X33fcon workshop

⚡PowerUp Red Team Ops with RedELK⚡

Lorenzo Bernardi
Marc Smeets
May 2023

x33fcon
When Red meets Blue...

OUTFLANK
clear advice with a hacker mindset

WORKSHOP BASICS

You will:

- Get better understanding of how RedELK 'power ups' your red team ops
- Get better understanding of OPSEC mistakes blue teams make
- Get hands on with RedELK using several exercises
- Play with Outflank's commercial 'Stage 1 C2'
- Play with Cobalt Strike

We aim for:

- Interactive
- Tech in-depth
- Hands-On

ABOUT YOUR SPEAKER

Lorenzo Bernardi - @fastlorenzo

- Loves playing with IT stuff > 20 years
- Leading roles within EY EMEIA/Global
- Broad range of IT knowledge, community contributor and entrepreneur mindset

Marc Smeets - @MarcOverIP

- Infosec class of 1998 (hobby) / 2006 (professionally)
- Part of the Outflank team, prior to that freelancing and KPMG
- Red Team operator, tool builder, trainer, some blue Threat Hunting experience

Workshop basics

WORKSHOP BASICS

Project url – you will need the wiki on there as well
https://github.com/outflanknl/RedELK

Slack workspace for this training
https://redelkworkshop.slack.com

Need a laptop with a browser ☺ chrome/chromium based prefered

Timing and breaks? We'll see.

You can win an Outflank hoodie with a quiz!

RedELK stickers available!

Lab basics

YOUR LAB SETUP

Each student will have the following machines:

- Labmaster: Cobalt Strike client + some useful tools
- Redirector: Haproxy configured
- C2: Cobalt Strike and Stage1 pre-installed and configured
- RedELK: Plain Ubuntu VM
- Target machine: Windows 10, domain joined, target machine

Access via Guacamole: https://access.redelk.rocks

Internal domain name: redelk.lab

Tip: copy hostnames from manual page 3 to a temp text file on your labmaster.

EXPORT CONTROLLED TOOLING

You get access to Export Controlled and copyright protected tools:

- Cobalt Strike
- Outflank Stage 1 C2

You are allowed to:

- Use the tools in the lab

You are not allowed to:

- Copy or otherwise export the tools outside of the lab

Access is monitored.

Violation of rules will result in immediate termination of your lab, as well as future denial of access to this software, or other Fortra software.

GETTING LAB ACCESS

To get access to your lab:

1. Send an email with your full name and nationality to the trainers (marc.smeets@fortra.com & lorenzo.bernardi@be.ey.com)

2. We validate your name with Gov ID

3. We invite that email address to the Slack workspace and a private channel

4. You receive lab access credentials in your private Slack channel

5. You verify access to your lab, and let us know via private Slack channel

RedELK basics

OFFENSIVE INFRA – TYPICAL SETUP FOR 1 OPERATION

Command and Control

- C2-servers (5+)
- Redirectors / reverse proxies (5+)
- Domain fronting CDN (2+)

Fake identities

- Social media profiles (2+)
- Websites (1+)

Tracking

- Tracking pixels (10+)

Delivery

- Web servers (2+)
- Email (2+)
- File sharing service (0+)
- Messaging platforms (0+)
- …

Generic backend components

- Communication channels (2+)
- Test environments (1+)
- Log aggregation (1+)

OFFENSIVE INFRA – TYPICAL CHALLENGES

Oversight

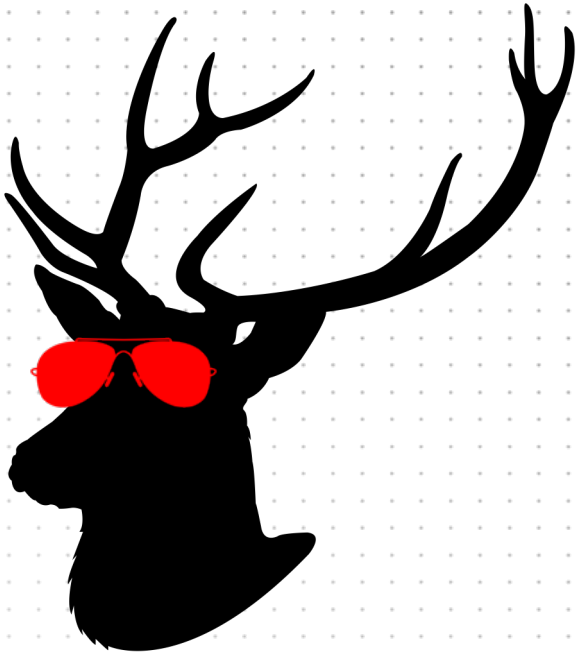
Insight

"Every contact leaves a trace" - Locard's exchange principle

TOOLING -> REDELK

+

=

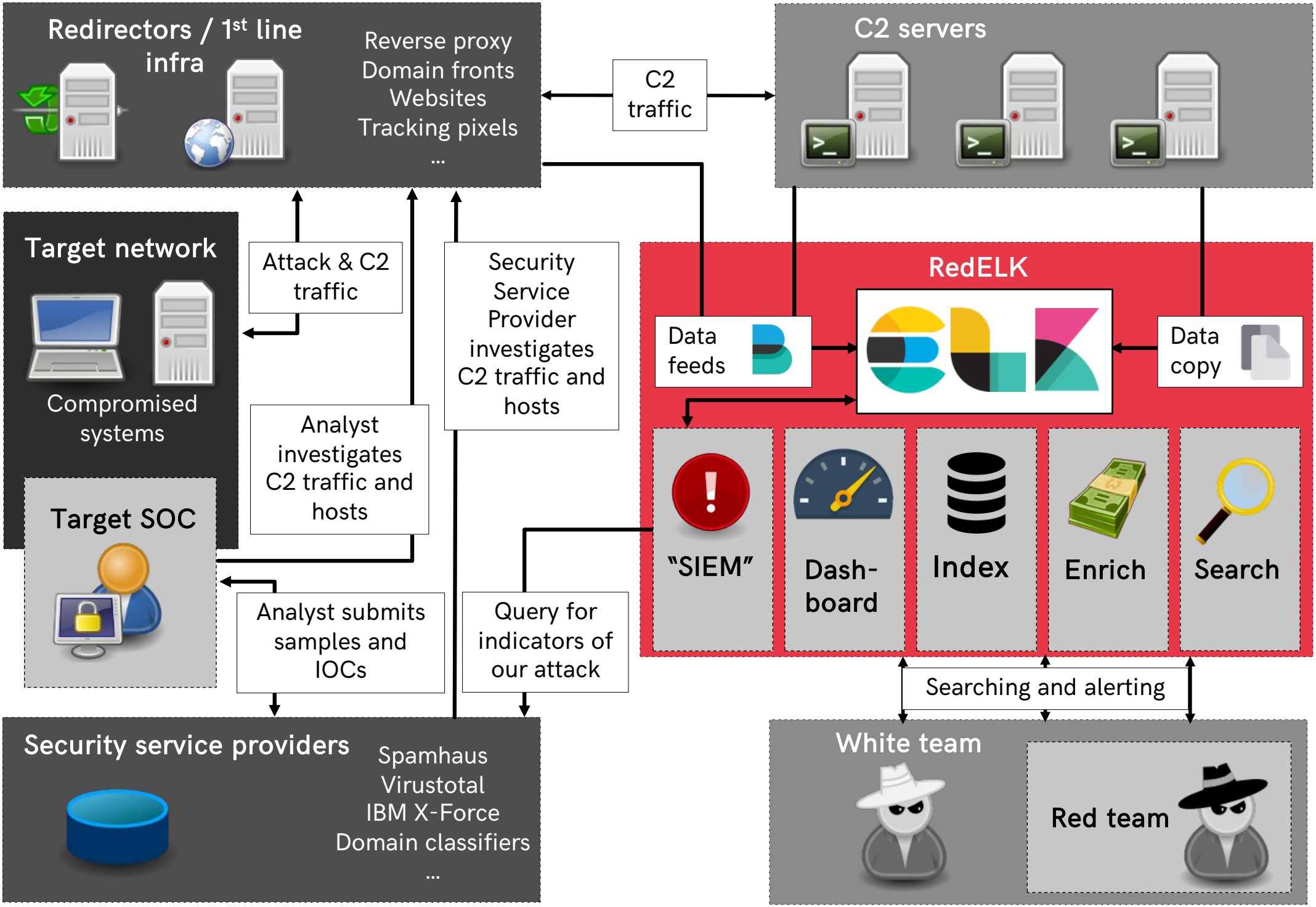


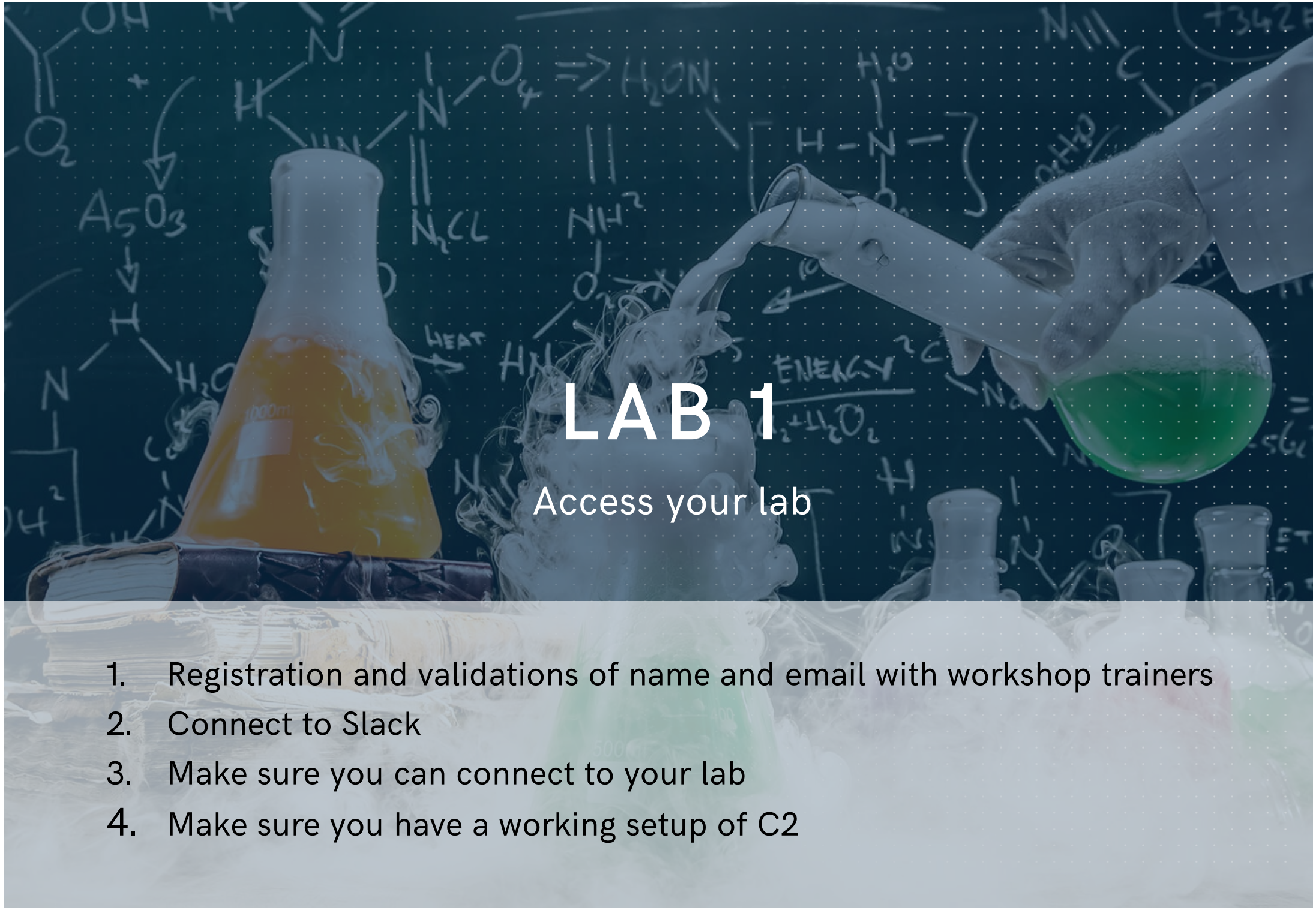
https://github.com/outflanknl/RedELK/

https://outflank.nl/blog/2019/02/14/introducing-redelk-part-1-why-we-need-it/

https://outflank.nl/blog/2020/02/28/redelk-part-2-getting-you-up-and-running/

https://outflank.nl/blog/2020/04/07/redelk-part-3-achieving-operational-oversight/


Redirectors / 1st line infra
Reverse proxy
Domain fronts
Websites
Tracking pixels
...
C2 traffic
C2 servers
Target network
Compromised systems
Attack & C2 traffic
Security Service Provider investigates C2 traffic and hosts
RedELK
Data feeds
Data copy
Target SOC
Analyst investigates C2 traffic and hosts
"SIEM"
Dash-board
Index
Enrich
Search
Analyst submits samples and IOCs
Query for indicators of our attack
Searching and alerting
Security service providers
Spamhaus
Virustotal
IBM X-Force
Domain classifiers
...
White team
Red team



LAB 1

Access your lab

1. Registration and validations of name and email with workshop trainers
2. Connect to Slack
3. Make sure you can connect to your lab
4. Make sure you have a working setup of C2

Lorenzo Bernardi & Marc Smeets

lorenzo@bernardi.be marc@outflank.nl