KYPO Cyber Range
Design and Use Cases

ICSOFT CONFERENCE
24.7.-26.7. 2017

Daniel Tovarňák
Masaryk University (ICS)
tovarnak@ics.muni.cz
Cyber Ranges

- *Cyber Range* is a platform for cyber security research and education – it is a simulated representation of an organization's network, system, tools, and applications connected in an isolated environment.

- **Generic testbeds**
  - Dedicated infrastructure
  - Mostly emulation of large network topologies

- **Lightweight platforms**
  - Lower resources requirements
  - Limited scope and functionality

- **Cyber ranges**
  - Costly, Complex
  - Versatile, Large-scale
Motivation

- CSIRT-MU (TI-certified team, 1st in CZ)
  - Applied research in network security monitoring and intrusion detection
  - Large campus network used as a “testbed” for evaluation of our detection methods
- Real-life testbed limitations
  - Malicious network traffic can do real harm to users and servers in the network
  - Essentially, only detection methods can be tested
  - Experiments cannot be repeated under the same conditions
- Existing cyber ranges did not fully support our use cases
  - Many other restrictions applied, e.g. no access to non-military users
- Decision to design, develop, and operate own platform with the following features
  - Built on existing cloud infrastructure (not dedicated HW)
  - Full emulation of operating systems and applications (not simulation)
  - Focused on the cybersecurity problem domain – e.g. embedded network and host monitoring
KYPO Architecture Requirements

- Flexibility
  - Arbitrary network topologies, ranging from single node networks to multiple fully-connected networks
- Scalability
  - w.r.t. of emulated topology nodes, processing, network size and bandwidth, the number of sandboxes, and the number of users
- Isolation vs. Interoperability
- Cost-effectiveness
- Built-in monitoring
- Easy access
  - users with a wide range of experience should be able to use the platform
- Service-based access (SaaS, PaaS internally)
- Open-source

Daniel Tovarňák, Institute of Computer Science, Masaryk University
KYPO Architecture – Full Overlay Networking

- Networking must be transparent in the sandbox
- The visible network topology in sandbox must be independent from real physical routing path – **overlay**
- The network traffic must be isolated from the infrastructure and from other sandboxes
- VLAN Tagging with Q-in-Q
  - VMs in one LAN network must be on a single physical node – in contradiction with cloud scheduler
- VXLAN – Virtual Extensible LAN
  - encapsulation of L2 frames into a UDP packet
  - MTU at least 1554 B
  - Physical infrastructure limitations
Sandbox Deployment Challenges in Cloud Environment

- **Automatization**
  - VMs image management and deployment
  - Infrastructure as a code is highly advisable
  - Use configuration and deployment automation tool e.g. Ansible, Puppet

- **Security issues**
  - Regular VMs are not allowed to act as a router in cloud
  - MAC IP spoofing is not allowed
  - Publicly accessible VMs such as Metasploit-able could pose a threat

- **VM deployment issues**
  - Random interfaces order after reboot (edit configuration in /etc/udev/rules.d/70-persistent-net.rules)
  - Various restart-sensitive configurations
User Interface and Experience – KYPO Portal

- Composed of predefined mutually collaborating interactive modules (portlets)
  - Rapid adaptation to new scenarios
  - Support of complex scenario-specific workflows
  - Reuse across scenarios
- Management of cyber exercises
  - Interactive management of the whole life cycle
- Access to sandboxes
  - VNC and SPICE web clients
- Network topology with situational awareness
  - E.g., logical roles of nodes, activities in the network
- Visual analysis of exercises
  - Course of the exercise, scoring feedback
- Analytic graphs
  - Analysis of monitored data
Cyber Range Physical Facility – KYPOLab

- Training area, multimedia control center, visitor's gallery
- 6 mobile audio-video tables with integrated all-in-one touch computers
- 6 mobile displays
- A wide projection screen and a display wall (information shared across teams)
- A content sent to all displays is managed centrally from the control center
KYPO Use Cases

- Cyber research, development and testing
  - This use case originally motivated the development of KYPO
  - Target user group: researchers and network administrators
  - Users can create networks of predefined desktops and servers or provide own virtual images
  - KYPO provides a sandbox for experiments

- Digital forensic analysis
  - Extension of the previous use case
  - Target user group: incident handlers and analysts
  - Users can deploy virtual images of unknown or malicious hosts and run a set of automated dynamic analyses
  - KYPO provides a sandbox with an analytic host with pre-configured tools

- Cybersecurity education and training
  - Target user group: organizers and participants of hands-on learning activities
  - KYPO supports two distinct formats
    - Capture the flag game, Cyber defence exercise
Capture the Flag Game

- KYPO provides framework for creating and running attacker-based capture-the-flag games (CtF).
- Each game is split into several levels, players search for correct answer (flag).
- Each level offers:
  - Hints that can be displayed in exchange for penalty points
  - Recommended solution
Cyber Defense Exercise

KYPO emulates a complex organization’s network with distinct roles of users in the exercise
- Attackers, defenders (target group), and instructors/referees

The platform provides the following
- Multiple interconnected sandboxes hosting the entire exercise infrastructure
- Scoring system based on advanced logging infrastructure
- Monitoring system for instant insight
KYPO Success Story

- **2014** – started with a prototype CtF game
  - In total 20 sessions with about 300 participants so far
  - Invaluable feedback from real users of various skills, background and nationality
  - KYPO CtFs used for the Czech national qualification to the ENISA European Cyber Security Challenge 2017

- **2014-present** – KYPO project contributes to the personal development and working experience of undergraduate students
  - A lot of KYPO features was originally developed as a part of bachelor or master theses
KYPO Success Story

- **2015** – a first national cyber defense exercise – *Cyber Czech*
  - A proof-of-concept application of KYPO which showed directions for future work and research
  - A 2-day exercise for 40 ppl., carried out 5 times with national and international participants (approx. 180 VMs)

- **2016** – KYPO platform enabled the creation of a new hands-on university seminar on simulation of cyber attacks

- **Q4/2016** – KYPO project received the Award of the Czech Minister of the Interior for security research