

CTF Contests: Hands-On Experience of the IT Security Culture – UE 06: Attack / Defense

Clemens Hlauschek, Daniel Marth, Florian Fankhauser



TJCTF Debriefing



Attack / Defense



Recap: Attack / Defense Mode

- Each team is given the same set of intentionally vulnerable services
- Goals:
 - Exploit vulnerabilities to steal flags from other teams
 - Fix vulnerabilities to avoid other teams stealing flags from you
 - Keep the service functional
- Teams permanently interact with each other
- By definition services need to be network-based
- Example services:
 - Web blog with open registration and comment functionality
 - Command Line Interface (CLI) file storage backed by custom compression

- Updated every round (“tick”)
- Commonly used scoring criteria:
 - Attack: Flags stolen from other teams by you
 - Defense: Flags stolen by other teams from you
 - Service Level Agreement (SLA): Service availability / functionality
- Details vary between events

- “vulnbox”
 - Virtual Machine (VM) containing the vulnerable services
 - One instance per participating team
- Game bot / check system
 - Event organizers connect to the services each tick
 - Legitimate functionality is triggered and checked for correctness
 - Flags are injected into the service
- Flag submission system
 - Submit flags of other teams to earn points

- Download the vulnbox image to your local machine
- Extract information from the (online) vulnbox
- Investigate network traffic (e.g., with Wireshark)
- Game bot interaction might provide crucial insights
- Keep the management sheet up to date!

Found a Vulnerability?

- Exploit it manually and submit a flag to verify correctness (and possibly claim first blood)
- Automate the exploitation and flag submission
- Fix the vulnerability in our own service

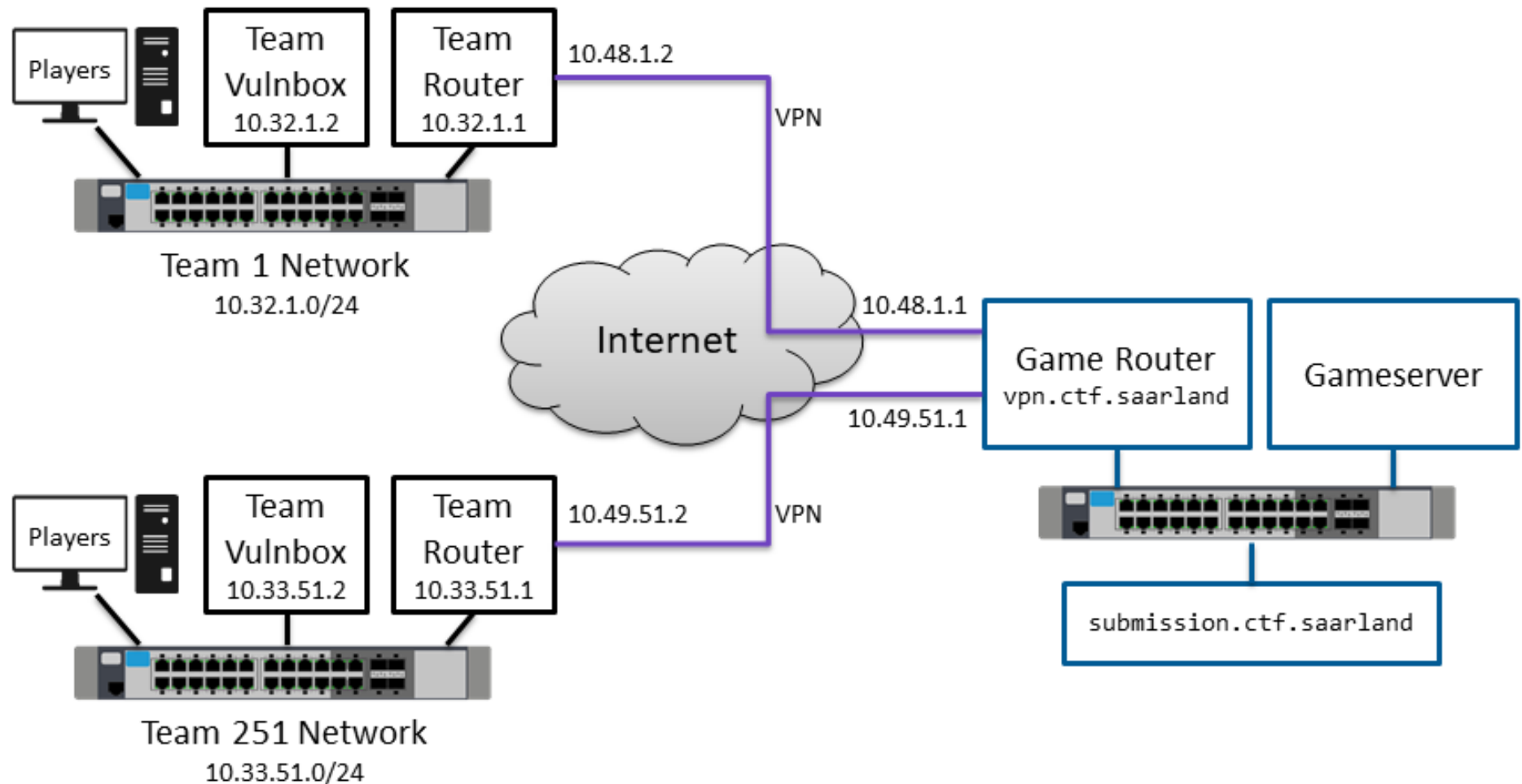
Upcoming Event: saarCTF



- <https://ctf.saarland/>
- 20 May 2022, 16:00 - Sat, 21 May 2022, 01:00
- Submit your writeup in TUWEL until 10 June 2022, 23:55
- Organizers will use Internet Relay Chat (IRC) for communication
- We will meet 20 May at 15:30 in the INSO library
 - Wiedner Hauptstraße 76, staircase 2, 2nd floor
 - Located inside the “Galerie Wieden”
 - <https://www.inso.tuwien.ac.at/index.html#office>

- We will use the cloud-hosted setup of saarCTF
- Participants connect to the game network via Virtual Private Network (VPN)
 - We will provide the team-specific OpenVPN configuration as soon as it is available
 - Reserve some setup time!

Network Structure (self-hosted)



(See <https://ctf.saarland/setup>)

Network Ranges

- Team ID: 66
- Game network: 10.32.0.0 - 10.33.255.255
- Team network: 10.32.66.0
- Router address: 10.32.66.1
- Vulnbox address: 10.32.66.2
- Network testbox address: 10.32.66.3

(See <https://ctf.saarland/setup>)

Ticks, Flags & Scoring

- Network will be closed during the first hour of the competition (preparation time)
- A tick takes 2-3 minutes
- Flags are valid for 10 ticks
- Flag format: SAAR\{ [A-Za-z0-9-_] {32} \}
- Scoring:
 - Attack
 - Defense
 - SLA

(See <https://ctf.saarland/rules>)

Flag Submission

- `submission.ctf.saarland` on port 31337 over Transmission Control Protocol (TCP)
- One flag per line
- Responses:
 - [OK]: Flag accepted
 - [ERR]: Flag permanently invalid
 - [OFFLINE]: Submission currently disabled (preparation time)

(See <https://ctf.saarland/setup>)

Thank you!

<https://security.inso.tuwien.ac.at/ctf-2022s/>

