Capture the Flag from WWE Bank

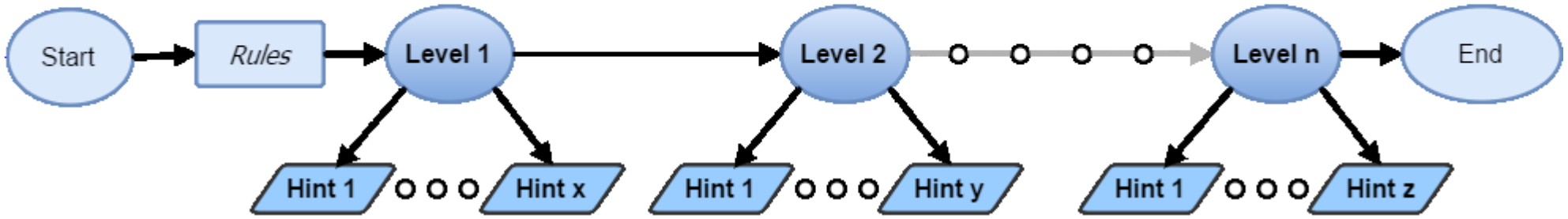
KYPO game for practising penetration testing

CSIRT-MU, Masaryk University, Brno

Game Essentials

Objective: **Steal confidential information from an internal database.**

- *Background:* fictitious WWE Bank organizes a hacking challenge.
- *Structure:* several levels (more than 4 and less than 8) with particular tasks.
- *Game characteristics:* learning by doing, fun, stress, frustration, uncertainty, time pressure, eureka, satisfaction.

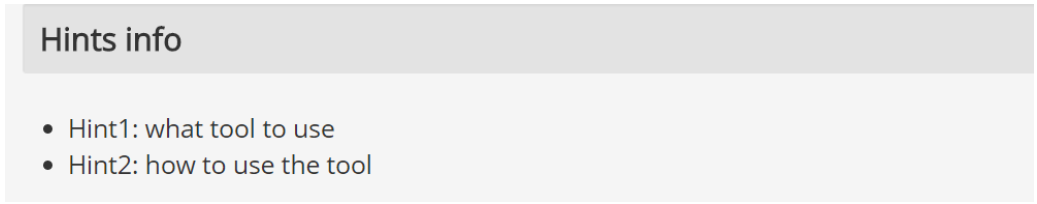


Attack Phases

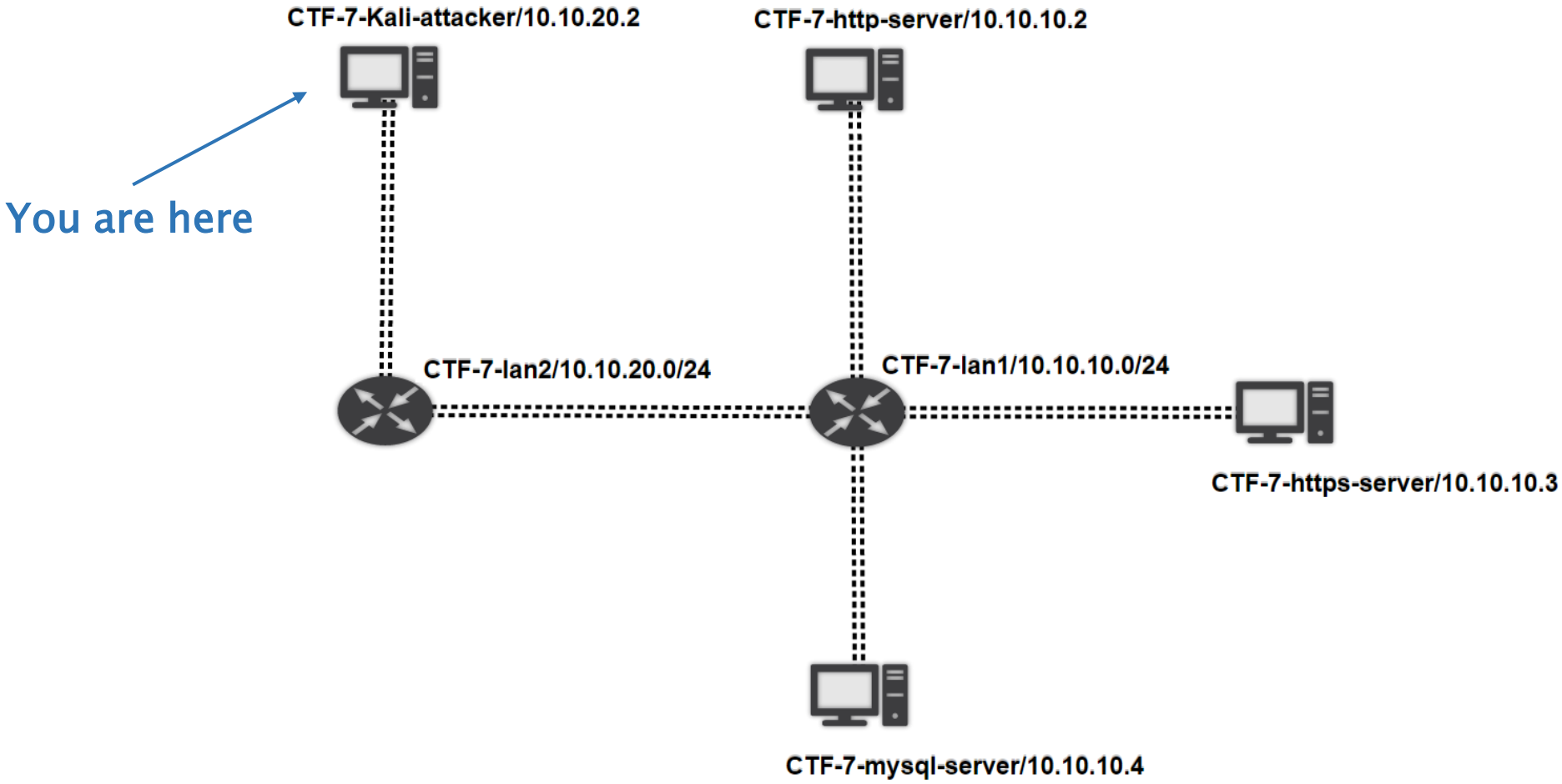
1. Getting familiar with the environment
2. Select target
3. Find *vulnerability*
4. Find a way to *exploit* vulnerability
5. Make the target useful for attacker

Game Hints and Solutions

- *Hints:* each level offer several hints for penalty points, hints can be taken in arbitrary order
- *Recommended solution:* if you are struggling, you can access step-by-step solution of the level
- *Game characteristics:* learning by doing, fun, stress, frustration, uncertainty, time pressure, eureka, satisfaction.



Network Topology



Recommendations

- 2-hour session allows your own pace.
- Ask us for help, we may tell you something useful.
- Each team/player has own sandbox, do not hesitate to try everything.
- Take hints and be prepared to spend some points for that.
- Use Google, use Google, use Google!

Let's Go!

- Open Chrome browser and go to **kypo2.ics.muni.cz**.
- Log in with your university account using Shibboleth.
- Choose **your** sandbox in a table.
- Now you can see network topology.
- Open **CTF game** in a new tab.
- Read introduction.
- Fill questionnaire.
- Start the game!

Let's Go!

Level 1 - Reconnassaince

You have been given the task - find vulnerabilities in WWE banks infrastructure. You also have been given IP addresses of their machines. Discover what services are these machines running. Scan their opened ports and sort them in ascending order to create the flag. So for example if the machines had ports opened as described in this table:

IP	10.10.10.1	10.10.10.2	10.10.10.3	10.10.10.4
Port	20, 5432	8080	20, 5432	22

Sort the opened ports, construct following string: **20,20,22,5432,5432,8080** and create the flag by executing following command:

```
$  echo '20,20,22,5432,5432,8080' | sha1sum
72eb621b9693497e69068c752f18d807127ce992  -
```

Now use first four characters as a flag, in this example it would be: **72eb**

QUESTIONS?

GOOD LUCK!

www.kypo.cz

@csirtmu

Martin Laštovička, Jan Vykopal

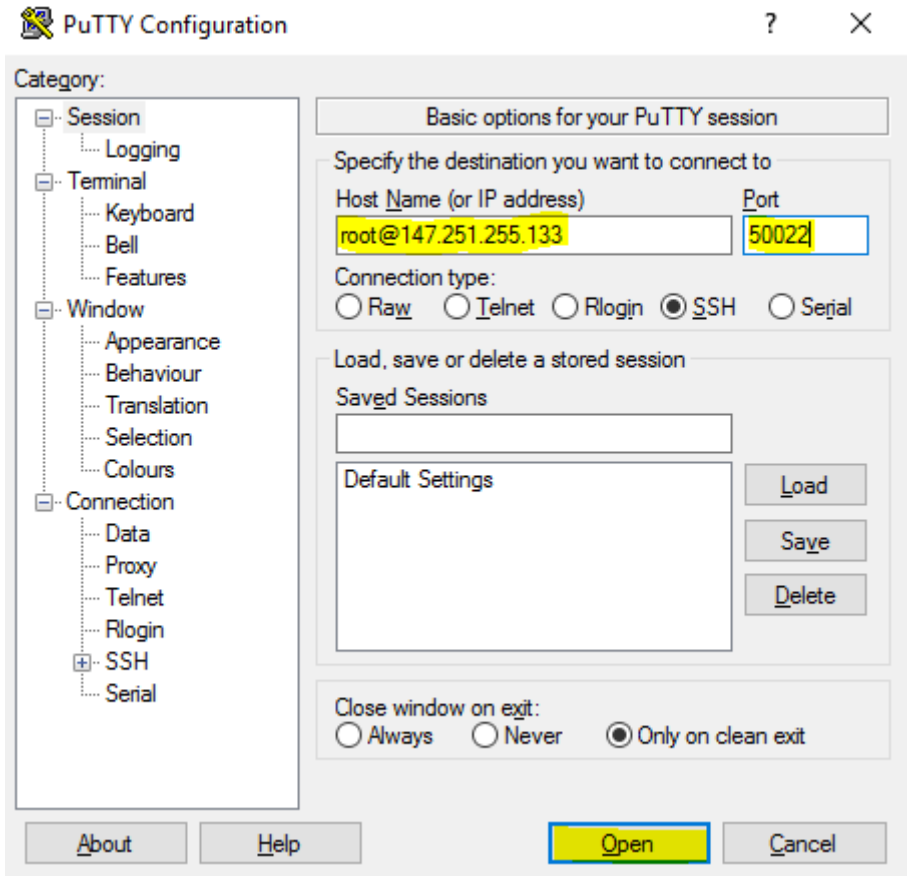
<surname>@ics.muni.cz

Homework

- You have access to a sandbox IP 147.251.255.133 with two networks
- The attacker is in the network 10.10.20.0/24
- Victims are in the network 10.10.10.0/24
- Use *nmap* and *Metasploit*
- Credentials for your machine login:root pass:toor

Homework – How to Connect on Windows

- Using Windows Putty



Homework – How to Connect on Linux

- Using Linux ssh:
  - ssh -p 50022 root@147.251.255.133

Homework – How to Submit

Submit the homework in a format:

- Number of active Ips in the 10.10.10.0/24 subnet
- Version of Samba servers from 10.10.10.0/24 subnet
- Ordered list of existing vulnerabilities of the Samba servers according to the CVE database (use cvedetails.com) having score >= 9.0
- Describe briefly used commands