INSTALLATION

Installation guide Linux

install_linux.sh, rights for nmap and the network helper, self-test, storage locations, update and uninstall.

1 Requirements

- Linux x86_64: Debian 12, Ubuntu 22.04/24.04 or newer, Fedora 39 or newer (Python 3.10 or newer); graphical desktop session.
- Administrator rights (sudo) for the setup, internet access for packages and pip, approx. 700 MB of free disk space.
- nmap comes from the distribution's package sources; the script installs it.
- For the new PDF reports: Chromium, Google Chrome or Microsoft Edge (Ubuntu: `sudo snap install chromium` or Chrome as .deb).

2 Set up

Extract the package as root to `/opt/otscan3` (the program folder must be owned by root):

```
sudo mkdir -p /opt/otscan3
sudo tar -xzf OTScan3_3.0.0_Linux.tar.gz -C /opt/otscan3 --strip-components=1
cd /opt/otscan3
sudo ./install_linux.sh --adapter "<scan-adapter>" <username>
```

- `<scan-adapter>`: the network adapter that OTScan 3 may reconfigure for scans (e.g. a USB adapter). List adapters: `ip -br link`. Do **not** release the adapter of the office network. Routed networks only: `--adapter ""`.
- `<username>`: the normal user who starts OTScan 3.
- Behind a proxy: `sudo env https_proxy=http://<proxy>:<port> ./install_linux.sh …`

The script

- installs nmap, Python with Tk, ip/arping, cron, xdg-open, Chromium (PDF reports), secret-tool (camera passwords) and fonts,
- creates the Python environment `./venv` (openpyxl, python-pptx, Pillow, fpdf2, lxml, pandas),
- creates the group `otscan3` and adds the user to it,
- grants nmap the capability `cap_net_raw` for members of this group only (SYN, UDP and ARP scans without root),
- installs the OT scripts (NSE: S7, Modbus, BACnet, PROFINET, OPC UA, CODESYS, Rexroth, Janitza, ONVIF …) for nmap,
- installs the network helper and a sudo rule that allows only this helper and only for the released adapters,
- creates the start menu entry **OTScan 3** and checks Python, nmap rights and the PDF browser.

> Afterwards log out and log in again once – only then does the group `otscan3` apply. For a first test without logging out: `sg otscan3 -c /opt/otscan3/otscan3.sh` (without `sg`: `su <user> -c …`).

3 Start and check

1. Start menu → **OTScan 3** or `/opt/otscan3/otscan3.sh`. First start as under Windows: language, license, setup wizard.
2. Self-test as a normal user: `./selbsttest.sh` in the program folder (via SSH: `xvfb-run -a ./selbsttest.sh`). Expected: "... ok, 0 Fehler" (0 errors).
3. Check rights: `getcap "$(readlink -f "$(command -v nmap)")"` → `cap_net_raw=eip`; `id` → group otscan3.

What	Where
Program	`/opt/otscan3` (owned by root)
Database, settings, adapter backups	`~/.local/share/OTScan3`
Reports, inventory, Splunk storage	Documents folder (e.g. `~/Documents` or `~/Dokumente`)
Schedule	the user's crontab
Camera passwords	the user's keyring (secret-tool)
Released adapters	`/etc/otscan3/adapter`

4 Differences from Windows

- Adapters are reconfigured with ip, arping and nmcli (released adapters only). With NetworkManager, OTScan 3 creates its own profile "OTScan 3 <network>"; "Reset" removes it again.
- The Splunk follow-up scan is a shell script `*_nachscan.sh` instead of a .bat file.
- Mail drafts of the initial commissioning are saved as `.eml` files under Documents/OTScan3_Mailentwuerfe – they are never sent.

5 Update and uninstall

```
sudo tar -xzf OTScan3_3.0.0_Linux.tar.gz -C /opt/otscan3 --strip-components=1
cd /opt/otscan3 && sudo ./install_linux.sh --adapter "<scan-adapter>" <username>
```

User data is kept; the script removes obsolete files of earlier versions (PRUEFSUMMEN.txt is the reference).

```
cd /opt/otscan3 && sudo ./uninstall_linux.sh
sudo rm -rf /opt/otscan3
```

`uninstall_linux.sh` removes the sudo rule, the network helper, `/etc/otscan3`, the OT scripts, the special nmap rights, the group and the start menu entries. Reset any adapters that were reconfigured by OTScan 3 beforehand. User data and system packages are kept.

The German `LIESMICH_Linux.txt` in the package contains further details (tested distributions, proxy with own certificate, NetworkManager). The English summary is this guide.