KYPO – A Platform for Cyber Defence Exercises

Pavel Čeleda, Jakub Čegan, Jan Vykopal, Daniel Tovarňák
Institute of Computer Science, Masaryk University, Botanická 554/68a, 602 00 Brno
CZECH REPUBLIC

{celeda,cegan,vykopal}@ics.muni.cz, danos@mail.muni.cz

ABSTRACT

Correct and timely responses to cyber attacks are crucial for the effective implementation of cyber defence strategies and policies. The number of threats and ingenuity of attackers is ever growing, as is the need for more advanced detection tools, techniques and skilled cyber security professionals. KYPO – Cyber Exercise & Research Platform is focused on modelling and simulating complex computer systems and networks in a virtualized and separated environment. The platform enables realistic simulations of critical information infrastructures in a fully controlled and monitored environment. Time-efficient and cost-effective simulation is feasible using cloud resources instead of a dedicated infrastructure. In this paper, we present the KYPO platform and its use cases. We aim to execute current and sophisticated cyber attacks against simulated infrastructure since this is one of the key premises for running successful cyber security training exercises. To make the desirable improvement in the skills of the participants, a powerful storyline for the exercise is essential. Last but not least, we understand that technical skills must be complemented by communication, strategy and other skills for effective cyber defence.

1.0 INTRODUCTION

Operational systems and networks are not suitable for testing cyber attacks. However, to train cyber defence and develop responses to cyber attacks, a dedicated infrastructure (cyber range, testbed) is usually built. A cyber range provides a place to practice correct and timely responses to cyber attacks. In such a way, the security teams (CSIRT/CERT) can practice skills such as network monitoring, attack detection and mitigation, penetration testing, and many others in a realistic environment.

In this paper, we shall present KYPO – Cyber Exercise & Research Platform. KYPO aims to provide a virtualised environment for performing complex cybernetic attacks against a simulated critical infrastructure. The KYPO platform was made for research and development of new security methods, tools and for training security teams and students. KYPO was developed, and is operated, by CSIRT-MU – the security team of Masaryk University.

Today, KYPO is the largest academic cyber range in the Czech Republic. The proposed platform is fully cloud-based and supports multiple use cases (research, training). To validate KYPO, we co-organized the Czech national cyber exercise, Cyber Czech 2015. In this paper, we shall provide a brief overview of the cyber exercise. The cyber exercise will be held in the KYPO Lab in October 2015.

This paper is divided into six sections. Section 2 shall provide background information about cyber defence exercises and cyber ranges. Section 3 will describe KYPO's architecture and list the main requirements for the proposed architecture. Section 4 shall describe three main KYPO use cases. Section 5 will explain the design of a cyber defence exercise, it's technical implementation, and demonstrates the KYPO Lab. Finally, Section 6 will conclude the paper and outline the future development of KYPO.

2.0 RELATED WORK

Cyber defence exercises and competitions are held in many diverse types of technical infrastructures. At the one end, there are table-top exercises of strategic skills (such as [1]) with no ICT interaction or ICT support during the actual exercise. At the other end, technical exercises (such as [2] or [3]) employ cyber ranges and supportive infrastructure for communication within the exercise and evaluation of participants' actions. The cyber ranges simulate complex network setups in a contained environment. Therefore, participants can realistically interact with an assigned host or network infrastructure, and their actions cannot interfere with the operational environment.

There are more than 30 known cyber ranges and testbeds that can be used for cyber exercises worldwide [4]. This number is based on publicly available, non-classified information. Since the development and operation of some cyber ranges is funded by the military of various countries, there may be other classified cyber ranges. An extensive survey of the state-of-the-art of cyber range implementations was published by Davis and Magrath from the Australian Department of Defence in 2013 [4].

Due to very limited public information about the usage of particular cyber ranges in the exercises, we can report only on the technical infrastructure used in the cyber defence exercises we participated in.

The Estonian Cyber Range, developed by NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE), is a backbone of two NATO exercises: Locked Shields [2] and Cyber Coalition [3]. The Estonian Cyber Range relies on a VMware vSphere platform which simulates a complete game network of hundreds of hosts with various OS platforms. All types of participants – attackers, defenders and evaluators – access their part of the game network remotely using their own devices connected to a Virtual Private Network (VPN) provided by the range. The participants were also provided with an ad-hoc support infrastructure: communication and reporting tools (Jabber, mail), systems for sharing indicators of compromise, online scoring, and web portal hosting knowledge base of the exercise (rules, scenario, access instructions etc.).

In contrast to the two NATO exercises, the technical phase of Cyber Europe 2014 [5] took a different approach. This is organized by European Union Agency for Network and Information Security (ENISA). The participants have access to several web applications which simulate social media networks, news, plain text sharing and data (images of compromised hosts, suspicious files, traffic traces) for analysis in accordance with an exercise scenario. Standard e-mail infrastructure and web portal were used for communication between the organizers and participants.

3.0 KYPO ARCHITECTURE

The KYPO platform was developed using requirements-driven development process. The most important design choices related to the high-level architecture were also based on functional and non-functional requirements defined in the preliminary phases of the project lifecycle. Some of the main requirements are listed below.

- **Flexibility** – the platform should support the instantiation of arbitrary network topologies, ranging from single node networks to multiple connected networks. For the topology nodes, a wide range of operating systems should be supported (including arbitrary software packages). The creation and configuration of such topologies should be as dynamic as possible.
- **Scalability** – the platform should scale well in terms of: the number of topology nodes, processing power and other available resources of the individual nodes, network size and bandwidth, the number of sandboxes (more on sandboxes later), and the number of users.
- **Isolation vs. Interoperability** – if required, different topologies and platform users should be isolated from the outside world and each other. On the other hand, integration with (or connection

to) external systems should be achieved with reasonable effort.

- **Cost-effectiveness** – the platform should support deployment on Commercial Off-The-Shelf (COTS) hardware without the need for a dedicated data center. The operational and maintenance costs should be kept as low as possible.
- **Built-in monitoring** – the platform should natively provide both real-time and post mortem access to detailed monitoring data. These data should be related to individual topologies, including flow data and captured packets from the network links, as well as node metrics and logs.
- **Easy access** – users with a wide range of experience should be able to use the platform. Web-based access to its core functions should be available.
- **Service-based access** – since the development effort and maintenance costs of a similar platform are non-trivial for a typical security team or a group of professionals, our goal is to provide transparent access to the platform in the form of a service (PaaS).
- **Open source** – the platform should reuse suitable open source projects (if possible) and its release artefacts should be distributed under an open source licences.

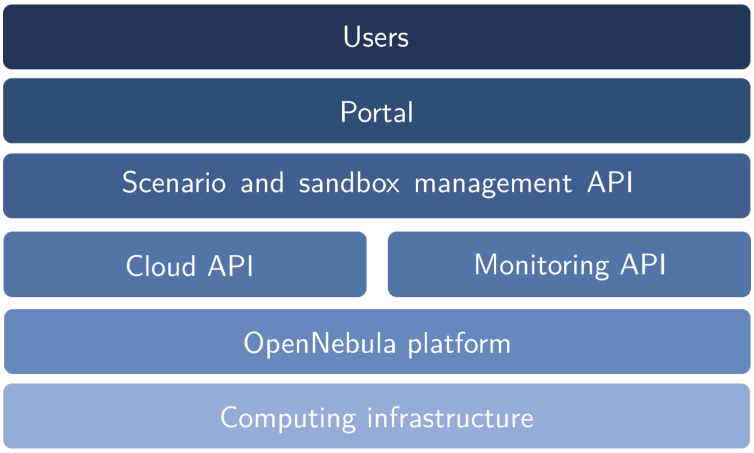

Figure 1: The core building blocks of the platform.

It can be seen that many of the requirements can be reasonably fulfilled by mapping the high-level architecture onto a cloud computing model. One of the main decisions to make was whether to develop the KYPO Platform as a Service and the high-level architecture reflects this fact. Since the traditional three-layer cloud service model (IaaS, PaaS and SaaS) is somewhat coarse grained, we describe the KYPO platform in more detail using the building blocks depicted on Figure 1 and described below (from bottom to top).

- **Computing infrastructure** includes housing facilities, physical machines, network devices, other hardware and related configuration artefacts. It forms the raw computing resources such as storage, operating memory, and processing power. The KYPO platform currently runs on top of the computing infrastructure provided by courtesy of CERIT‘s Scientific Cloud [6].
- **The OpenNebula platform** [7] allows for the management of heterogeneous computing resources (usually virtualized) in order to implement the Infrastructure as a Service model. OpenNebula is still managed by CERIT-SC and it is transparently used by the upper layers of KYPO to provide and create virtual machines and configure networking. OpenNebula GUI is sometimes used by KYPO developers to edit and configure particular virtual machines.
- **The cloud API** serves as a common interface to the shield upper layers from a particular IaaS implementation, which allow for greater flexibility of the KYPO platform. A driver is currently at its

core which translates OpenNebula-specific commands to common API methods.

- **The monitoring API** is responsible for monitoring management, i.e. it provides fine-grained control over network links and hosts monitoring configuration (starting, stopping, and attributes manipulation). It interacts both with OpenNebula and with created virtual machines.
- **The scenario and sandbox management API** is used to configure, create, edit and destroy the main logical entities of the platform – sandboxes – by the means of the underlying layers. A Sandbox is an isolated set of virtual machines, networks and monitoring configuration, and provides key features to users, e.g., the flexibility and repeatability of an experiment. Figure 2 illustrates the deployment of two sandboxes in the KYPO platform.
- **The portal** is a Graphical User Interface (GUI) of the platform based on the Liferay Portal project. It is used by the users in order to interact with the created sandboxes. The GUI is based on the concept of portlets – independent building blocks that encapsulate well-defined functionality. For example, the Topology portlet enables the users to view the network topology of a particular sandbox and open Virtual Network Computing (VNC) connections to its machines using a VNC portlet.
- **Users** with a wide range of experience can interact with the KYPO platform via Portal and underlying APIs. The mode of interaction heavily depends on the use case they employ the platform for. For the description of main use cases, see Section 4.

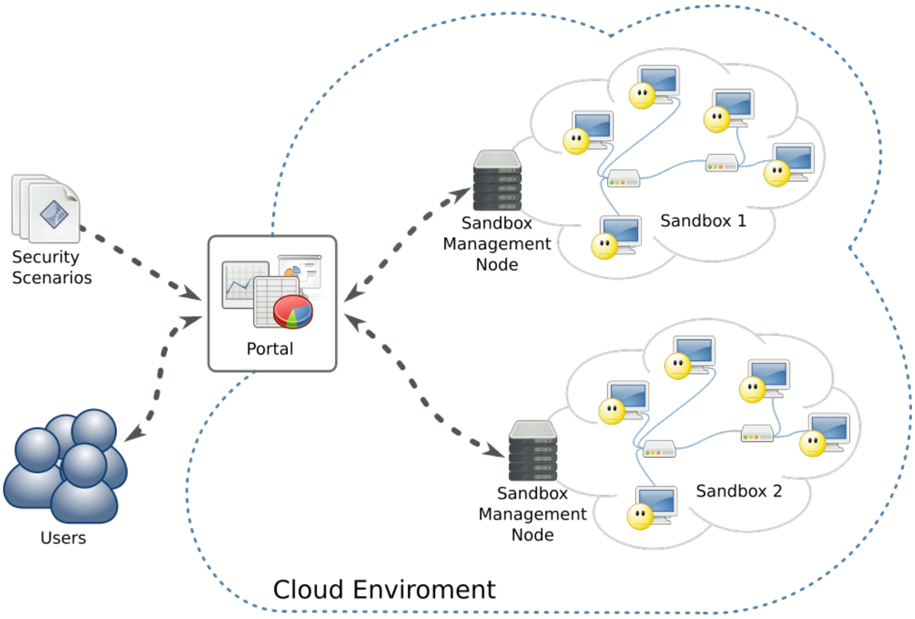

Figure 2: An illustration of two isolated sandboxes deployed in the KYPO platform.

4.0 KYPO USE CASES

The architecture and implementation of the KYPO follows three main use cases:

- cyber research and development,
- forensics analysis and network simulations,
- security training and exercises.

All these use cases have similar requirements on the infrastructure, but they differ in the expected knowledge, skills, and effort level of its users. However, the concept of sandboxes helps us to cope with this fact, i.e. various types of sandboxes can be provided – from an empty sandbox for researchers, to a fully populated and configured sandbox for a basic security training.

4.1 CYBER RESEARCH AND DEVELOPMENT

The first use case is oriented towards research and the development of new methods for detecting and defending against cyber attacks on infrastructures of various types. In this case, KYPO provides an empty sandbox and optional monitoring infrastructure for experiments. Users are able to create various networks populated with desktops, servers, and even mobile devices in this sandbox. Network traffic and host based statistics can be monitored and stored within KYPO infrastructure, where they are available for further analysis.

This case is designed for security researchers and experienced network administrators because it requires a good level of knowledge about networking, host configuration and some knowledge of virtualization techniques. However, we are able to provide generic types of images to ease the work, such as desktops running common operating systems and applications.

4.2 FORENSICS ANALYSIS AND NETWORK SIMULATIONS

The second use case covers basic forensic analysis, which can be partly automated by tools deployed in the sandbox. Users can deploy an image of a malicious machine to the sandbox, connect available probes and run a basic automated analysis. They can also continue with an advanced manual analysis of the machine.

A great advantage of this case is that users need only basic knowledge of forensics to perform an automated analysis. The precious time of forensic analysts can be therefore be used for more complicated and detailed forensic analysis.

4.3 SECURITY TRAINING AND EXERCISES

The last use case focuses on training security skills and cyber exercises and competitions. This case has zero requirements for user knowledge of KYPO infrastructure, virtualization and other underlying infrastructure. The organizers prepare and deploy a scenario for users who can focus only on the training subject, such as a penetration testing tutorial or game. Furthermore, we can facilitate training such as this with experienced lecturers to improve the learning curve.

Cyber exercises are much more complex than games and tutorials. While they require substantial preparation effort from the organizers, the end users (participants) are not affected. They can still focus only on the exercise subject, but requirements on the infrastructure team are significantly higher. This is caused by the fact that training tutorials can be repeated numerous times, but an exercise is a one-off event.

5.0 THE DESIGN OF A CYBER DEFENCE EXERCISE

We have designed a one-day cyber defence exercise for 20 players (Blue team) as proof of the last use case listed above. The exercise involves:

- training objectives, story and a detailed scenario,
- about 40 participants grouped into Red, Blue, White and Green teams,
- a KYPO sandbox with the game network simulated according to the scenario,

- a physical facility hosting all participants.

5.1 EXERCISE OBJECTIVES, STORY AND SCENARIO

The designed exercise is focused on defending critical information infrastructure against skilled and coordinated attackers with unclear motivations. Similarly to other defence exercises, participants are put into the role of members of emergency security teams which are sent into organisations to recover compromised networks. They have to secure the simulated critical infrastructure, investigate possible data exfiltration and collaborate with other emergency teams, the coordinator of the operation and the media.

Participants are provided with a background story to introduce them to the situation before they enter the compromised networks. This is very important since the exercise is not set in a real environment and participants have no previous knowledge who is who in the fictitious scenario (their users, popular news portal, superordinate security team). They are also provided with technical facts related to the game network: network topology including “their” network that will be defended, network architecture and current setup, access credentials etc. Before the actual exercise, participants access their simulated network in KYPO to get familiar with the exercise.

The exercise is driven by a scenario which includes the actions of attackers and assignments for defenders prepared by the organizers. The attackers exploit specific vulnerabilities left in the compromised network in a fixed order. The completion of each successful attack is recorded by the attackers. On top of that, participants should also answer to media requests. The performance of each defending team is scored based on successful attacks or their mitigation, the availability of specified critical services and the quality of reporting.

5.2 PARTICIPANT ROLES

Participants are divided into four groups according their skills, role and tasks in the exercise. These are now listed according as commonly used in other cyber exercises:

- **Green team** – a group of operators responsible for the exercise infrastructure (the KYPO sandbox in this case). They configure all virtual computers and networks, complex monitoring and scoring infrastructure. The Green team also monitors the sandbox’s health and fixes crashes and infrastructure issues if needed.
- **White team** – masterminds, referees and organizers of the cyber defence exercise. They provide the background story, exercise rules and framework for the Red team and Blue teams’ competition. The White team sends tasks (called injects) to the Blue teams and thus simulates media and the operation coordinator. They also provide hints to a Blue teams if in trouble.
- **Red team** – plays the role of attackers and consists of cyber security professionals. They do not attack targets in the infrastructure of a Blue team randomly, but they carefully follow a predefined attack scenario to equally load the Blue teams. This means the Red team exploits vulnerabilities left in a Blue team’s network. They should not use any other arbitrary means of attack against the Blue teams. They are also not allowed to attack the service infrastructure.
- **Blue team** – several Blue teams (five in our case) are responsible for securing compromised networks and dealing with the Red team’s attacks. They have to follow exercise rules and local cyber law. Members of Blue teams are the main target user group of the exercise.

Interactions between the four groups of players are depicted in Figure 3.

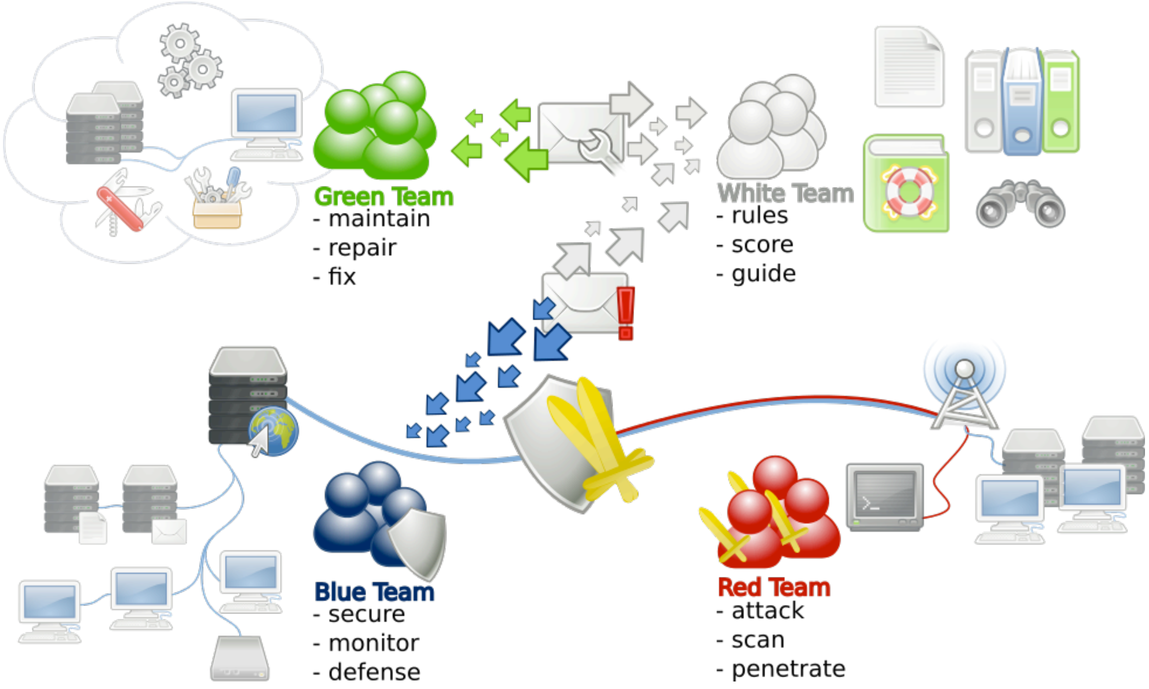

Figure 3: Groups of exercise participants, their interactions and tasks.

5.3 TECHNICAL IMPLEMENTATION

The technical part of the exercise relies on the built-in capabilities of KYPO described in Section 3. On top of that, we have prepared and developed the following:

- a sandbox containing approximately 110 interconnected hosts and other network architecture,
- a scoring system for real-time performance evaluation of participating Blue teams,
- a logging infrastructure for detailed post-mortem analysis and overall evaluation of the exercise.

5.3.1 Exercise Network Setup

The essential component of the exercise is the simulated network which serves as a virtual battlefield. Figure 4 shows the logical topology of the network, whereas Figure 5 is a screenshot of the deployed topology in the KYPO platform. All participants use the interface in Figure 5 to access hosts. The exercise network is segmented into two main types of subnetworks:

- **The global network** – hosting attackers and common network infrastructure, such as DNS and e-mail; this network simulates the global Internet.
- **The network of a Blue team** – representing the defended network with all critical (and vulnerable) services; this subnetwork is further segmented into a demilitarized zone, desktops and servers.

The main effort in the preparation phase is spent on setting up all hosts, especially hosts within networks of Blue teams, since they contain vulnerabilities which will be exploited according to the exercise scenario.

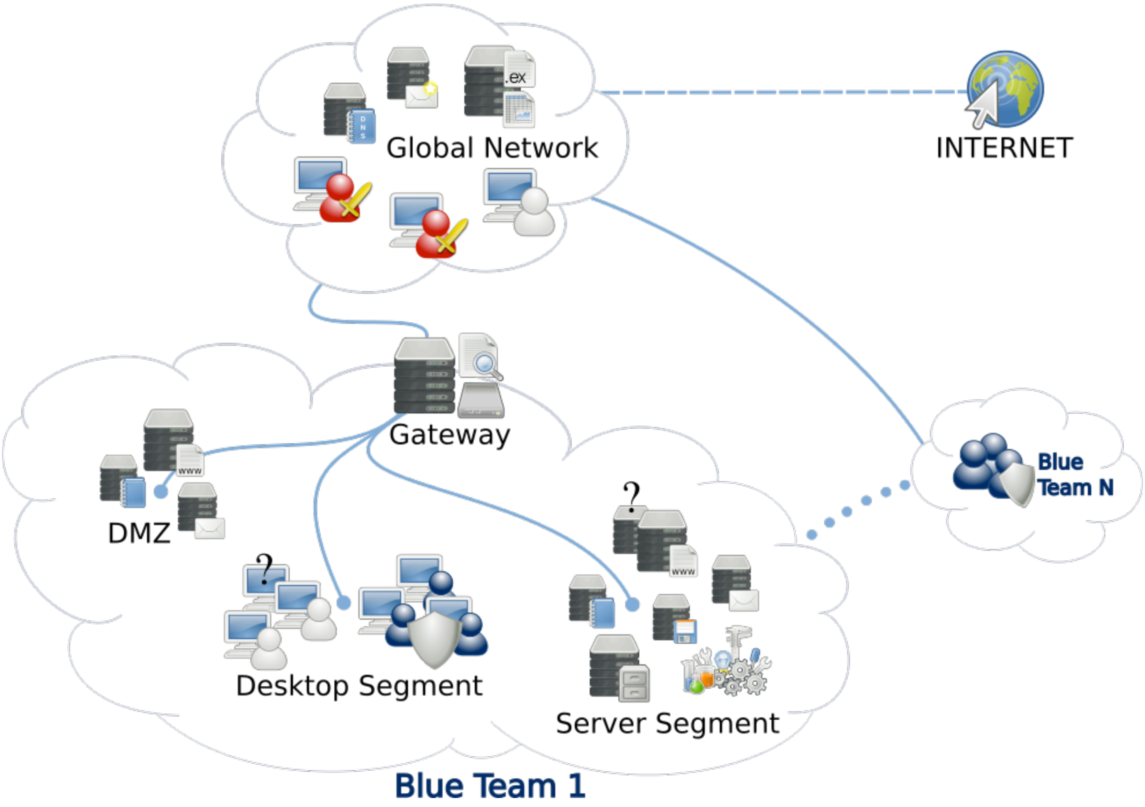

Figure 4: The logical topology of the simulated exercise network.

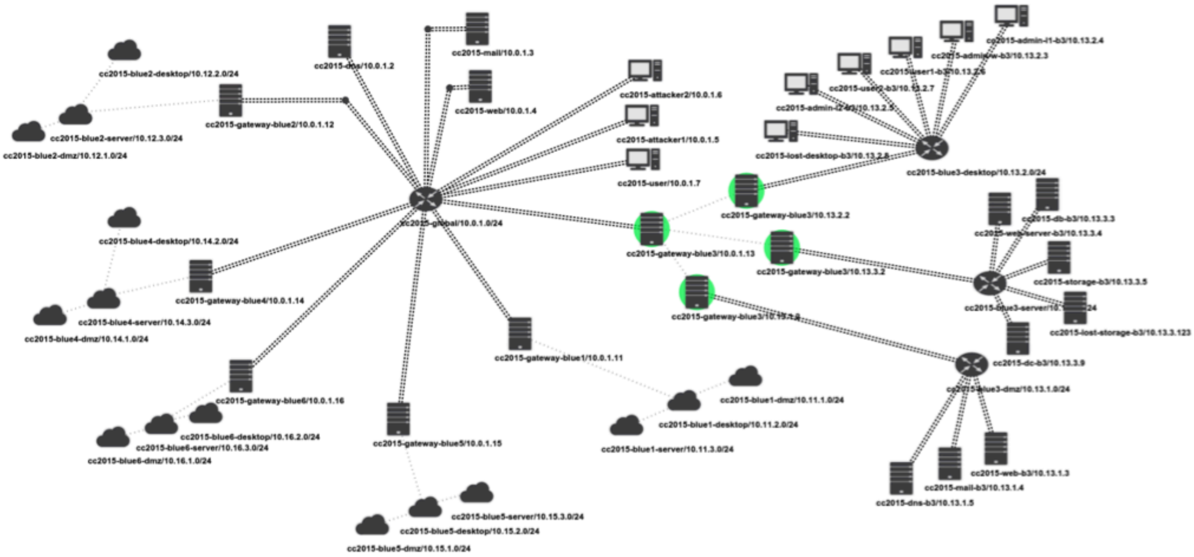
cc2015-dns/10.0.1.2
cc2015-mail/10.0.1.3
cc2015-web/10.0.1.4
cc2015-blue2-desktop/10.12.2.0/24
cc2015-gateway-blue2/10.0.1.12
cc2015-blue2-server/10.12.3.0/24
cc2015-blue2-dmz/10.12.1.0/24
cc2015-attacker2/10.0.1.6
cc2015-attacker1/10.0.1.5
cc2015-user/10.0.1.7
cc2015-admin-l1-b3/10.13.2.4
cc2015-admin-w-b3/10.13.2.3
cc2015-user1-b3/10.13.2.6
cc2015-user2-b3/10.13.2.7
cc2015-admin-l2-b3/10.13.2.5
cc2015-lost-desktop-b3/10.13.2.8
cc2015-blue3-desktop/10.13.2.0/24
cc2015-global/10.0.1.0/24
cc2015-gateway-blue3/10.13.2.2
cc2015-gateway-blue3/10.0.1.13
cc2015-gateway-blue3/10.13.3.2
cc2015-gateway-blue3/10.13.1.2
cc2015-db-b3/10.13.3.3
cc2015-web-server-b3/10.13.3.4
cc2015-storage-b3/10.13.3.5
cc2015-blue3-server/10.13.3.0/24
cc2015-lost-storage-b3/10.13.3.123
cc2015-dc-b3/10.13.3.9
cc2015-blue3-dmz/10.13.1.0/24
cc2015-web-b3/10.13.1.3
cc2015-mail-b3/10.13.1.4
cc2015-dns-b3/10.13.1.5
cc2015-blue4-desktop/10.14.2.0/24
cc2015-gateway-blue4/10.0.1.14
cc2015-blue4-server/10.14.3.0/24
cc2015-blue4-dmz/10.14.1.0/24
cc2015-gateway-blue1/10.0.1.11
cc2015-blue1-dmz/10.11.1.0/24
cc2015-blue1-desktop/10.11.2.0/24
cc2015-blue1-server/10.11.3.0/24
cc2015-gateway-blue6/10.0.1.16
cc2015-blue6-desktop/10.16.2.0/24
cc2015-blue6-server/10.16.3.0/24
cc2015-blue6-dmz/10.16.1.0/24
cc2015-gateway-blue5/10.0.1.15
cc2015-blue5-server/10.15.3.0/24
cc2015-blue5-desktop/10.15.2.0/24
cc2015-blue5-dmz/10.15.1.0/24

Figure 5: The topology of the simulated exercise network, which is deployed in a KYPO portal. Some hosts are hidden for better clarity of the user interface. They appear after clicking on the symbol of a cloud.

5.3.2 Logging Infrastructure

Apart from built-in network-based monitoring (provided by the KYPO platform), we have designed and developed dedicated logging infrastructure. It is the basis of the scoring system and an indispensable source of monitoring data for post-mortem analysis. Each host is configured to forward all log messages (all syslog facilities to be precise) to the central logging server.

A processing chain of additional tools is deployed on the central server in order to provide real-time transparent access to the normalized log data from the exercise topology. In addition to this, the state of a Blue team's network services are periodically checked by Nagios [8], a popular monitoring system. Events related to service state changes are logged into the central logging server, where they are further processed by the scoring system.

5.3.3 Scoring System

The choice of scoring components is tightly connected to its technical implementation. The weights of scoring components are directed by the exercise's objectives – one may prefer availability, whilst another confidentiality. In the designed exercise, we focused on service availability and defensive capabilities against the actions of the Red team.

Scoring based on availability can be handled automatically using the logging infrastructure described above. The logging infrastructure caters the scoring system with events which are then transferred to the score. The more time a service is up and running, the more points are granted to the particular Blue team responsible for the service.

Since the Red team conducts attacks manually, the score is assigned manually too. Members of the Red team enter points for each attack objective via the web interface of the scoring system. The same applies for injects (tasks) of the White team.

Based on our experience from participation in other exercises, we present a real-time total score of all teams on a scoreboard produced by the scoring system. We believe that this is an important factor fuelling participants with stress as well as a competitive mood.

5.4 PHYSICAL FACILITY

Although the KYPO platform provides remote access, we decided to invite all participants to one physical place. The participants come from different institutions, but there is the potential for their cooperation even after the exercise. Furthermore, we believe that one physical place allows us to deliver a better experience of the exercise, improve the learning curve of participants, and manage the whole exercise in a more agile and responsive manner for any possible changes.

To accommodate all participants, we use a KYPO Lab complemented with other meeting rooms on our premises [9]. Figure 6 depicts the seating of the Blue teams in the KYPO Lab. Each table accommodates one Blue team. Members of Blue teams communicate with each other in person. Communication with other teams (Red, White and Green) is delivered via e-mail. They access the exercise sandbox via a web browser. The most important global information, such as the scenario topology and score of all teams is displayed on a display wall and projector for their convenience.

Other teams (Red, White and Green) share detached meeting rooms. Considering the need for resolving issues and managing of the exercise efficiently, we established communication between other teams as a conference call (audio and video). Teams also access the sandbox via their browser. In addition to this, they interact with the scoring system (e.g., log successful attacks) according to their role in the exercise.

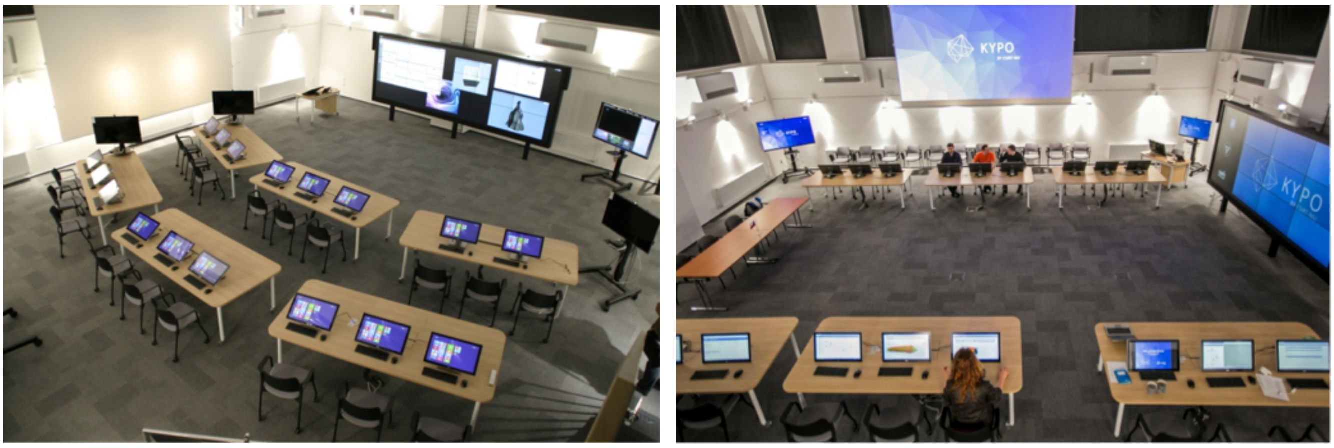

Figure 6: The KYPO Lab is a versatile room. Its setting can be adjusted to best fit the needs of ongoing exercises.

6.0 CONCLUSION

In this paper we have presented KYPO – Cyber Exercise & Research Platform. Using the KYPO platform, the trainers may focus on the exercise objectives, story and scenario. We prepared a set of use cases to evaluate KYPO and to demonstrate its benefits for common users. Various groups of users have successfully participated in our Capture the Flag (CTF) exercise in the past two years. We have designed a one-day cyber defence exercise to demonstrate the key features of KYPO. This technical exercise will be used at Cyber Czech 2015.

Our future work will focus on research into tools for a more economically-and-time efficient simulation of real critical infrastructures. We will create tools to automate the preparation and execution of security teams' training and exercises. We plan to connect KYPO to other facilities (e.g., SCADA, ICS and LTE networks) to provide a more realistic environment. We would like to continue with our involvement in co-organising national cyber exercises and challenges.

ACKNOWLEDGEMENT

This material is based upon work supported by Cybernetic Proving Ground project (VG20132015103) funded by the Ministry of the Interior of the Czech Republic.

Access to the CERIT-SC computing and storage facilities provided under the programme Center CERIT Scientific Cloud, part of the Operational Program Research and Development for Innovations, reg. no. CZ. 1.05/3.2.00/08.0144, is greatly appreciated.

7.0 REFERENCES

[1] European Defence Agency. Comprehensive and Strategic Decision Making on Cyber Security and Defence. [online]. 2015. [Accessed September 1, 2015]. Available from: https://www.eda.europa.eu/info-hub/press-centre/latest-news/2015/06/22/cyber-defence-exercise-for-decision-makers

[2] NATO Cooperative Cyber Defence Centre of Excellence. Locked Shields 2015. [online]. 2015. [Accessed September 1, 2015]. Available from: https://ccdcoe.org/locked-shields-2015.html

[3] NATO Communications and Information Agency. Exercise Cyber Coalition 2014. [online]. 2015. [Accessed April 13, 2015]. Available from: https://www.ncia.nato.int/NewsRoom/Pages/141126-cyber-coalition.aspx

[4] DAVIS, Jon; MAGRATH, Shane. A Survey of Cyber Ranges and Testbeds. Defence Science and Technology Organisation Edinburgh (Australia) Cyber and Electronic Warfare Div, 2013. URL: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA594524 [Accessed on September 1, 2015]

[5] European Union Agency for Network and Information Security (ENISA). Cyber Europe 2014 Information. [online]. 2014. [Accessed April 13, 2015]. Available from: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information

[6] CERIT Scientific Cloud. [online]. 2015. [Accessed August 28, 2015]. Available from: https://www.cerit-sc.cz

[7] MORENO-VOZMEDIANO, R.; MONTERO, R. S.; LLORENTE, I. M. IaaS Cloud Architecture: From Virtualized Datacenters to Federated Cloud Infrastructures. IEEE Computer, vol. 45, pp. 65-72, Dec. 2012.

[8] Nagios Enterprises. Nagios – The Industry Standard In IT Infrastructure Monitoring. [online]. 2015. [Accessed August 28, 2015]. Available from: https://www.nagios.org/

[9] Google. Virtual tour of KYPO Lab in Brno. [online]. 2015. [Accessed 1 September 2015]. Available from: https://goo.gl/maps/dAzSe