Kickstart 2: SIEM and Log Analysis – SELKS

This material is prepared for use in *SIEM and Log Analysis course* and was prepared by Henrik Kramselund Jereminsen, `xhek@kea.dk` `hkj@zencurity.dk`. It contains the very basic information to get started!

The course had some problems with Elastic stack version 8 – which is updated on multiple fronts, like HTTPS/TLS. This is giving us a lot of headache. The students meet with different obstacles, so this kickstart 2 document is a way out!

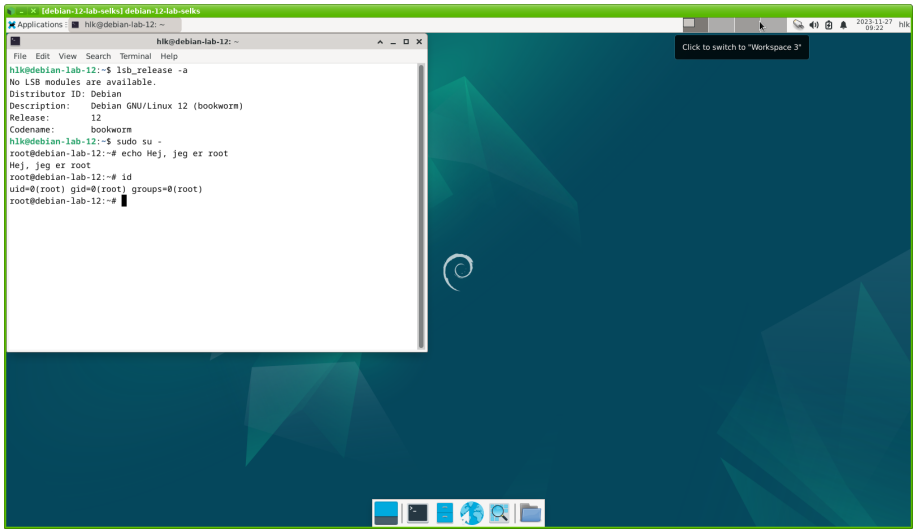
I would like for you to install Docker and try out SELKS `https://www.stamus-networks.com/selks`

If you want to use the same as me with Debian VM, which installs in less than 30minutes:

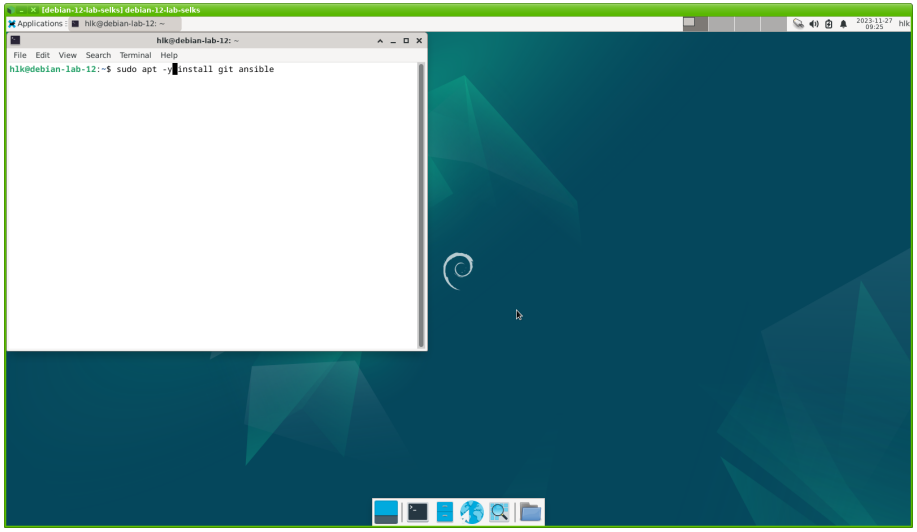
- ☐ Install a basic Debian 12 Bookworm with Sudo configured
- ☐ Install git and Ansible, see our exercise:
  `sudo apt install git ansible`
- ☐ Clone the Github repo: https://github.com/kramse/kramse-labs
  `git clone https://github.com/kramse/kramse-labs`
- ☐ Go into this repository and install Docker, there is a small README.md too:
  `cd kramse-labs/docker-install` and then `ansible-playbook 1-dependencies.yml`
- ☐ Enable Docker: `systemctl enable docker` and reboot the VM
- ☐ Check docker, `docker run hello-world`
- ☐ Clone the SELKS repository:
  `git clone https://github.com/StamusNetworks/SELKS.git`
- ☐ Go into this and run docker-compose as described in the instructions:
  `https://github.com/StamusNetworks/SELKS/wiki/Docker`
  make sure to select the right network interface, so Suricata can sniff packets I did NOT install Portainer
- ☐ Use a browser to access the platform on `https://127.0.0.1`
- ☐ Relax

This will provide a basic Elasticsearch version 7, with Kibana and Suricata

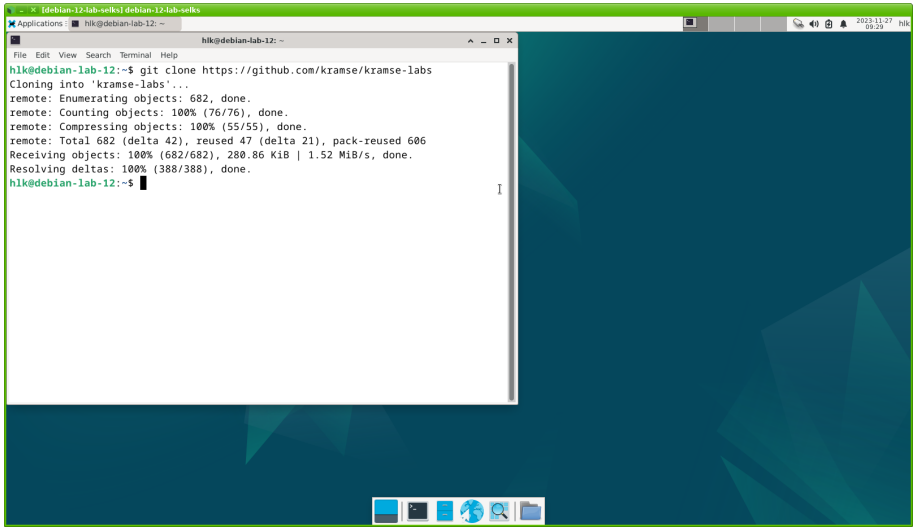
Basic Debian with Sudo:



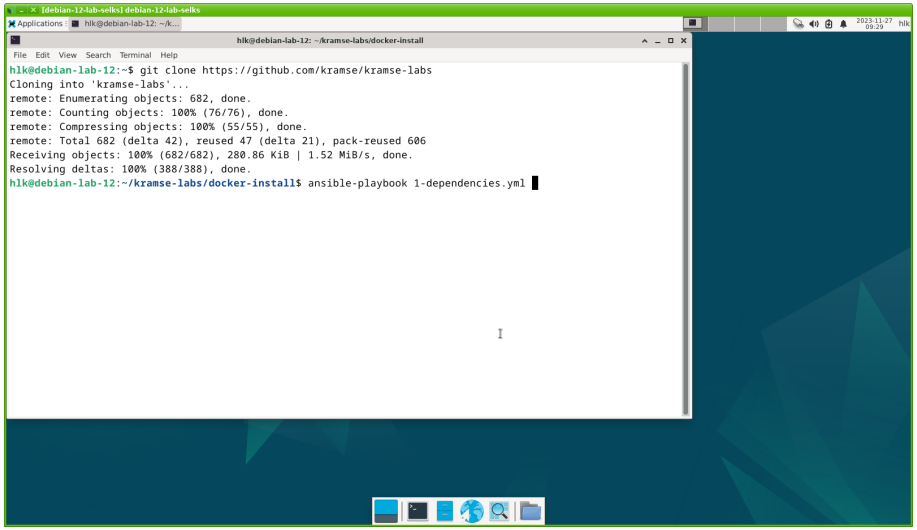
Install git and ansible:



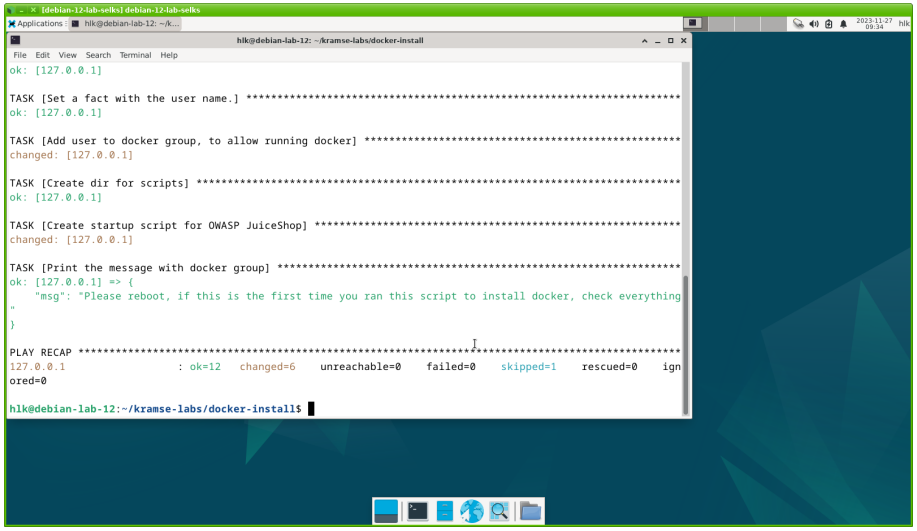
Git clone kramse-labs:



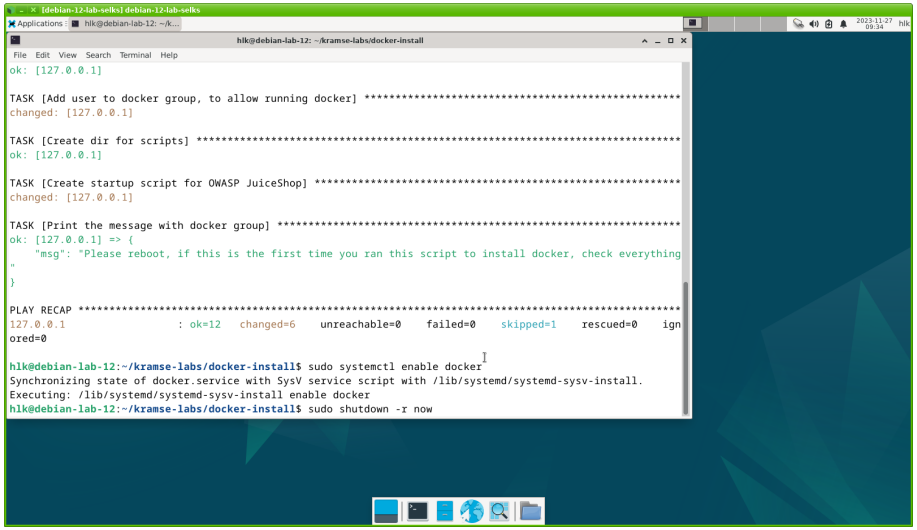
Use Ansible to install Docker:



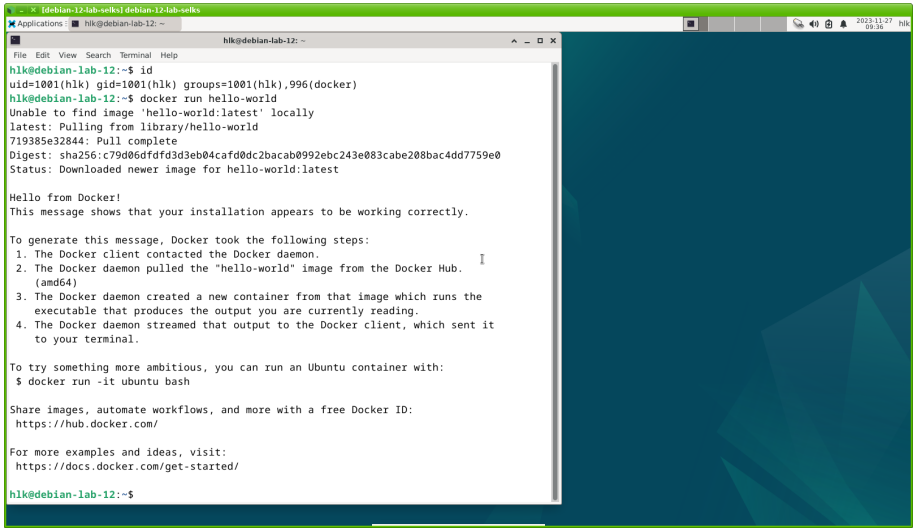
Wait for docker to be installed:



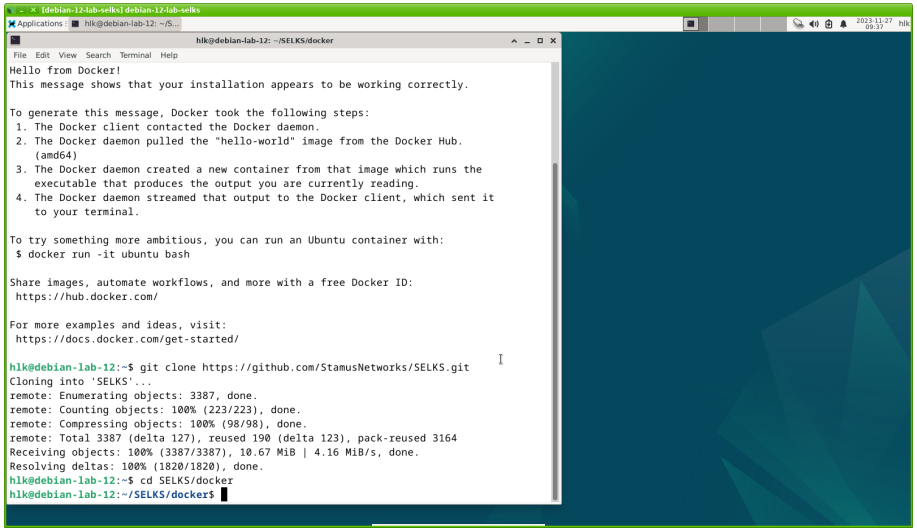
Enable it for reboot and reboot:



Check docker – if it only works for root it is also OK to use that:

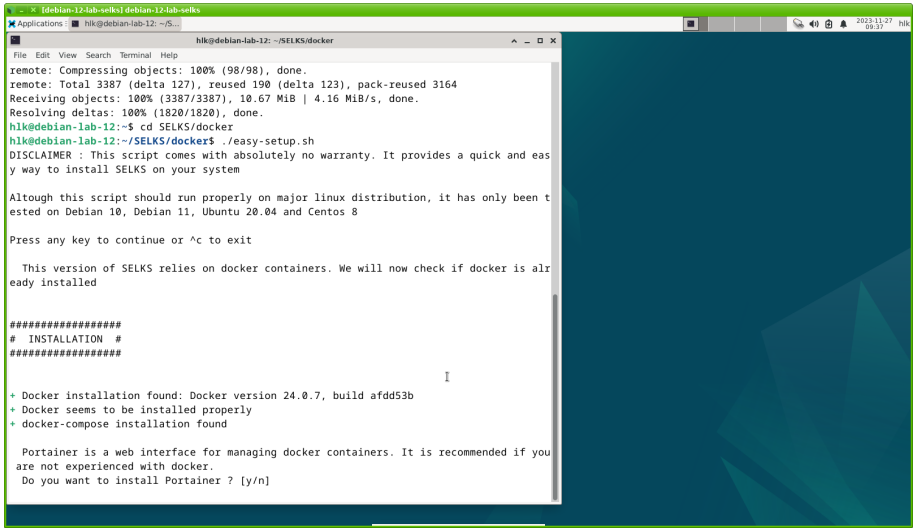


Git clone SELKS repository:

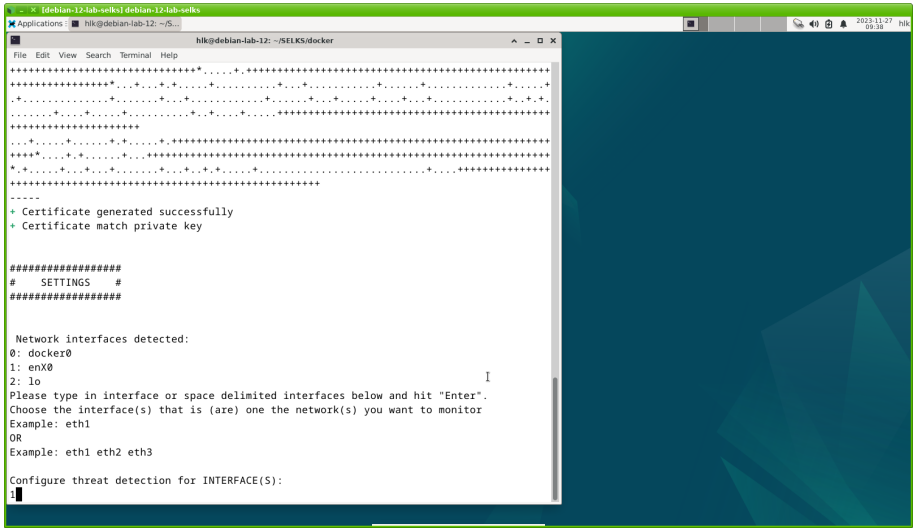


Kickstart 2: SIEM and Log Analysis – SELKS

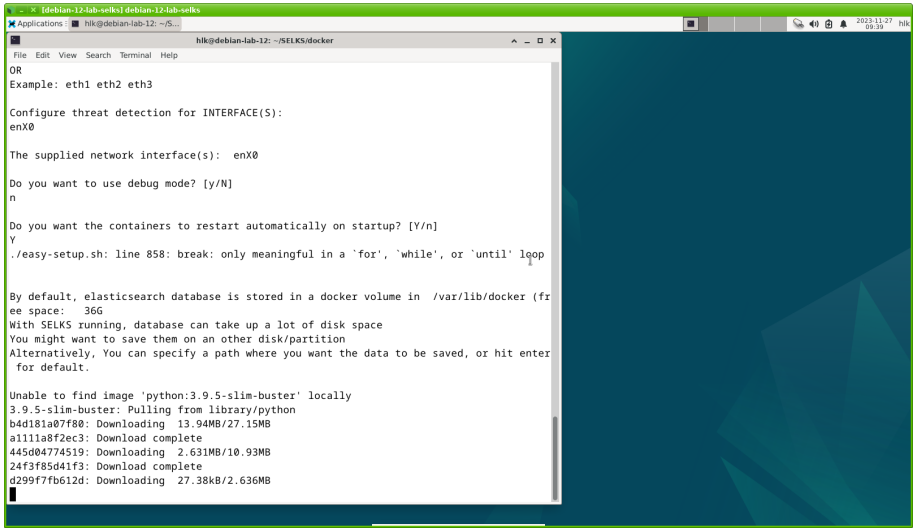
Run the ./easy-setup script:

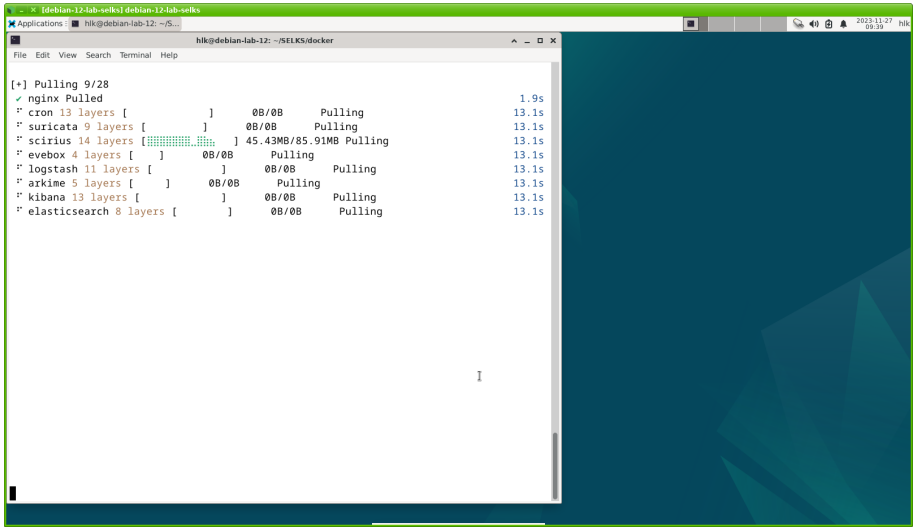


Answer questions about network interface

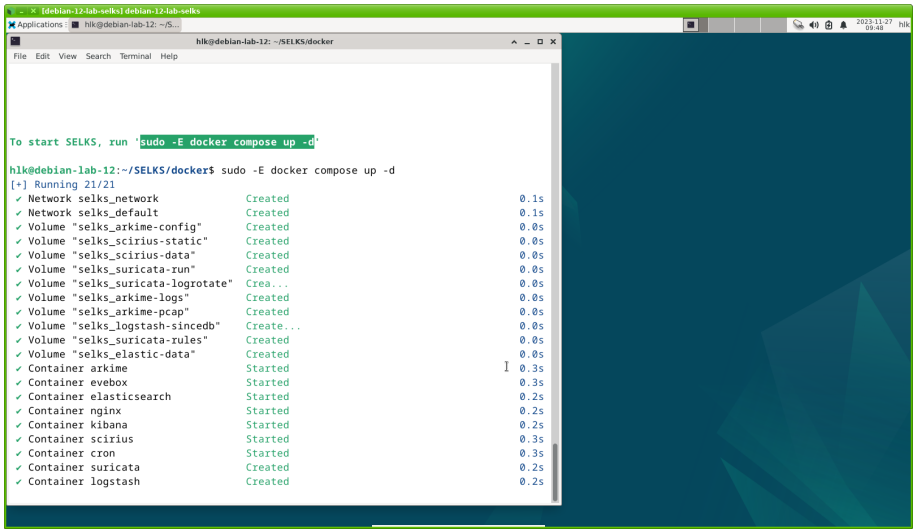


Docker will start fetching the images – took about 5 minutes on 4G router:

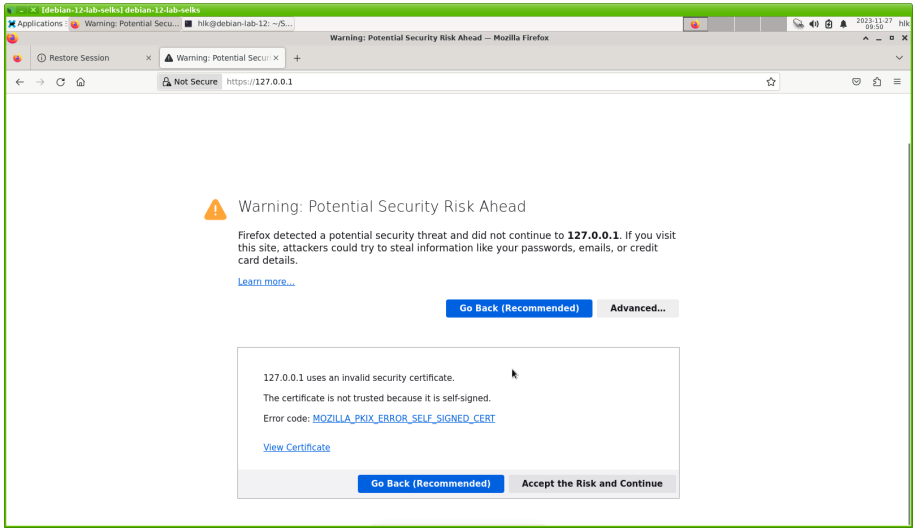




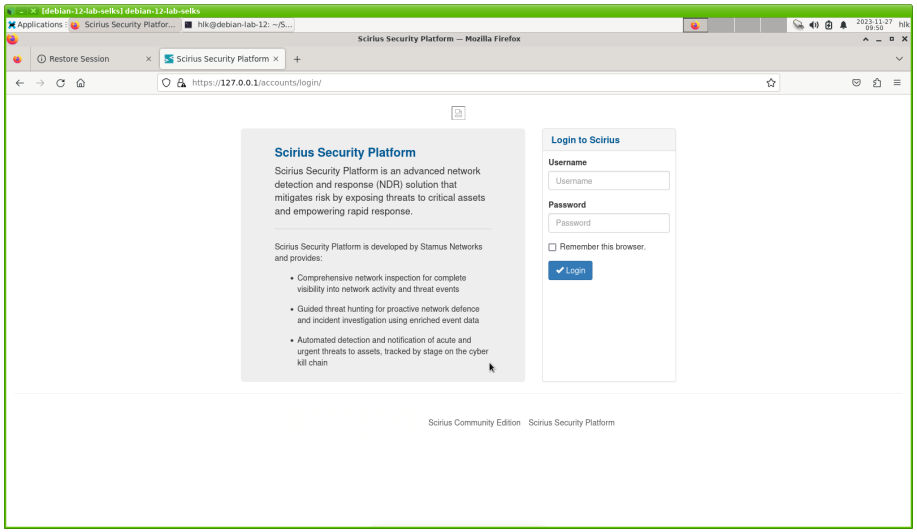
Start the docker containers:



Start a browser and accept the self-signed certificate:



Success – hopefully, login with username: `selks-user` and password: `selks-user`:



After browsing to a few sites::