

Capture the Flag Game on Pentesting in the KYPO Cyber Range

PA197 Secure Network Design

May 9—10, 2018

Valdemar Švábenský

Masaryk University, Brno, Czech Republic

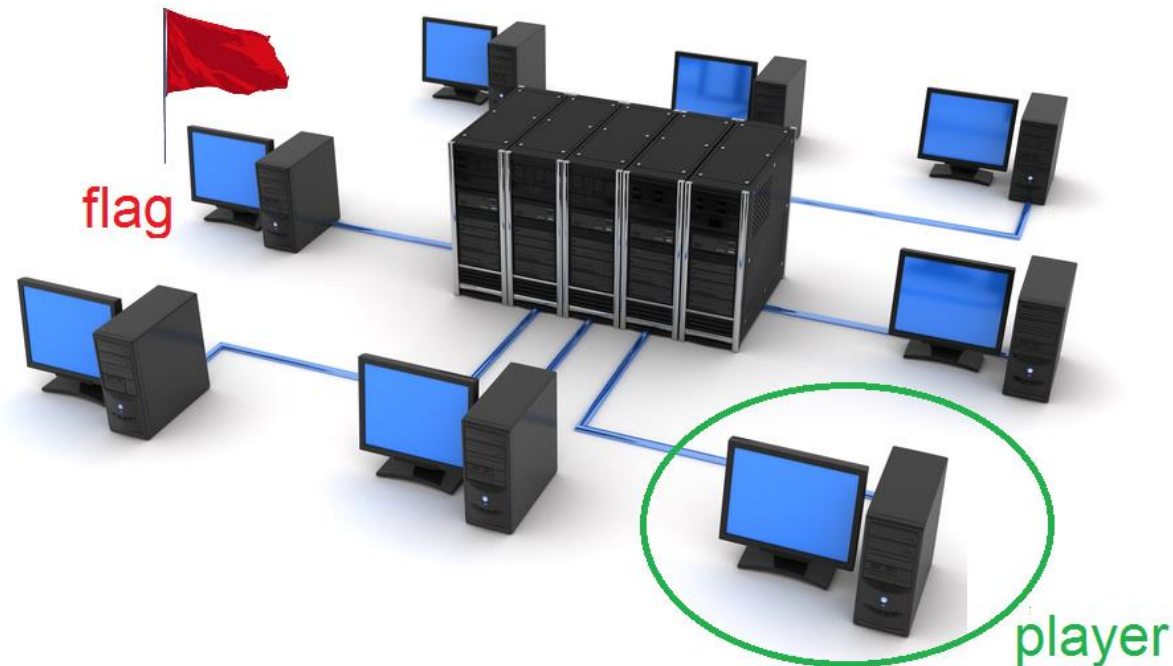


KYPO

BY CSIRT-MU

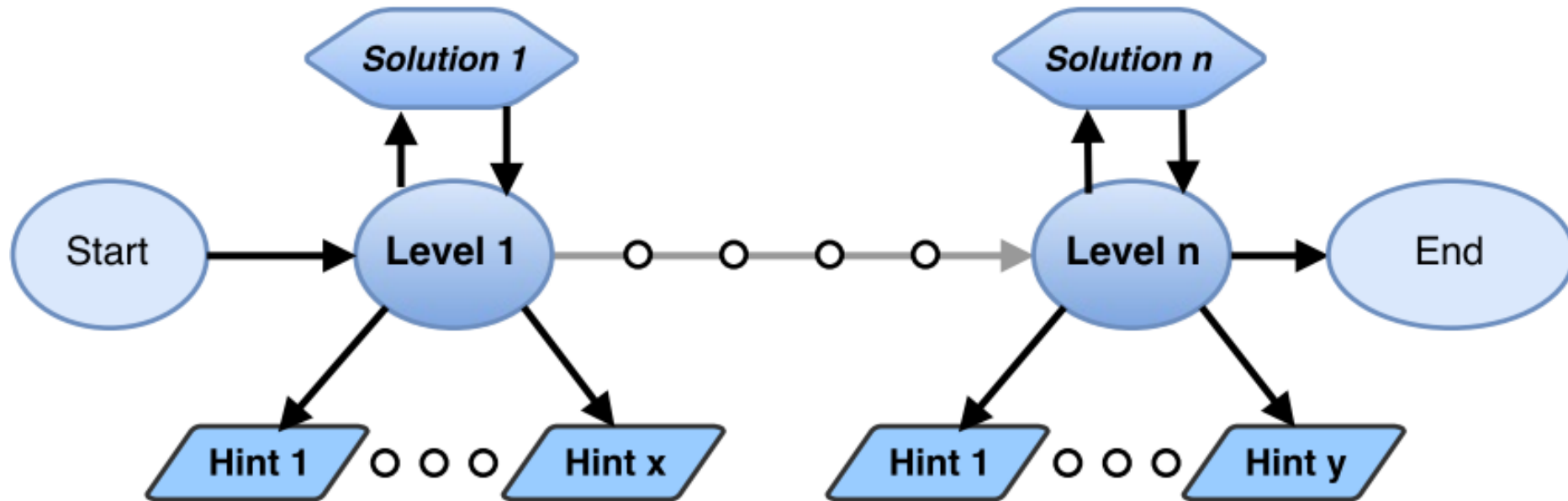
Capture the Flag (CTF) game

- Application for exercising cybersecurity skills
 - We focus on **Attack-only** games
- Original idea: hacker conference DEF CON 1996, modern form in 2003
- Benefits: practicing, learning, competing



CTF games in KYPO: structure

- Completing security-related tasks in linearly connected levels
 - Penetration testing skills



CTF games in KYPO: topology and machine view

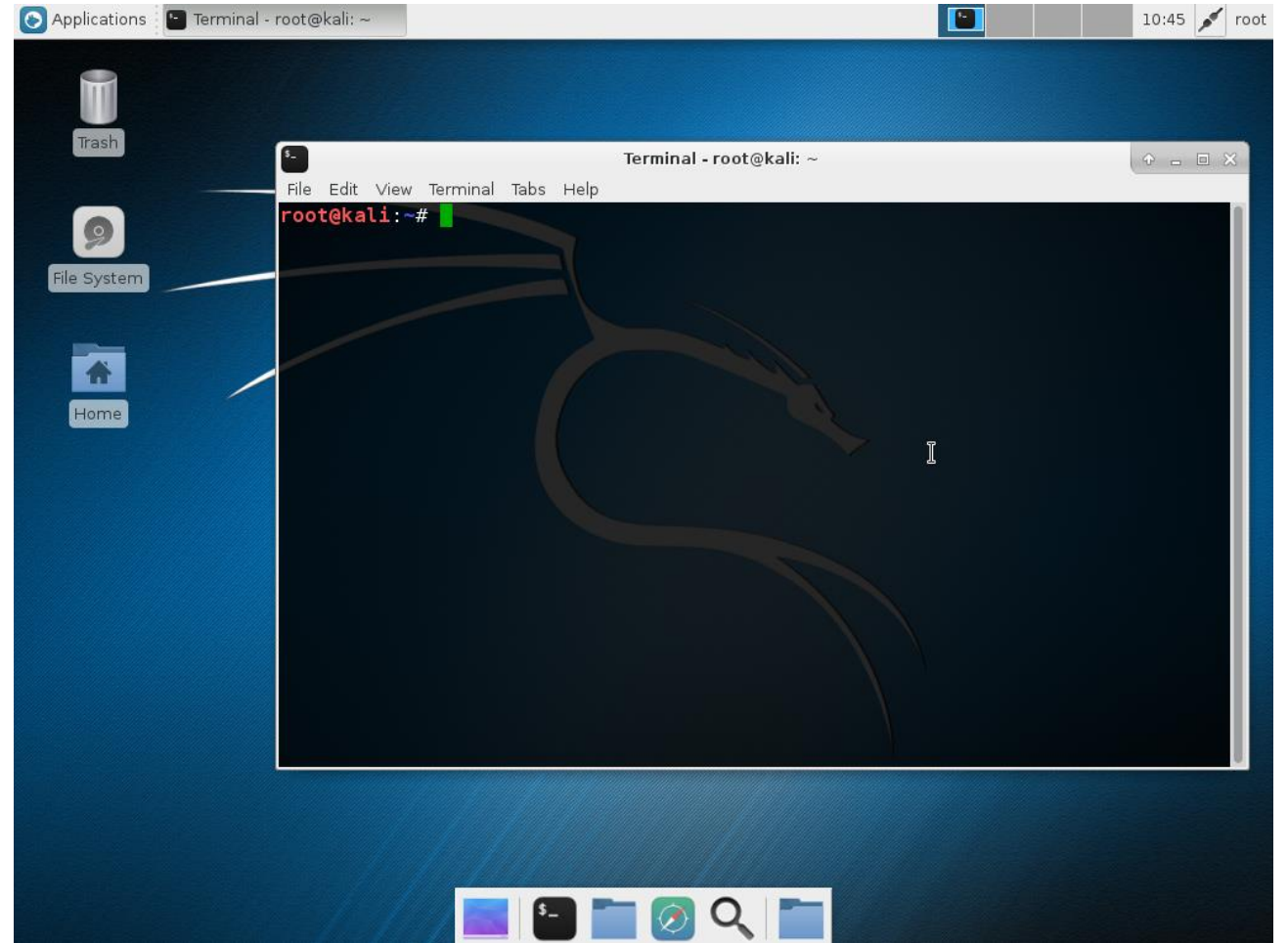
CTF-7-Kali-attacker/10.10.20.2



CTF-7-lan2/10.10.20.0/24



CTF-7-http-server/10.10.10.2



CTF games in KYPO: game view

- Task description
- Game control panel:

The screenshot displays the game interface with two main panels: 'Level info' and 'Hints info'.

Level info panel:

- Time left: 00:08:48
- Skip level button
- Level code: and
- Points available: 4/8
- Level flag input field
- Submit button
- Total points earned: 0
- Exit game button

Hints info panel:

- Hint1: what tool to use
- Hint2: how to use the tool
- Need help? section
- Help level button
- Get hint #1 button
- Penalty: -2 points
- Hint #1: use Nmap to scan the target network

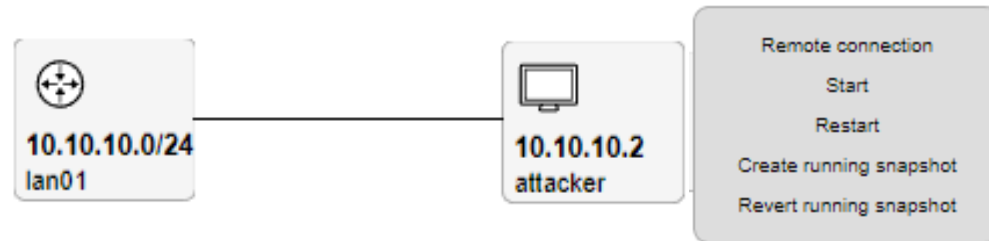
Photo Hunter Game

- Background story: a paparazzi blackmails a celebrity, who asks for your help
- You start by receiving an e-mail from her
- Goal: find the photos on the paparazzi's server
- 4 levels to practice 4 stages of a cyber attack:
 1. **Reconnaissance** (network exploration)
 2. **Scanning** the target host
 3. **Gaining access** (SQL injection)
 4. **Exploiting a vulnerability** (password cracking)



Your tasks

1. **Log in** at <https://kypo2.ics.muni.cz/> via Shibboleth using your UČO
2. **Access the attacker machine** (login/password: root/toor)



3. **Have fun** and try everything! :) (restart the machine in case of trouble)
4. After you finish, we'd love to hear your feedback on the game! Please, **fill out the questionnaire** at <https://goo.gl/forms/rfcqZjCPKJsGxQu13>

Extra resources: check them out for homework

- <https://www.kali.org/>
- <https://ctftime.org/>
- <https://defcon.org/>
- <https://www.hackthebox.eu/>
- <http://overthewire.org/wargames/>
- <https://avatao.com/>
- <https://www.hackthissite.org/>
- <https://hack.me/>
- <http://www.dvwa.co.uk/>



QUESTIONS?

THANKS FOR YOUR ATTENTION!

www.kypo.cz

 @csirtmu

Valdemar Švábenský et al.

svabensky@ics.muni.cz



KYPO

BY CSIRT-MU