

Andiamo su [Kali.or](https://kali.or/), nella sezione **download** e scarichiamo la **versione VirtualBox**.



Da ambiente Windows

Win + R

Nella casella digitiamo il comando **powershell**,
SHIFT+CTRL+INVIO per avviare come amministratore la powershell.

Get-FileHash kali-linux-2025.4-virtualbox-amd64.7z -Algorithm SHA256

Per ottenere hash del ISO appena scaricata.

```
Administrator: PowerShell 7
PS C:\VM\AAA IMMAGINI OS> Get-FileHash kali-linux-2025.4-virtualbox-amd64.7z -Algorithm SHA256
Algorithm      Hash                                         Path
-----      ----                                         -----
SHA256       6E3A70E3BE441F6EAB8C034493338DC032E4F5A87F93692D5FC486F1E8022AC4
C:\VM\AAA IMMAGINI OS\kali-linu...
```

Torniamo nella sezione download del portale ufficiale e verifichiamo **HASH**.

The image consists of two side-by-side screenshots. The left screenshot shows the Kali.or download page with a red arrow pointing to the 'sum' button at the bottom of the download row. The right screenshot shows a modal window titled 'SHA256sum' containing the following text:

```
6e3a70e3be441f6ea
b8c034493338dc032
e4f5a87f93692d5fc
486f1e8022ac4
```

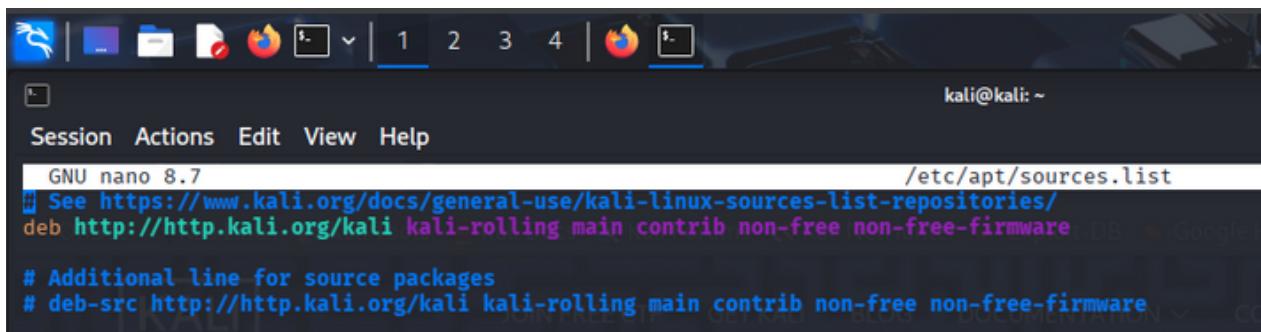
Confrontiamolo, l'**Hash corrisponde** a quello originale pubblicato sul portale ufficiale.
Abbiamo così verificato l'integrità del file tramite confronto degli HASH.

sudo nano /etc/apt/sources.list

Per controllare l'elenco dei repository da cui il sistema scarica pacchetti e aggiornamenti.

```
(kali㉿kali)-[~]
$ sudo nano /etc/apt/sources.list
```

controlliamo che sia presente **solo** quello **ufficiale**



A screenshot of a terminal window titled "Session Actions Edit View Help". The title bar shows "kali@kali: ~". The terminal window displays the file "/etc/apt/sources.list" with the following content:

```
GNU nano 8.7
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware

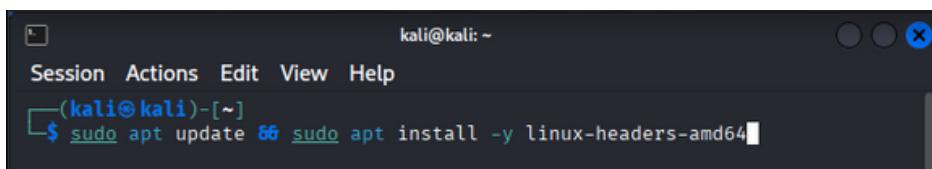
# Additional line for source packages
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
```

Installazione degli Headers

Gli headers del kernel sono file che contengono le definizioni delle interfacce (API) e delle strutture dati usate dal kernel. Servono come "progetto" per permettere la compilazione di moduli esterni, come driver, hardware proprietari o le Guest Additions che devono "parlare" direttamente con il kernel attualmente in uso, senza dover ricompilare l'intero sistema operativo.

sudo apt update && sudo apt install -y linux-headers-amd64

Per installare headers.



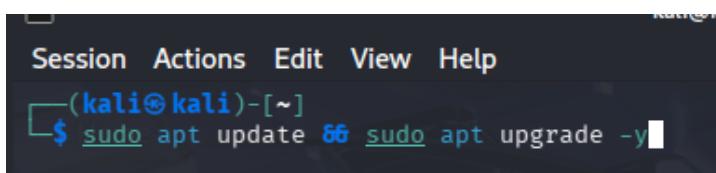
A screenshot of a terminal window titled "Session Actions Edit View Help". The title bar shows "kali@kali: ~". The terminal window displays the command:

```
(kali㉿kali)-[~]
$ sudo apt update && sudo apt install -y linux-headers-amd64
```

sudo apt update && sudo apt upgrade -y

Aggiorna il database locale dei pacchetti disponibili dal repository.

Se ha successo (&&), **scarica e installa** le **nuove versioni** dei software già presenti nel sistema, confermando **automaticamente** (-y).

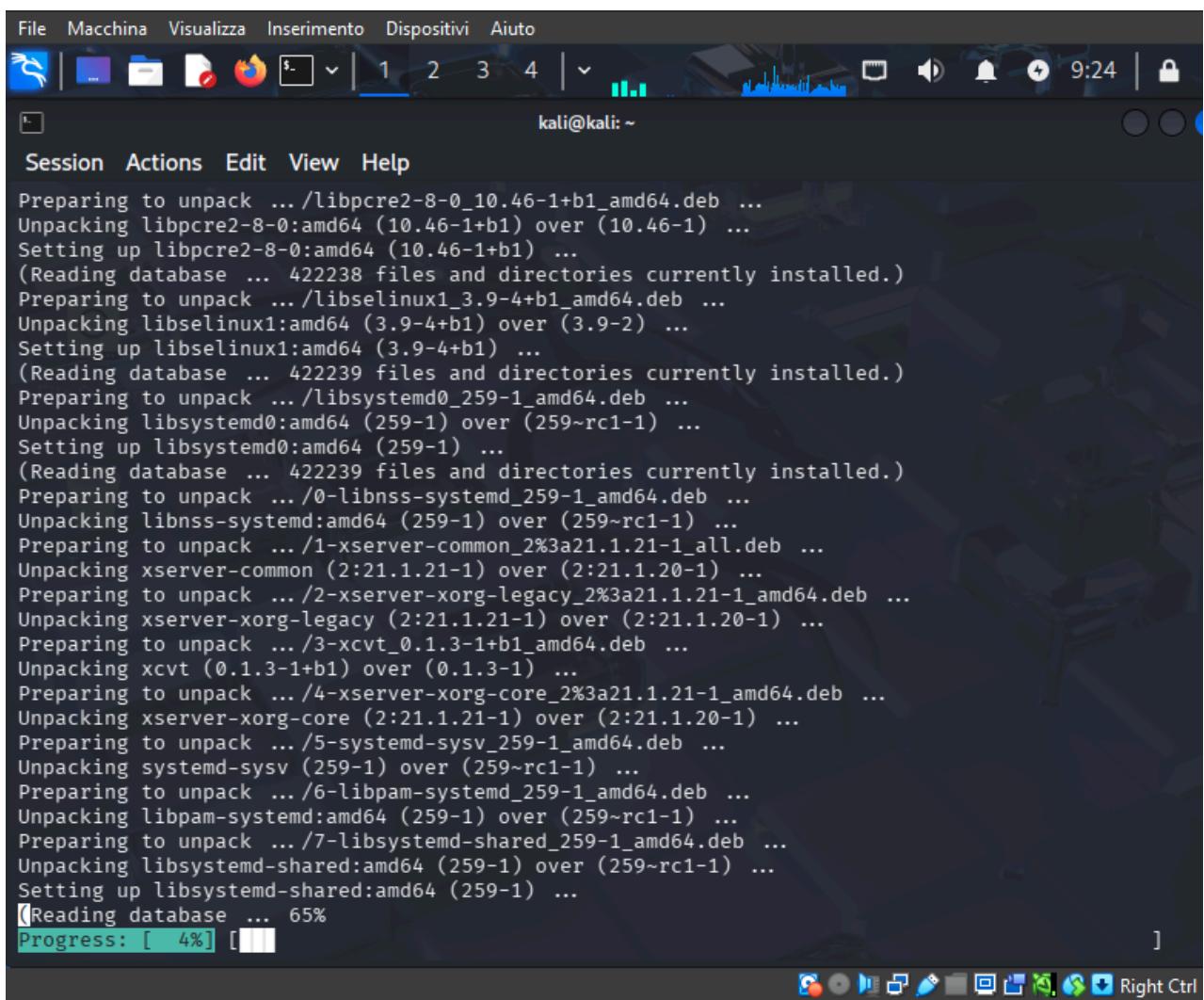


A screenshot of a terminal window titled "Session Actions Edit View Help". The title bar shows "kali@kali: ~". The terminal window displays the command:

```
(kali㉿kali)-[~]
$ sudo apt update && sudo apt upgrade -y
```

```
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [30.0 kB]
Fetched 74.4 MB in 4s (18.0 MB/s)
1411 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
  bloodhound.py          libfuse2t64           libpocketsphinx3   mesa-vdpau-drivers
  curlftps               libgavl-1             libpostproc58     pocketsphinx-en-us
  libavfilter10          libmjpegutils-2.1-0t64  libsphinxbase3t64 python3-fs
  libavformat61          libmpeg2encpp-2.1-0t64  libswscale8       vdpau-driver-all
  libconfig-inifiles-perl libimplex2-2.1-0t64   libvdpau-va-gl1
Use 'sudo apt autoremove' to remove them.

Upgrading:
  7zip                      libqmi-glib5
  accountsservice            libqmi-proxy
  acl                        libqmi-utils
  adduser                     libqrencode4
  alsa-ucm-conf              libqrtr-glib0
  amd64-microcode            libqt5core5t64
  apache2                     libqt5dbus5t64
  apache2-bin                 libqt5designer5
  apache2-data                libqt5gui5t64
  apache2-utils                libqt5help5
  apparmor                    libqt5network5t64
```



Finito l'aggiornamento, riavviamo il sistema.

sudo apt install -y virtualbox-guest-x11 virtualbox-guest-utils



```
kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ sudo apt install -y virtualbox-guest-x11 virtualbox-guest-utils
```

Le Guest Additions sono un pacchetto di driver e applicazioni di sistema progettati per essere installati all'interno della macchina virtuale (il "guest").

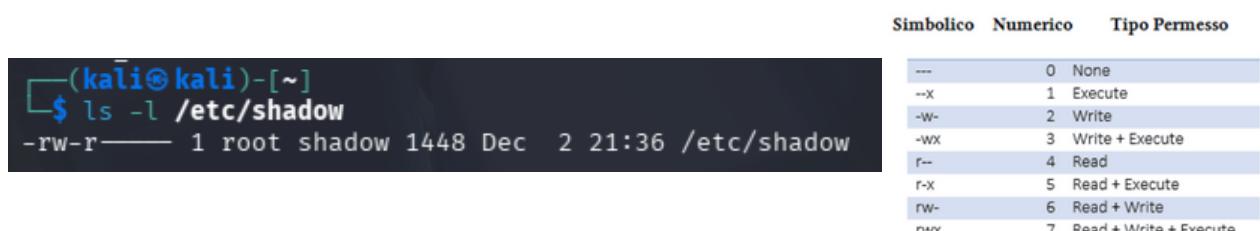
*Migliorano drasticamente l'usabilità dell'ambiente di lavoro abilitando:
Ridimensionamento Dinamico, Cartelle e Appunti Condivisi.*

I file **shadow** contiene gli **hash** delle **password** degli utenti. Verificare i suoi permessi (dovrebbero essere root:shadow e leggibili solo da root).

ls -l /etc/shadow

Per controllare i permessi di /etc/shadow e valutarli in base alle necessita'.

	Simbolico	Numerico	Tipo Permesso
	---	0	None
	--x	1	Execute
	-w-	2	Write
	-wx	3	Write + Execute
	r--	4	Read
	r-x	5	Read + Execute
	rw-	6	Read + Write
	rwx	7	Read + Write + Execute



```
(kali㉿kali)-[~]
$ ls -l /etc/shadow
-rw-r— 1 root shadow 1448 Dec 2 21:36 /etc/shadow
```

Modifichiamo ora il comportamento del terminale per renderlo uno strumento più potente, migliorando la leggibilità e la tracciabilità delle operazioni.

Molto utile in caso di troubleshooting o indagini forense.

echo \$SHELL

Verifichiamo quale shell stiamo usando.

```
(kali㉿kali)-[~]
$ echo $SHELL
/usr/bin/zsh
```

sudo nano ~/.zshrc

Modifichiamo il file .zshrc per modificare come la shell ricorda i comandi registrati.

```
(kali㉿kali)-[~]
$ sudo nano ~/.zshrc
```

CTRL + W

Cerchiamo alias history

Modifichiamo l'alias di default in **history='fc -l -E'** (o **history -E**).

Questo aggiunge il timestamp completo (dd.mm.yyyy hh:mm) accanto a ogni comando eseguito. Fondamentale per l'audit forense e il troubleshooting, perché permette di correlare l'esecuzione dei comandi con gli eventi nei file di log di sistema.

```
# force zsh to show the complete history
alias history="history -E"
```

Aggiungiamo alla fine del file

export HISTTIMEFORMAT="%F %T " definisce come si vuole visualizzare la data.
setopt EXTENDED_HISTORY e' il "motore di registrazione".
setopt HIST_EXPIRE_DUPS_FIRST gestione intelligente dello spazio.
setopt HIST_IGNORE_DUPS elimina comandi di fila ripetuti aumentando la leggibilita'.
setopt HIST_IGNORE_SPACE inserendo uno spazio prima di un comando non viene salvato nella history.
setopt HIST_VERIFY quando richiami un comando vecchio, invece di eseguirlo subito, chiede conferma.
setopt SHARE_HISTORY se hai due terminali aperti, condividono la history in tempo reale.

```
# History Timestamp configuration
export HISTTIMEFORMAT="%F %T "

# Configurazione History per Zsh
setopt EXTENDED_HISTORY      # Salva il timestamp di ogni comando
setopt HIST_EXPIRE_DUPS_FIRST
setopt HIST_IGNORE_DUPS
setopt HIST_IGNORE_SPACE
setopt HIST_VERIFY
setopt SHARE_HISTORY          # Condivide la history tra terminali aperti

[

^G Help           ^O Write Out      ^F Where Is      ^K Cut            ^T Execut
^X Exit           ^R Read File     ^\ Replace       ^U Paste          ^J Justif
```

Abbiamo configurato il sistema per mostrarc ci sempre la data e l'ora esatta di esecuzione accanto a ogni comando, invece del solo numero progressivo.

Per connessione a reti ostili o **non sicure** installiamo il pacchetto **Uncomplicated Firewall**. UFW è un'**interfaccia** semplificata per **iptables/nftables**, il **firewall** standard di Linux.

sudo apt install ufw

```
(kali㉿kali)-[~]
$ sudo apt install ufw
```

```
(kali㉿kali)-[~]
$ sudo apt install ufw
Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1
  Download size: 169 kB
  Space needed: 880 kB / 61.4 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 0s (463 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 450646 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36.2-9_all.deb ...
Unpacking ufw (0.36.2-9) ...
Setting up ufw (0.36.2-9) ...
Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
```

sudo ufw default deny incoming

*Blocca tutto il traffico in entrata non esplicitamente autorizzato. (**IMPORTANTE**)*

```
(kali㉿kali)-[~]
$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

sudo ufw allow ssh

Esempio per autorizzare traffico remoto tramite TCP/Porta 22 (SSH).

sudo ufw enable/disable

Attiva/disattiva il firewall e lo imposta per avviarsi automaticamente al boot del sistema.

```
(kali㉿kali)-[~]
$ sudo ufw enable
Firewall is active and enabled on system startup
```

sudo systemctl status ufw

Mostra lo stato tecnico del **processo in background** (demone) di UFW.

```
(kali㉿kali)-[~]
$ sudo systemctl status ufw
[sudo] password for kali:
● ufw.service - Uncomplicated firewall
  Loaded: loaded (/usr/lib/systemd/system/ufw.service; enabled; preset: enabled)
  Active: active (exited) since Tue 2026-01-20 06:04:00 EST; 16min ago
    Invocation: 61f1bb353da14e85a055057588fe5ae1
      Docs: man:ufw(8)
   Process: 471 ExecStart=/usr/lib/ufw/ufw-init start quiet (code=exited, status=0/>>
 Main PID: 471 (code=exited, status=0/SUCCESS)
  Mem peak: 3.4M
     CPU: 97ms

Jan 20 06:04:00 kali systemd[1]: Starting ufw.service - Uncomplicated firewall ...
Jan 20 06:04:00 kali systemd[1]: Finished ufw.service - Uncomplicated firewall.
lines 1-12/12 (END)
```

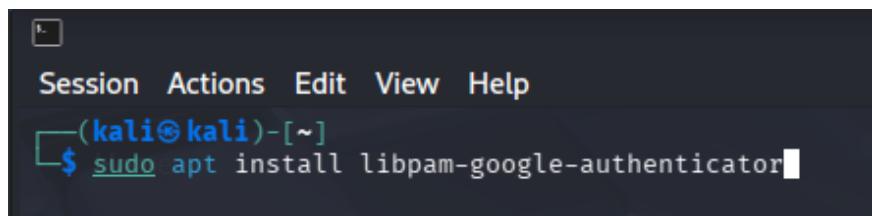
sudo ufw status per vedere lo **stato** del **firewall** e le **regole attive**.

```
(kali㉿kali)-[~]
$ sudo ufw status
Status: active
```

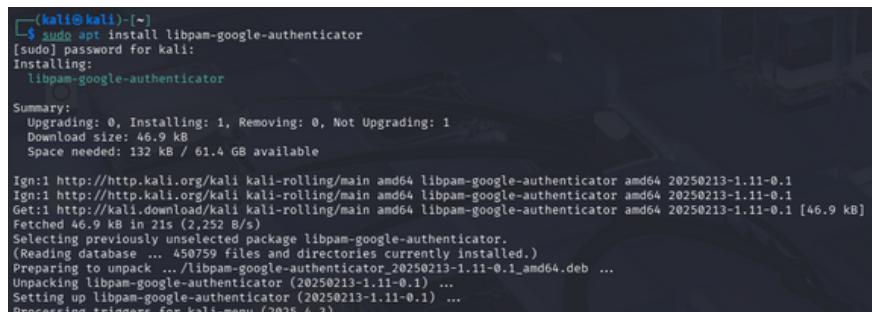
Aggiungiamo un secondo fattore di autenticazione (**2FA**) per l'accesso locale o SSH.

Il modulo **PAM** (Pluggable Authentication Module) di **Google Authenticator** permette di implementare **l'autenticazione a due fattori** (2FA) basata su **TOTP** (Time-based One-Time Password) per **proteggere** l'accesso **SSH** e **servizi del sistema**.

sudo apt install libpam-google-authenticator per avviare l'installazione



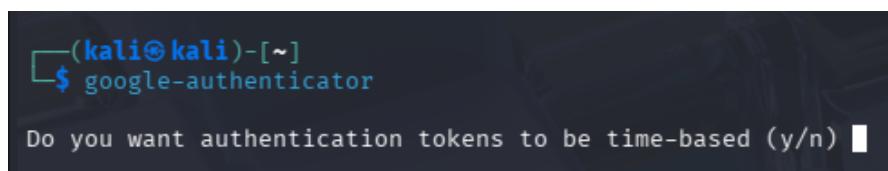
```
(kali㉿kali)-[~]
$ sudo apt install libpam-google-authenticator
```



```
(kali㉿kali)-[~]
$ sudo apt install libpam-google-authenticator
[sudo] password for kali:
Installing:
 libpam-google-authenticator

Summary:
 Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1
 Download size: 46.9 kB
 Space needed: 132 kB / 61.4 GB available

Ign:1 http://http.kali.org/kali kali-rolling/main amd64 libpam-google-authenticator amd64 20250213-1.11-0.1
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 libpam-google-authenticator amd64 20250213-1.11-0.1
Get:1 http://kali.download/kali kali-rolling/main amd64 libpam-google-authenticator amd64 20250213-1.11-0.1 [46.9 kB]
Fetched 46.9 kB in 21s (2,252 B/s)
Selecting previously unselected package libpam-google-authenticator.
(Reading database ... 450759 files and directories currently installed.)
Preparing to unpack .../libpam-google-authenticator_20250213-1.11-0.1_amd64.deb ...
Unpacking libpam-google-authenticator (20250213-1.11-0.1) ...
Setting up libpam-google-authenticator (20250213-1.11-0.1) ...
Processing triggers for kali-menu (2025.4.3) ...
```



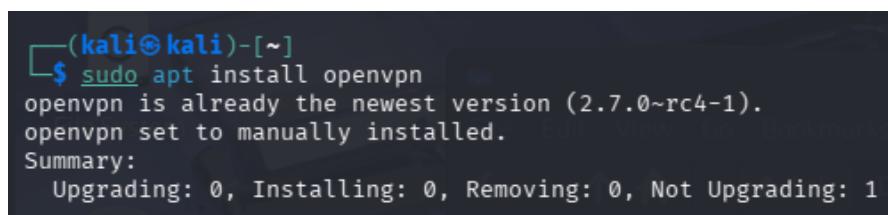
```
(kali㉿kali)-[~]
$ google-authenticator

Do you want authentication tokens to be time-based (y/n) ?
```

confermare con **YES**

Procediamo all'installazione del **client VPN**. Questa tecnologia crea un **tunnel cifrato** essenziale per **accedere** a **infrastrutture isolate** (come reti aziendali o laboratori pratici), **garantire l'anonimato** durante i test e **proteggere il traffico** su reti ostili. Permette di **aggirare blocchi geografici** e **isolare le connessioni** durante l'analisi di malware.

sudo apt install openvpn



```
(kali㉿kali)-[~]
$ sudo apt install openvpn
openvpn is already the newest version (2.7.0~rc4-1).
openvpn set to manually installed.
Summary:
 Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1
```

Installazione servizio Tor

Fondamentale per le attività di **OSINT** (Open Source Intelligence).
Aumenta l'**anonimato** nella navigazione.

sudo apt install tor



```
(kali㉿kali)-[~]
$ sudo apt install tor
Installing:
  tor

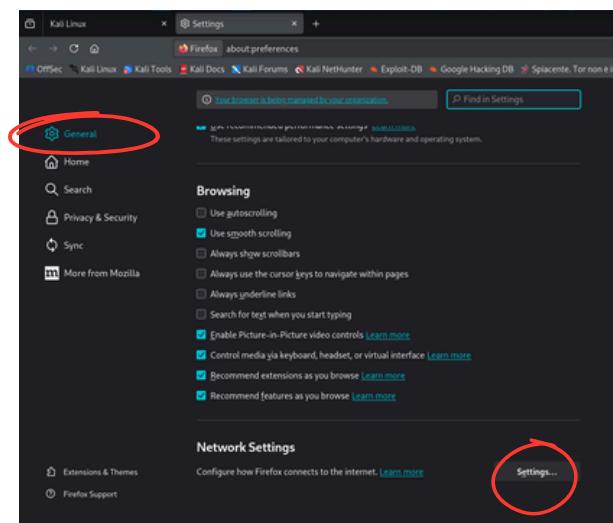
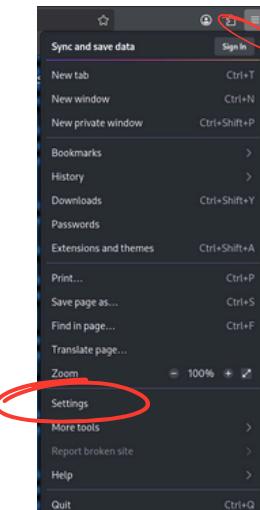
Installing dependencies:
  libtorsocks  tor-geoipdb  torsocks

Suggested packages:
  mixmaster  torbrowser-launcher  apparmor-utils  nyx  obfs4proxy

Summary:
  Upgrading: 0, Installing: 4, Removing: 0, Not Upgrading: 1
  Download size: 4,857 kB
  Space needed: 32.2 MB / 61.4 GB available

Continue? [Y/n] y
```

confermiamo con **YES**



General

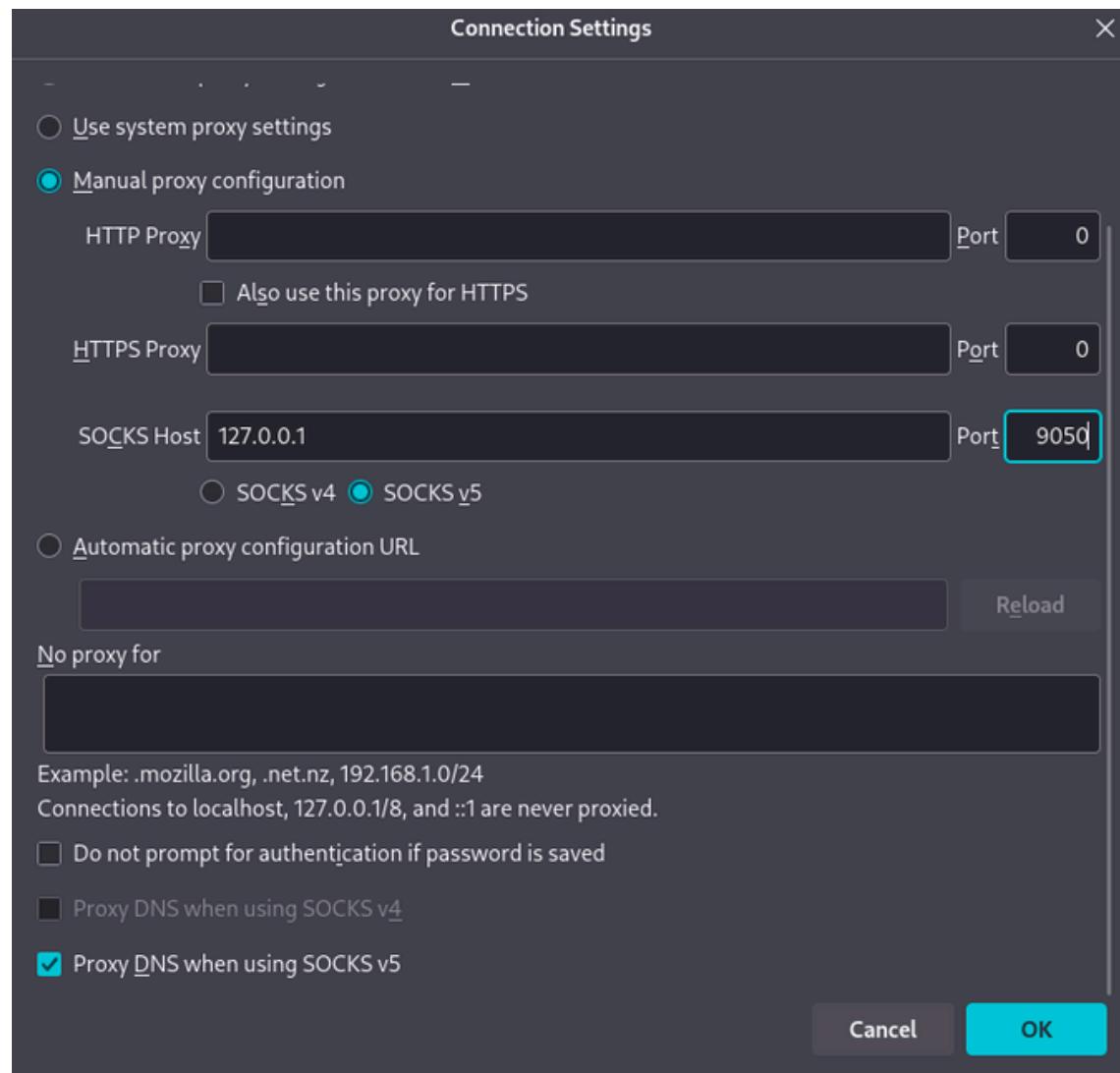
scrolliamo in basso tutta la scheda
e clicchiamo su **Settings**

Selezioniamo **Manual proxy configuration**

SOCKS Host **127.0.0.1** Port **9050**

selezioniamo **SOCK v5**

Controlliamo sia attivo Proxy DNS when using SOCKS v5



sudo systemctl enable tor

Abilita il servizio tor.

```
(kali㉿kali)-[~]
$ sudo systemctl enable tor
Synchronizing state of tor.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable tor
Created symlink '/etc/systemd/system/multi-user.target.wants/tor.service' → '/usr/lib/systemd/system/tor.service'.

(kali㉿kali)-[~]
$ sudo systemctl status tor
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
  Loaded: loaded (/usr/lib/systemd/system/tor.service; enabled; preset: disabled)
  Active: inactive (dead)
```

sudo systemctl status tor

Verifica lo stato operativo attuale del servizio Tor (The Onion Router).

Visualizza lo stato del servizio:

- attivo - **active/running**
- spento - **inactive/dead**
- errori all'avvio - **failed**

Verifica l'anonymato collegandoti a questo indirizzo; il sistema ti notificherà immediatamente se la navigazione è protetta o se stai esponendo il tuo indirizzo IP.

<https://check.torproject.org>

The screenshot shows a web page with a purple header bar containing links like OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and Spicciante. Below the header, there's a purple bar with the text "Questa pagina è disponibile anche nelle seguenti lingue: Italiano" and a "Conferma" button. The main content area features a large green onion logo at the top, followed by the text "Congratulazioni. Questo browser è configurato per usare Tor." in green. Below this, it says "L'indirizzo IP sembra essere: 176.65.149.192". Further down, it says "Visita il [sito web di Tor](#) per ulteriori informazioni su come usare Tor in modo sicuro. È ora possibile navigare in Internet in forma anonima. Per maggiori informazioni su questo exit relay: [Cerca Relay](#)". At the bottom, there's a blue button labeled "Dona per sostenere Tor", and links for "Forum Tor", "Volontario", "Gestisci un Relay", and "Rimani anonimo". A small note at the very bottom says "Il Tor Project è un'organizzazione 501(c)(3) no-profit americana dedicata alla ricerca, sviluppo ed educazione sull'anonymato e privacy online. [Ulteriori informazioni](#) - JavaScript è abilitato."

NOTA: Abbiamo aumentato l'anonymato, ma non siamo invisibili.

Tecniche come il Fingerprinting permettono di identificarsi analizzando la configurazione unica del nostro hardware e software, bypassando la protezione dell'IP.

Installazione docker

Docker è una piattaforma di containerizzazione che permette di eseguire applicazioni in **ambienti isolati** e indipendenti dal sistema ospite. Offre la **flessibilità** di creare **istanze effimere**.

sudo apt install docker.io

```
(kali㉿kali)-[~]
└─$ sudo apt install docker.io
Installing:
  docker.io

Installing dependencies:
  containerd docker-buildx libcompecli libintlx-s perl libproc-processtable-perl needrestart python3-pycrui tini-static
  criu docker-cl libintlx-perl libmodule-find-perl libsort-naturally-perl python3-protobuf runc

Suggested packages:
  containernetworking-plugins docker-doc btrfs-progs debootstrap rinse rootlesskit xfsprogs zfs-fuse | zfsutils-linux

Summary:
  Upgrading: 0, Installing: 16, Removing: 0, Not Upgrading: 1
  Download size: 86.9 MB
  Space needed: 364 MB / 61.3 GB available

Continue? [Y/n] Y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 runc amd64 1.3.3+ds1-2 [6,686 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 containerd amd64 1.7.24-ds1-10 [33.6 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 tini-static amd64 0.19.0-6 [277 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 docker.io amd64 27.5.1+dfsg4-1 [23.2 MB]
Get:5 http://kali.download/kali kali-rolling/main amd64 libcompecli amd64 4.2-1 [64.2 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 criu amd64 4.2-1 [557 kB]
Get:8 http://http.kali.org/kali kali-rolling/main amd64 docker-cl amd64 27.5.1+dfsg4-1 [7,650 kB]
Get:9 http://kali.download/kali kali-rolling/main amd64 libintlx-perl all 1.35-1 [699 kB]
Get:10 http://kali.download/kali kali-rolling/main amd64 libintlx-s perl all 1.35-1 [15.3 kB]
Get:11 http://kali.download/kali kali-rolling/main amd64 libmodule-find-perl all 0.17-1 [10.7 kB]
Get:12 http://kali.download/kali kali-rolling/main amd64 libproc-processtable-perl amd64 0.637-1 [42.1 kB]
Get:13 http://kali.download/kali kali-rolling/main amd64 libsort-naturally-perl all 1.03-4 [13.1 kB]
Get:14 http://kali.download/kali kali-rolling/main amd64 needrestart all 3.11-1 [68.6 kB]
Get:16 http://kali.download/kali kali-rolling/main amd64 python3-pycrui all 4.2-1 [44.3 kB]
85% [Connecting to kali.mirror.garr.it]■
Check out https://www.kali.org for the latest release of Kali Linux
```

sudo docker run -it kalilinux/kali-rolling /bin/bash

Per avviare un'istanza "usa e getta" di Kali Linux dentro il tuo sistema attuale

```
(kali㉿kali)-[~]
└─$ sudo docker run -it kalilinux/kali-rolling /bin/bash
Unable to find image 'kalilinux/kali-rolling:latest' locally
latest: Pulling from kalilinux/kali-rolling
e92b9ba620f5: Pull complete
Digest: sha256:3b5099ef6913d0fc230dc4e7532bedbea0a5ac44703d03eb4a67ff9cd2d13b73
Status: Downloaded newer image for kalilinux/kali-rolling:latest
└─[root@1a378003ed0b]─[~/]
└─#
```

Docker presenta **configurazioni di default non sicure** che possono portare alla compromissione **totale** del sistema (es. Privilege Escalation). Se non è stato sottoposto a **hardening** specifico, utilizzalo **esclusivamente in ambiente locale** e mai esposto direttamente su Internet.