NextRedOS

"RATKIT"

Version 1.04

MANUALE UTENTE

Hardened Linux Distribution — Made in Europe 🇪🇺

www.nextred.it | info@nextred.it

1. Introduzione

NextRedOS 1.04 "Ratkit" è una distribuzione Linux hardened basata su Debian Trixie, progettata per professionisti della sicurezza informatica, sysadmin, ethical hacker e utenti attenti alla privacy.

Il progetto nasce con una filosofia chiara: European Open Source First. Ogni scelta software privilegia alternative europee e open source, riducendo al minimo la dipendenza da Big Tech americane.

> ⚠ *NextRedOS è destinato a utenti con conoscenze base di Linux. Per assistenza visitare www.nextred.it*

1.1 Requisiti di sistema

Architettura	`x86_64 (amd64)`
RAM minima	`2 GB (4 GB consigliati)`
Spazio disco	`20 GB per installazione`
CPU	`1 GHz o superiore`
Connessione	`Consigliata per aggiornamenti`

1.2 Credenziali Live

Username	`admin`
Password	`live`
Hostname	`nextredos`
Codename	`Ratkit`
Architettura	`amd64`

> ⚠ *Cambiare immediatamente la password dopo l'installazione con il comando: passwd*

2. Installazione

2.1 Creazione USB avviabile

Da Linux — comando raccomandato:

```
sudo dd if=NextRedOS-amd64.hybrid.iso of=/dev/sdX bs=4M status=progress oflag=sync
```

> ⚠️ *Sostituire /dev/sdX con il dispositivo USB corretto. Verificare con: lsblk*

Da Windows — usare Rufus (https://rufus.ie) o Balena Etcher.

2.2 Avvio dal dispositivo USB

- Inserire la USB nel PC
- Riavviare e accedere al BIOS/UEFI (tasto F2, F12, DEL o ESC a seconda del produttore)
- Impostare la USB come primo dispositivo di avvio
- Salvare e riavviare

2.3 Modalità Live

All'avvio selezionare 'NextRedOS Live' dal menu GRUB. Il sistema si avvierà in modalità live senza modificare il disco.

Per avviare l'installazione permanente dal desktop live:

```
sudo debian-installer-launcher
```

2.4 Post-installazione

Dopo l'installazione eseguire i seguenti comandi:

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

> ⚠️ *Impostare una password robusta di almeno 12 caratteri con lettere maiuscole, minuscole, numeri e simboli.*

3. Software Preinstallato

3.1 Browser e Privacy

Software	Origine	Descrizione
LibreWolf 🇪🇺	Europa	Browser hardened basato su Firefox. No telemetria, no tracking, HTTPS-only di default.
FreeTube	Open Source	Player YouTube privacy-focused. Nessun account Google richiesto, nessun tracciamento.

3.2 Comunicazione

Software	Origine	Descrizione
Element 🇬🇧	UK	Client Matrix open source. Chat cifrata, federata e decentralizzata.
Claws Mail 🇫🇷	Francia	Client email leggero e configurabile. Supporto PGP integrato.
Tuba 🇪🇺	Europa	Client Mastodon per il social network decentralizzato e open source.

3.3 VPN e Rete

Software	Origine	Descrizione
Proton VPN 🇨🇭	Svizzera	VPN no-log open source. Piano gratuito disponibile.
Netbird 🇩🇪	Germania	VPN mesh basata su WireGuard. Ideale per home network e accesso remoto.
OpenVPN	Open Source	Client VPN tradizionale per connessioni aziendali.
Tor	Open Source	Rete di anonimizzazione. Alias: torstart, torstop, torstatus.

3.4 Password e Sicurezza

Software	Origine	Descrizione
KeePassXC 🇩🇪	Germania	Password manager offline. Database cifrato con AES-256.
Goldwarden	Open Source	Client Bitwarden/Vaultwarden per sync cloud con server self-hosted.

3.5 Produttività

Software	Origine	Descrizione
LibreOffice 🇩🇪	Germania	Suite office completa: Writer, Calc, Impress, Draw.
Nextcloud 🇩🇪	Germania	Client cloud per sincronizzazione file con server Nextcloud self-hosted.
GIMP 🇪🇺	Europa	Editor grafico professionale open source.
Inkscape 🇪🇺	Europa	Editor grafica vettoriale SVG.
Kdenlive 🇪🇺	Europa	Editor video non-lineare professionale.
VLC 🇫🇷	Francia	Media player universale che supporta tutti i formati.
CoMaps	Open Source	Navigazione basata su OpenStreetMap. Funziona offline.
Flameshot	Open Source	Screenshot avanzato con annotazioni e selezione area.
Timeshift	Open Source	Snapshot del sistema per rollback in caso di problemi.

4. Funzionalità di Sicurezza

4.1 Firewall UFW

UFW è attivo con policy deny in/out per default. Solo le porte essenziali sono aperte.

Comandi utili:

```
firewall          # stato firewall (alias)
sudo ufw status verbose    # stato dettagliato
sudo ufw allow out 8123/tcp  # esempio: apri porta HA
sudo ufw deny in 22/tcp      # esempio: blocca SSH
```

4.2 AppArmor

AppArmor è attivo in modalità enforce su tutti i profili disponibili.

```
apparmor-status           # stato AppArmor (alias)
sudo aa-status            # dettaglio completo
sudo aa-enforce /etc/apparmor.d/*  # enforce tutti i profili
```

4.3 Tor e ProxyChains

Tor è preinstallato e configurato. ProxyChains instrada il traffico attraverso Tor.

```
torstart          # avvia Tor (alias)
torstop           # ferma Tor (alias)
torstatus         # stato Tor (alias)
proxychains4 firefox  # avvia Firefox via Tor
torscan           # scansione via Tor (alias)
```

4.4 Audit e Monitoraggio

```
auditlog          # visualizza log audit (alias)
checkrootkit      # scansione rootkit (alias)
lynis-scan        # audit completo sistema (alias)
clamcheck         # scansione antivirus (alias)
connections       # connessioni attive (alias)
netmon            # monitoraggio rete (alias)
```

4.5 USBGuard

USBGuard è installato per il controllo dei dispositivi USB. Va abilitato manualmente dopo aver generato la policy:

```
sudo usbguard generate-policy > /etc/usbguard/rules.conf
sudo systemctl enable --now usbguard
```

Comandi utili:

```
usblist           # lista dispositivi USB (alias)
```

```
usballow          # autorizza dispositivo (alias)
usbblock          # blocca dispositivo (alias)
```

> ⚠️ *Generare la policy con i dispositivi USB desiderati già collegati, altrimenti verranno bloccati.*

5. Home Assistant

Home Assistant Container è preinstallato via Podman e pronto all'uso.

5.1 Avvio rapido

```
hastart           # avvia Home Assistant
```

Oppure manualmente:

```
cd ~/homeassistant
podman-compose up -d
```

Accesso all'interfaccia web:

```
http://localhost:8123
```

5.2 Alias disponibili

hastart	Avvia Home Assistant
hastop	Ferma Home Assistant
halogs	Visualizza log in tempo reale
hastatus	Stato del container
haupdate	Aggiorna all'ultima versione

5.3 Configurazione

I file di configurazione si trovano in:

```
~/homeassistant/config/
```

Il file docker-compose.yml si trova in:

```
~/homeassistant/docker-compose.yml
```

> ⚠️ *Home Assistant richiede una connessione internet al primo avvio per scaricare l'immagine del container.*

6. VPN e Privacy

6.1 Proton VPN

Proton VPN è preinstallato con client grafico. Per avviarlo:

```
protonvpn-app
```

Creare un account gratuito su https://protonvpn.com per accedere ai server VPN.

6.2 Netbird (VPN Mesh)

Netbird è ideale per connettere dispositivi in una rete privata sicura. Comandi:

```
nbup              # connetti a Netbird (alias)
nbdown            # disconnetti (alias)
nbstatus          # stato connessione (alias)
```

Per configurare Netbird creare un account su https://app.netbird.io

6.3 MAC Address Randomization

Il MAC address viene randomizzato automaticamente su tutte le interfacce di rete ad ogni avvio. Nessuna configurazione richiesta.

7. Aggiornamenti

7.1 Aggiornamento sistema

Per aggiornare tutti i pacchetti del sistema:

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

> ⚠️ *Eseguire regolarmente per mantenere il sistema sicuro e aggiornato.*

7.2 Aggiornamento da NextRedOS 1.0

Per gli utenti che hanno NextRedOS 1.0 installato, è disponibile uno script di aggiornamento ufficiale:

```
wget https://www.nextred.it/web/NROS/nextredos-update.sh
chmod +x nextredos-update.sh
sudo ./nextredos-update.sh
```

Lo script eseguirà automaticamente:

- Backup della home directory
- Aggiornamento pacchetti base
- Installazione nuovi software 1.04
- Applicazione nuove configurazioni hardening
- Verifica finale del sistema

> ⚠️ *Lo script di aggiornamento è destinato a utenti esperti. Si raccomanda di eseguire un backup completo prima di procedere.*

8. Verifica Integrità ISO

Ogni release di NextRedOS è firmata con chiave GPG RSA 4096-bit. Verificare sempre l'autenticità prima di installare.

8.1 Verifica GPG

```
gpg --import NextRedOS-public-key.asc
gpg --verify NextRedOS-amd64.hybrid.iso.asc NextRedOS-amd64.hybrid.iso
```

8.2 Verifica SHA256

```
sha256sum -c NextRedOS-amd64.hybrid.iso.sha256
```

9. Supporto e Contatti

Sito web	`https://www.nextred.it/web/`
Email	`info@nextred.it`
GitHub	`https://github.com/nextredos/NextRedOS`
Codeberg	`https://codeberg.org/nextredos/NextRedOS`
Download	`https://www.nextred.it/web/nextredos`

> ⚠️ *Per segnalare bug o problemi aprire una issue su GitHub o Codeberg.*

NextRedOS 1.04 "Ratkit" — Simple by design. Secure by default.