HOW TO ORGANIZE A CTF

STEPHAN AND STEAN

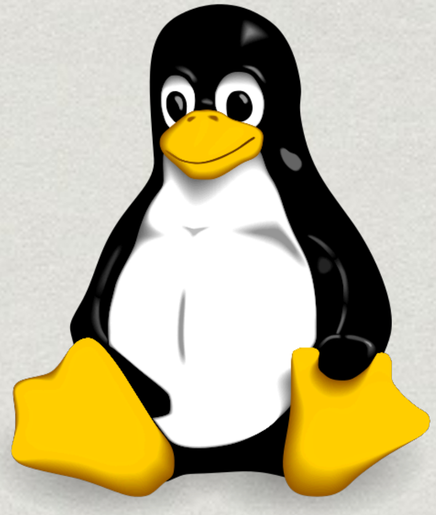
Agenda

- What is a CTF?
- Why should you organize one?
- What kinds of CTFs exist?
- Ingredients
- Challenge-Design
- DOs and DON'Ts
- Q&A

Who are we?

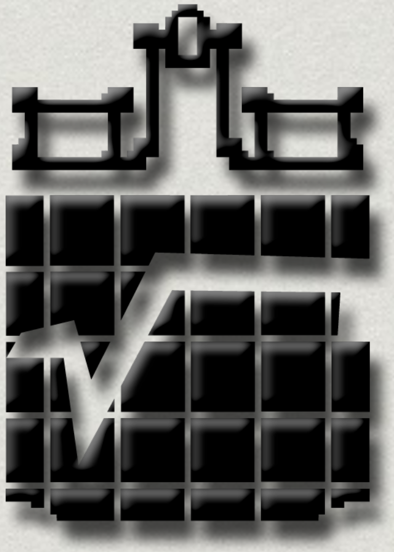
Squares

+



root

=



Squareroots

- CTF Team - University of Mannheim
- Playing CTFs since 2006
- Organized 2 public and 2 newbie CTFs per year

What is a CTF?

- CTF = Capture the Flag
- information security competition
- Goal: Get as many flags as possible
- example for flags:
  e303640fbc9aa49a840b6ea77fdb1086
  ctf{this_is_an_example_for_a_flag}

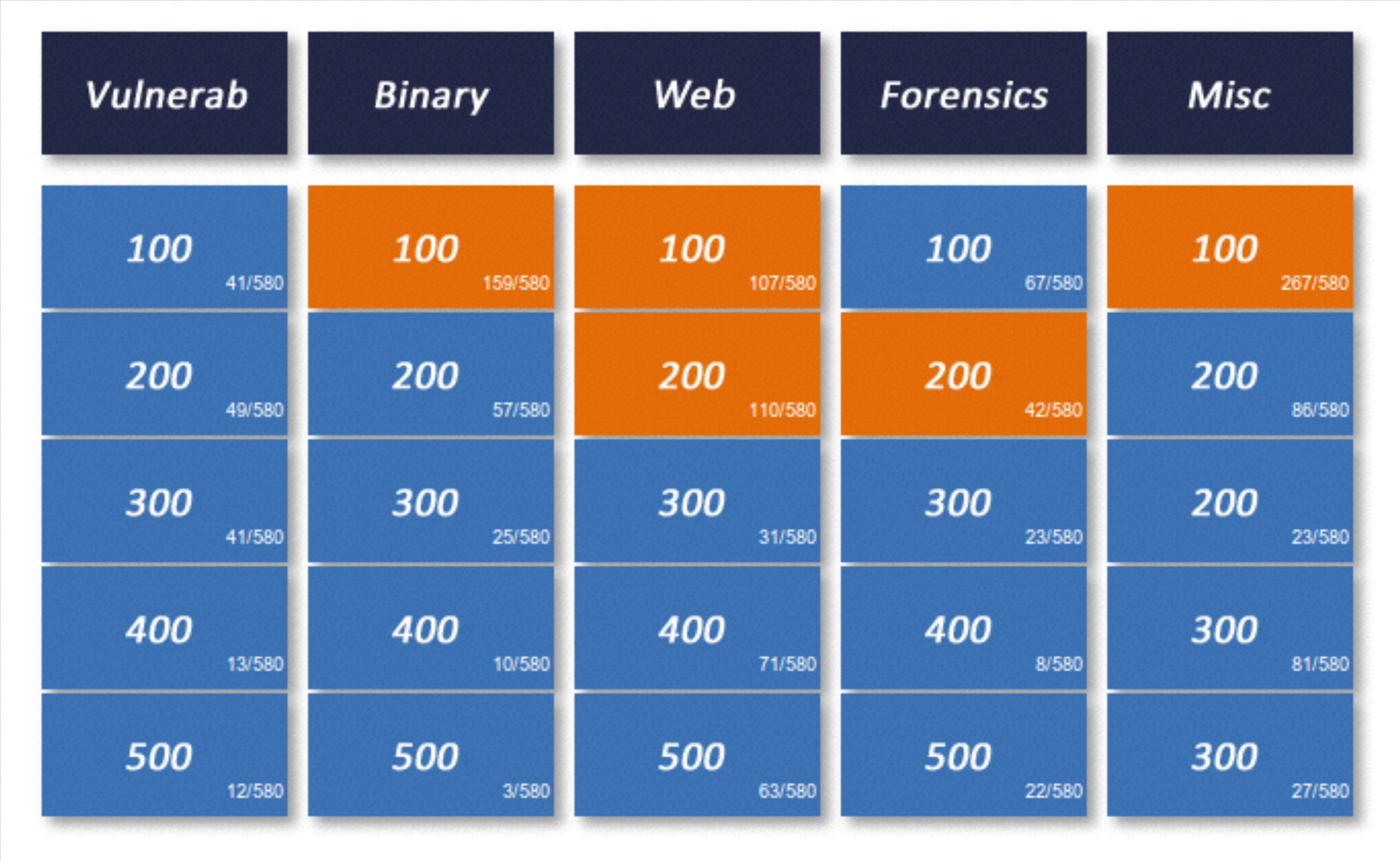
Classic kinds of CTFs

- Challenge-based
- Server-based
- mixed

Challenge-based/ Jeopardy-style

- Challenges from all over infosec:
  - Reversing
  - Trivia
  - Crypto
  - Programming
  - …
- Each solved Challenge yields a flag
- Challenges are usually arranged as Jeopardy-Overview
- Time frame: days
- Example: DEF CON CTF Qualifier, PlaidCTF

Challenge-based/ Jeopardy-style



Vulnerab	Binary	Web	Forensics	Misc
100 41/580	100 159/580	100 107/580	100 67/580	100 267/580
200 49/580	200 57/580	200 110/580	200 42/580	200 86/580
300 41/580	300 25/580	300 31/580	300 23/580	200 23/580
400 13/580	400 10/580	400 71/580	400 8/580	300 81/580
500 12/580	500 3/580	500 63/580	500 22/580	300 27/580

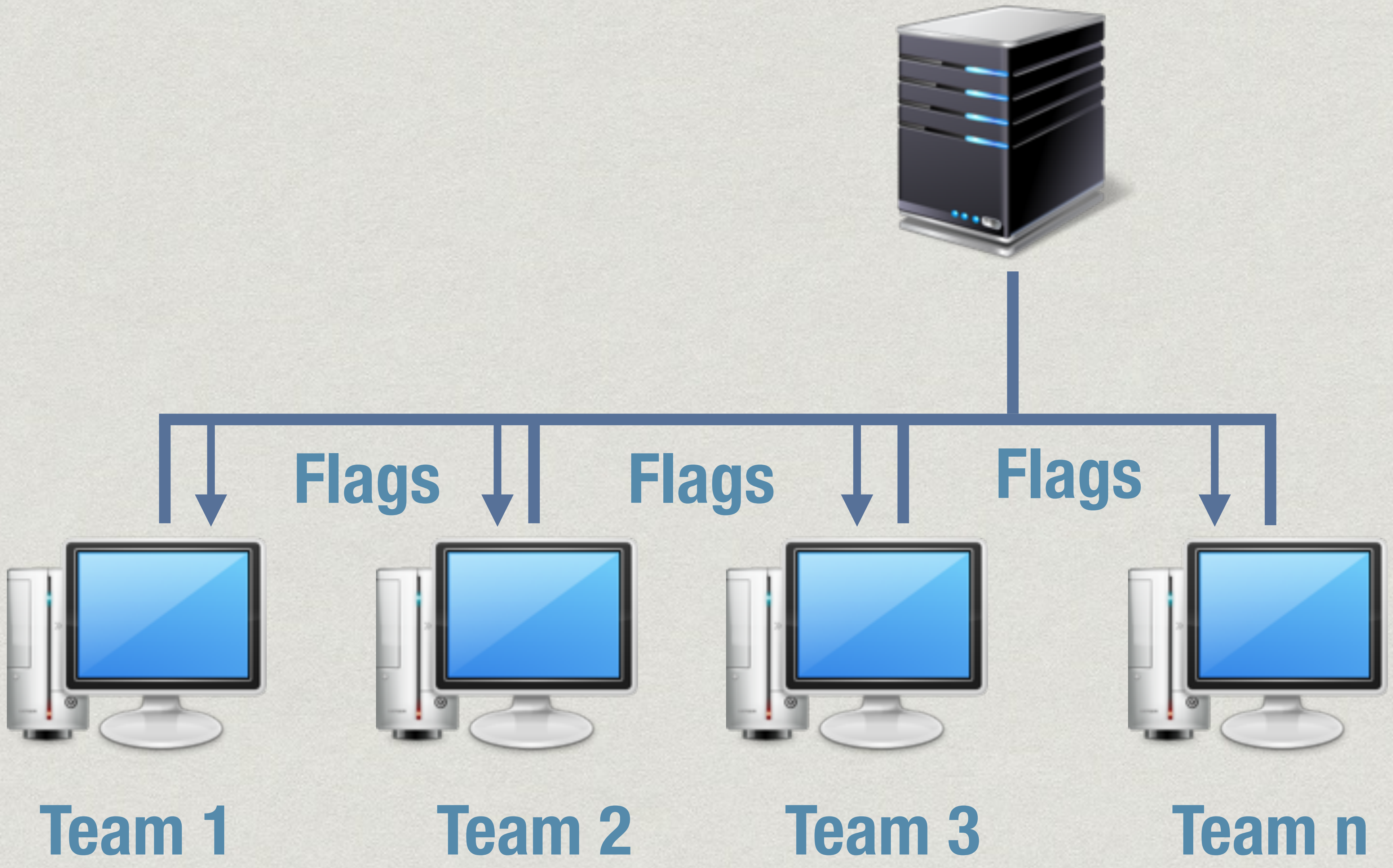
Source: Codegate CTF 2013

Server-based/Attack-Defense

- *fight other teams and protect yourself*
- One network, one VM image, several vulnerabilities
- Time frame: hours
- Example: ruCTF, iCTF

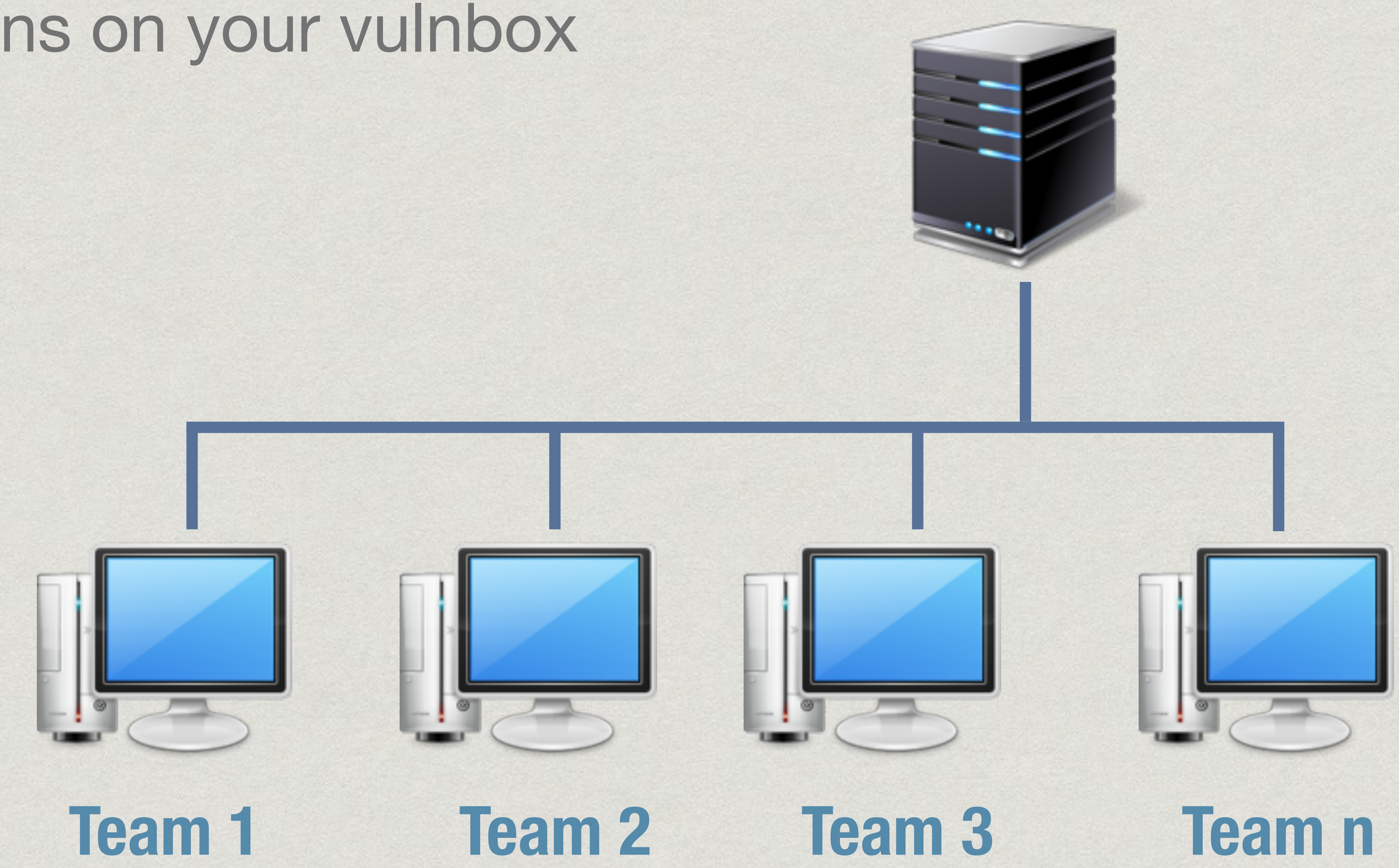
Server-based/Attack-Defense

1. Keep your services up for the game server



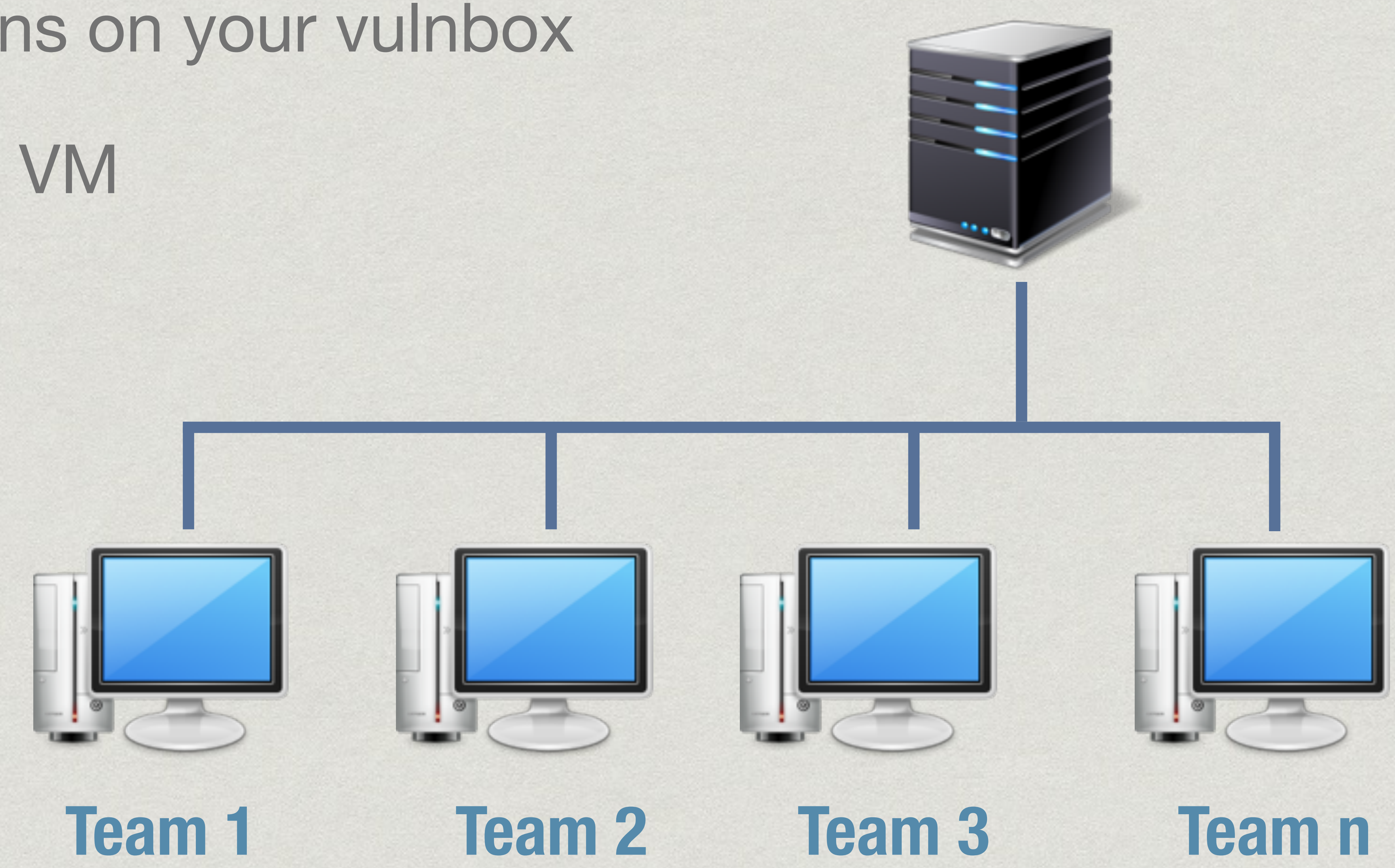
Server-based/Attack-Defense

1. Keep your services up for the game server
2. Find vulns on your vulnbox



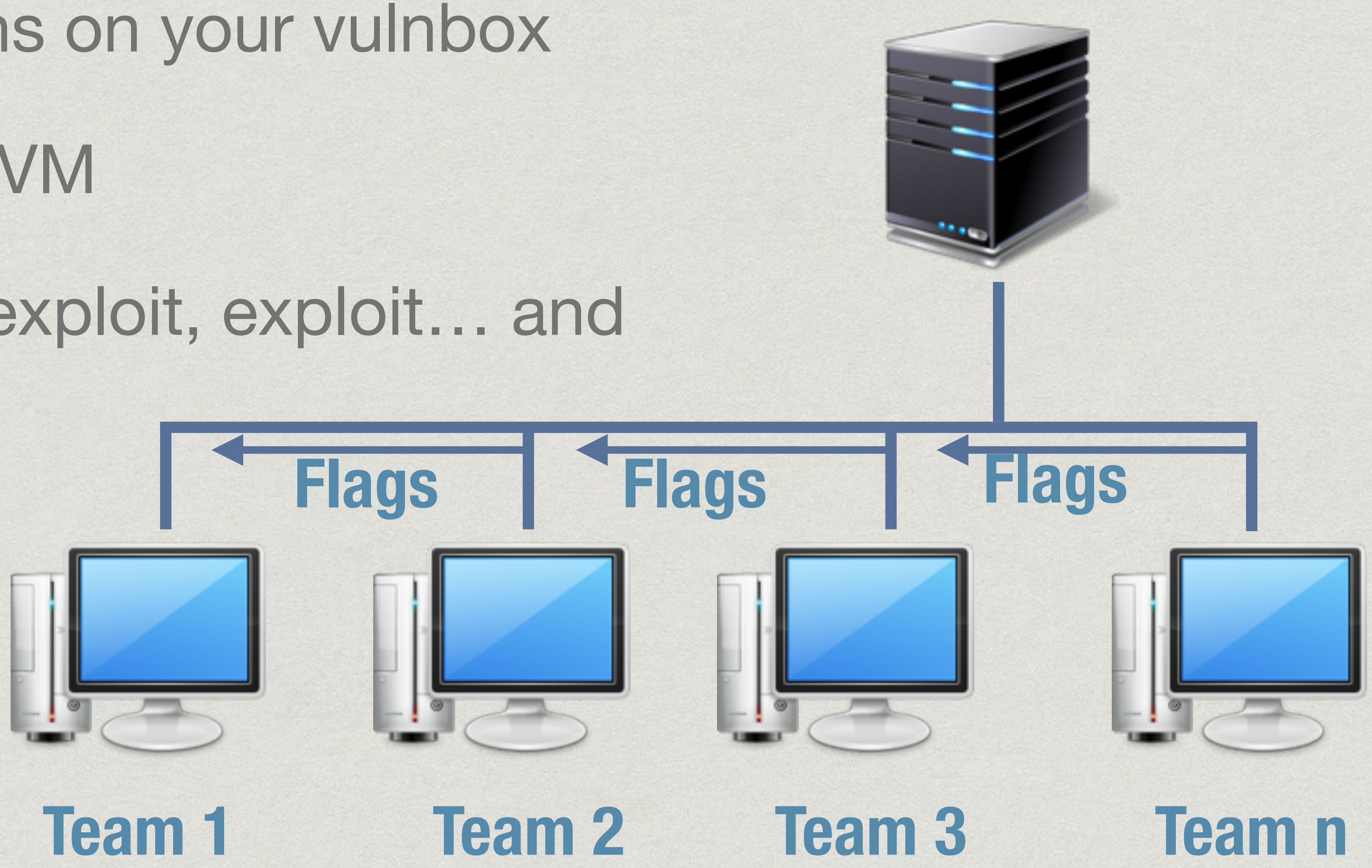
Server-based/Attack-Defense

1. Keep your services up for the game server
2. Find vulns on your vulnbox
3. Fix your VM



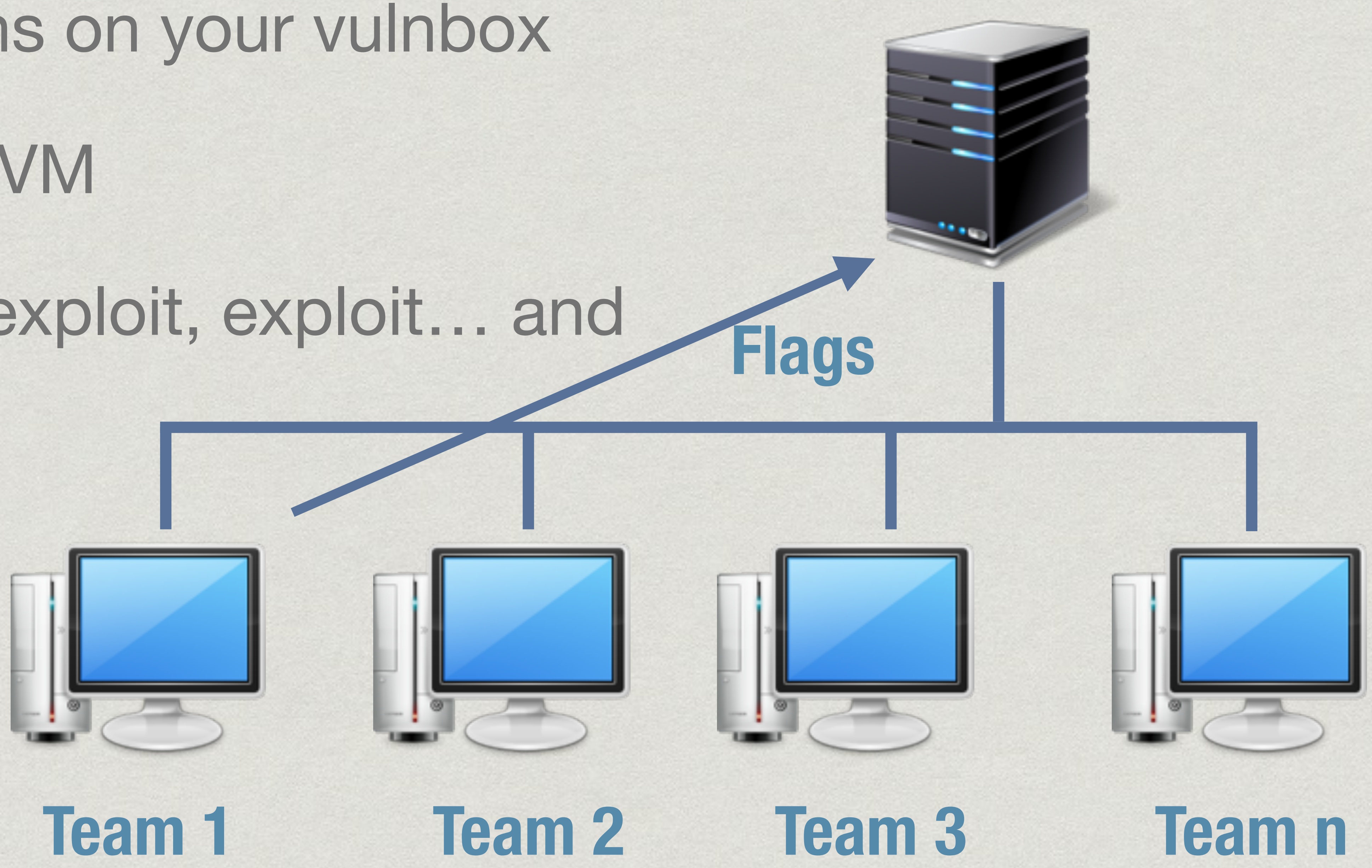
Server-based/Attack-Defense

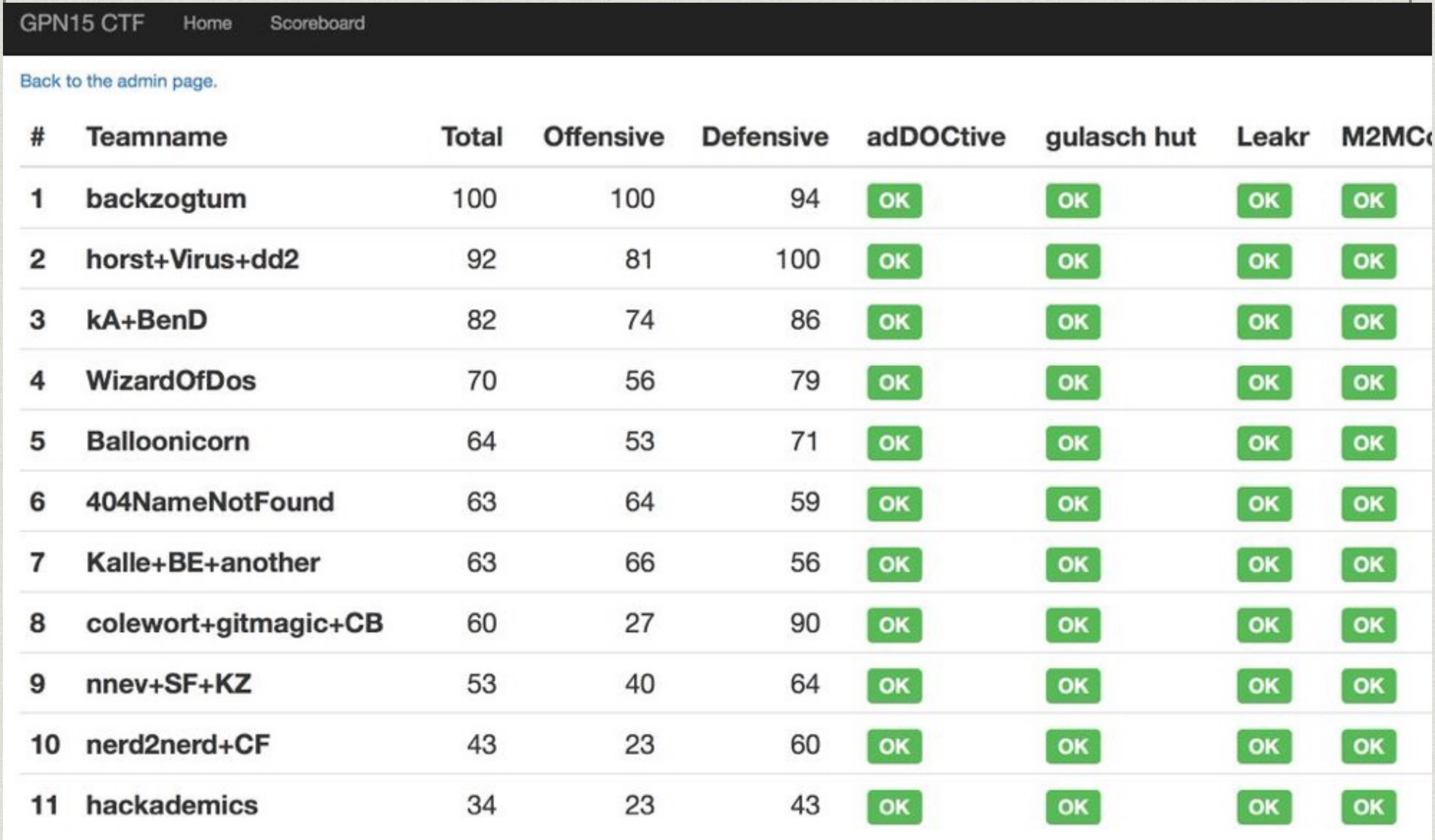
1. Keep your services up for the game server
2. Find vulns on your vulnbox
3. Fix your VM
4. Exploit, exploit, exploit… and get flags



Server-based/Attack-Defense

1. Keep your services up for the game server
2. Find vulns on your vulnbox
3. Fix your VM
4. Exploit, exploit, exploit… and get flags





GPN15 CTF Home Scoreboard

Back to the admin page.

#	Teamname	Total	Offensive	Defensive	adDOCtive	gulasch hut	Leakr	M2MC
1	backzogtum	100	100	94	OK	OK	OK	OK
2	horst+Virus+dd2	92	81	100	OK	OK	OK	OK
3	kA+BenD	82	74	86	OK	OK	OK	OK
4	WizardOfDos	70	56	79	OK	OK	OK	OK
5	Balloonicorn	64	53	71	OK	OK	OK	OK
6	404NameNotFound	63	64	59	OK	OK	OK	OK
7	Kalle+BE+another	63	66	56	OK	OK	OK	OK
8	colewort+gitmagic+CB	60	27	90	OK	OK	OK	OK
9	nnev+SF+KZ	53	40	64	OK	OK	OK	OK
10	nerd2nerd+CF	43	23	60	OK	OK	OK	OK
11	hackademics	34	23	43	OK	OK	OK	OK

Mixed

- *Attack central infrastructure*
- Teams meet usually physically in one location
- The unknown network contains some services, which need to be found and owned
- Different Rounds with different goals
- Example: PacketWars

Why organize a CTF?

- Implement your ideas
- Gain knowledge
- Challenge yourself
- Improving communication and collaboration with other teams
- Contribute back to the community
- It’s fun :-)

Ingredients

- **Commitment and Time!**
- Challenges!
- Workforce
- Infrastructure: Scoreboard, Servers, Network, …

Challenge-Design

- be versatile
- be unpredictable
- be precise
- have different difficulty levels
- have rules & enforce them

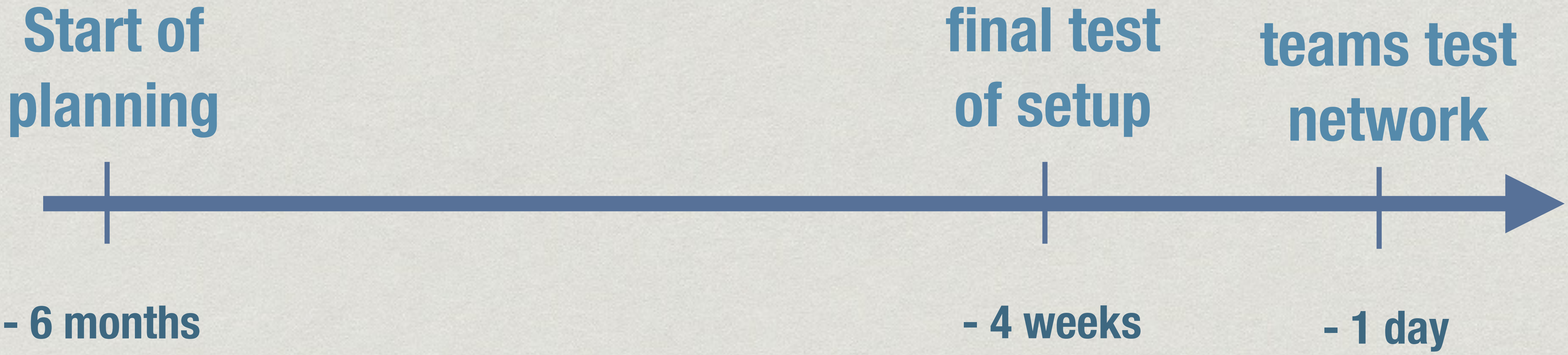
Infrastructure

- No infrastructure = No CTF
- **Always keep in mind:** Your network is attacked or attacking
  - Expect the unexpected
  - Contain attacks
- Scoreboard: No competition without comparison
  - CTFd for jeopardy CTFs
- Servers: Adjust to the load, have backup systems ready

DOs and DON’Ts

- **Start early**
  - there is much to get done
  - planing and preparation is key
  - speak with your local on-site orga

Schedule



Start of planning

- 6 months

final test of setup

- 4 weeks

teams test network

- 1 day

DOs and DON’Ts

- **Keep it simple**
  - debugging is much easier
  - less pre-CTF work
  - new or complex tech might crack down on you
  - also: multi-stage challenges can be frustrating

DOs and DON’Ts

- **Organize your team**
  - CTFs are a team effort
  - distribute responsibilities

DOs and DON’Ts

- **Test, test, test…**
    - Check your challenges for other vulnerabilities
    - Let somebody else run through your challenges
    - Also test your setup
    - Think like an attacker

DOs and DON'Ts

- **Refrain from last second changes**
  - probably not tested
  - your team does not know about changes
  - = stuff breaks

Getting publicity

- Spread the word among other teams
- CTFtime.org (http://ctftime.org/)
- On site: use talks to get attention

REMINDER:
CAMP CTF JUST STARTED

HTTPS://CAMPCTF.CCC.AC/