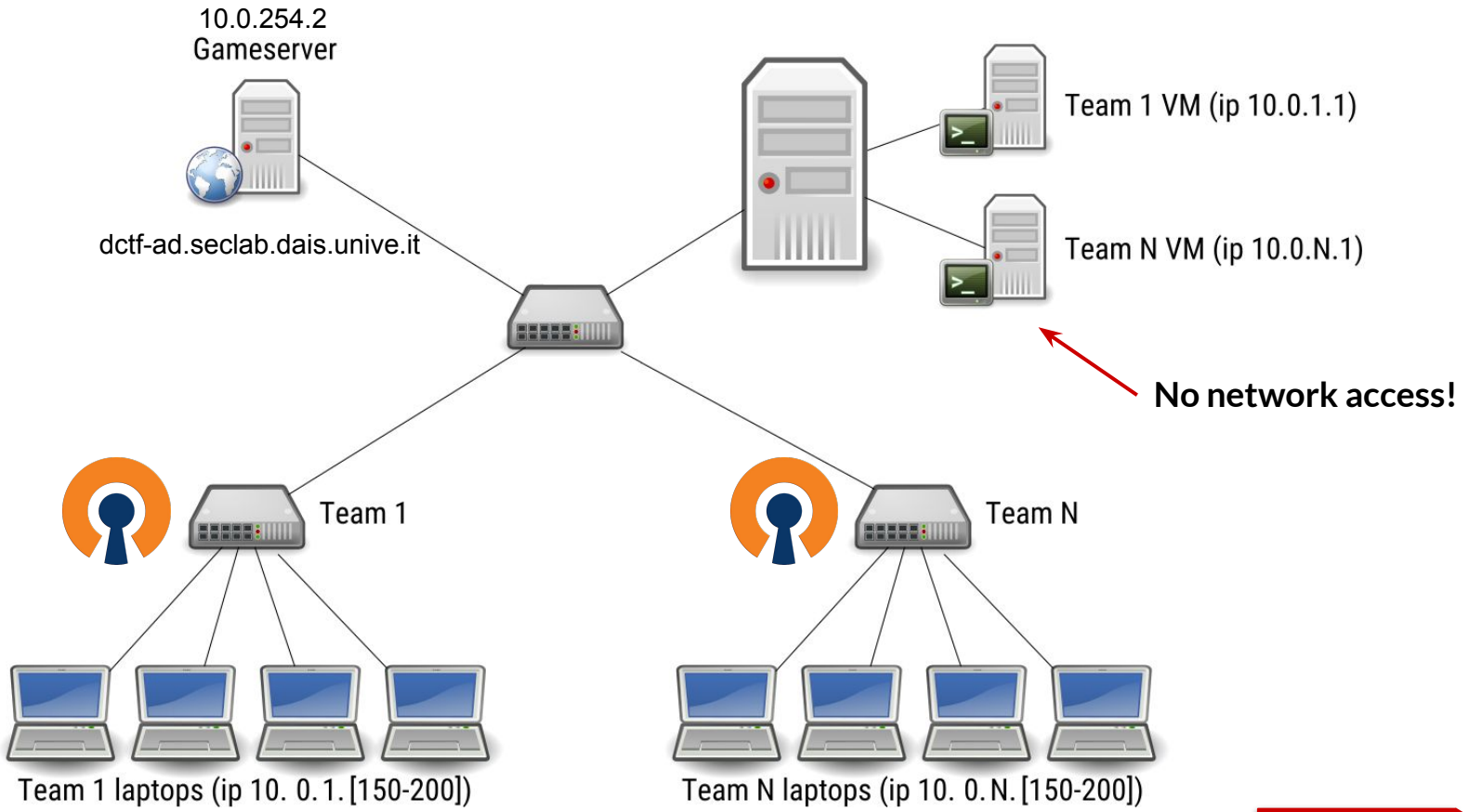
CTF training
attack and flag submission

Security 2 2018-19

Univeristà Ca' Foscari Venezia
www.dais.unive.it/~focardi
secgroup.dais.unive.it



https://dctf-ad.seclab.dais.unive.it/design

CTForge

Scoring

Game Design

- The game is divided in ***rounds*** (also called *ticks*) having the duration of **120 seconds**.
- During each round, a bot will add **new flags** to your vulnerable machine.
- Moreover it will **check the integrity of services** by interacting with them and by retrieving the flags through a legitimate accesses.

https://dctf-ad.seclab.dais.unive.it/design

Scoring
Scoreboard

Service State

Service is **online** and behaves as expected

service could be **offline** or **broken** (wrong patch? missing **flag**?)

The checker has not yet verified the status of the service

Attack point (flags)

Defense point (flags)

SLA

https://dctf-ad.seclab.dais.unive.it/design

Let’s Begin...

- Team Extraction
- VPN Access
- VM Login

Tips For the CTF

Change your password

- The first thing you have to do when the competition starts is to change the root password of your virtual machine!

```
root@diff:~# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

https://secgroup.dais.unive.it/teaching/security-course/tips-for-the-ctf/

Tips For the CTF

Unix utilities

- Change user with `su - <username>`
- Find files with the `find` utility
- Check processes running on the VM: `ps aux`
- Kill processes with `kill`
- Check network connections with `netstat` (`netstat -natup`)
- Netcat is your friend! (`nc localhost 65534`)
- Copy file to and from the VM using `scp`

https://secgroup.dais.unive.it/teaching/security-course/tips-for-the-ctf/

Tips For the CTF

Python Sockets

https://secgroup.dais.unive.it/teaching/security-course/tips-for-the-ctf/

Tips For the CTF
PWNTOOLS

- CTF framework and exploit development library
- Install with `pip install pwntools`

```
>>> conn = remote('ftp.ubuntu.com',21)
>>> conn.recvline()
'220 ...'
>>> conn.send('USER anonymous\r\n')
>>> conn.recvuntil(' ', drop=True)
'331'
>>> conn.recvline()
'Please specify the password.\r\n'
>>> conn.close()
```

http://docs.pwntools.com/en/stable/

Submitter

Flag submission

- To manually submit a flag, click on the *flag submission service*.
- During the CTF, anyway, you may want to automatically submit flags.

```
#!/usr/bin/python
import requests

url = 'http://10.0.254.2/submit'
team_token = '<your_token>'
stolen_flag = 'flg{abcdefghilmnopqrstuvz0123}'

r = requests.post(url, data={'team_token': team_token, 'flag': stolen_flag})
```

https://dctf-ad.seclab.dais.unive.it/design

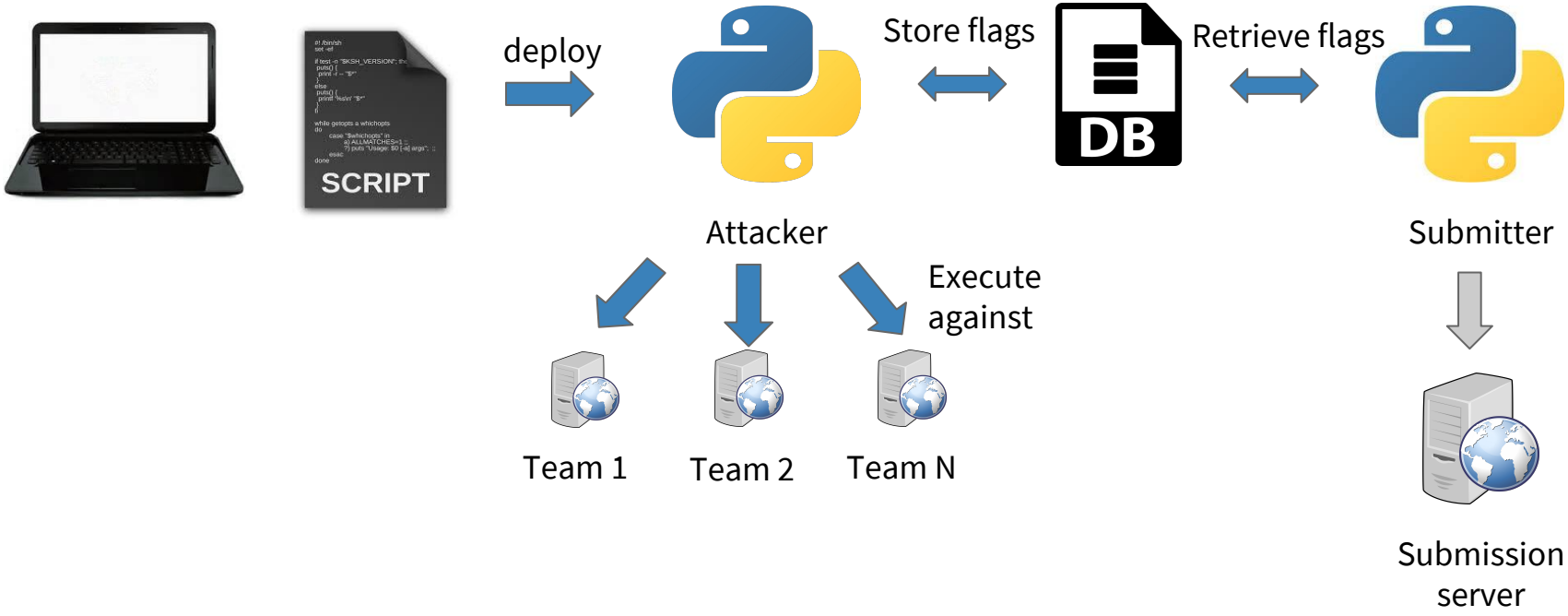
Attacker and Submitter

Attacking and submitting

- Rounds are 2 minutes long
- Attacking every team and submitting flags manually is **unfeasible**!
- We need to script!

Attacker and Submitter

Suggested/typical design



Training CTF

- Training service: `safe`
- Scripting an attack
- Submitting a flag