TU Graz

SCIENCE
PASSION
TECHNOLOGY

Introduction to Attack Defense CTF's

LosFuzzys Beginner Trainings

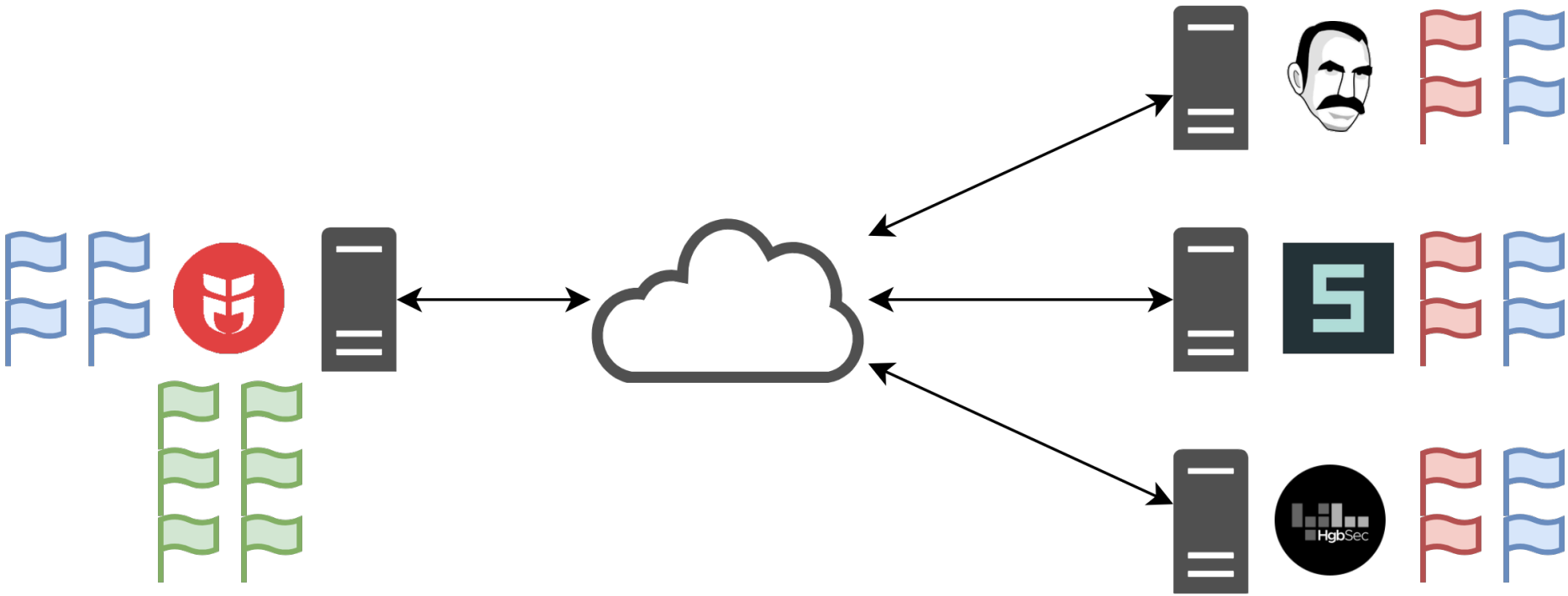
Andreas Samonik

Winter Semester 2025

The Concept

- A CTF where each team attacks and defends simultaneously.
- All teams get an identical VM (Vulnbox) on a shared network.
- Each VM runs custom-built, vulnerable “services.”
- Goal 1 **Attack**: Find exploits and steal flags from other teams.
- Goal 2 **Defend**: Find flaws and patch them before others exploit us.

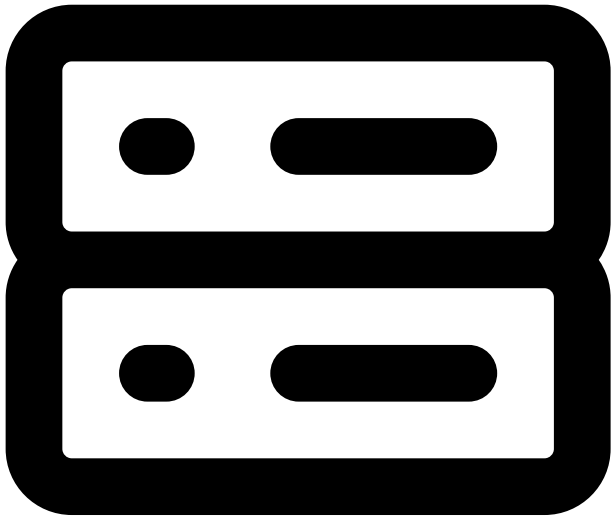
A/D Setup



ansa@losfuzzys.net

What is a “Vulnbox”?

> The “Vulnbox” is the identical Virtual Machine for each team provided by the organizers



- It runs all the vulnerable services
- Connected to the game network
- Needs to be defended

ansa@losfuzzys.net

What is a Service?

> Services are the custom, vulnerable programs we attack and defend

Any **Language**

Services can be in `python`, `go`, `rust`, `java`, `php`, `c`, `fortran`, ...

Any **Vulnerability**

could be `crypto`, `web`, `pwn`, `misc`, or a unique combination.

Should stay **intact**

Must be patched **without** breaking the service.

ansa@losfuzzys.net

Scoring

> Tick based → Happens every 2-3 Minutes

Attack: Points awarded for every flag we steal from opponent's services.

Defense: Points awarded for each round, more if we are **less** exploited by other teams.

SLA: Points awarded for our services being online and passing automated checks. A broken patch loses points

ansa@losfuzzys.net

Tooling

- Network Monitoring: **Tulip**
- Exploit Runner: **LADA**
- Dropping Traffic: **Suricata**
- VPN Connection (e.g. Vulnbox): **Wireguard**

ansa@losfuzzys.net

TULIP

- Monitor Network Traffic
  - Service related ingoing/outgoing traffic
- Filter & Tag flows
  - FlagOut Filter
    - Flags can be base64 encoded to avoid filters
  - Service Filter
- Copy other teams exploits
- Random traffic sent by other teams for confusion

LADA

- Custom A/D central Exploit Runner (@Xer0 [Sebastian])
- LADA and WG guide will be on Saturday **before** SaarCTF

Exploitation v1

(Demo)

Exploitation v1

- Sample service at **bestkebap.at**
- Web beginner training could be useful ;)
- I’ve heard the service uses SQL
- More info: **src.bestkebap.at**

Defending

(Demo)

Defending Time!

- Detect leaked flags via Tulip
- Patch the service
- In a real CTF: Copy the exploit and attack other teams

Exploitation v2

(Demo)

Exploitation v2

- Maybe you already saw it: service is still vulnerable
- Find and exploit this as well
- OR: just wait until someone solves it and copy it ;)

Conclusion

Next Events

- ~~8th Oct: (Training) CTFs~~
- ~~15th Oct: LosOktoberfest~~
- ~~22nd Oct: (Training) Web Security~~
- ~~29th Oct: (Training) Cryptography~~
- ~~5th Nov: (Training) A/D Training~~
- 8th Nov: saarCTF 2025
- : (Training) Binary Exploitation (?)
- 22nd Nov: GlacierCTF 2025

SaarCTF 2025

Saturday, 08.11.2025 @ 13:00

- Be here **early**, we will do the setup together (WireGuard, ...)
- **11:30**, some of us will already be here in the morning

Hepful tools

- Previous SaarCTF services are available (github.com/saarsec/saarctf-2024)
- Wireguard
- Pwntools, requests