
t
instead remove the current version first, following the instructions for th
e
operating system.

If your system simply has the remains of a version of the Additions you cou
ld
not remove you should probably continue now, and these will be removed duri
ng
installation.

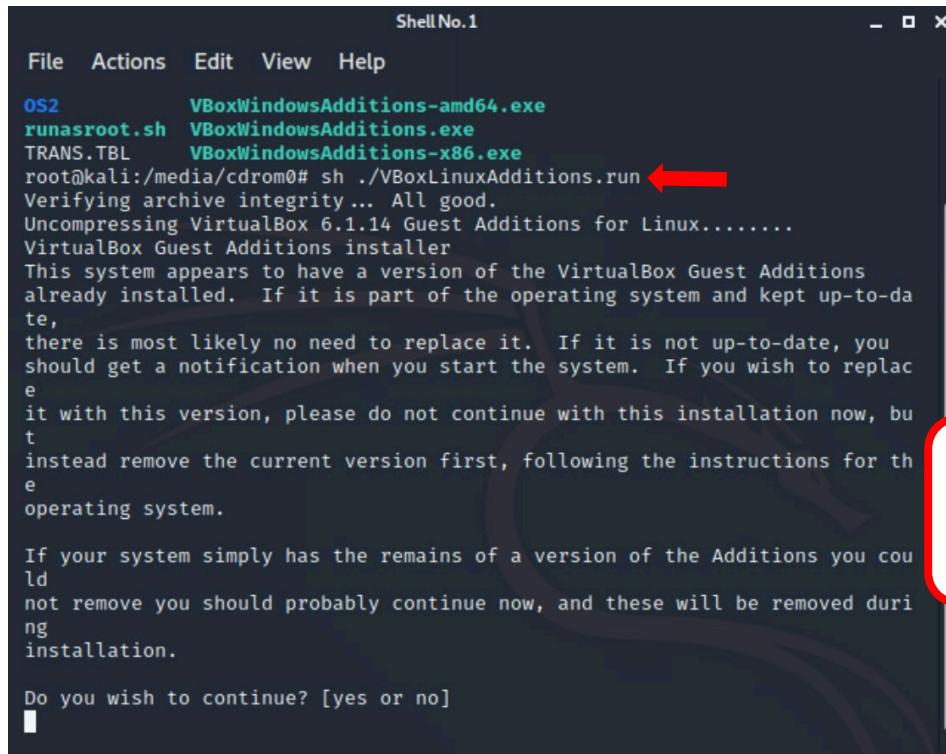
Do you wish to continue? [yes or no]
|
```

**sh ./VBoxLinuxAdditions.run**

Eseguire **VBoxLinuxAdditions.run** mediante il comando **sh** per installare i VirtualBox Guest Additions

# Kali Linux

## VirtualBox Guest Additions – Installazione (3/4)



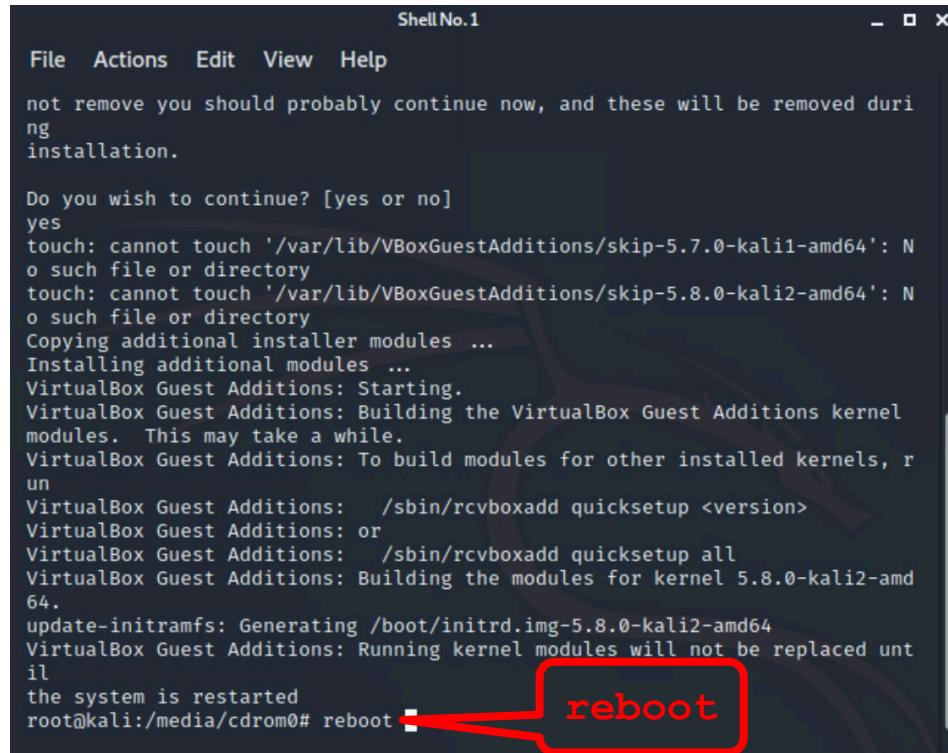
```
File Actions Edit View Help  
OS2      VBoxWindowsAdditions-amd64.exe  
runasroot.sh  VBoxWindowsAdditions.exe  
TRANS.TBL   VBoxWindowsAdditions-x86.exe  
root@kali:/media/cdrom0# sh ./VBoxLinuxAdditions.run ←  
Verifying archive integrity ... All good.  
Uncompressing VirtualBox 6.1.14 Guest Additions for Linux.....  
VirtualBox Guest Additions installer  
This system appears to have a version of the VirtualBox Guest Additions  
already installed. If it is part of the operating system and kept up-to-da  
te,  
there is most likely no need to replace it. If it is not up-to-date, you  
should get a notification when you start the system. If you wish to replac  
e  
it with this version, please do not continue with this installation now, bu  
t  
instead remove the current version first, following the instructions for th  
e  
operating system.  
  
If your system simply has the remains of a version of the Additions you cou  
ld  
not remove you should probably continue now, and these will be removed duri  
ng  
installation.  
  
Do you wish to continue? [yes or no]  
[
```

Per maggiori informazioni  
sul comando **sh** digitare  
**man sh**

Eseguire **VBoxLinuxAdditions.run** mediante il comando **sh** per installare i  
VirtualBox Guest Additions (N.B. digitare **yes** per proseguire l'installazione)

# Kali Linux

## VirtualBox Guest Additions – Installazione (4/4)



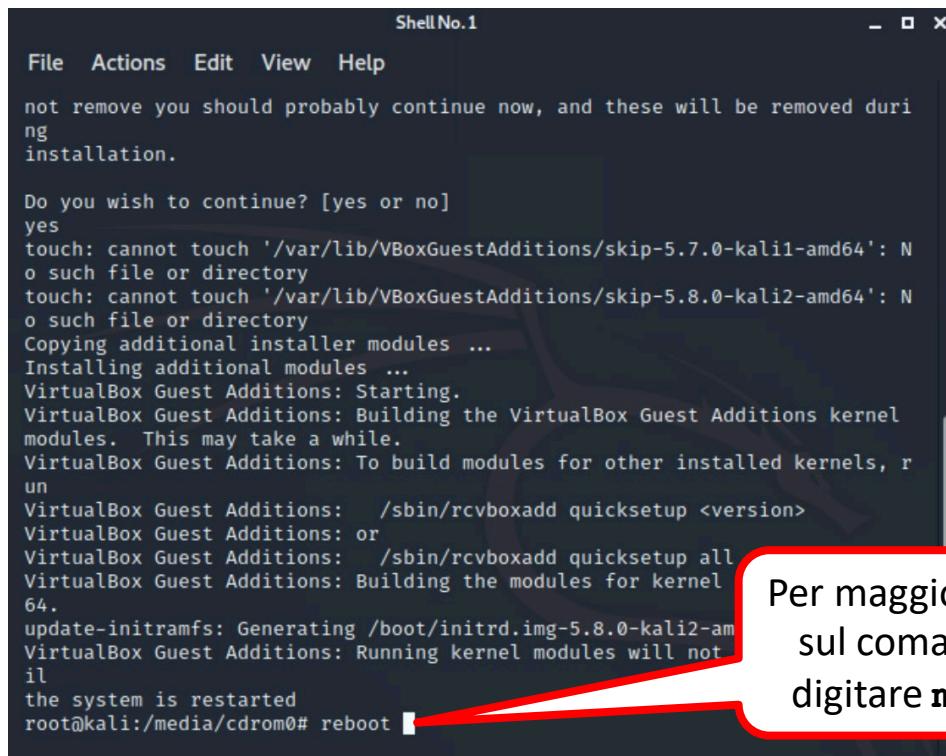
```
not remove you should probably continue now, and these will be removed during installation.

Do you wish to continue? [yes or no]
yes
touch: cannot touch '/var/lib/VBoxGuestAdditions/skip-5.7.0-kali1-amd64': No such file or directory
touch: cannot touch '/var/lib/VBoxGuestAdditions/skip-5.8.0-kali2-amd64': No such file or directory
Copying additional installer modules ...
Installing additional modules ...
VirtualBox Guest Additions: Starting.
VirtualBox Guest Additions: Building the VirtualBox Guest Additions kernel modules. This may take a while.
VirtualBox Guest Additions: To build modules for other installed kernels, run
VirtualBox Guest Additions: /sbin/recvboxadd quicksetup <version>
VirtualBox Guest Additions: or
VirtualBox Guest Additions: /sbin/recvboxadd quicksetup all
VirtualBox Guest Additions: Building the modules for kernel 5.8.0-kali2-amd64.
update-initramfs: Generating /boot/initrd.img-5.8.0-kali2-amd64
VirtualBox Guest Additions: Running kernel modules will not be replaced until
the system is restarted
root@kali:/media/cdrom0# reboot
```

Riavviare Kali Linux mediante il comando **reboot**

# Kali Linux

## VirtualBox Guest Additions – Installazione (4/4)



```
not remove you should probably continue now, and these will be removed during installation.

Do you wish to continue? [yes or no]
yes
touch: cannot touch '/var/lib/VBoxGuestAdditions/skip-5.7.0-kali1-amd64': No such file or directory
touch: cannot touch '/var/lib/VBoxGuestAdditions/skip-5.8.0-kali2-amd64': No such file or directory
Copying additional installer modules ...
Installing additional modules ...
VirtualBox Guest Additions: Starting.
VirtualBox Guest Additions: Building the VirtualBox Guest Additions kernel modules. This may take a while.
VirtualBox Guest Additions: To build modules for other installed kernels, run
VirtualBox Guest Additions: /sbin/recvboxadd quicksetup <version>
VirtualBox Guest Additions: or
VirtualBox Guest Additions: /sbin/recvboxadd quicksetup all
VirtualBox Guest Additions: Building the modules for kernel 64.
update-initramfs: Generating /boot/initrd.img-5.8.0-kali2-amd64
VirtualBox Guest Additions: Running kernel modules will not
il
the system is restarted
root@kali:/media/cdrom0# reboot
```

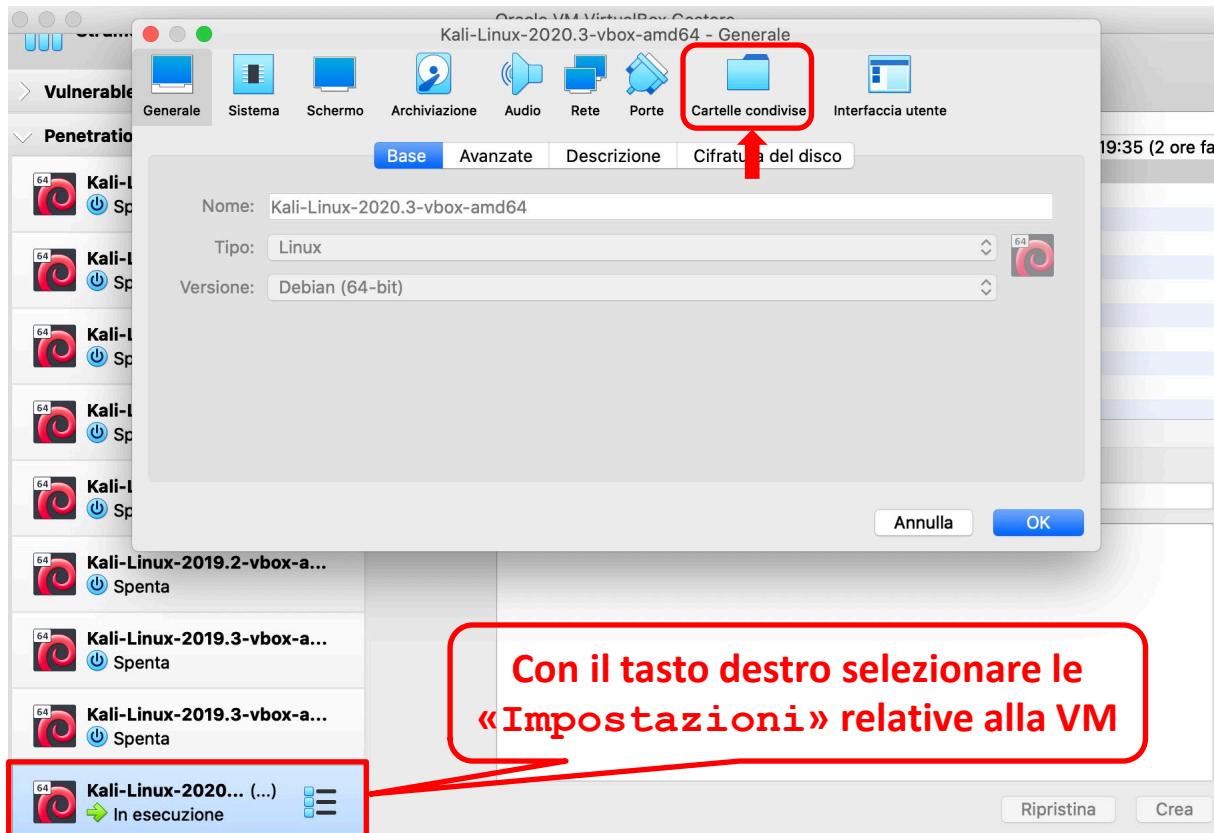
Per maggiori informazioni  
sul comando **reboot**  
digitare **man reboot**

Riavviare Kali Linux mediante il comando **reboot**

# Kali Linux

## Cartelle Condivise

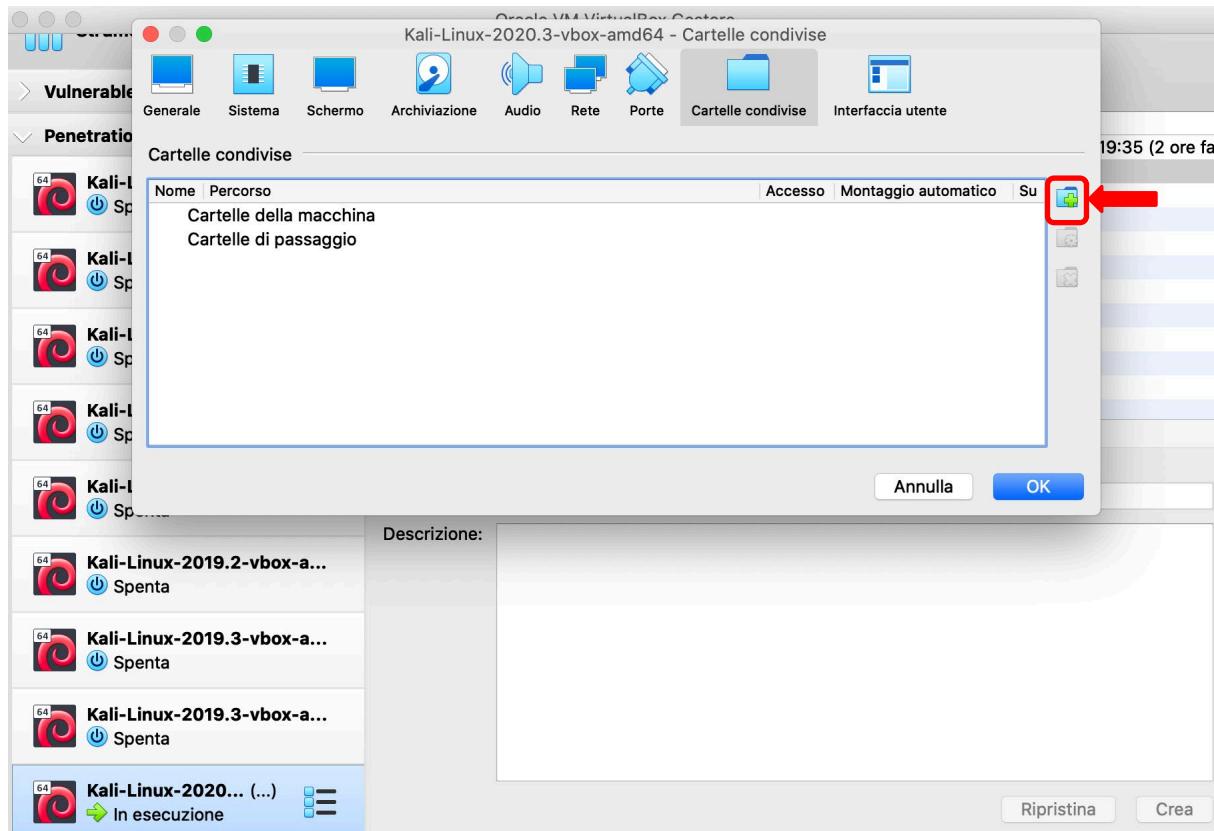
- È possibile creare cartelle condivise tra la VM e la macchina host



# Kali Linux

## Cartelle Condivise

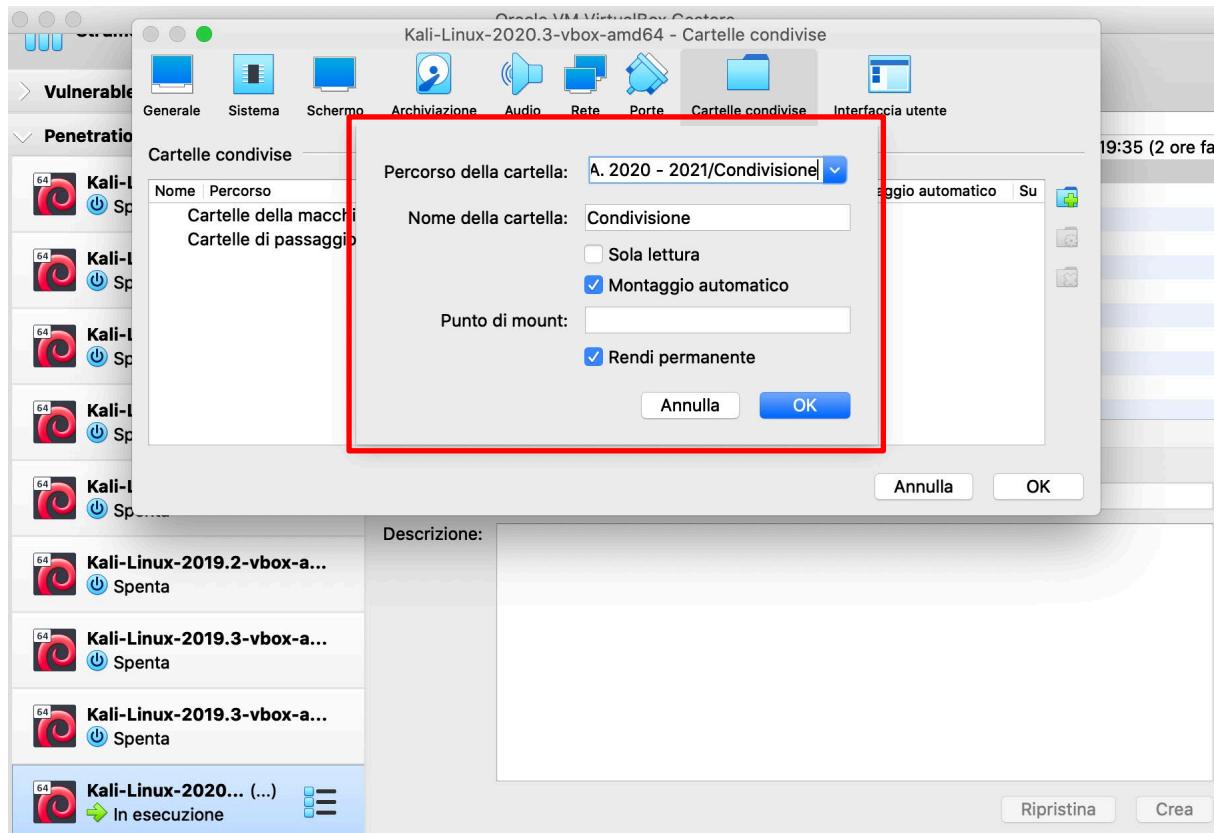
- È possibile creare cartelle condivise tra la VM e la macchina host



# Kali Linux

## Cartelle Condivise

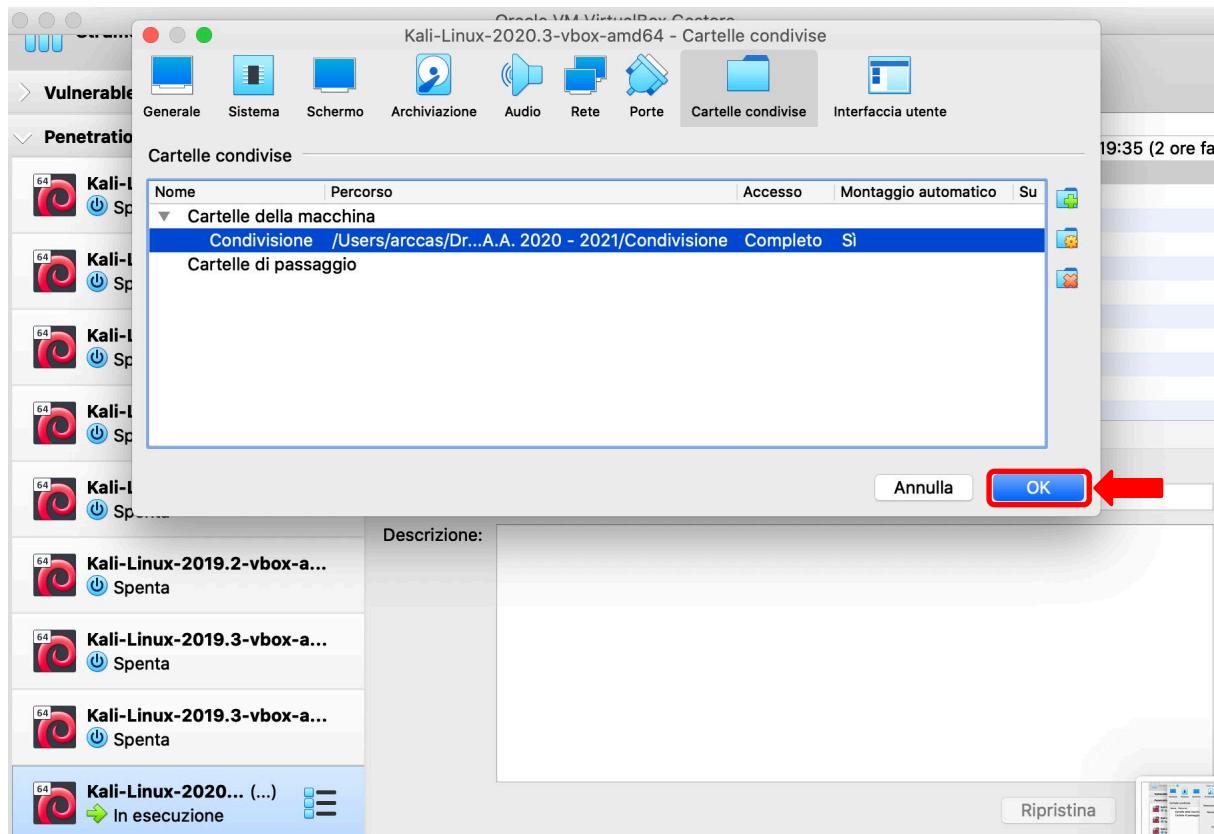
- È possibile creare cartelle condivise tra la VM e la macchina host



# Kali Linux

## Cartelle Condivise

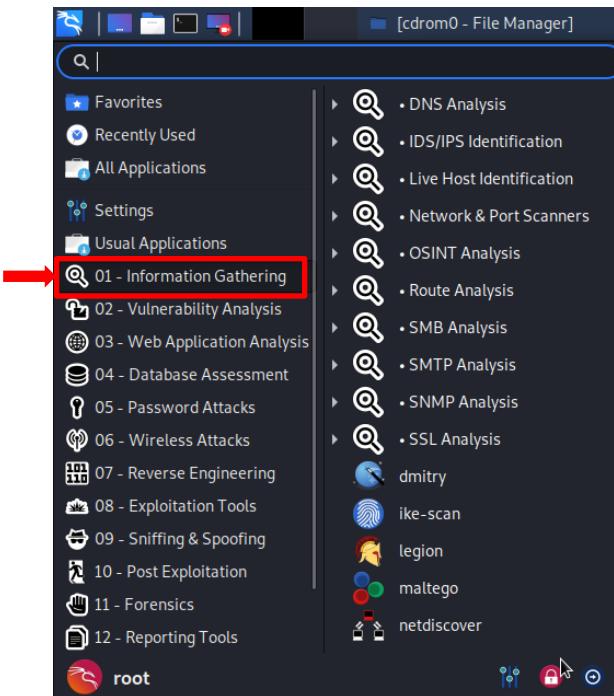
- È possibile creare cartelle condivise tra la VM e la macchina host



# Kali Linux

## Categorie di Strumenti – Information Gathering

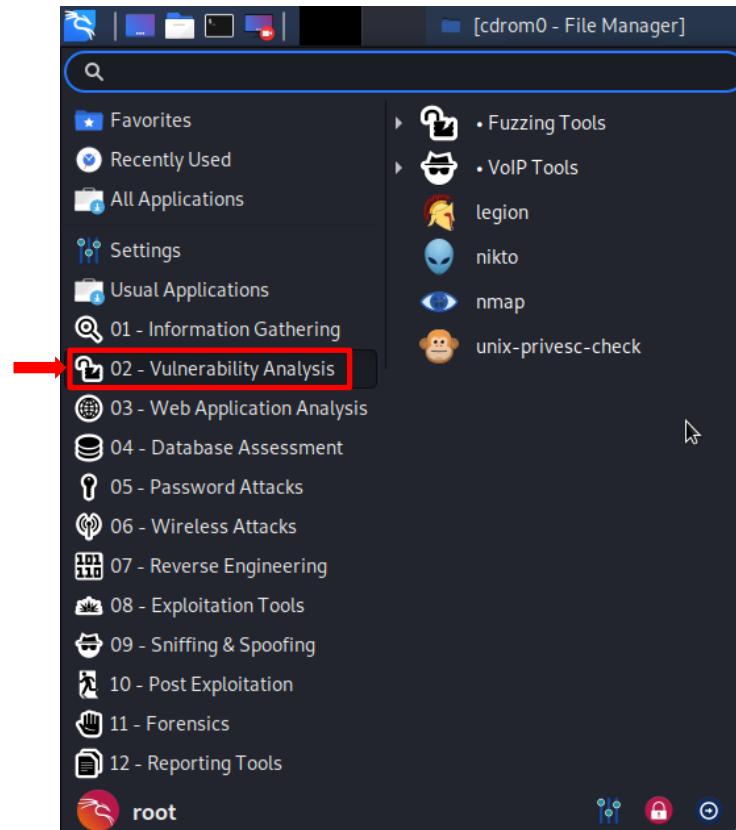
- Strumenti per raccogliere varie informazioni su DNS, IDS/IPS, scansioni di rete, Open Source Intelligence (OSINT), routing, SMB, SNMP, SSL indirizzi e-mail, etc



# Kali Linux

## Categorie di Strumenti – Vulnerability Analysis

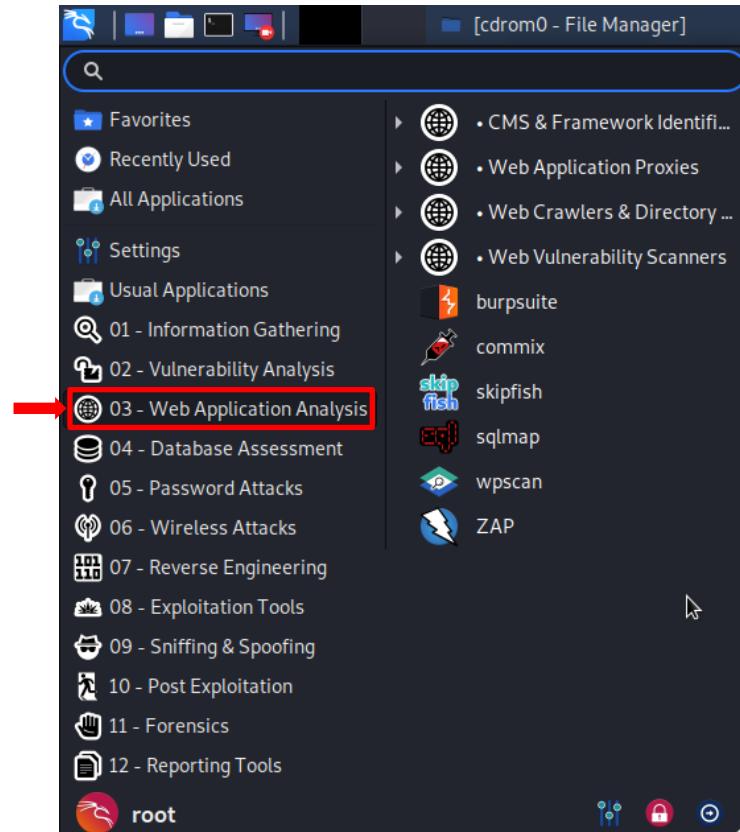
### ➤ Strumenti rilevare le vulnerabilità



# Kali Linux

## Categorie di Strumenti – Web Applications Analysis

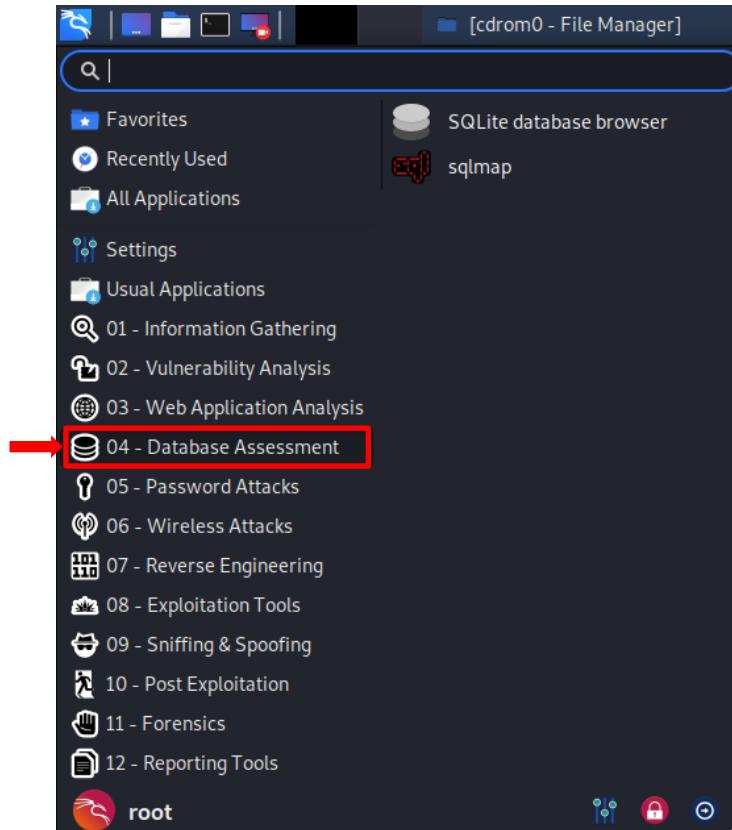
- Strumenti per analizzare la sicurezza delle applicazioni Web



# Kali Linux

## Categorie di Strumenti – Database Assessment

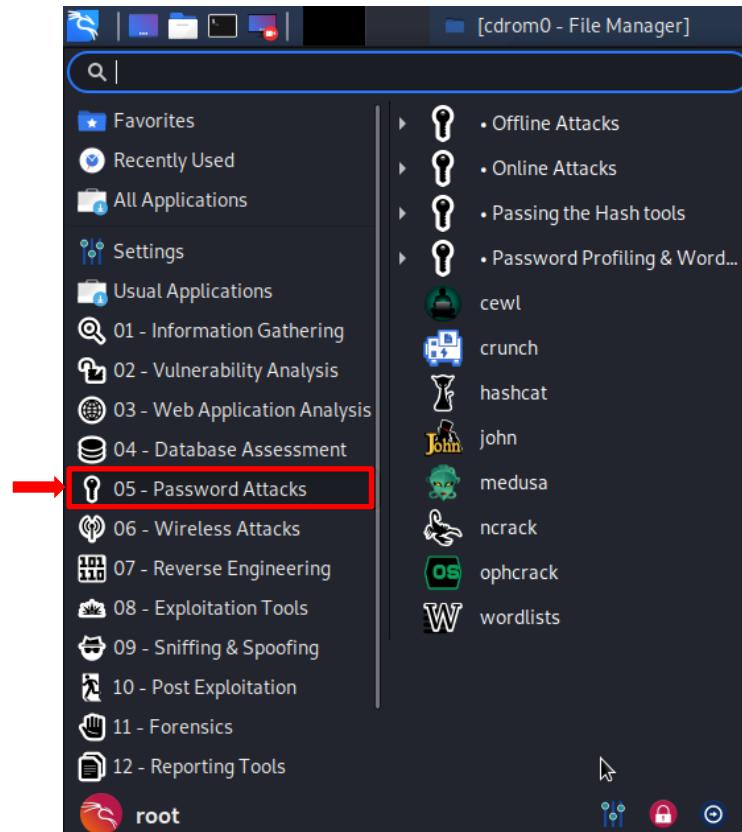
- Strumenti per analizzare la sicurezza dei database



# Kali Linux

## Categorie di Strumenti – Password Attacks

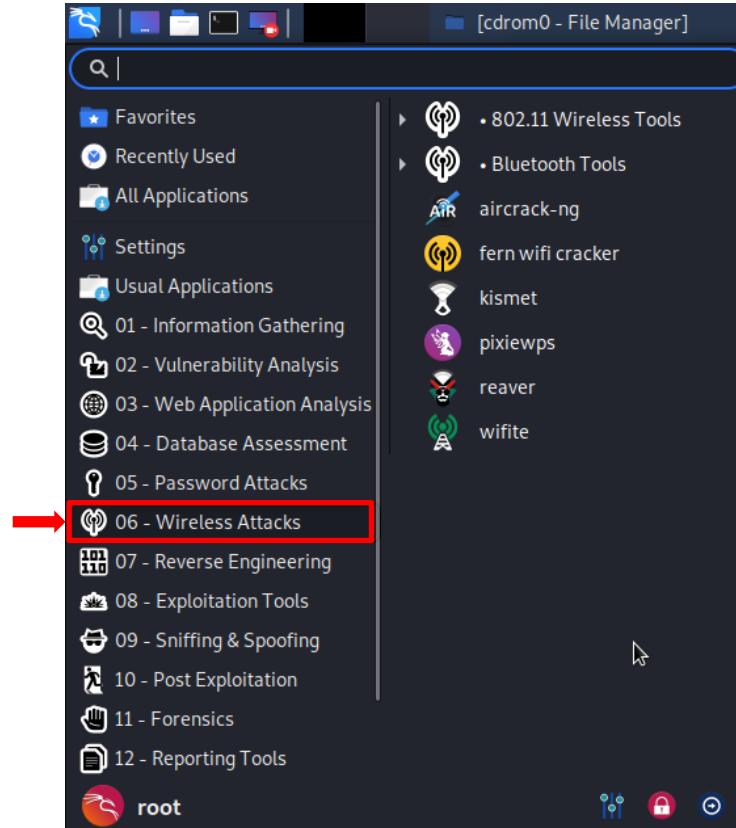
- Strumenti per effettuare attacchi alle password



# Kali Linux

## Categorie di Strumenti – Wireless Attacks

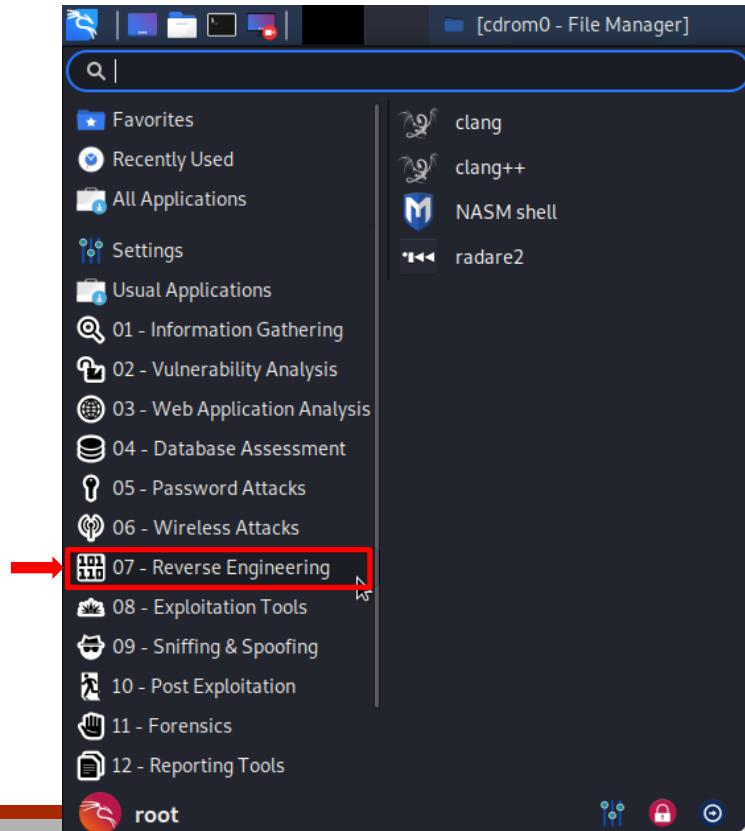
- Strumenti per analizzare la sicurezza di dispositivi Bluetooth, RFID / NFC e Wi-Fi



# Kali Linux

## Categorie di Strumenti – Reverse Engineering

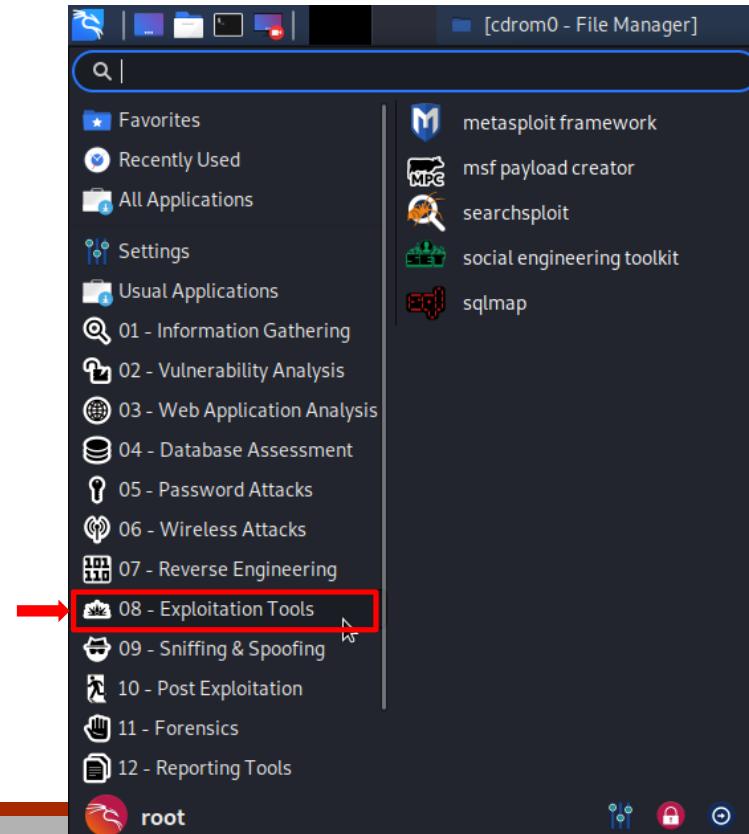
- Strumenti per effettuare il debug di un programma o il disassemblaggio di un file eseguibile



# Kali Linux

## Categorie di Strumenti – Exploitation Tools

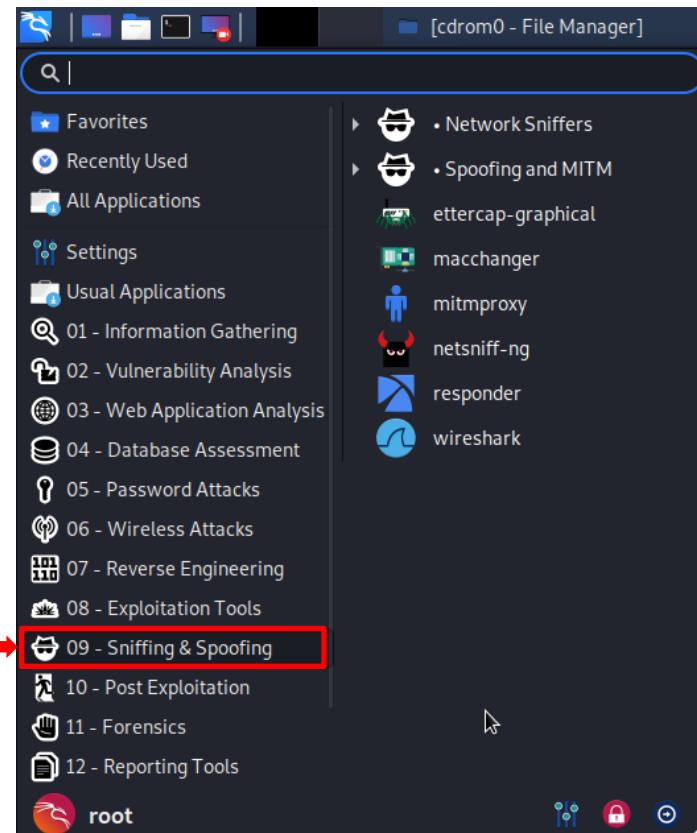
- Strumenti per sfruttare le vulnerabilità



# Kali Linux

## Categorie di Strumenti – Sniffing & Spoofing

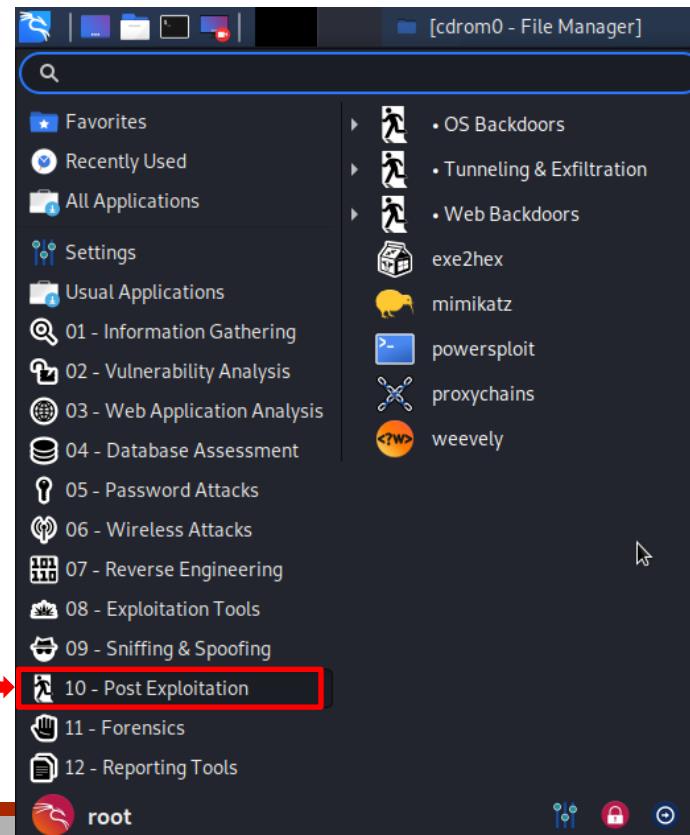
- Strumenti per «intercettare» il traffico di rete



# Kali Linux

## Categorie di Strumenti – Post Exploitation

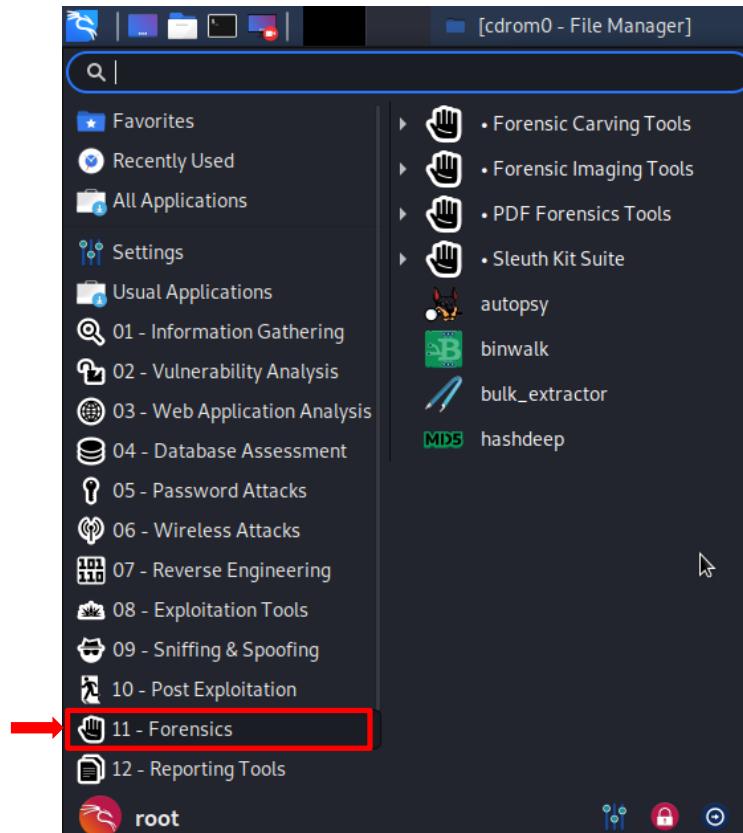
- Strumenti per mantenere l'accesso su un dispositivo violato durante la fase di Exploitation e/o per «aumentare» i privilegi all'interno di esso



# Kali Linux

## Categorie di Strumenti – Forensics

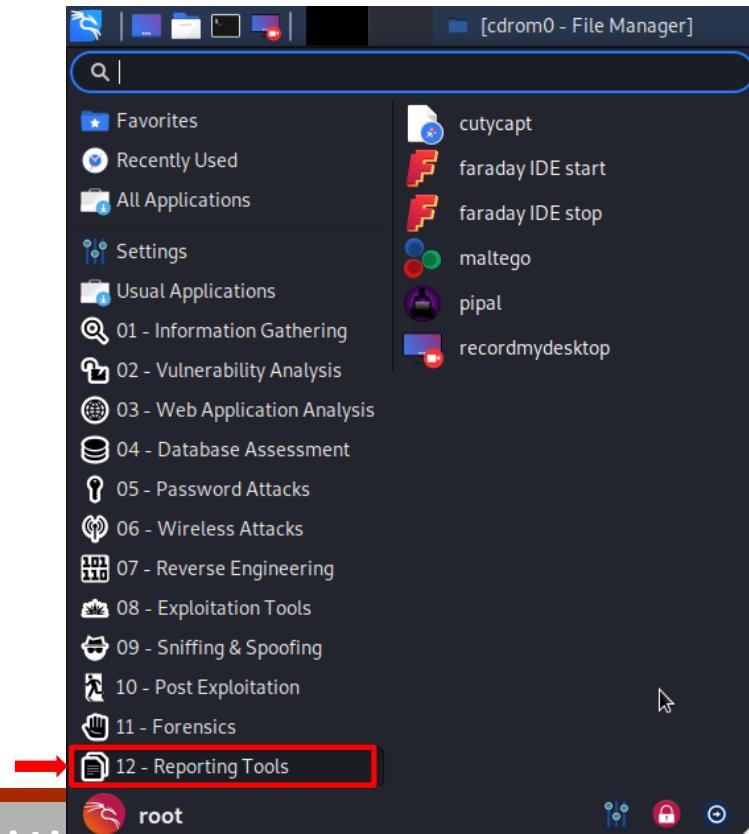
### ➤ Strumenti per condurre attività di Digital Forensics



# Kali Linux

## Categorie di Strumenti – Reporting Tools

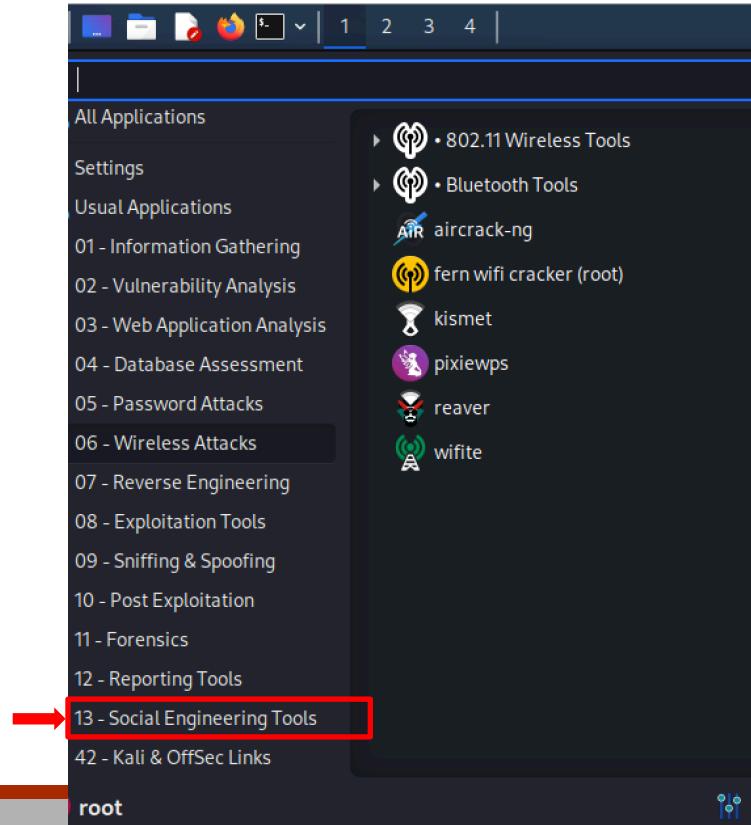
- Strumenti per documentare il processo di penetration testing ed i relativi risultati



# Kali Linux

## Categorie di Strumenti – Social Engineering Tools

- Strumenti per attuare tecniche di Social Engineering



# Kali Linux

## Altri Strumenti – Stress Testing & Hardware Hacking

---

- **Stress testing:** strumenti per lo stress testing delle reti, del Web e del VOIP
  - <https://allabouttesting.org/stress-test-tools-kali-linux/>
  
- **Hardware hacking:** strumenti per analizzare applicazioni Android e Arduino

# Outline

---

- Kali Linux
- **Altre Distribuzioni per il Pentesting**
- Fondamenti di Linux
  - Struttura del File System
  - Comandi di Base

# Altre Distribuzioni per il Pentesting

## OSBOXES

- <https://www.osboxes.org/>
  - Permette di scaricare Sistemi Operativi UNIX/Linux già «importabili» in VirtualBox o VMware



• •

# Altre Distribuzioni per il Pentesting

## Parrot Linux

➤ <https://distrowatch.com/table.php?distribution=parrot>

 **Parrot**

Ultimo aggiornamento: 2025-02-01 14:12 UTC

- **Tipo:** [Linux](#)
- **Basata su:** [Debian](#)
- **Provenienza:** [Italy](#)
- **Architetture:** [x86\\_64](#)
- **Desktop:** [KDE Plasma](#), [MATE](#)
- **Categoria:** [Forensics](#), [Live Medium](#), [Security](#)
- **Stato:** Attiva
- **Popolarità:** [36 \(267 visite al giorno\)](#)

Parrot (formerly Parrot Security OS) is a Debian-based, security-oriented distribution featuring a collection of utilities designed for penetration testing, computer forensics, reverse engineering, hacking, privacy, anonymity and cryptography. The product, developed by Frozenbox, comes with MATE as the default desktop environment.

**Popolarità (visite al giorno):** 12 mesi: 39 (231), 6 mesi: 36 (267), 3 mesi: 38 (268), 4 settimane: 57 (202), 1 settimana: 56 (201)

**Average visitor rating:** 8.35/10 from 49 [review\(s\)](#).



# Altre Distribuzioni per il Pentesting

## Parrot Linux

---

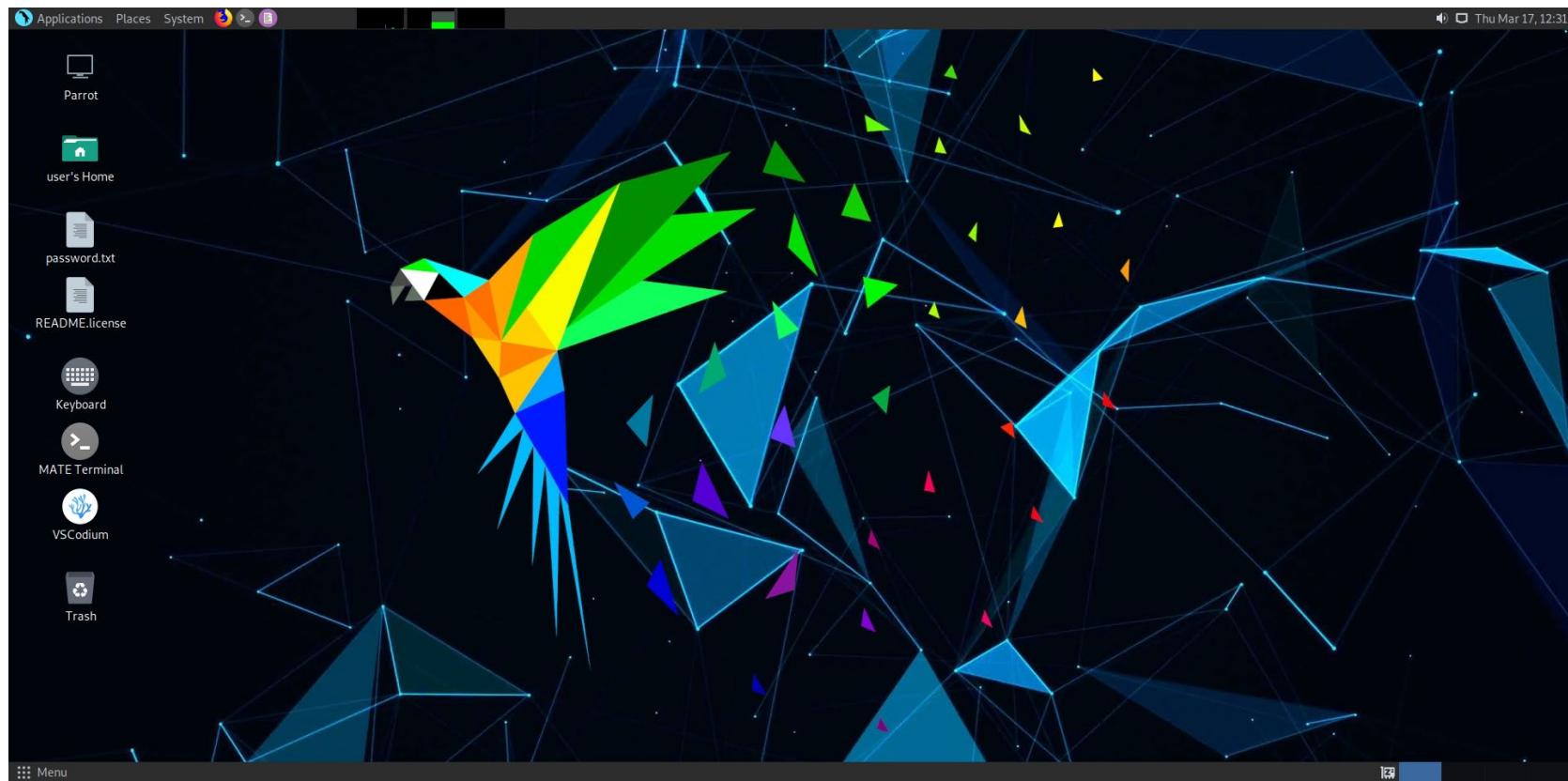
### ➤ Parrot Linux

- <https://www.parrotsec.org/>
- <https://www.parrotsec.org/docs/>
- <https://www.parrotsec.org/download/>



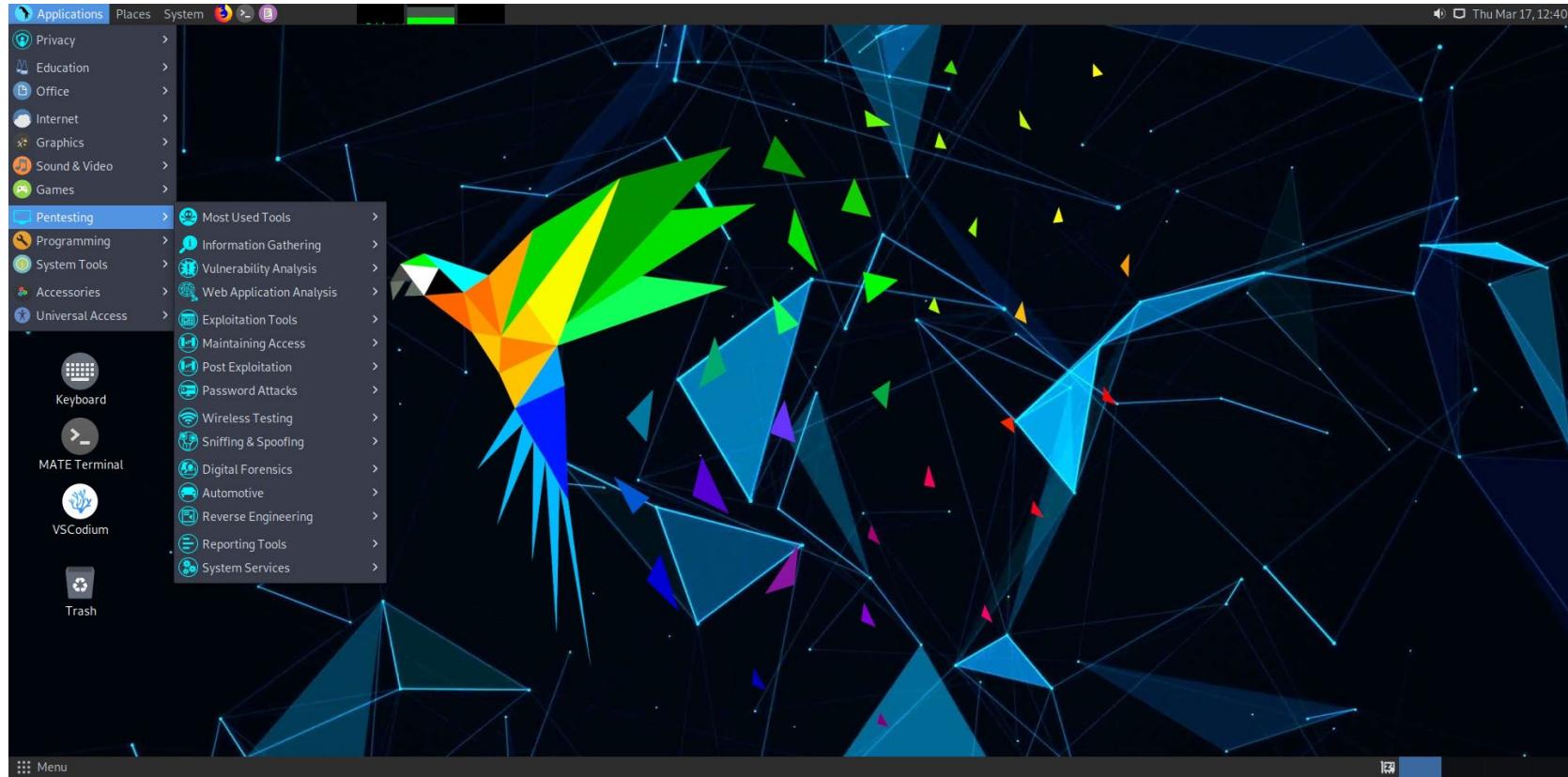
# Altre Distribuzioni per il Pentesting

## Parrot Linux



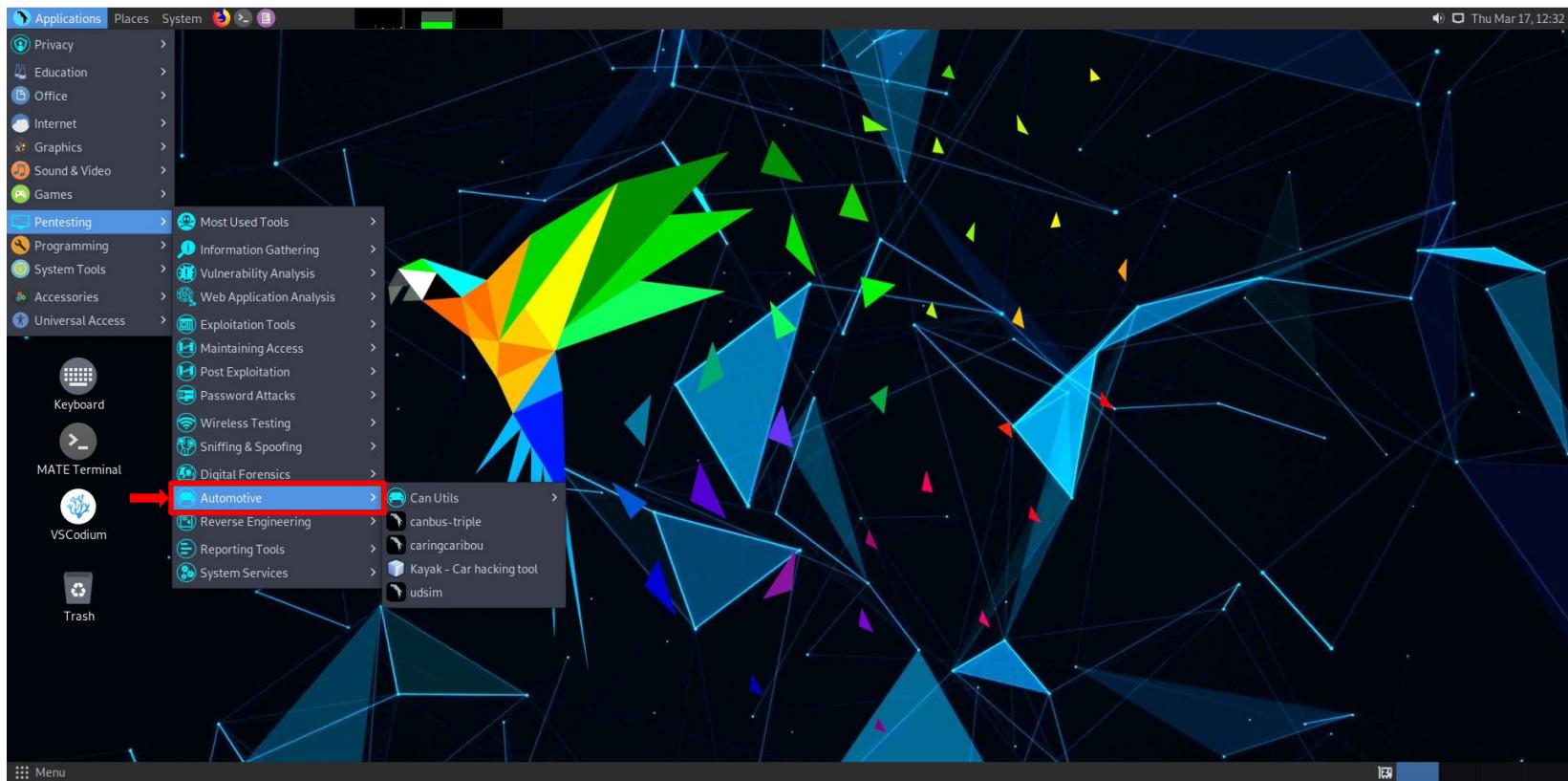
# Altre Distribuzioni per il Pentesting

## Parrot Linux



# Altre Distribuzioni per il Pentesting

## Parrot Linux



# Altre Distribuzioni per il Pentesting

## BackBox Linux

➤ <https://distrowatch.com/table.php?distribution=backbox>



### BackBox Linux

Ultimo aggiornamento: 2024-02-02 02:44 UTC

- **Tipo:** [Linux](#)
- **Basata su:** [Debian](#), [Ubuntu \(LTS\)](#)
- **Provenienza:** [Italy](#)
- **Architetture:** [x86\\_64](#)
- **Desktop:** [Xfce](#)
- **Categoria:** [Data Rescue](#), [Forensics](#), [Security](#), [Live Medium](#)
- **Stato:** Attiva
- **Popolarità:** [110 \(95 visite al giorno\)](#)

BackBox Linux is an Ubuntu-based distribution developed to perform penetration tests and security assessments. It is designed to be fast and easy to use. It provides a minimal yet complete desktop environment, thanks to its own software repositories, which are always updated to the latest stable versions of the most often used and best-known ethical hacking tools.

**Popolarità (visite al giorno):** 12 mesi: 121 (74), 6 mesi: 110 (95), 3 mesi: 142 (56), 4 settimane: 131 (55), 1 settimana: 121 (53)

**Average visitor rating:** 8.33/10 from 3 [review\(s\)](#).



# Altre Distribuzioni per il Pentesting

## BackBox Linux

---

### ➤ **BackBox Linux**

- <https://www.backbox.org/download/>
- <https://wiki.backbox.org/>



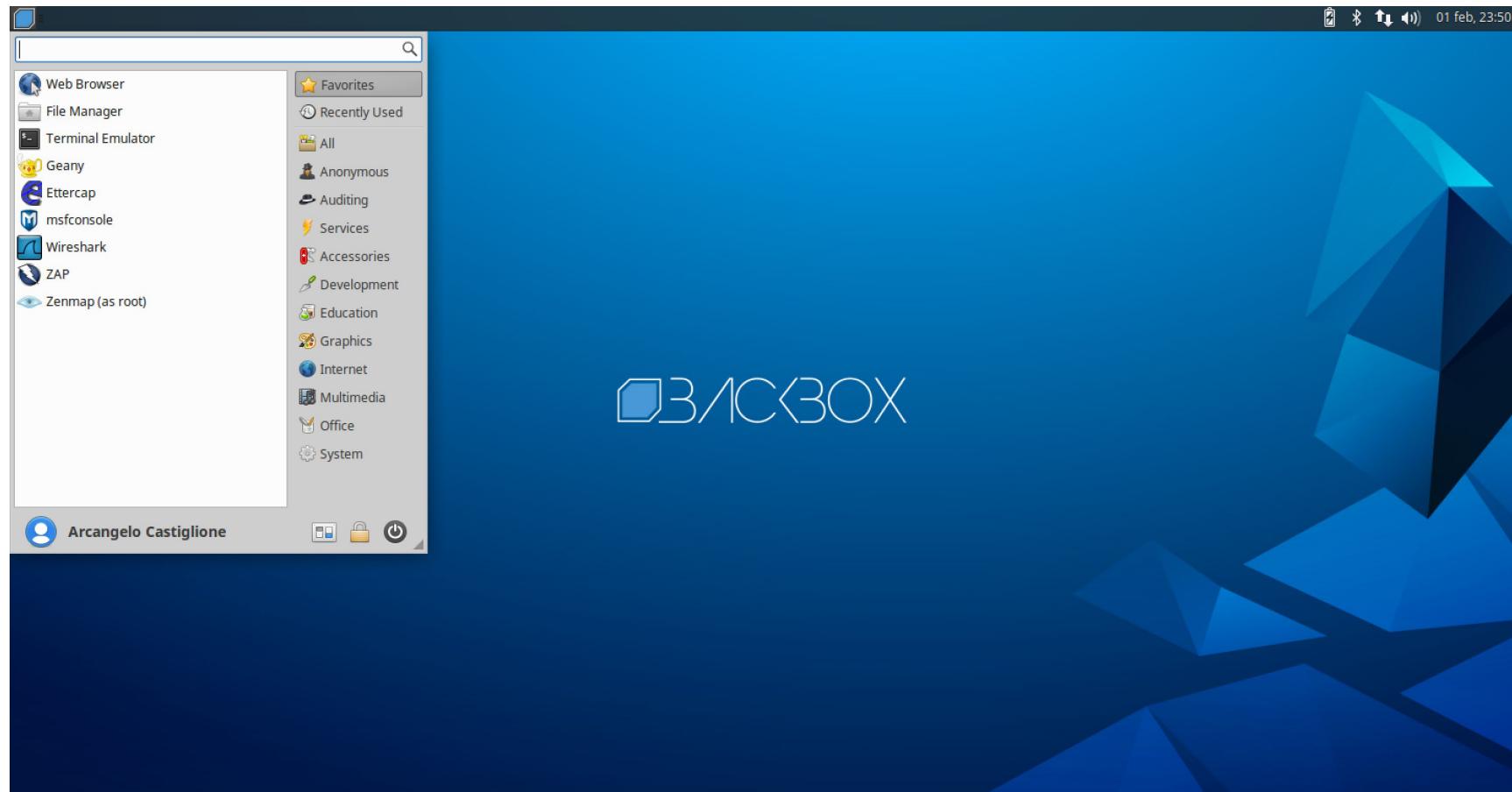
# Altre Distribuzioni per il Pentesting

## BackBox Linux



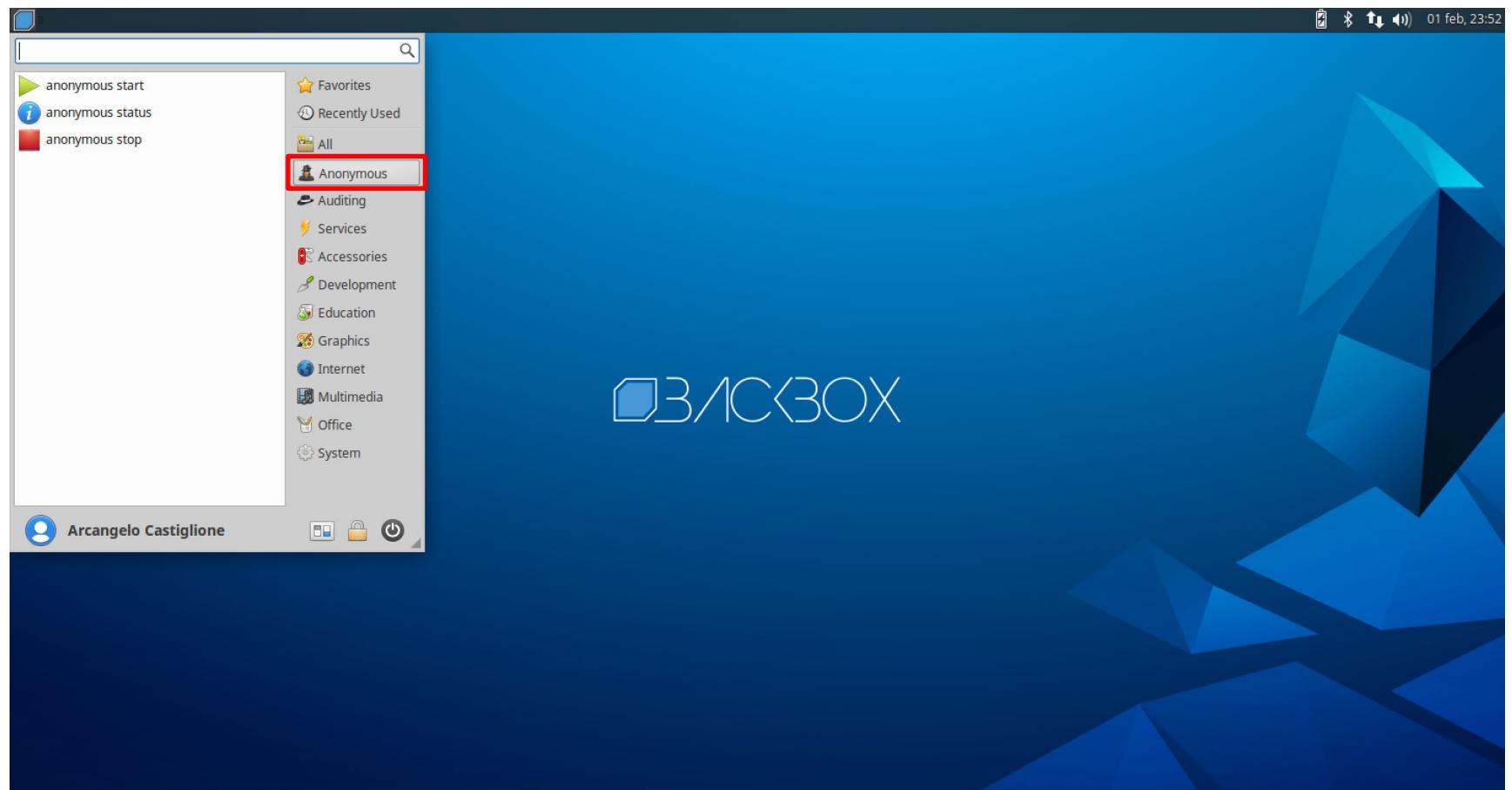
# Altre Distribuzioni per il Pentesting

## BackBox Linux



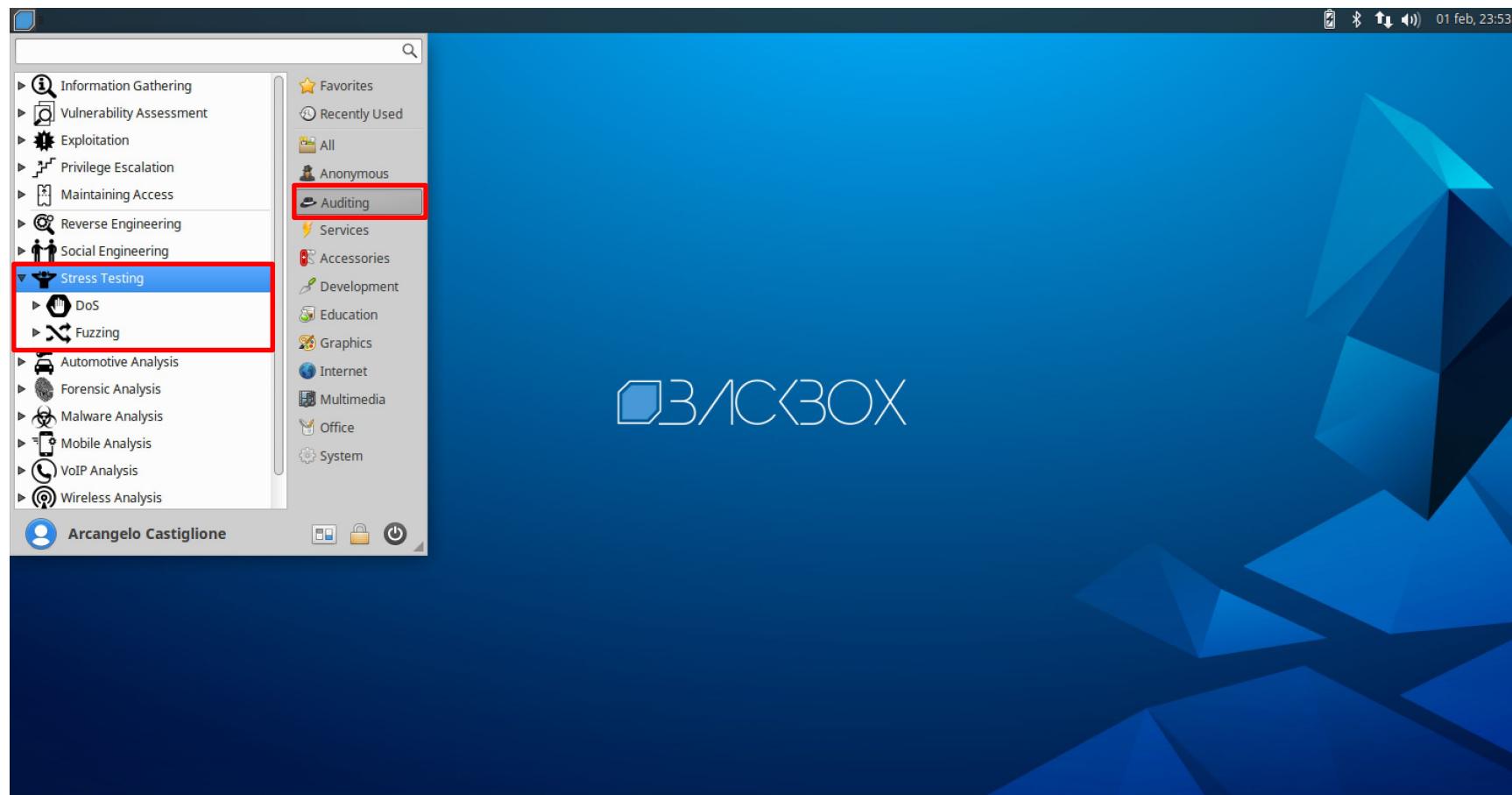
# Altre Distribuzioni per il Pentesting

## BackBox Linux



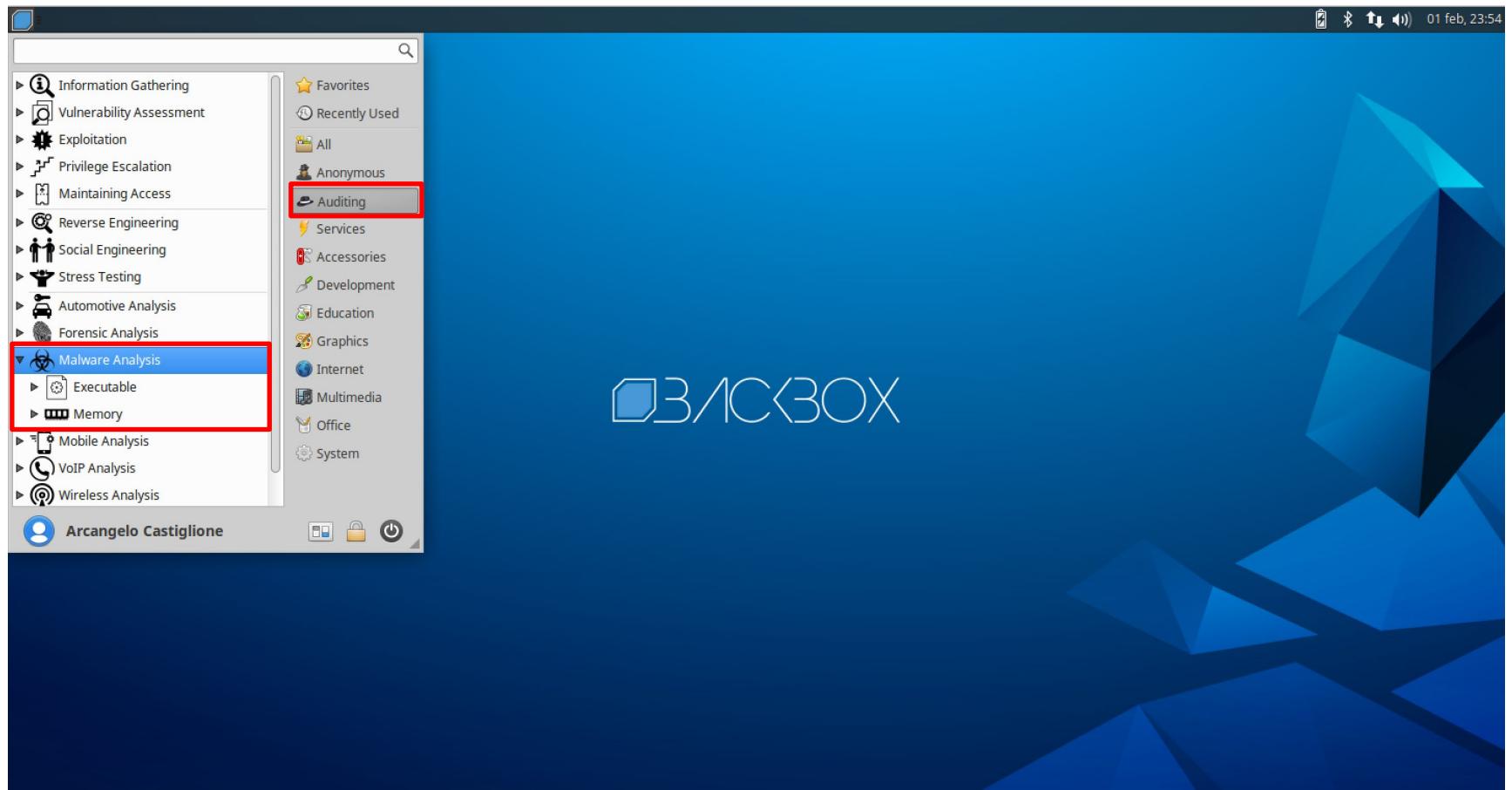
# Altre Distribuzioni per il Pentesting

## BackBox Linux



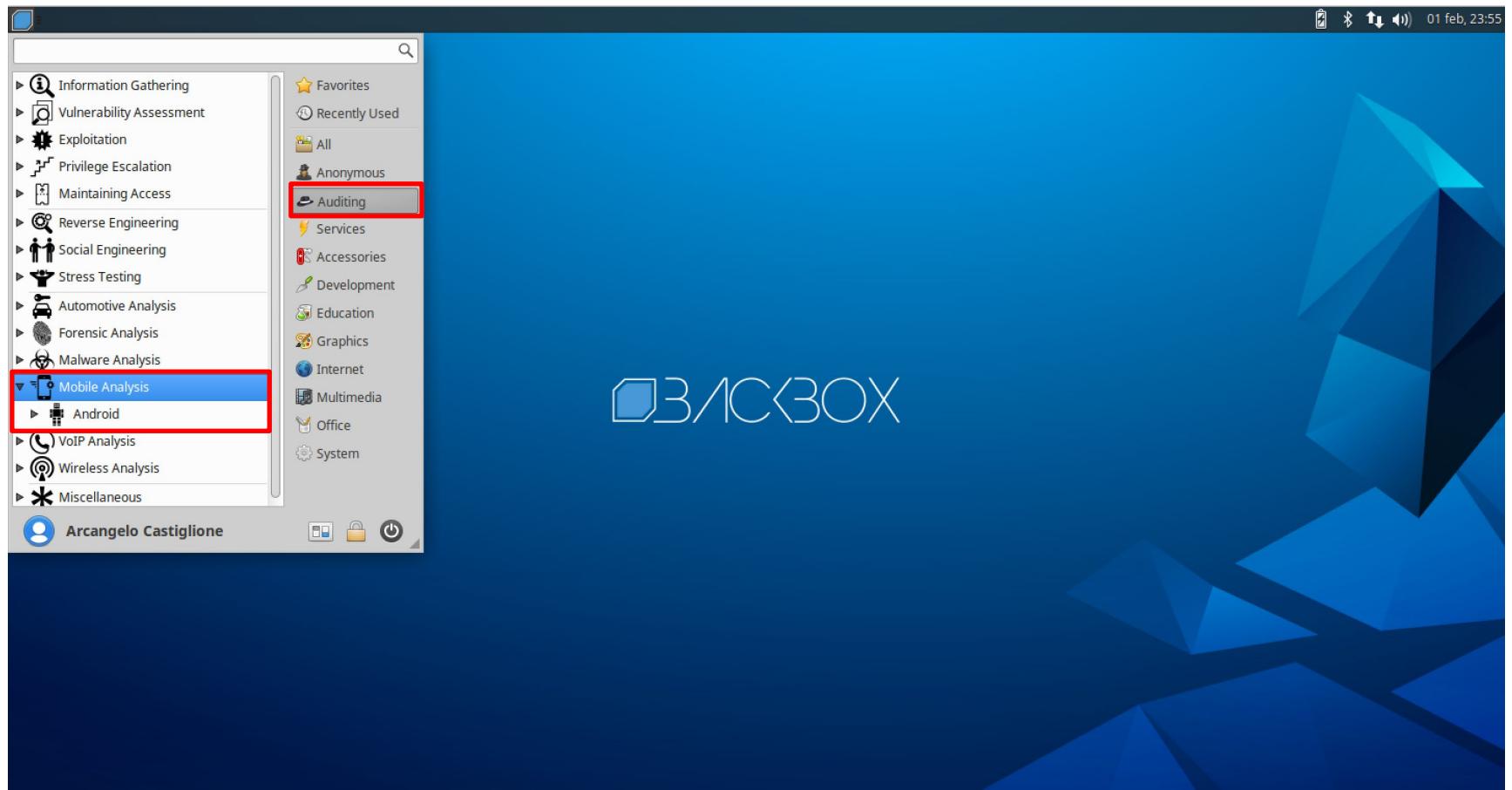
# Altre Distribuzioni per il Pentesting

## BackBox Linux



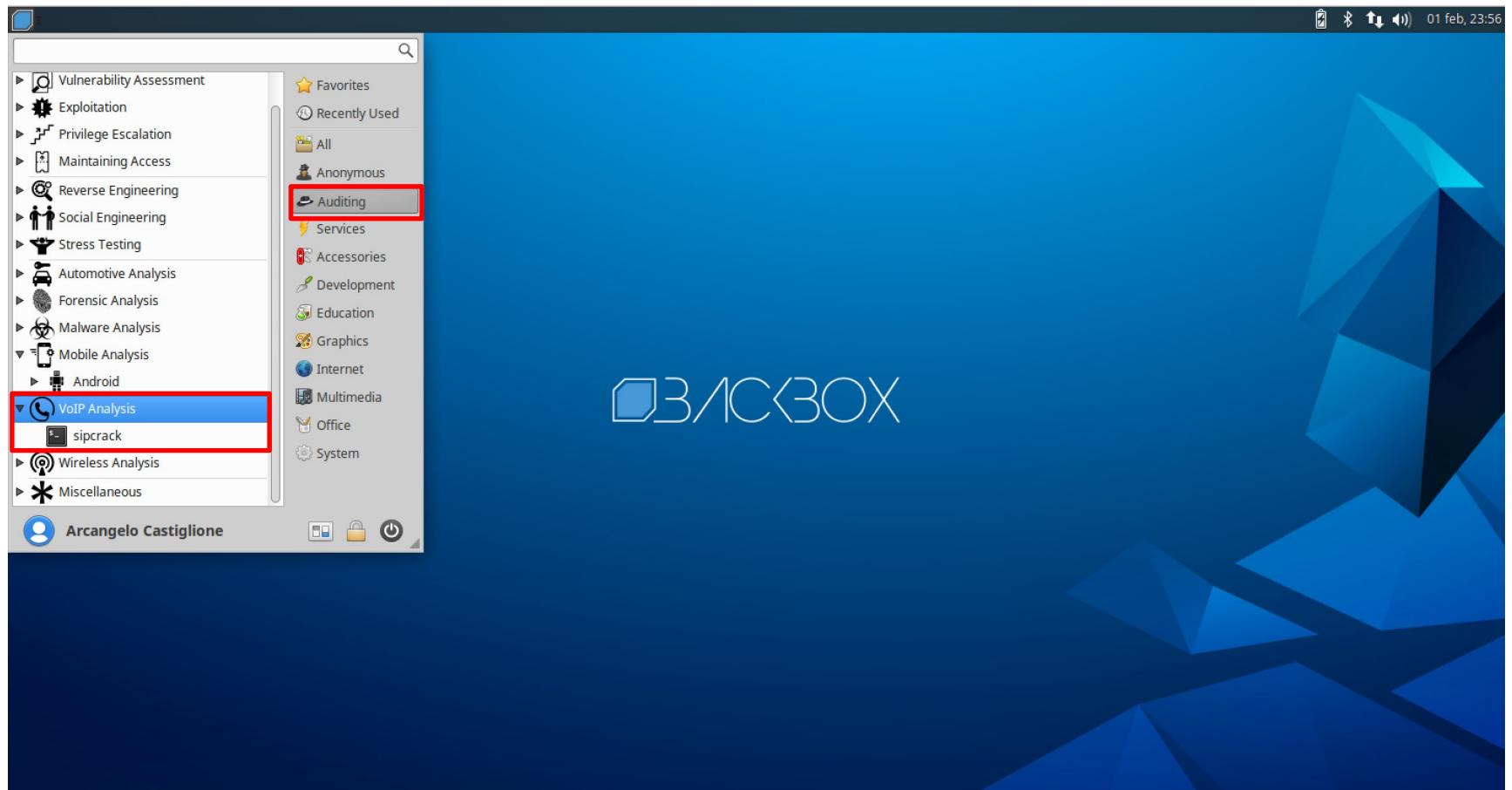
# Altre Distribuzioni per il Pentesting

## BackBox Linux



# Altre Distribuzioni per il Pentesting

## BackBox Linux



# Altre Distribuzioni per il Pentesting

## BlackArch Linux

➤ <https://distrowatch.com/table.php?distribution=blackarch>



### BlackArch Linux

Ultimo aggiornamento: 2024-03-08 06:06 UTC

- **Tipo:** [Linux](#)
- **Basata su:** [Arch](#)
- **Provenienza:** [USA](#)
- **Architetture:** [x86\\_64](#)
- **Desktop:** [Xfce](#)
- **Categoria:** [Live Medium](#), [Security](#), [Forensics](#)
- **Stato:** Attiva
- **Popolarità:** [148 \(55 visite al giorno\)](#)

BlackArch Linux is an Arch Linux-based distribution designed for penetration testers and security researchers. It is supplied as a live DVD image that comes with several lightweight window managers, including Fluxbox, Openbox, Awesome and spectrwm. It ships with over a thousand specialist tools for penetration testing and forensic analysis.

**Popolarità (visite al giorno):** 12 mesi: **161** (55), 6 mesi: **148** (55), 3 mesi: **144** (55), 4 settimane: **127** (56), 1 settimana: **119** (55)

**Average visitor rating:** 9.2/10 from 5 [review\(s\)](#).



# Altre Distribuzioni per il Pentesting

## BlackArch Linux

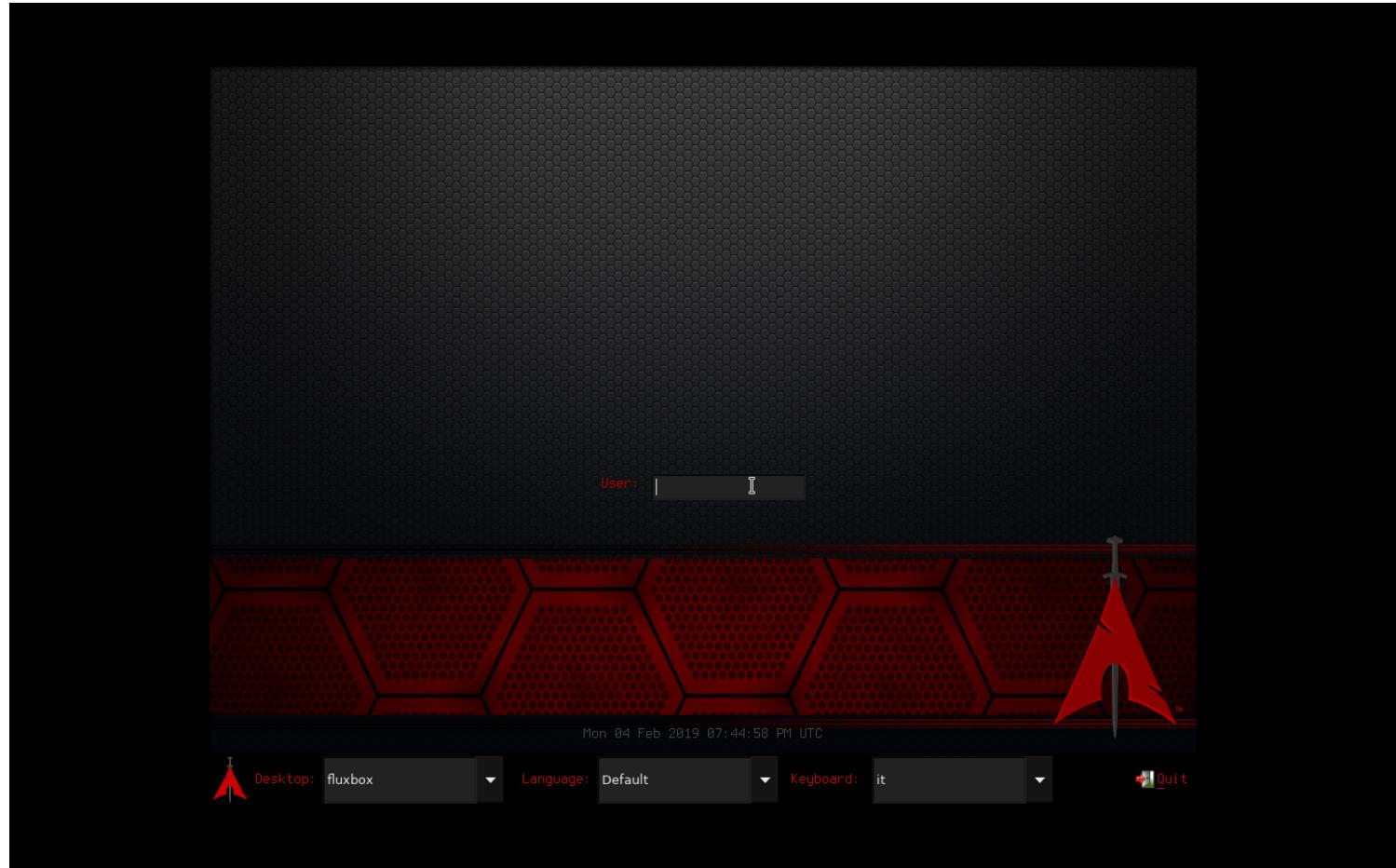
### ➤ BlackArch Linux

- <https://blackarch.org/downloads.html>
- <https://blackarch.org/blackarch-guide-it.pdf>



# Altre Distribuzioni per il Pentesting

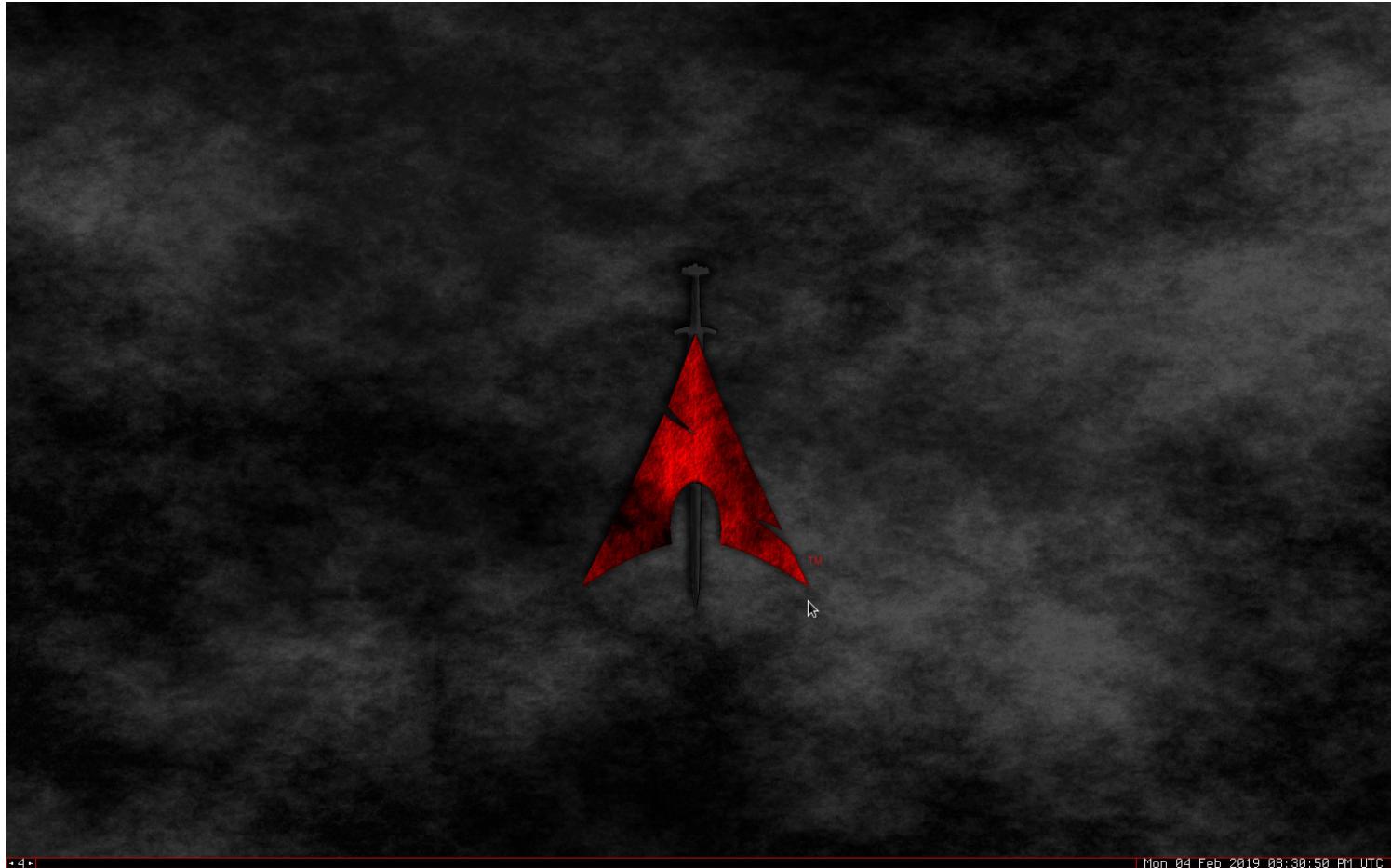
## BlackArch Linux



# Altre Distribuzioni per il Pentesting

## BlackArch Linux

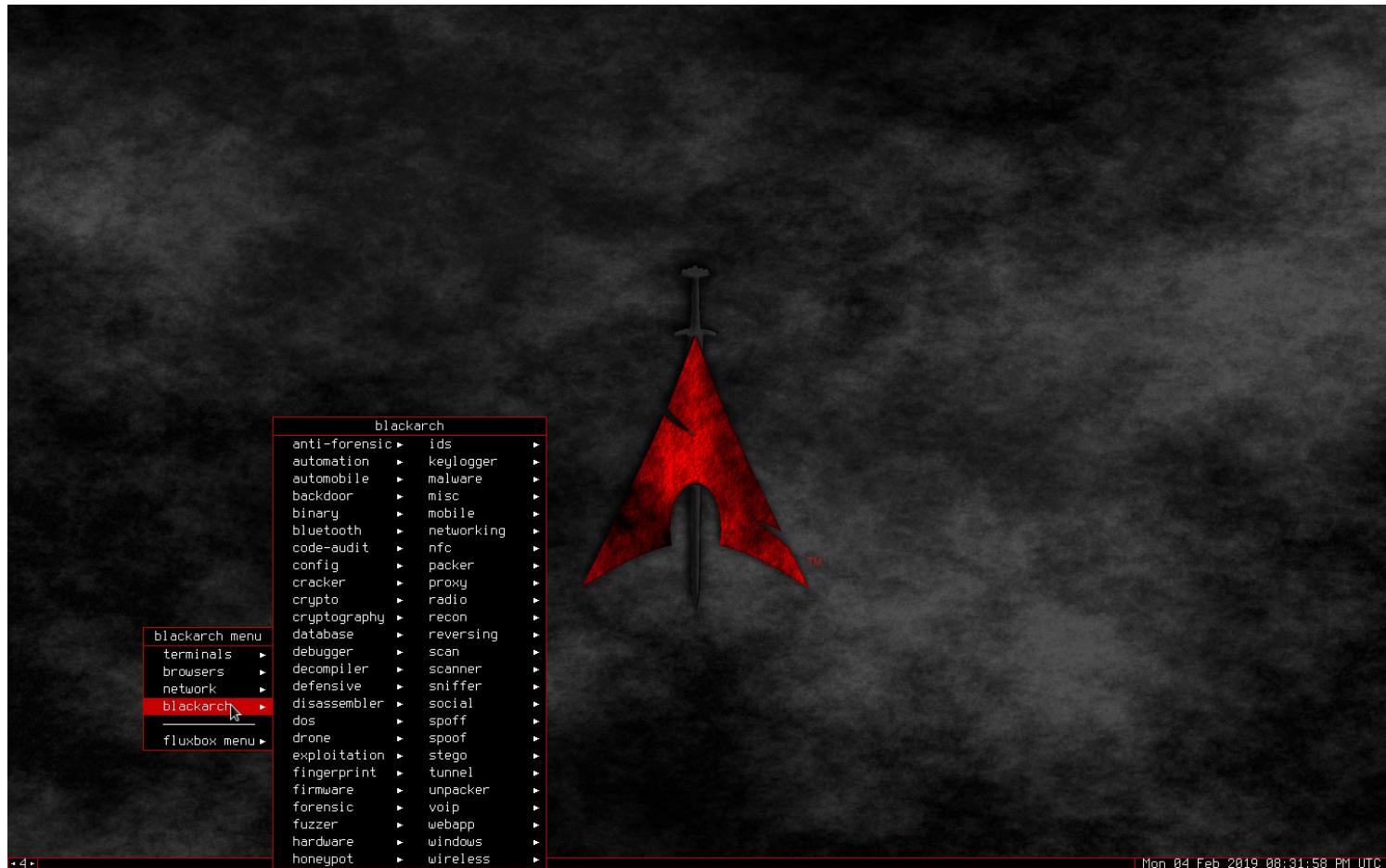
---



Mon 04 Feb 2019 08:30:50 PM UTC

# Altre Distribuzioni per il Pentesting

## BlackArch Linux



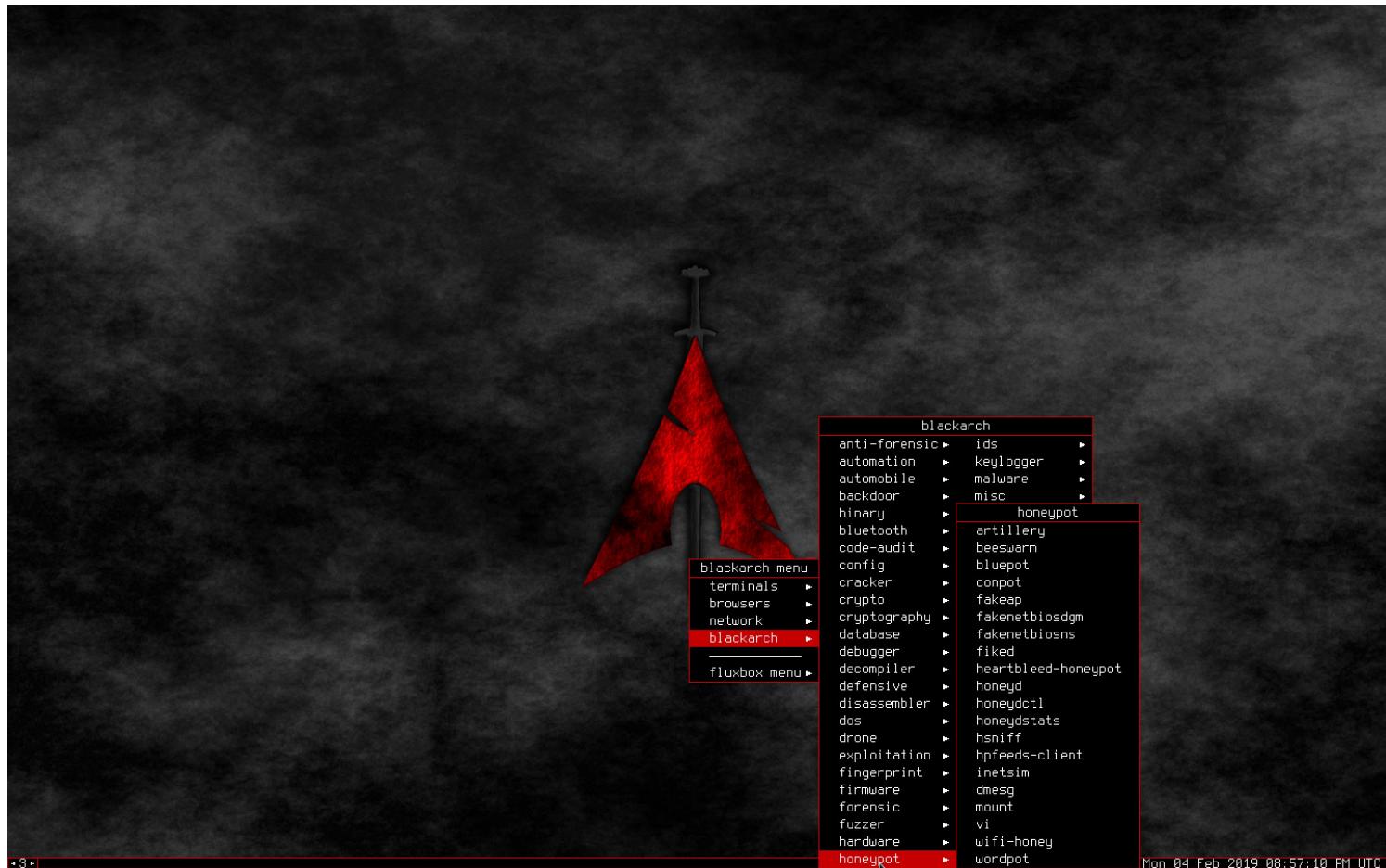
# Altre Distribuzioni per il Pentesting

## BlackArch Linux



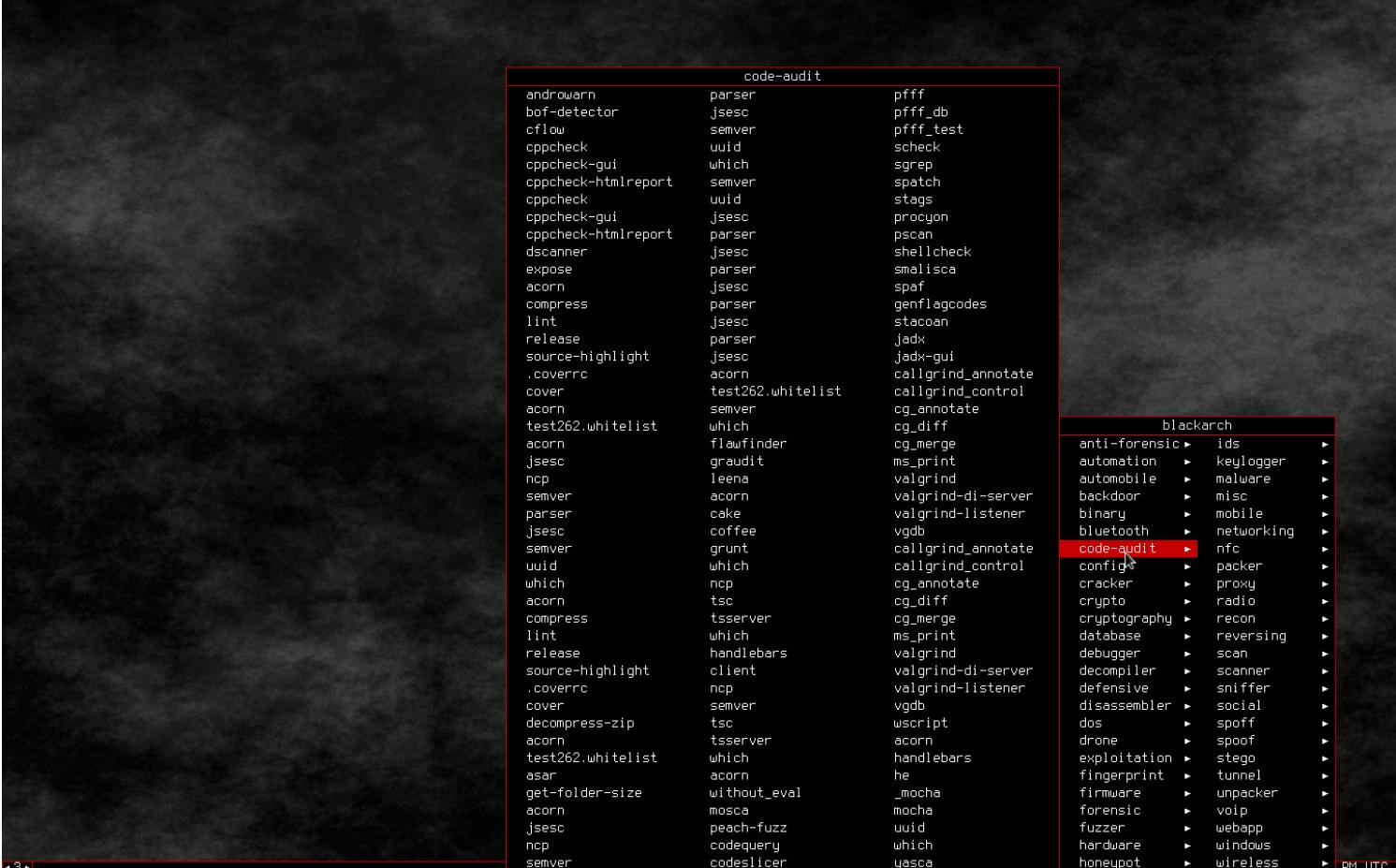
# Altre Distribuzioni per il Pentesting

## BlackArch Linux



# Altre Distribuzioni per il Pentesting

## BlackArch Linux



```
code-audit
androwarn      parser      pfff
bof-detector   jsecc       pfff_db
cflow          semver     pfff_test
cppcheck       uid         scheck
cppcheck-gui   which       sgrep
cppcheck-htmlreport semver    spatch
cppcheck       uid         stags
cppcheck-gui   jsecc       procyon
cppcheck-htmlreport parser    pscan
dscanner       jsecc       shellcheck
expose         parser    smalisa
acorn          jsecc       spaf
compress       parser    genflagcodes
lint           jsecc       stacoan
release        parser    jadx
source-highlight jsecc     jadx-gui
.coverrc       acorn      callgrind_annotate
cover          test262.whitelist callgrind_control
acorn          semver     cg_annotate
test262.whitelist which     cg_diff
acorn          flawfinder cg_merge
jsecc          graudit    ms_print
ncp            leema      valgrind
semver         acorn      valgrind-di-server
parser         cake       valgrind-listener
jsecc          coffee     vgdb
semver         grunt      callgrind_annotate
uid            which     callgrind_control
which          ncp       cg_annotate
acorn          tsc       cg_diff
compress       tserver    cg_merge
lint           which     ms_print
release        handlebars valgrind
source-highlight client    valgrind-di-server
.coverrc       ncp       valgrind-listener
cover          semver     vgdb
decompress-zip tserver    wscript
acorn          tserver    acorn
test262.whitelist which     handlebars
asar           acorn      he
get-folder-size without_eval mocha
acorn          mosca      mocha
jsecc          peach-fuzz  uuid
ncp            codequery   which
semver         codeslicer yasca
```

blackarch	
anti-forensic	ids
automation	keylogger
automobile	malware
backdoor	misc
binary	mobile
bluetooth	networking
code-audit	nfc
config	packer
cracker	proxy
crypto	radio
cryptography	recon
database	reversing
debugger	scan
decompiler	scanner
defensive	sniffer
disassembler	social
dos	spoff
drone	spoof
exploitation	stego
fingerprint	tunnel
firmware	unpacker
forensic	voip
fuzzer	webapp
hardware	windows
honeypot	wireless

PM UTC

# Outline

---

- Kali Linux
- Altre Distribuzioni per il Pentesting
- Fondamenti di Linux
  - Struttura del File System
  - Comandi di Base

# Outline

---

- Kali Linux
- Altre Distribuzioni per il Pentesting
- Fondamenti di Linux
  - Struttura del File System
- Comandi di Base

# Fondamenti di Linux

## Struttura del File System

- Il comando **tree** permette di visualizzare la struttura gerarchica «ad albero» del file system di Linux
  - Per avere maggiori informazioni sul comando
  - **man tree**

```
TREE(1)          General Commands Manual          TREE(1)

NAME
    tree - list contents of directories in a tree-like format.

SYNOPSIS
    tree [-acdfghilnpqrstuvxACDFQNSUX] [-L level [-R]] [-H baseHREF] [-T
    title] [-o filename] [--nolinks] [-P pattern] [-I pattern] [--inodes]
    [--device] [--noreport] [--dirsfirst] [--version] [--help] [--filelimit
    #] [--si] [--prune] [--du] [--timefmt format] [--matchdirs] [--from-
    file] [--] [directory ...]
```

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /
/
bin    -> usr/bin
boot
dev
etc
home
lib    -> usr/lib
lib32  -> usr/lib32
lib64  -> usr/lib64
libx32 -> usr/libx32
lost+found
media
mnt
opt
proc
root
run
sbin   -> usr/sbin
srv
sys
tmp
usr
var
```

`tree -L 1 -d /`

Vengono mostrate tutte le directory «figlie» del nodo radice /

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /
```

```
/  
├── bin    -> usr/bin  
├── boot  
├── dev  
├── etc  
├── home  
├── lib    -> usr/lib  
├── lib32  -> usr/lib32  
├── lib64  -> usr/lib64  
├── libx32 -> usr/libx32  
├── lost+found  
├── media  
├── mnt  
├── opt  
├── proc  
├── root  
├── run  
├── sbin   -> usr/sbin  
├── srv  
├── sys  
└── tmp  
└── usr  
└── var
```

La directory / (o directory root) rappresenta la radice dell'albero delle directory all'interno del File System



# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /  
/ |  
+-- bin    -> usr/bin  
+-- boot  
+-- dev  
+-- etc  
+-- home  
+-- lib    -> usr/lib  
+-- lib32  -> usr/lib32  
+-- lib64  -> usr/lib64  
+-- libx32 -> usr/libx32  
+-- lost+found  
+-- media  
+-- mnt  
+-- opt  
+-- proc  
+-- root  
+-- run  
+-- sbin   -> usr/sbin  
+-- srv  
+-- sys  
+-- tmp  
+-- usr  
+-- var
```

Directory «figlie» della directory root

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /
/
bin -> usr/bin
boot
dev
etc
home
lib -> usr/lib
lib32 -> usr/lib32
lib64 -> usr/lib64
libx32 -> usr/libx32
lost+found
media
mnt
opt
proc
root
run
sbin -> usr/sbin
srv
sys
tmp
usr
var
```

Directory contenente programmi di uso comune, accessibili sia dall'utente root (utente con i maggiori permessi in un sistema Linux) che dagli altri utenti

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /
/
bin -> usr/bin
boot
dev
etc
home
lib -> usr/lib
lib32 -> usr/lib32
lib64 -> usr/lib64
libx32 -> usr/libx32
lost+found
media
mnt
opt
proc
root
run
sbin -> usr/sbin
srv
sys
tmp
usr
var
```

A red arrow points from the word "boot" in the terminal output to a text annotation in red: "Directory contenente i file necessari all'avvio del sistema operativo".

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /
/
bin  -> usr/bin
boot
dev
etc
home
lib  -> usr/lib
lib32 -> usr/lib32
lib64 -> usr/lib64
libx32 -> usr/libx32
lost+found
media
mnt
opt
proc
root
run
sbin  -> usr/sbin
srv
sys
tmp
usr
var
```

Directory contenente riferimenti alle periferiche hardware usate dal sistema operativo, che sono viste come file con «proprietà speciali»

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /
/
bin  -> usr/bin
boot
dev
etc
home
lib  -> usr/lib
lib32 -> usr/lib32
lib64 -> usr/lib64
libx32 -> usr/libx32
lost+found
media
mnt
opt
proc
root
run
sbin  -> usr/sbin
srv
sys
tmp
usr
var
```

Directory contenente i più importanti file di configurazione usati dal sistema operativo

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /
/
bin  -> usr/bin
boot
dev
etc
home
lib  -> usr/lib
lib32 -> usr/lib32
lib64 -> usr/lib64
libx32 -> usr/libx32
lost+found
media
mnt
opt
proc
root
run
sbin  -> usr/sbin
srv
sys
tmp
usr
var
```

Home Directory dei vari utenti. In questa directory sono memorizzati i file appartenenti allo *User Space* di un utente

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /
/
bin  -> usr/bin
boot
dev
etc
home
lib  -> usr/lib
lib32 -> usr/lib32
lib64 -> usr/lib64
libx32 -> usr/libx32
lost+found
media
mnt
opt
proc
root
run
sbin  -> usr/sbin
srv
sys
tmp
usr
var
```

Directory contenente i file di libreria usati dai programmi

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /
/
bin  -> usr/bin
boot
dev
etc
home
lib  -> usr/lib
lib32 -> usr/lib32
lib64 -> usr/lib64
libx32 -> usr/libx32
lost+found
media
mnt
opt
proc
root
run
sbin  -> usr/sbin
srv
sys
tmp
usr
var
```

Directory contenente i file recuperati o ripristinati in  
seguito ad eventi anomali del sistema operativo

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /  
/  
├── bin    -> usr/bin  
├── boot  
├── dev  
├── etc  
├── home  
├── lib    -> usr/lib  
├── lib32  -> usr/lib32  
├── lib64  -> usr/lib64  
├── libx32 -> usr/libx32  
└── lost+found  
/media ←  
/mnt  
/opt  
/proc  
/root  
/run  
└── sbin  -> usr/sbin  
└── srv  
└── sys  
└── tmp  
└── usr  
└── var
```

Mount point di default per File System esterni a quello di Linux

- **Mount:** processo tramite cui il sistema operativo rende disponibili agli utenti i file e le directory memorizzate su un dispositivo esterno (hard disk, CD-ROM, penne USB, etc)
  - Così che tali utenti possano accedervi tramite il File System del sistema operativo

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /  
/  
├── bin    -> usr/bin  
├── boot  
├── dev  
├── etc  
├── home  
├── lib    -> usr/lib  
├── lib32  -> usr/lib32  
├── lib64  -> usr/lib64  
├── libx32 -> usr/libx32  
├── lost+found  
├── media  
├── mnt ←  
├── opt  
├── proc  
├── root  
├── run  
├── sbin  -> usr/sbin  
├── srv  
├── sys  
└── tmp  
└── usr  
└── var
```

Mount point di default nelle vecchie versioni di Linux  
per File System esterni a quello di Linux

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /  
/  
├── bin    -> usr/bin  
├── boot  
├── dev  
├── etc  
├── home  
├── lib    -> usr/lib  
├── lib32  -> usr/lib32  
├── lib64  -> usr/lib64  
├── libx32 -> usr/libx32  
├── lost+found  
├── media  
├── mnt  
├── opt ←  
├── proc → Directory contenente software aggiuntivo o di  
│           applicazioni di terze parti  
├── root  
├── run  
├── sbin  -> usr/sbin  
├── srv  
├── sys  
└── tmp  
└── usr  
└── var
```

# Fondamenti di Linux

## Struttura del File System

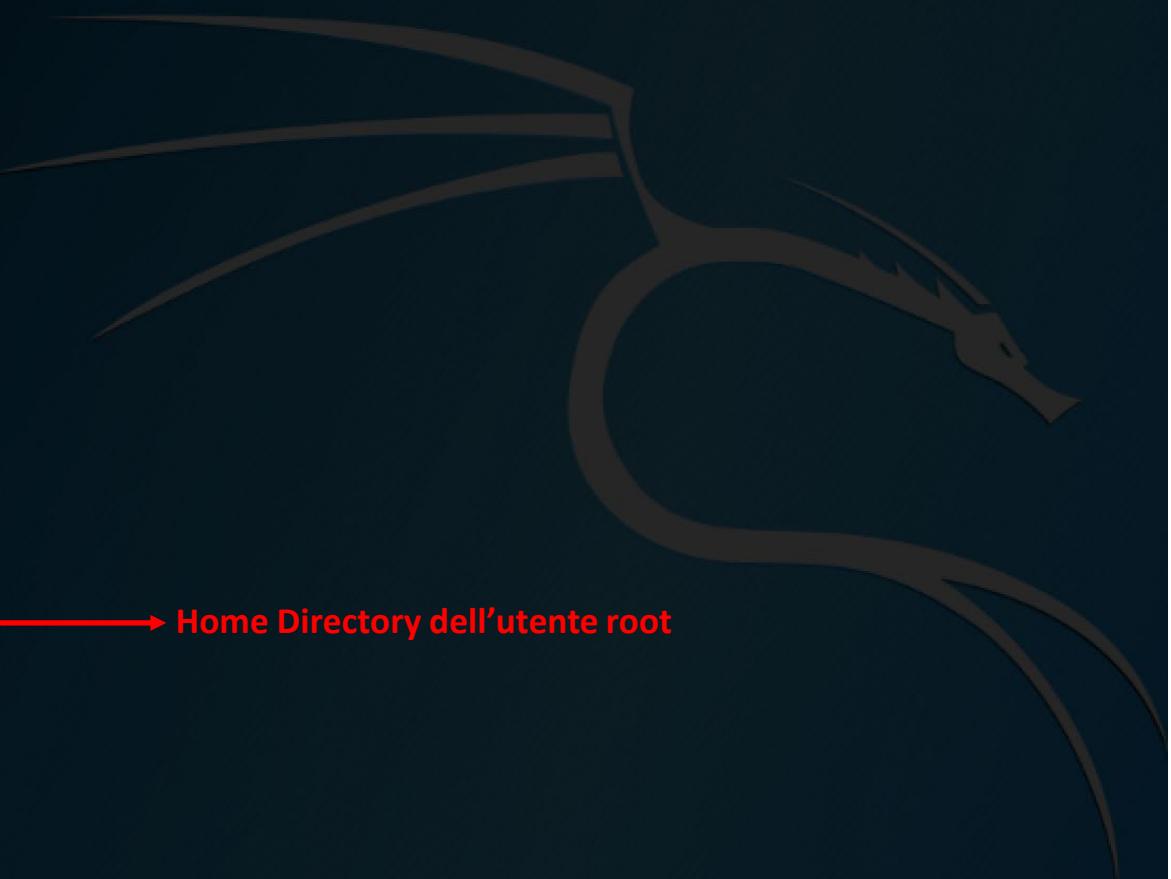
```
root@kali:~# tree -L 1 -d /
/
bin  -> usr/bin
boot
dev
etc
home
lib  -> usr/lib
lib32 -> usr/lib32
lib64 -> usr/lib64
libx32 -> usr/libx32
lost+found
media
mnt
opt
proc
root
run
sbin  -> usr/sbin
srv
sys
tmp
usr
var
```

File System virtuale contenente informazioni  
riguardanti le risorse di sistema

# Fondamenti di Linux

## Struttura del File System

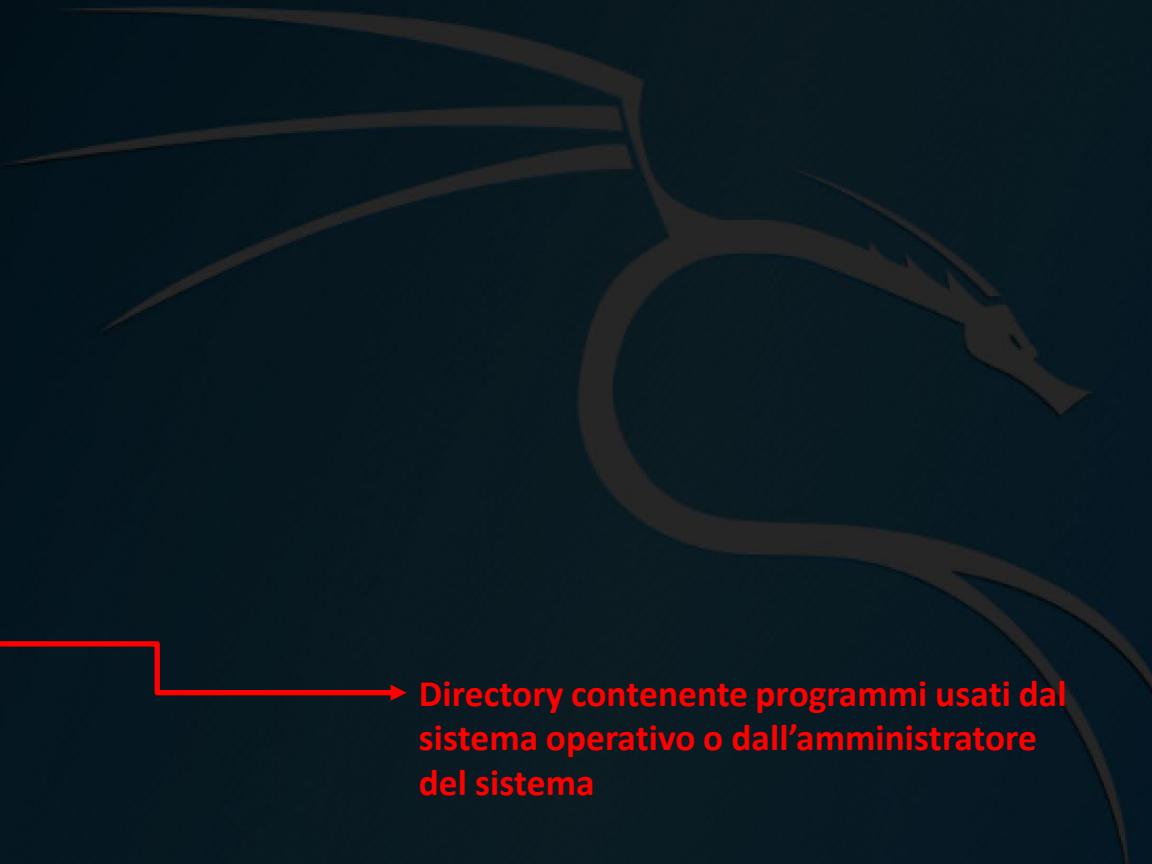
```
root@kali:~# tree -L 1 -d /  
/  
├── bin    -> usr/bin  
├── boot  
├── dev  
├── etc  
├── home  
├── lib    -> usr/lib  
├── lib32  -> usr/lib32  
├── lib64  -> usr/lib64  
├── libx32 -> usr/libx32  
├── lost+found  
├── media  
├── mnt  
├── opt  
├── proc  
└── root   ←  
    └── run  
        └── sbin  -> usr/sbin  
    └── srv  
    └── sys  
    └── tmp  
    └── usr  
    └── var
```



# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /
/
bin  -> usr/bin
boot
dev
etc
home
lib  -> usr/lib
lib32 -> usr/lib32
lib64 -> usr/lib64
libx32 -> usr/libx32
lost+found
media
mnt
opt
proc
root
run
sbin  -> usr/sbin
srv
sys
tmp
usr
var
```



→ Directory contenente programmi usati dal  
sistema operativo o dall'amministratore  
del sistema

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /
/
bin  -> usr/bin
boot
dev
etc
home
lib  -> usr/lib
lib32 -> usr/lib32
lib64 -> usr/lib64
libx32 -> usr/libx32
lost+found
media
mnt
opt
proc
root
run
sbin  -> usr/sbin
srv
sys
tmp
usr
var
```

➤ **Directory contenente file temporanei usati dal sistema operativo.**  
➤ **N.B. Il contenuto di questa directory viene cancellato ad ogni riavvio del sistema operativo**

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /  
/  
├── bin    -> usr/bin  
├── boot  
├── dev  
├── etc  
├── home  
├── lib    -> usr/lib  
├── lib32  -> usr/lib32  
├── lib64  -> usr/lib64  
├── libx32 -> usr/libx32  
├── lost+found  
├── media  
├── mnt  
├── opt  
├── proc  
├── root  
├── run  
├── sbin   -> usr/sbin  
├── srv  
├── sys  
└── tmp  
   └── usr  
      └── var
```

Directory contenente file eseguibili, librerie e documentazione per i programmi degli utenti

# Fondamenti di Linux

## Struttura del File System

```
root@kali:~# tree -L 1 -d /  
/ |  
+-- bin    -> usr/bin  
+-- boot  
+-- dev  
+-- etc  
+-- home  
+-- lib    -> usr/lib  
+-- lib32  -> usr/lib32  
+-- lib64  -> usr/lib64  
+-- libx32 -> usr/libx32  
+-- lost+found  
+-- media  
+-- mnt  
+-- opt  
+-- proc  
+-- root  
+-- run  
+-- sbin   -> usr/sbin  
+-- srv  
+-- sys  
+-- tmp  
+-- usr  
+-- var
```

Directory contenente informazioni temporanee utilizzate dal sistema operativo, tra le quali file di log, e-mail in uscita, spool di stampa, etc

# Outline

---

- Kali Linux
- Altre Distribuzioni per il Pentesting
- Fondamenti di Linux
  - Struttura del File System
  - Comandi di Base

# Comandi di Base

## Navigazione delle Directory

- Mediante il comando **pwd** è possibile visualizzare («stampare») il percorso (*path*) della **current working directory (cwd)**

```
root@kali:~# pwd  
/root  
root@kali:~#
```

pwd

# Comandi di Base

## Navigazione delle Directory

- Mediante il comando **cd** è possibile spostarsi da una directory all'altra

A terminal window with a black background and white text. It shows a root shell session on a Kali Linux system. The user types 'cd Desktop/' and then 'pwd'. Red callout boxes with arrows point from the text 'cd Desktop/' and 'pwd' to their respective occurrences in the terminal output.

```
root@kali:~# cd Desktop/
root@kali:~/Desktop# pwd
/root/Desktop
root@kali:~/Desktop#
```

- **Directory speciali**

- ~ Home directory dell'utente
- . Directory corrente
- .. Directory «padre» di quella corrente

**man cd** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Navigazione delle Directory

```
root@kali:~/Desktop/Esami# pwd  
/root/Desktop/Esami  
root@kali:~/Desktop/Esami# tree -L 2 -d /root/  
/root/  
└── ADd  
    ├── 32Bit  
    ├── 64Bit  
    ├── cert  
    └── OS2  
└── Desktop  
    └── Esami ←  
└── Documents  
└── Downloads  
    └── vega  
└── Music  
└── Pictures  
└── Public  
└── Templates  
└── Videos  
  
15 directories  
root@kali:~/Desktop/Esami#
```

pwd

tree -L 2 -d /root/

# Comandi di Base

## Navigazione delle Directory

```
root@kali:~/Desktop/Esami# pwd
/root/Desktop/Esami
root@kali:~/Desktop/Esami# tree -L 2 -d /root/
/root/
    └── ADD
        ├── 32Bit
        ├── 64Bit
        ├── cert
        └── OS2
    └── Desktop
        └── Esami
    ├── Documents
    ├── Downloads
    │   └── vega
    ├── Music
    ├── Pictures
    ├── Public
    ├── Templates
    └── Videos

15 directories
root@kali:~/Desktop/Esami# cd ..
root@kali:~/Desktop# pwd
/root/Desktop
```

# Comandi di Base

## Proprietà dei File – Tipologie di File

---

- In Linux ogni cosa è vista come un file oppure come un processo
- Oltre ai file convenzionali (**Regular File**), ne esistono altri con caratteristiche particolari
  - **Directory:** file che sono liste di altri file
  - **Link:** collegamenti a file o directory per renderli visibili in altre parti del File System
  - **File Speciali:** usati per «comunicare» con dispositivi di I/O (i.e., Character Device e Block Device)
  - **Socket:** simili alle socket TCP/IP, consentono la comunicazione tra processi
  - **Pipe:** simili alle Socket, consentono la comunicazione tra processi

# Comandi di Base

## Proprietà dei File – Tipologie di File

- In Linux a ciascuna **tipologia di file** è associato un determinato **simbolo**

Simbolo	Significato
-	Regular File
d	Directory
l	Link
c	Character Device
b	Block Device
s	Socket
p	Pipe

# Comandi di Base

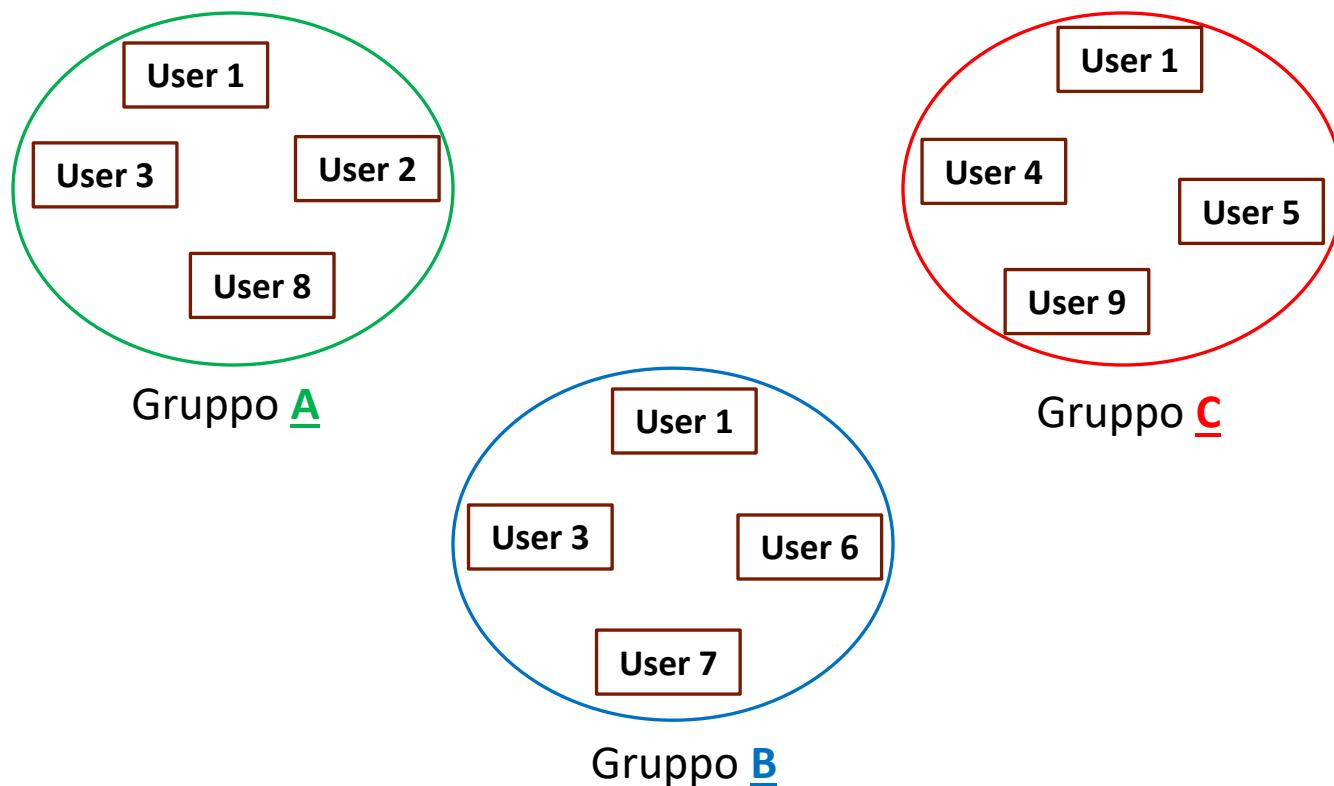
## Proprietà dei File – Proprietario, Gruppi, Utenti

---

- I permessi nei sistemi Unix/Linux sono organizzati in base a **tre classi di utenti**: *Proprietario, Gruppo e Tutti gli Altri*
  
- In Unix/Linux
  - Ciascun file ha un proprietario ed un gruppo di appartenenza
  - Ciascun utente può appartenere a più gruppi
  
- L'uso dei gruppi consente
  - Di delegare capacità aggiuntive in modo organizzato (ad es., accesso a dischi, stampanti ed altre periferiche)
  - Al «superutente» (*root*) di delegare alcune attività amministrative ad utenti «normali»

# Comandi di Base

Proprietà dei File – Proprietario, Gruppi, Utenti



# Comandi di Base

## Proprietà dei File – Permessi dei File

---

- In Linux per **ciascun file** i permessi sono assegnati in base a **tre categorie di utenti**
  - **Owner:** I permessi si applicano solo al proprietario del file e non riguardano gli altri utenti
  - **Group:** I permessi si applicano solo agli utenti appartenenti al gruppo associato al file e non riguardano gli altri utenti
  - **All Users/Others:** I permessi si applicano a tutti gli utenti del sistema che non rientrano nelle altre due categorie

# Comandi di Base

## Proprietà dei File – Permessi dei File

---

- A ciascuna categoria di utenti (**Owner**, **Group**, **Others**) sono assegnati tre tipi di permessi (*Tripla di Permessi*)
  - **Read (r)**: L'utente può leggere i contenuti di un file
  - **Write (w)**: L'utente può scrivere o modificare un file
  - **Execute (x)**: L'utente può eseguire un file



- La prima tripla di permessi partendo da sinistra sarà sempre associata all'Owner, la seconda al Group, la terza ad Others

# Comandi di Base

## Proprietà dei File – Permessi dei File

- La **tripla di permessi** può essere assegnata a ciascuna categoria di utenti tramite un **valore numerico decimale**, basandosi su una **Notazione Posizionale**
  - Permesso **ABILITATO** -> bit settato ad **1**
  - Permesso **DISABILITATO** -> bit settato a **0**



# Comandi di Base

## Proprietà dei File – Permessi dei File – Esempio 1

---

- **OWNER:** tutti i permessi abilitati
  - **rwx** → Binario **111** → Decimale  $4+2+1 = \textcolor{red}{7}$
- **GROUP:** abilitati i permessi di lettura (**r**) e di scrittura (**w**) ma non quello di esecuzione (**x**)
  - **rw-** → Binario **110** → Decimale  $4+2+0 = \textcolor{green}{6}$
- **OTHERS:** abilitato solo il permesso di scrittura (**r**)
  - **r--** → Binario **100** → Decimale  $4+0+0 = \textcolor{blue}{4}$

**rwxrw-r--** → 764

# Comandi di Base

Proprietà dei File – Permessi dei File – Esempio 2

---

- **rwxrw-rw-** → 766
- **rwxrwxrwx** → 777
- **rwx-----** → 700

# Comandi di Base

## Proprietà dei File – Permessi dei File – Esempio 3

Tipo di File	Permessi del Proprietario	Permessi del Gruppo	Permessi degli Altri	Cosa verrà mostrato	Valore decimale
-	<b>rw-</b>	<b>rw-</b>	<b>r--</b>	<b>-rw-rw-r--</b>	<b>664</b>
<b>d</b>	<b>r--</b>	<b>r--</b>	<b>r--</b>	<b>dr--r--r--</b>	<b>444</b>
<b>l</b>	<b>rwx</b>	<b>rwx</b>	<b>rwx</b>	<b>l rwxrwxrwx</b>	<b>777</b>
<b>s</b>	<b>rwx</b>	<b>r-x</b>	<b>r-x</b>	<b>s rwxr-xr-x</b>	<b>755</b>
<b>b</b>	<b>rw-</b>	<b>rw-</b>	<b>---</b>	<b>brw-rw----</b>	<b>660</b>
<b>c</b>	<b>rw-</b>	<b>-w-</b>	<b>---</b>	<b>crw--w----</b>	<b>620</b>

- - → Regular file    **d** → Directory                         **l** → Link
- **s** → Socket                        **b** → Block Device                        **c** → Character Device

# Comandi di Base

## Proprietà dei File

- Mediante il comando **ls** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r-- 1 root      root      10, 235 Jan 31 03:10 autofs
drwxr-xr-x 2 root      root      140 Jan 31 03:10 block
drwxr-xr-x 2 root      root      80 Jan 31 03:10 bsg
crw----- 1 root      root      10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x 3 root      root      60 Jan 31 03:10 bus
lrxwxrwxrwx 1 root      root      3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x 2 root      root      2.8K Jan 31 03:10 char
crw----- 1 root      root      5,   1 Jan 31 03:12 console
lrxwxrwxrwx 1 root      root      11 Jan 31 03:10 core -> /proc/kcore
```

**man ls** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Proprietà dei File

- Mediante il comando **ls** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r-- 1 root      root    10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root      root    140 Jan 31 03:10 block
drwxr-xr-x  2 root      root     80 Jan 31 03:10 bsg
crw-----  1 root      root    10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root      root    60 Jan 31 03:10 bus
lrwxrwxrwx  1 root      root      3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root      root    2.8K Jan 31 03:10 char
crw-----  1 root      root     5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root      root    11 Jan 31 03:10 core -> /proc/kcore
```

Tipologia  
di file

**man ls** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Proprietà dei File

- Mediante il comando **ls** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r-- 1 root      root    10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root      root    140 Jan 31 03:10 block
drwxr-xr-x  2 root      root     80 Jan 31 03:10 bsg
crw-----  1 root      root    10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root      root    60 Jan 31 03:10 bus
lwxrwxrwx  1 root      root      3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root      root    2.8K Jan 31 03:10 char
crw-----  1 root      root     5,   1 Jan 31 03:12 console
lwxrwxrwx  1 root      root    11 Jan 31 03:10 core -> /proc/kcore
```



**Permessi associati  
al file**

**man ls** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Proprietà dei File

- Mediante il comando **ls** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r-- 1 root      root    10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root      root    140 Jan 31 03:10 block
drwxr-xr-x  2 root      root     80 Jan 31 03:10 bsg
crw-----  1 root      root    10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root      root    60 Jan 31 03:10 bus
lrwxrwxrwx  1 root      root      3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root      root    2.8K Jan 31 03:10 char
crw-----  1 root      root     5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root      root    11 Jan 31 03:10 core -> /proc/kcore
```



**Numero di  
hard link**

**man ls** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Proprietà dei File

- Mediante il comando **ls** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r-- 1 root      root      10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root      root      140 Jan 31 03:10 block
drwxr-xr-x  2 root      root      80 Jan 31 03:10 bsg
crw-----  1 root      root      10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root      root      60 Jan 31 03:10 bus
lrwxrwxrwx  1 root      root      3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root      root      2.8K Jan 31 03:10 char
crw-----  1 root      root      5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root      root      11 Jan 31 03:10 core -> /proc/kcore
```

Utente proprietario  
del file

**man ls** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Proprietà dei File

- Mediante il comando **ls** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r-- 1 root      root      10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root      root      140 Jan 31 03:10 block
drwxr-xr-x  2 root      root      80 Jan 31 03:10 bsg
crw-----  1 root      root      10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root      root      60 Jan 31 03:10 bus
lrwxrwxrwx  1 root      root      3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root      root      2.8K Jan 31 03:10 char
crw-----  1 root      root      5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root      root      11 Jan 31 03:10 core -> /proc/kcore
```

**Gruppo associato al file**

**man ls** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Proprietà dei File

- Mediante il comando **ls** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r-- 1 root      root    10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root      root    140 Jan 31 03:10 block
drwxr-xr-x  2 root      root     80 Jan 31 03:10 bsg
crw-----  1 root      root    10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root      root    60 Jan 31 03:10 bus
lrwxrwxrwx  1 root      root      3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root      root   2.8K Jan 31 03:10 char
crw-----  1 root      root      5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root      root     11 Jan 31 03:10 core -> /proc/kcore
```



Dimensione del file

**man ls** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Proprietà dei File

- Mediante il comando **ls** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r-- 1 root      root    10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root      root    140 Jan 31 03:10 block
drwxr-xr-x  2 root      root     80 Jan 31 03:10 bsg
crw-----  1 root      root    10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root      root    60 Jan 31 03:10 bus
lrwxrwxrwx  1 root      root      3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root      root    2.8K Jan 31 03:10 char
crw-----  1 root      root     5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root      root     11 Jan 31 03:10 core -> /proc/kcore
```

**Ultima modifica al  
file**

**man ls** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Proprietà dei File

- Mediante il comando **ls** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r-- 1 root      root    10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root      root    140 Jan 31 03:10 block
drwxr-xr-x  2 root      root     80 Jan 31 03:10 bsg
crw-----  1 root      root    10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root      root    60 Jan 31 03:10 bus
lrwxrwxrwx  1 root      root      3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root      root    2.8K Jan 31 03:10 char
crw-----  1 root      root     5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root      root    11 Jan 31 03:10 core -> /proc/kcore
```

Nome del file

**man ls** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Modificare i Permessi dei File

---

- I principali comandi per modificare i permessi associati ad un file sono i seguenti
  - **chmod** Permette di cambiare i permessi di un file
  - **chown** Permette di cambiare il proprietario di un file
  - **chgrp** Permette di cambiare il gruppo di appartenenza di un file

Per maggiori informazioni su tali comandi, utilizzare **man nomecomando**

# Comandi di Base

## Modificare i Permessi dei File – Esempio 1

```
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rw-r--r-- 1 root root 42 Mar 19 21:33 pippo.txt
```

Regular file

# Comandi di Base

## Modificare i Permessi dei File – Esempio 1

```
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rw-r--r-- 1 root root 42 Mar 19 21:33 pippo.txt
```

File **pippo.txt**

# Comandi di Base

## Modificare i Permessi dei File – Esempio 1

```
root@kali:~/De Owner root -lh  
total 4.0K  
-rw-r--r-- 1 root root 42 Mar 19 21:33 pippo.txt
```

# Comandi di Base

## Modificare i Permessi dei File – Esempio 1

```
root@kali:~/Desktop Group root
total 4.0K
-rw-r--r-- 1 root root 42 Mar 19 21:33 pippo.txt
```

# Comandi di Base

## Modificare i Permessi dei File – Esempio 1

```
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rw-r--r-- 1 root root 42 Mar 19 21:33 pippo.txt
```

### Permessi

- Owner: lettura e scrittura: 6

# Comandi di Base

## Modificare i Permessi dei File – Esempio 1

```
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rw-r--r-- 1 root root 42 Mar 19 21:33 pippo.txt
```

Permessi  
➤ Group: lettura: 4

# Comandi di Base

## Modificare i Permessi dei File – Esempio 1

```
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rw-r--r-- 1 root root 42 Mar 19 21:33 pippo.txt
```

Permessi

➤ Others: lettura: 4

# Comandi di Base

## Modificare i Permessi dei File – Esempio 1

```
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rw-r--r-- 1 root root 42 Mar 19 21:33 pippo.txt
root@kali:~/Desktop/permessi# chmod 744 pippo.txt
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rwxr--r-- 1 root root 42 Mar 19 21:33 pippo.txt
```

- Assegno all'Owner del file anche il permesso di esecuzione
- **chmod 744 pippo.txt**



# Comandi di Base

## Modificare i Permessi dei File – Esempio 2

```
root@kali:~/Desktop/permessi# ls
total 4.0K
-rw-r--r-- 1 root root 42 Mar 19
root@kali:~/Desktop/permessi# ch
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rwxr--r-- 1 root root 42 Mar 19 21:33 pippo.txt
root@kali:~/Desktop/permessi# chown arccas pippo.txt
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rwxr--r-- 1 arccas root 42 Mar 19 21:33 pippo.txt
```

- Creo un nuovo utente di sistema (**arccas**)
  - **adduser arccas**
- Cambio l'Owner del file **pippo.txt**, che non sarà più l'utente **root** ma l'utente **arccas**
  - **chown arccas pippo.txt**

# Comandi di Base

## Modificare i Permessi dei File – Esempio 3

```
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rw-r--r-- 1 root root 42 Mar 19 21:33 pippo.txt
root@kali:~/Desktop/permessi# chmod 744 pippo.txt
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rwxr--r-- 1 root root 42 Mar 19 21:33 pippo.txt
root@kali:~/Desktop/permessi# chown
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rw xr--r-- 1 arccas root 42 Mar 19 21:33 pippo.txt
root@kali:~/Desktop/permessi# chgrp arccas pippo.txt
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rwxr--r-- 1 arccas arccas 42 Mar 19 21:33 pippo.txt
root@kali:~/Desktop/permessi#
```

➤ Cambio il gruppo del file **pippo.txt**,  
che non è più **root** ma **arccas**  
➤ **chgrp arccas pippo.txt**

# Comandi di Base

## Processi

- Mediante il comando **ps** è possibile visualizzare i processi in esecuzione



```
root@kali:/dev# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.4 1824  1000 ?        Ss   03:10   0:01 /sbin/init
root         2  0.0  0.0   240   120 ?        S    03:10   0:00 [kthreadd]
root         3  0.0  0.0   240   120 ?        I<   03:10   0:00 [rcu_gp]
root         4  0.0  0.0     0     0 ?        I<   03:10   0:00 [rcu_par_gp]
root         6  0.0  0.0     0     0 ?        I<   03:10   0:00 [kworker/0:0H-kblockd]
root         8  0.0  0.0     0     0 ?        I<   03:10   0:00 [mm_percpu_wq]
```

**man ps** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Processi

- Mediante il comando **ps** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  0.0  0.4 182380  9028 ?      Ss   03:10  0:01 /sbin/init
root        2  0.0  0.0     0     0 ?      S    03:10  0:00 [kthreadd]
root        3  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_gp]
root        4  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_par_gp]
root        6  0.0  0.0     0     0 ?      I<   03:10  0:00 [kworker/0:0H-kblockd]
root        8  0.0  0.0     0     0 ?      I<   03:10  0:00 [mm_percpu_wq]
```



Utente proprietario  
del processo

**man ps** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Processi

- Mediante il comando **ps** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  0.0  0.4 182380  9028 ?      Ss   03:10  0:01 /sbin/init
root        2  0.0  0.0     0     0 ?      S    03:10  0:00 [kthreadd]
root        3  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_gp]
root        4  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_par_gp]
root        6  0.0  0.0     0     0 ?      I<   03:10  0:00 [kworker/0:0H-kblockd]
root        8  0.0  0.0     0     0 ?      I<   03:10  0:00 [mm_percpu_wq]
```



Process ID  
(PID)

**man ps** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Processi

- Mediante il comando **ps** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  0.0  0.4 182380  9028 ?      Ss   03:10  0:01 /sbin/init
root        2  0.0  0.0     0     0 ?      S    03:10  0:00 [kthreadd]
root        3  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_gp]
root        4  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_par_gp]
root        6  0.0  0.0     0     0 ?      I<   03:10  0:00 [kworker/0:0H-kblockd]
root        8  0.0  0.0     0     0 ?      I<   03:10  0:00 [mm_percpu_wq]
```



Percentuale di CPU  
utilizzata dal processo

**man ps** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Processi

- Mediante il comando **ps** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  0.0  0.4 182380  9028 ?      Ss   03:10  0:01 /sbin/init
root        2  0.0  0.0     0     0 ?      S    03:10  0:00 [kthreadd]
root        3  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_gp]
root        4  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_par_gp]
root        6  0.0  0.0     0     0 ?      I<   03:10  0:00 [kworker/0:0H-kblockd]
root        8  0.0  0.0     0     0 ?      I<   03:10  0:00 [mm_percpu_wq]
```



Rapporto tra la quantità di memoria utilizzata dal processo e la memoria fisica disponibile sulla macchina

**man ps** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Processi

- Mediante il comando **ps** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  0.0  0.4 182380  9028 ?      Ss   03:10  0:01 /sbin/init
root        2  0.0  0.0     0     0 ?      S    03:10  0:00 [kthreadd]
root        3  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_gp]
root        4  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_par_gp]
root        6  0.0  0.0     0     0 ?      I<   03:10  0:00 [kworker/0:0H-kblockd]
root        8  0.0  0.0     0     0 ?      I<   03:10  0:00 [mm_percpu_wq]
```



**Virtual Memory Size (VSZ): Memoria  
virtuale che un processo può usare**

**man ps** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Processi

- Mediante il comando **ps** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  0.0  0.4 182380  9028 ?      Ss   03:10  0:01 /sbin/init
root        2  0.0  0.0     0     0 ?      S    03:10  0:00 [kthreadd]
root        3  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_gp]
root        4  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_par_gp]
root        6  0.0  0.0     0     0 ?      I<   03:10  0:00 [kworker/0:0H-kblockd]
root        8  0.0  0.0     0     0 ?      I<   03:10  0:00 [mm_percpu_wq]
```

Resident Set Size (RSS): memoria fisica  
«non swapped») che un processo ha usato

**man ps** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Processi

- Mediante il comando **ps** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  0.0  0.4 182380  9028 ?      Ss   03:10  0:01 /sbin/init
root        2  0.0  0.0     0     0 ?      S    03:10  0:00 [kthreadd]
root        3  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_gp]
root        4  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_par_gp]
root        6  0.0  0.0     0     0 ?      I<   03:10  0:00 [kworker/0:0H-kblockd]
root        8  0.0  0.0     0     0 ?      I<   03:10  0:00 [mm_percpu_wq]
```



TeleTYpewriter (TTY) Terminal che  
controlla il processo

**man ps** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Processi

- Mediante il comando **ps** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  0.0  0.4 182380  9028 ?      Ss   03:10  0:01 /sbin/init
root        2  0.0  0.0     0     0 ?      S    03:10  0:00 [kthreadd]
root        3  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_gp]
root        4  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_par_gp]
root        6  0.0  0.0     0     0 ?      I<   03:10  0:00 [kworker/0:0H-kblockd]
root        8  0.0  0.0     0     0 ?      I<   03:10  0:00 [mm_percpu_wq]
```



Status e priorità  
del processo

**man ps** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Processi

- Mediante il comando **ps** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  0.0  0.4 182380  9028 ?      Ss   03:10  0:01 /sbin/init
root        2  0.0  0.0     0     0 ?      S    03:10  0:00 [kthreadd]
root        3  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_gp]
root        4  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_par_gp]
root        6  0.0  0.0     0     0 ?      I<   03:10  0:00 [kworker/0:0H-kblockd]
root        8  0.0  0.0     0     0 ?      I<   03:10  0:00 [mm_percpu_wq]
```



Ora di inizio o data  
del processo

**man ps** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Processi

- Mediante il comando **ps** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  0.0  0.4 182380  9028 ?      Ss   03:10  0:01 /sbin/init
root        2  0.0  0.0     0     0 ?      S    03:10  0:00 [kthreadd]
root        3  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_gp]
root        4  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_par_gp]
root        6  0.0  0.0     0     0 ?      I<   03:10  0:00 [kworker/0:0H-kblockd]
root        8  0.0  0.0     0     0 ?      I<   03:10  0:00 [mm_percpu_wq]
```



Tempo di utilizzo  
totale della CPU

**man ps** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Processi

- Mediante il comando **ps** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  0.0  0.4 182380  9028 ?      Ss   03:10  0:01 /sbin/init
root        2  0.0  0.0     0     0 ?      S    03:10  0:00 [kthreadd]
root        3  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_gp]
root        4  0.0  0.0     0     0 ?      I<   03:10  0:00 [rcu_par_gp]
root        6  0.0  0.0     0     0 ?      I<   03:10  0:00 [kworker/0:0H-kblockd]
root        8  0.0  0.0     0     0 ?      I<   03:10  0:00 [mm_percpu_wq]
```

Nome del processo

**man ps** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Processi – Visualizzazione ad Albero

- Mediante il comando **pstree** è possibile visualizzare l'«albero dei processi» in esecuzione

```
root@kali:~# pstree
systemd—ModemManager—2*[{ModemManager}]
      └─NetworkManager—dhclient
          └─2*[{NetworkManager}]
      └─2*[VBoxClient]—VBoxClient—{VBoxClient}
      └─VBoxClient—VBoxClient
      └─VBoxClient—VBoxClient—2*[{VBoxClient}]
      └─VBoxService—7*[{VBoxService}]
      └─accounts-daemon—2*[{accounts-daemon}]
      └─boltd—2*[{boltd}]
      └─colord—2*[{colord}]
      └─cron
      └─dbus-daemon
      └─fwupd—4*[{fwupd}]
      └─gdm3—gdm-session-wor—gdm-x-session—Xorg—3*[{Xorg}]
          └─gnome-session-b—gnome-shell+
              └─gsd-ally-s+
              └─gsd-clipbo+
```

**man pstree** (Per avere maggiori informazioni sul comando)

# Comandi di Base

## Processi – Invio di Segnali

- Mediante il comando **kill** è possibile inviare un **segnale** ad un processo specificando il *Process ID (PID)* di tale processo

```
KILL(1)                               User Commands
                                         root@kali: ~ 62x19
NAME root@kali:~# ps -e | grep less
    301 kill [-s /? | send] [pid] [sig]
      send a signal to a process
root@kali:~# 
SYNOPSIS
    kill [options] <pid> [...]
DESCRIPTION
    The default signal for kill is TERM. Use -l or -L to list available
    signals. Particularly useful signals include HUP, INT, KILL, STOP,
    CONT, and QUIT. Alternate signals may be specified in three ways: -9,
    -SIGKILL or -KILL. Negative PID values may be used to choose whole
    process groups; see the PGID column in ps command output. A PID of -1
    is special; it indicates all processes except the kill process itself
    and init.
```

# Comandi di Base

## Processi – Invio di Segnali

- Mediante il comando **killall** è possibile arrestare un processo specificando il nome di tale processo

```
KILLALL(1)           User Commands           KILLALL(1)

NAME
    killall - kill processes by name

SYNOPSIS
    killall [-Z, --context pattern] [-e, --exact] [-g, --process-group]
    [-i, --interactive] [-n, --ns PID] [-o, --older-than TIME]
    [-q, --quiet] [-r, --regexp] [-s, --signal SIGNAL, -SIGNAL] [-u, --user
    user] [-v, --verbose] [-w, --wait] [-y, --younger-than TIME] [-I, --ig-
    nore-case] [-V, --version] [--] name ...
    killall -l
    killall -V, --version

DESCRIPTION
    killall sends a signal to all processes running any of the specified
    commands. If no signal name is specified, SIGTERM is sent.

    Signals can be specified either by name (e.g. -HUP or -SIGHUP) or by
    number (e.g. -1) or by option -s.

    If the command name is not regular expression (option -r) and contains
    a slash (/), processes executing that particular file will be selected
```

# Comandi di Base

## Ricerca di Stringhe nei File – Esempio

- Ricerca di stringhe all'interno di file
- Comando **grep**

File

Stringa da ricercare all'interno del File

```
root@kali:~# less /etc/services | grep http
# Updated from https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml .
http          80/tcp        www
https         443/tcp       webcache
http-alt      8080/tcp
http-alt      8080/udp
# WorldWideWeb HTTP
# http protocol over TLS/SSL
# WWW caching service
```

Esempio

# Comandi di Base

## Ricerca di Stringhe nei File – Esempio

### ➤ Ricerca di stringhe all'interno di file

#### ➤ Comando **grep**

- Il comando **less** permette di leggere un file
  - Per maggiori informazioni **man less**

- L'operatore **|** è detto **pipe** e permette di inviare informazioni tra processi
  - L'output del processo a sinistra della pipe diventa input di quello a destra

```
root@kali:~# less /etc/services | grep http
# Updated from https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml .
http          80/tcp        www
https         443/tcp       webcache
http-alt      8080/tcp
http-alt     8080/udp
root@kali:~#
```

Esempio

# Comandi di Base

## Ricerca di Stringhe nei File – Esempio

- Ricerca di stringhe all'interno di file
- Comando **grep**

➤ Il comando **less** permette di leggere un file  
➤ Per maggiori informazioni **man less**

➤ Il comando **grep** stampa le linee di un file contenenti la stringa o il pattern cercato  
➤ Per maggiori informazioni **man grep**

```
root@kali:~# less /etc/services | grep http
# Updated from https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml .
http          80/tcp        www
https         443/tcp       webcache
http-alt      8080/tcp
http-alt      8080/udp
root@kali:~#
```

Esempio

# Comandi di Base

## Ricerca di File

---

### ➤ Comando **locate**

- Prima di eseguire il comando è necessario aggiornare il database di sistema su cui tale comando andrà ad effettuare la ricerca
- Comando **updatedb**

### ➤ Esempio

- **updatedb**
- **locate named.conf**

```
root@kali:~# updatedb
root@kali:~# locate named.conf
/usr/share/samba/setup/named.conf
/usr/share/samba/setup/named.conf.dlz
/usr/share/samba/setup/named.conf.update
root@kali:~#
```

# Comandi di Base

## Ricerca di File

---

### ➤ Comando **find**

### ➤ Esempio

➤ **find / -iname pippo.txt**

```
root@kali:~# find / -iname pippo.txt
/root/Desktop/pippo.txt
root@kali:~#
```

# Comandi di Base

## Ricerca di File

### ➤ Comando **find**

### ➤ Esempio

➤ `find / -iname pippo.txt`

Directory di sistema a partire  
dalla quale inizierà la ricerca

```
root@kali:~# find / -iname pippo.txt
/root/Desktop/pippo.txt
root@kali:~#
```

# Comandi di Base

## Ricerca di File

### ➤ Comando **find**

La ricerca avviene in maniera  
**case insensitive**

### ➤ Esempio

➤ `find / -iname pippo.txt`

```
root@kali:~# find / -iname pippo.txt
/root/Desktop/pippo.txt
root@kali:~#
```

# Comandi di Base

## Ricerca di File

### ➤ Comando **find**

### ➤ Esempio

➤ `find / -iname pippo.txt`

```
root@kali:~# find / -iname pippo.txt
/root/Desktop/pippo.txt
root@kali:~#
```

File che si intende ricercare

# Comandi di Base

## Ricerca di File Eseguibili e Man Page

---

➤ Mediante il comando **whereis** è possibile effettuare la ricerca di un file eseguibile (comando di sistema) e della relativa *man page*

➤ **Esempio**

➤ **whereis dd**

```
root@kali:~# whereis dd
dd: /usr/bin/dd /usr/share/man/man1/dd.1.gz
root@kali:~#
```

# Comandi di Base

## Informazioni sul Sistema

- Il comando **uptime** fornisce informazioni sull'*uptime* del sistema

```
root@kali:~# uptime
 17:54:57 up 38 min,  1 user,  load average: 0.15, 0.04, 0.01
root@kali:~# █
```

- I comandi **date** ed **ncal** forniscono informazioni su data, ora e calendario di sistema

```
└─(root㉿kali)-[~]
# ncal
      March 2022
Su       6 13 20 27
Mo       7 14 21 28
Tu       1  8 15 22 29
We       2  9 16 23 30
Th       3 10 17 24 31
Fr       4 11 18 25
Sa       5 12 19 26
```

# Comandi di Base

## Informazioni sul Sistema

- Il comando **w** fornisce informazioni sugli utenti connessi al sistema

```
root@kali:~# w
17:58:35 up 42 min, 1 user, load average: 0.08, 0.03, 0.00
USER   TTY      FROM          LOGIN@    IDLE    JCPU   PCPU WHAT
root    :1      :1          17:16    ?xdm?   14.56s  0.00s /usr/lib/gdm3/g
root@kali:~#
```

- Il comando **finger** fornisce informazioni su un determinato utente registrato al sistema

```
root@kali:~# finger arccas
Login: arccas
Directory: /home/arccas
Never logged in.
No mail.
No Plan.
root@kali:~#
```

Name: Arcangelo Castiglione
Shell: /bin/bash

# Comandi di Base

## Informazioni sul Sistema

- Per ottenere informazioni sul processore utilizzato dal sistema
  - `cat /proc/cpuinfo`

```
root@kali:~# cat /proc/cpuinfo
processor      : 0
vendor_id     : GenuineIntel
cpu family    : 6
model         : 70
model name    : Intel(R) Core(TM) i7-4980HQ CPU @ 2.80GHz
stepping       : 1
cpu MHz       : 2793.532
cache size    : 6144 KB
physical id   : 0
siblings       : 2
core id        : 0
cpu cores     : 2
apicid         : 0
initial apicid: 0
fpu            : yes
fpu_exception  : yes
cpuid level   : 13
wp             : yes
```

# Comandi di Base

## Informazioni sul Sistema

---

- Per ottenere informazioni sulla memoria utilizzata dal sistema
  - `cat /proc/meminfo`

```
root@kali:~# cat /proc/meminfo
MemTotal:      2043172 kB
MemFree:       91188 kB
MemAvailable:  1089616 kB
Buffers:        296220 kB
Cached:         736192 kB
SwapCached:     28 kB
Active:         1163244 kB
Inactive:       524292 kB
Active(anon):   598912 kB
Inactive(anon): 73696 kB
Active(file):   564332 kB
Inactive(file): 450596 kB
Unevictable:    0 kB
Mlocked:        0 kB
SwapTotal:      2095100 kB
SwapFree:       2094576 kB
Dirty:          0 kB
Writeback:      0 kB
AnonPages:      653152 kB
Mapped:         200460 kB
Shmem:          17488 kB
```

# Comandi di Base

## Informazioni sul Sistema

---

- Per ottenere informazioni sul processo che ha aperto un determinato file è possibile utilizzare il comando **lsof**
  
- Fornisce numerose altre funzionalità
  - Visualizzare i file aperti da un determinato utente
  - Trovare i processi in esecuzione su una porta specifica
  - Etc
  
- Esempio
  - **lsof /var/log/messages**

```
root@kali:~# lsof /var/log/messages
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
rsyslogd 425 root    10w   REG      8,1  6288032 799595 /var/log/messages
```

# Comandi di Base

## Informazioni sul Sistema

- Per ottenere informazioni sulle interfacce di rete del sistema è possibile utilizzare il comando **ifconfig**

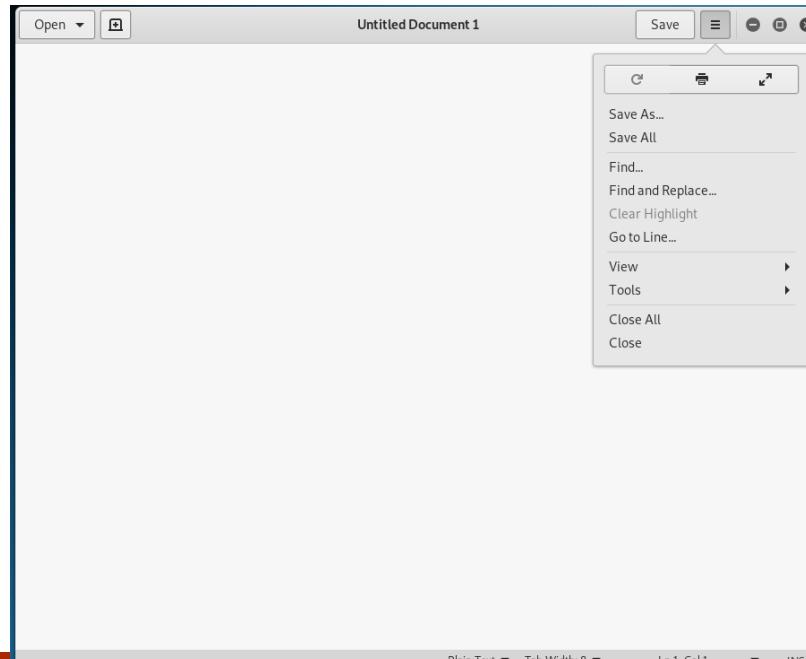
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
      inet6 fe80::a00:27ff:fe95:8c5e prefixlen 64 scopeid 0x20<
          ether 08:00:27:95:8c:5e txqueuelen 1000 (Ethernet)
          RX packets 38 bytes 11059 (10.7 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 80 bytes 9083 (8.8 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
          RX packets 24 bytes 1356 (1.3 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 24 bytes 1356 (1.3 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

# Comandi di Base

## Editor di Testi - Gedit

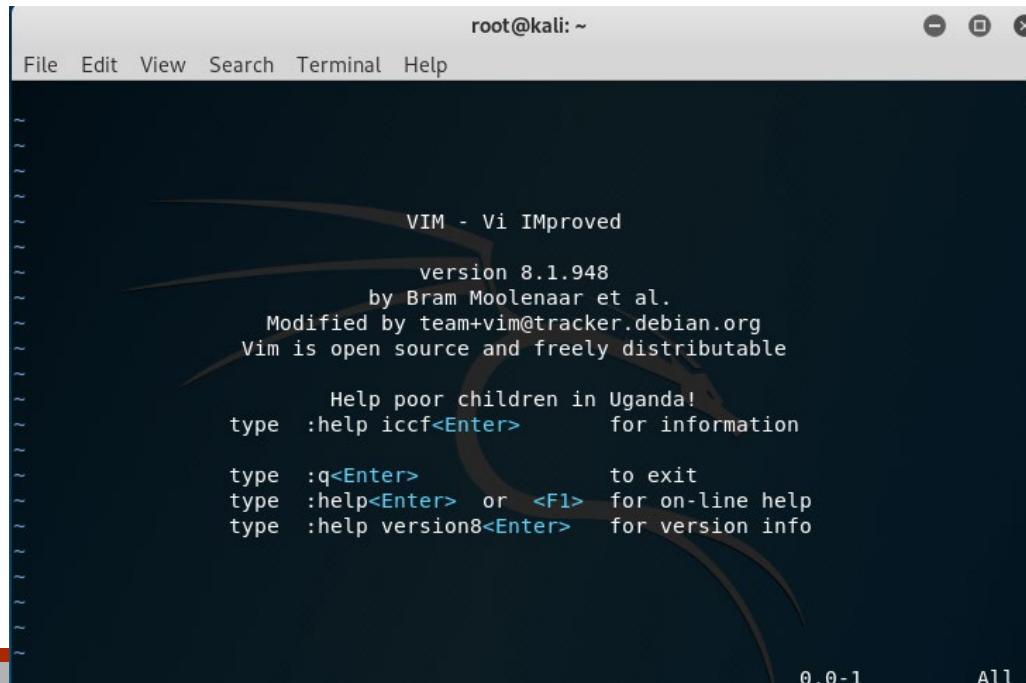
- Utile e comodo editor di testi con interfaccia grafica
- Non presente di default in Kali Linux -> **apt-get install gedit**
- Può essere eseguito mediante il comando **gedit**



# Comandi di Base

## Editor di Testi - vim

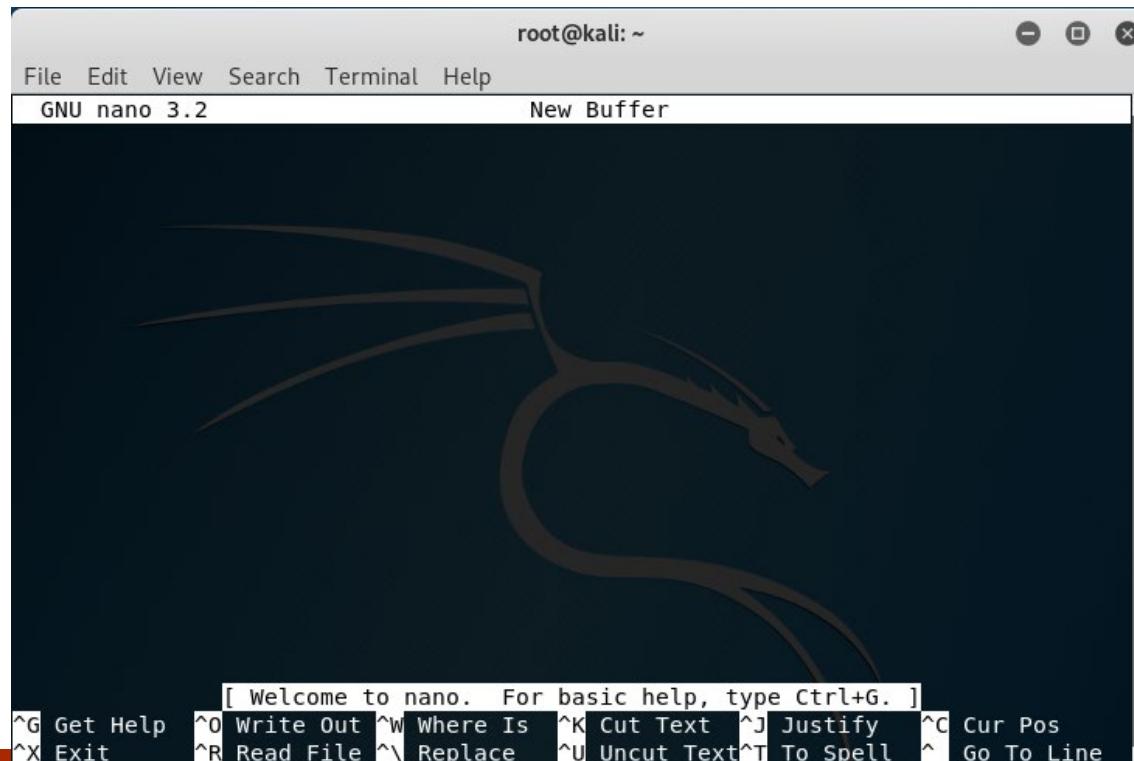
- Editor di testi senza interfaccia grafica
- Può essere eseguito mediante il comando **vim**
- In generale è sempre presente sui sistemi UNIX-based



# Comandi di Base

## Editor di Testi - nano

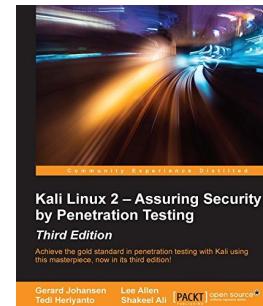
- Editor di testi senza interfaccia grafica
- Può essere eseguito mediante il comando **nano**



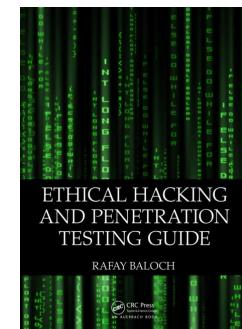
# Bibliografia

---

- **Kali Linux 2 - Assuring Security by Penetration Testing.**  
**Third Edition.** Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing. 2016
  - Capitolo 1



- **Ethical Hacking and Penetration Testing Guide.** Rafay Baloch. CRC Press. 2014
  - Capitolo 2
    - Da pagina 19 a pagina 30 (Escluso «What Is BackTrack»)
    - Da pagina 44 a pagina 47 (Fino a «Removing a File» incluso)



# Bibliografia

---

- **Kali Linux Revealed**
  - <https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf>
- **Bash Guide for Beginners**
  - <https://www.tldp.org/LDP/Bash-Beginners-Guide/Bash-Beginners-Guide.pdf>
- **Advanced Bash-Scripting Guide**
  - <https://www.tldp.org/LDP/abs/abs-guide.pdf>
- **Text Processing Commands**
  - <https://www.tldp.org/LDP/abs/html/textproc.html>
- **Linux Commands List**
  - <https://www.mediacollege.com/linux/command/linux-command.html>