Pregled kibernetičkog poligona KYPO CRP

Ivan Kovačević

Sadržaj

- KYPO CRP - pozadina
- Osnovni koncepti
- Potpora provođenju vježbe
- Diskusija i zaključci
- Primjer opisa sandboxa i vježbe (ako ostane vremena)
- Reference

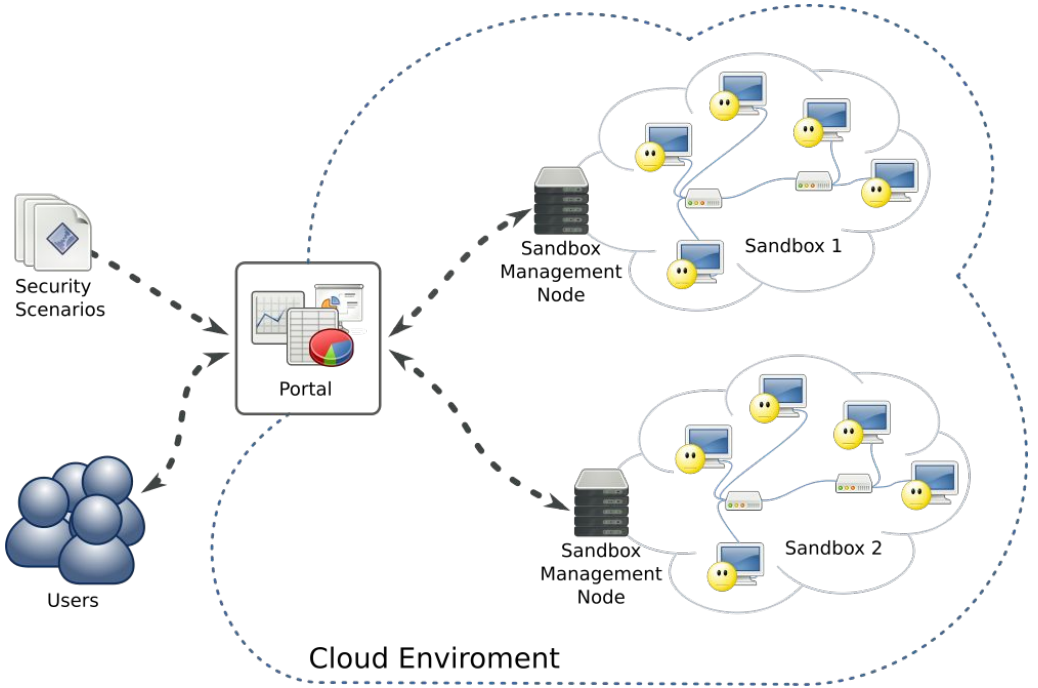
KYPO CRP - pozadina (1)

- KYPO Cyber Range Platform
- Razvija ga Masarykovo sveučilište (Brno, CZ) uz financiranje MVCR-a
- Uporaba na brojnim vježbama, uključujući Cyber Czech
- U razvoju od 2013., najnovija verzija je iz 2018.
- Od kraja 2020. je open source

KYPO CRP - pozadina (2)

Osnovni koncepti: sandbox (1)

- Sandbox je izolirana virtualna infrastruktura
  - Virtualne mreže i računala
- Overlay networking
  - Svaki sandbox je izoliran unutar svog VLAN-a
  - Ugniježđeni VLAN-ovi (VXLAN, Q-in-Q) predstavljaju virtualne mreže



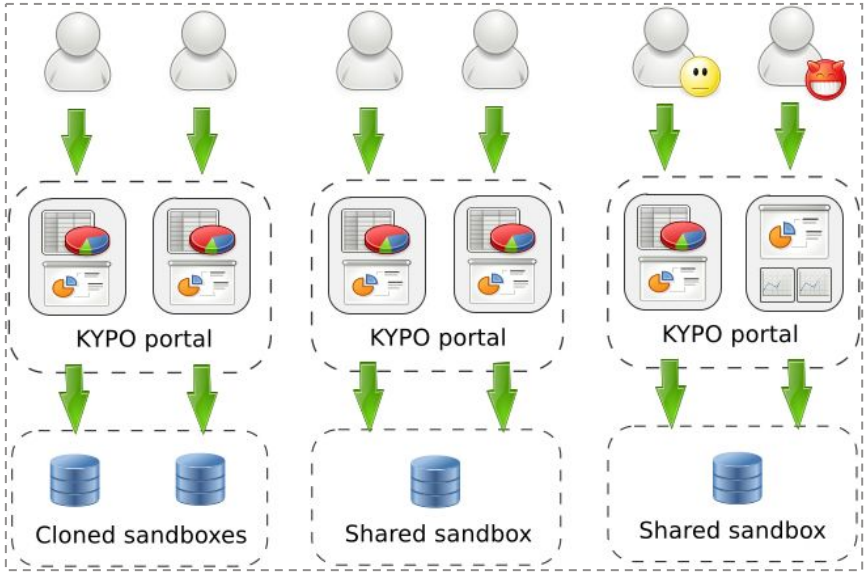
Osnovni koncepti: sandbox (2)

- Definicija topologije (YAML)
  - Opis infrastrukture unutar sandboxa
  - *OpenStack* na temelju opisa postavlja virtualne mreže i računala

- Opskrbljivanje (*provisioning*) sandboxa (YAML)
  - Konfiguracija, instalacija softvera i podataka
  - Obavlja se pomoću alata *Ansible*

Osnovni koncepti: mogućnosti uporabe

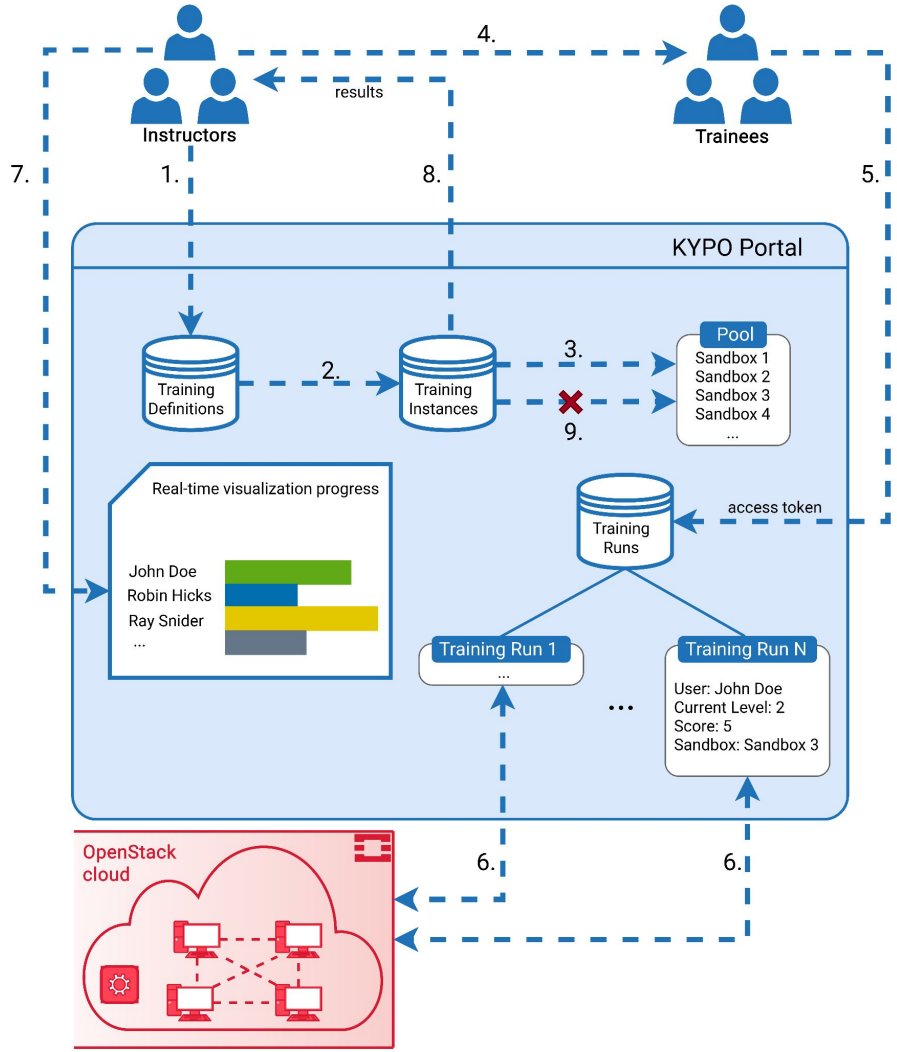
- Istraživanja u kibernetičkoj sigurnosti
- Forenzika: dinamička analiza uzoraka u sandbox-u
- Vježbe u kibernetičkoj sigurnosti
  - Capture the Flag (CTF) - obuka
  - Cyber Defense Exercises (CDX)



Osnovni koncepti: CTF

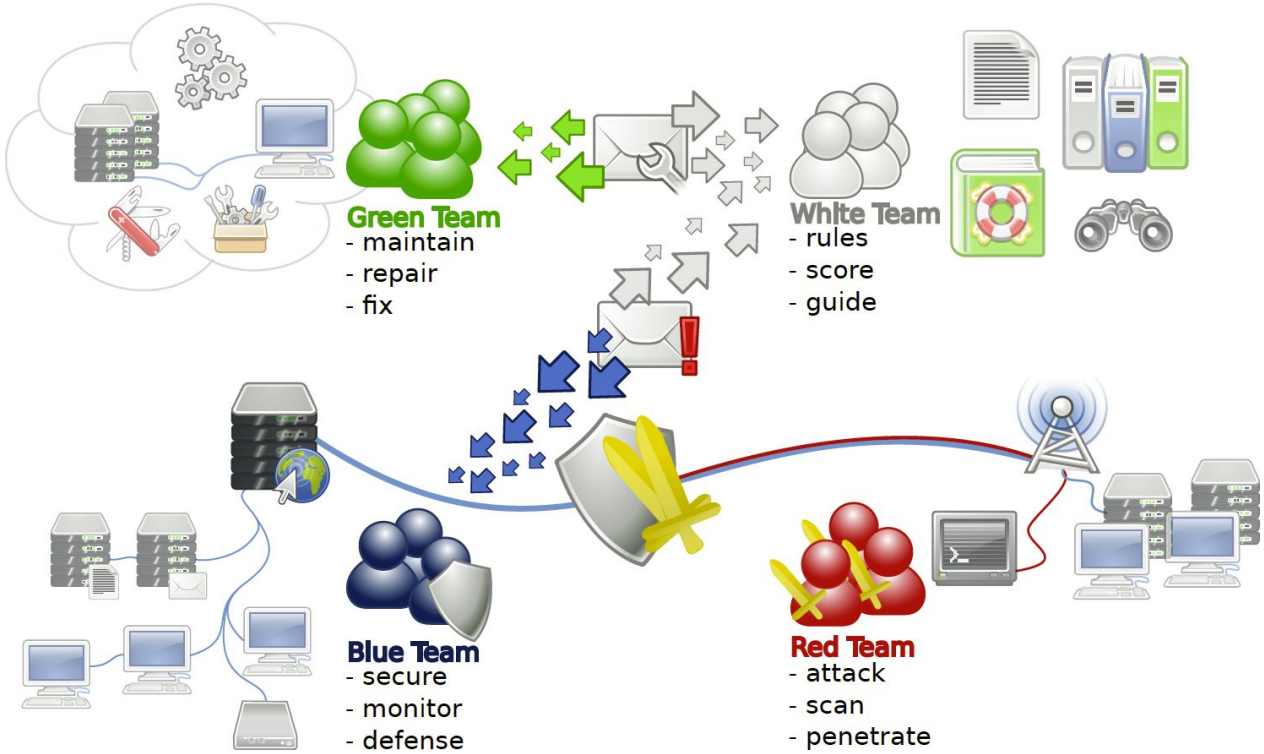
- Obuka se definira nezavisno od sandboxa

- Zadaće, hintovi, pitanja, rješenja
- Unos kroz GUI ili JSON-om



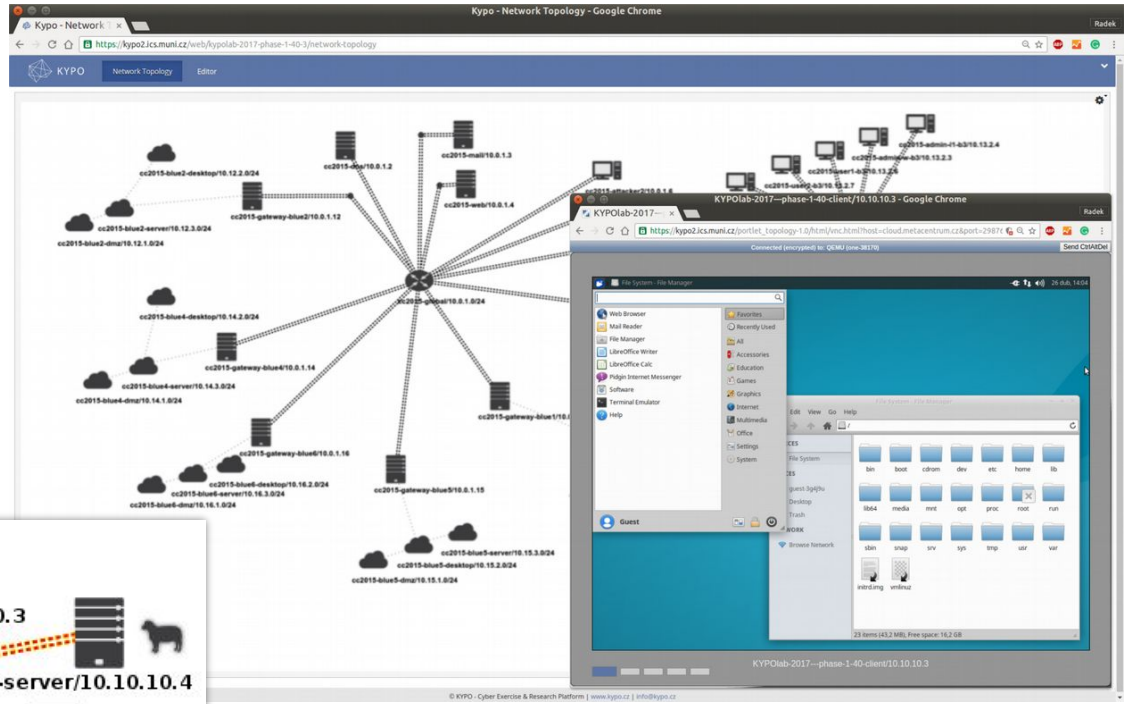
Osnovni koncepti: CDX

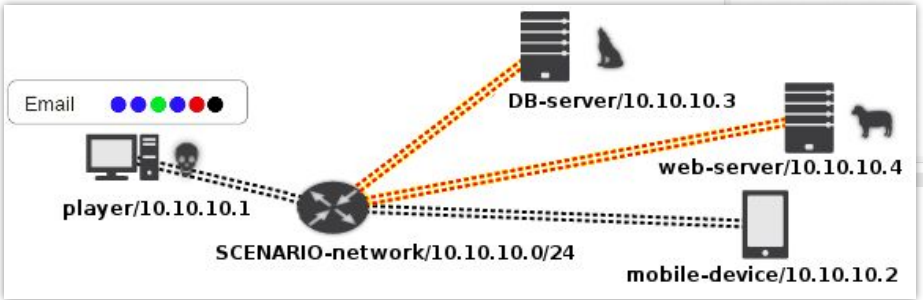
- Veći broj potpornih timova
- Zaseban tim može glumiti korisnike



Potpora provođenju vježbe: pristup resursima

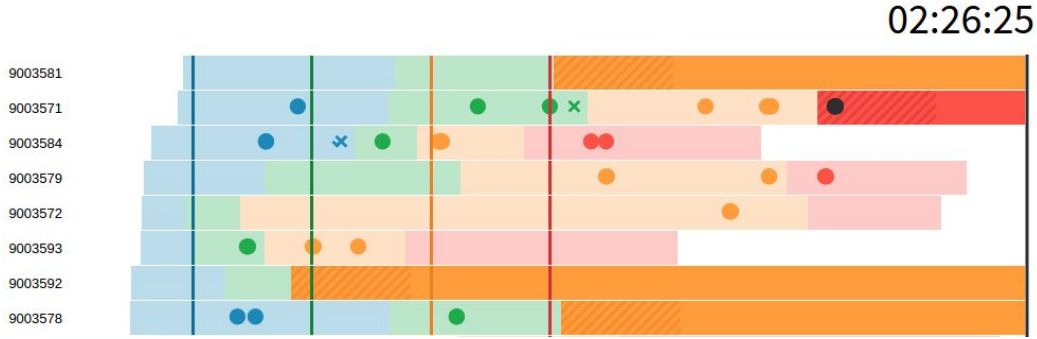
- Web GUI koji podržava RDP i SSH
- Pregled stanja na mreži





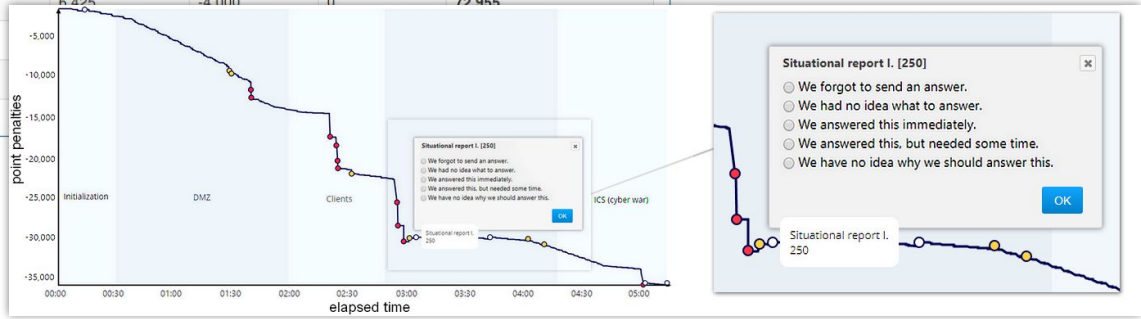
Potpora provođenju vježbe: tijek i bodovanje

- Veći broj vizualizacija za edukatore i vježbenike
- Snimanje događaja i prometa



Cyber Exercise Score

Team Name	Services	Attacks	Injects	Users	VNC	Total Score
Blue Team 1	91,843	-8,500	9,000	-1,100	0	**91,243**
Blue Team 5	92,230	-5,000	3,600	-400	0	**90,430**
Blue Team 2	81,280	-10,750	6,425	-4,000	0	**72,955**
Blue Team 4	74,518	-11,000				
Blue Team 3	85,756	-12,000				



Primjer opisa sandboxa i vježbe

- https://gitlab.ics.muni.cz/muni-kypo-crp/prototypes-and-examples/sandbox-definitions/kypo-crp-demo-training

Diskusija i zaključci

- KYPO CRP se validira uporabom na CTF i CDX vježbama
- Ne spominju generatore prometa, što je potencijalno veliko ograničenje
  - Korisnike sustava simulira zaseban tim
- Opis sandboxa i scenarija se obavlja ručno kroz YAML i GUI
  - Ne spominju automatsku verifikaciju scenarija
- Postavljanje i opskrbljivanje (*provisioning*) se obavljaju automatski
- Određena razina automatizacija ocjenjivanja CTF-ova, manje kod CDX
- Nisu se ranije bavili OT sustavima, no razmatraju uvođenje (KYPO4INDUSTRY)
- Sustav se i dalje razvija i može se očekivati poboljšanja u ovim područjima

Reference

- Eichler, Zdenek, Radek Ošlejšek, and Dalibor Toth. "Kypo: A tool for collaborative study of cyberattacks in safe cloud environment." International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer, Cham, 2015.
- Vykopal, Jan, et al. "Kypo cyber range: Design and use cases." (2017).
- Tovarňák, Daniel. "KYPO Cyber Range: Design and Use Cases" (prezentacija)
  - https://is.muni.cz/publication/1386573/2017-ICSOFT-kypo-cyber-range-design-presentation.pdf
- Ošlejšek, Radek, et al. "Conceptual Model of Visual Analytics for Hands-on Cybersecurity Training." IEEE transactions on visualization and computer graphics (2020).
- https://docs.crp.kypo.muni.cz/