X33fcon workshop - module 4 advanced configuration

⚡PowerUp Red Team Ops with RedELK⚡

Lorenzo Bernardi
Marc Smeets
May 2023

x33fcon

When Red meets Blue...

OUTFLANK

clear advice with a hacker mindset

Module 4

RedELK configuration

THINGS TO CONFIGURE

Advanced config includes:

- Main config file:
  `mounts/redelk-config/etc/redelk/config.json`
- IP list and other config files:
  `mounts/redelk-config/etc/redelk/*`

MAIN CONFIG FILE

The config file defines:

- General settings
- Enrichment modules – generally no need to modify
- Alarm modules – enable and config to your liking

https://github.com/outflanknl/RedELK/wiki/RedELK-server-installation#Configuration

MAIN CONFIG FILE

The config file defines:

- General settings
- Enrichment modules - generally no need to modify
- Alarm modules - enable and config to your liking.

Few remarks:

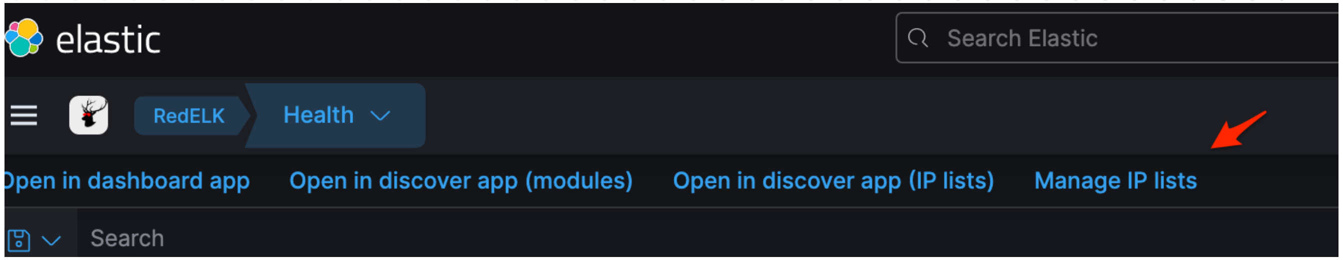
- Use the `project_name` setting
- No `notifications` configured -> no alarms for you
- `alarms` require API kets
- Alarm modules source -> `docker/redelk-base/redelkinstalldata/scripts/module`

https://github.com/outflanknl/RedELK/wiki/RedELK-server-installation#Configuration

IP LIST AND OTHER CONFIG FILES

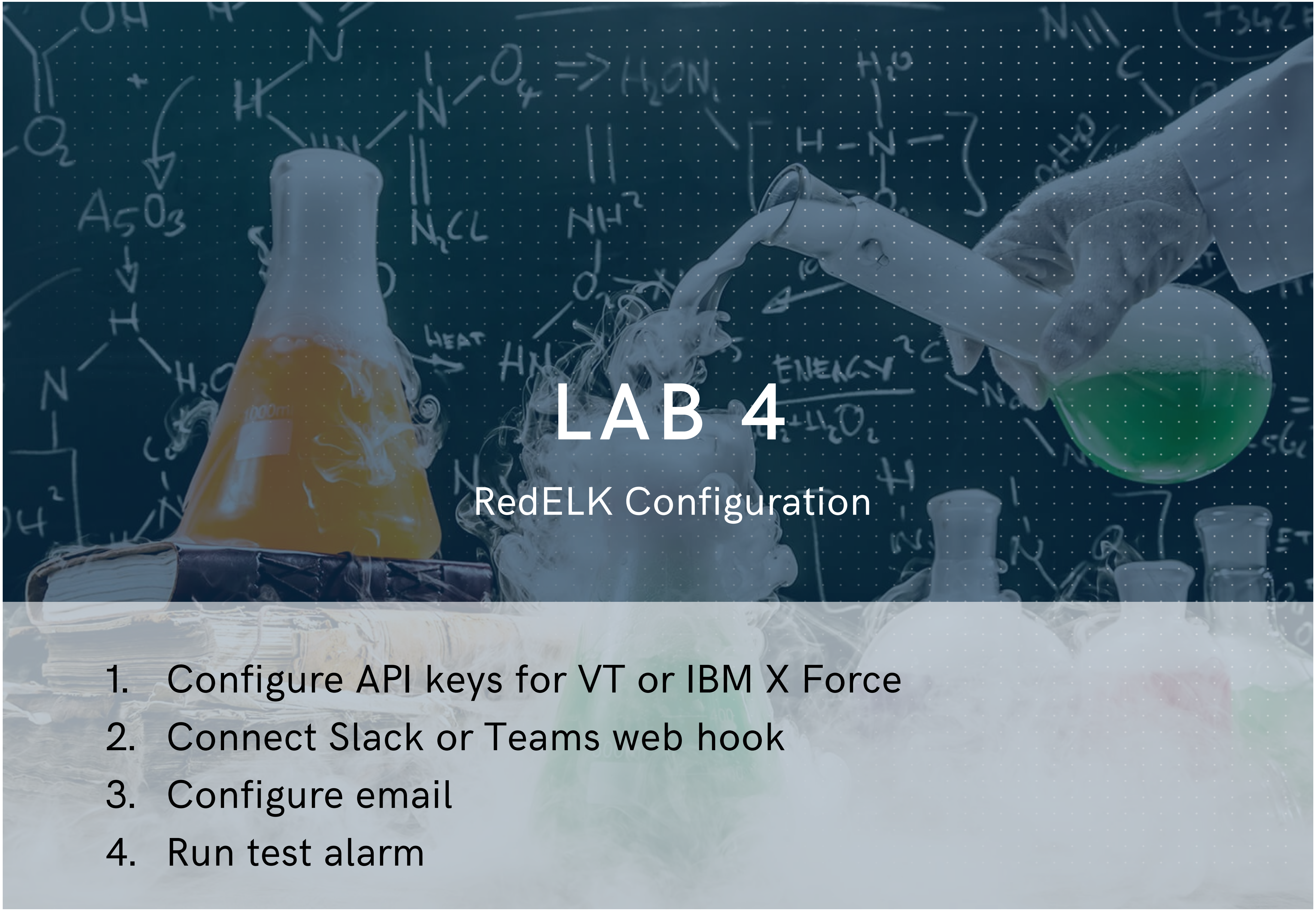
Several files you may want to look at:

- All in `mounts/redelk-config/etc/redelk`
- Replicated to Kibana App



- Define IP addresses you (don't) want to be warned about
- Define domains you want to track classification of
- Define user agents you want to be alarmed about

https://github.com/outflanknl/RedELK/wiki/RedELK-server-installation#Configuration



LAB 4

RedELK Configuration

1. Configure API keys for VT or IBM X Force
2. Connect Slack or Teams web hook
3. Configure email
4. Run test alarm

Lorenzo Bernardi & Marc Smeets

lorenzo@bernardi.be marc@outflank.nl