Lessons Learned from KYPO – Cyber Exercise & Research Platform Project

Jakub Čegan

cegan@ics.muni.cz

Institute of Computer Science
Masaryk University
Brno,Czech Republic

Martin Vizváry

vizvary@ics.muni.cz

Institute of Computer Science
Masaryk University
Brno,Czech Republic

Abstract

Cyber attacks became a significant threat for a critical information infrastructure of a state. In order to face them it is necessary to study them, understand them, and train personnel to recognize them. For this purpose we developed a KYPO - Cyber Exercise & Research Platform for simulation of numerous cyber attacks. In this paper we present the KYPO framework and first experience gained from Capture the Flag game training.

Keywords:

critical information infrastructure, cloud, penetration testing, learning, training, workshop.

1 Introduction

In these days is challenging to keep pace with attackers in a rapidly changing world of a cyber security. Particularly critical information infrastructure of the state should be protected against attackers. There is a variety of fields where it is necessary to stay up to date, such as research and development of new defensive methods, malware analysis, forensic analysis, and cyber security training. There are some solutions supporting security-related simulations. Existing solutions employ the Emulab/Netbed [1] infrastructure solution or require their own dedicated infrastructure. It simplifies many tasks related to deploying and building various network topologies, however it brings several restrictions, e. g., use of IPv4 only, OS and HW restrictions.

In this paper, we describe a novel framework, KYPO - Cyber Exercise & Research Platform, that we have developed and our experience from running of cyber security trainings in this framework. KYPO is built on top of a cloud provided as Infrastructure as a Service. It uses advanced visualization and integrated monitoring for implementation of three important cyber security use cases -- cyber trainings and exercises; research and development of detection and mitigation methods; and forensics analysis and network simulations. We have already gained operational experience from running cyber security trainings and exercises for users with various skills. We found out that realization of the trainings and exercises is laborious and time consuming. Another observation revealed issues of different levels of skills and knowledge of training attendees.

This paper is organized into five sections. In Section 2 we briefly describe KYPO use cases, architecture, and implementation. In Section 3 we describe and evaluate the training and exercises use case. In Section 4 we propose a future work on the framework. In section 5 we conclude our paper.

2 KYPO – Cyber Exercise & Research Platform

We have developed a unique framework to create sandboxes for simulation of numerous cyber attacks. Even though there are many solutions designed to support of security-related simulations, they are all expecting to establish a dedicated infrastructure. Our KYPO framework is built on top of a common cloud provided as Infrastructure as a Service. It benefits from cloud computing without building one.

2.1 Use Cases

The requirements and implementation follow three main use cases – Security Training and Exercises; Cyber Research and Development; and Forensics Analysis. All these use cases have common requirements on infrastructure. However, they differ in expected users' skills and level of interaction. To evaluate the framework against these use cases we have prepared several demonstrative and training scenarios. Demonstrative scenarios

were used in given lectures while training scenarios were used for hands-on trainings. Further in this paper we describe gained experience gained from several trainings.

2.1.1 Security Training and Exercises

The first use case covers Security Training and Exercises. In the process of designing the framework for this use case we have taken advantage of our experience from various exercises, e. g., Cyber Europe 2014 [2], Cyber Coalition 2014 [3], and Locked Shields 2015 [4]. KYPO allows to create various security scenarios covering numerous computer skills needed by both users and ICT administrators. Benefiting from virtualization we are able to simulate various scenarios using different types and versions of operating systems, e.g., MS Windows, Linux, Android, in same environment. The main advantages of these exercises are high rate of interactivity, monitoring of network traffic and host modifications, and remote access to all computers for lecturer.

2.1.2 Cyber Research and Development

The second use case is oriented on Cyber Research and Development of new methods of defense against cybernetic attacks on critical infrastructure. Testing and evaluation form significant part in development of new detection and mitigation methods. However, researchers complains about lack of data sets or testing environments for evaluation of new or improved methods [5]. We have designed our framework regarding to these demands. The framework provides network and host-based monitoring using NetFlow [6] technology and packet capture (pcap). Acquired data is stored in sandbox for further analysis or fast replay of experiment. There is also option to backup measured data for comparison with another experiment in new sandbox. The use of non-persistent virtual images and sandbox configuration files make experiments easily repeatable.

2.1.3 Forensics Analysis and Network Simulations

The last use case is devoted to Forensics Analysis and Network Simulations. The KYPO framework supports three main goals of forensics analysis. The first is tracking of malware's actions. Due to the network and host-based monitoring we are able to track every action of malware. We can also benefit from information gained from hypervisor. The second is an ability to promptly adjust the sandbox according to malware actions, e.g., change IP addressing, and create new host or service from preconfigured virtual images. The last goal is to keep malware in safe environment without the possibility of accessing real infrastructure. This is achieved because of

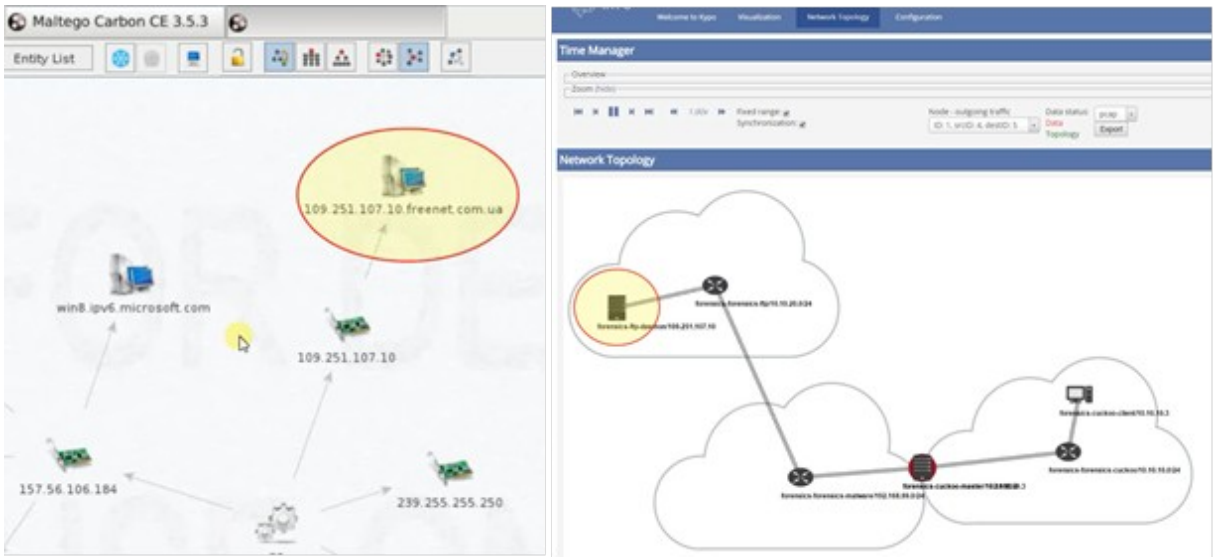

Figure 1Using Maltego in KYPO sandbox. According to the results of an analysis in Maltego, there is added new LAN and FTP server into sandbox.

separation of the sandbox in virtualized environment without access to hypervisor and encapsulation of network communication into separate VLANs.

Various forensics tools can be used tools during the analysis in the sandbox. For example, in the Figure 1, there is described the use of Maltego [7] during a malware analysis. Maltego returned some IP addresses which the

analyzed computer, infected with malware, is trying to contact. According to the results of this analysis, we can then add a new network with a host that the malware is trying to contact. Then the malware can connect to our host and can unknowingly reveal used credentials without the need to do reverse engineering on the malware.

2.2 Architecture

KYPO was designed in consideration of the three use cases described in section 2.1. Apart from requirements coming out of the use cases there are two more requirements. The first is using of a common cloud technology. Some existing solutions employ the Emulab/Netbed [1] infrastructure solution, e.g. DETER [8], and TWISC [9]. Even though it simplifies many tasks related to deploying and building various network topologies, it brings several restrictions, e. g., use of IPv4 only, OS and HW restrictions. Other similar projects require their own dedicated infrastructure to be established, e.g. ViSe [10], and V-NetLab [11]. The second important requirement was a multi-user access.

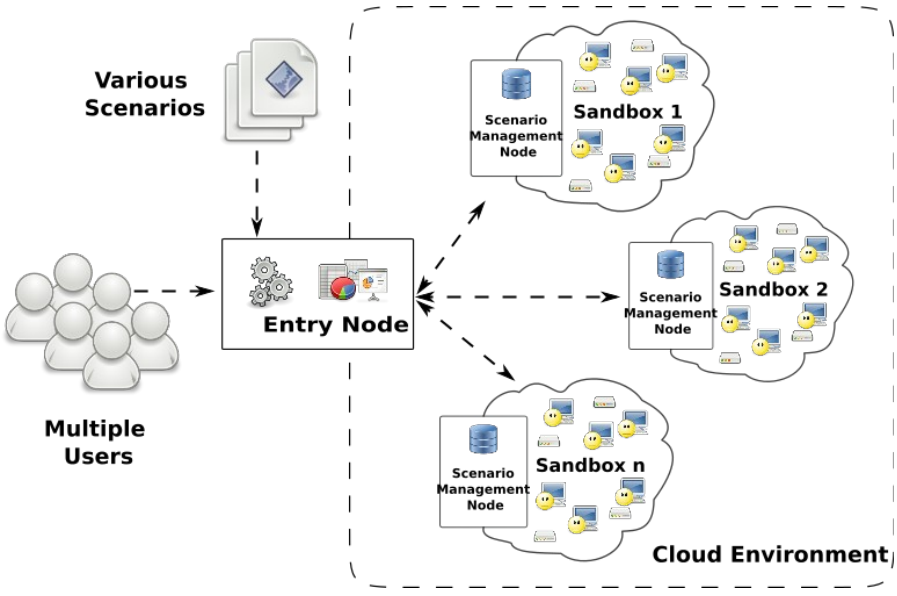

Figure 2: Caption: KYPO architecture schema. Users can access sandboxes via one entry node.

The proposed architecture of KYPO is described in Figure 2. A complete description of architecture is described in [12]. The KYPO is composed from two main parts. The first one, the Entry Node, could be deployed on a regular server outside or inside of a cloud environment. This node maintains user access to the KYPO framework. This node is authenticated against cloud interface and maintains access to virtual images, sandbox and scenario configurations, and users' authorization to access KYPO resources.

The second part, the sandboxes, is deployed purely in cloud environment. Users are able to deploy many independent and isolated sandboxes. Users can use preconfigured virtual images and sandbox configurations, i.e., there are various preconfigured scenarios which describes the network topology and used virtual images needed for sandbox deployment. Each sandbox is accessible via Scenario Management Node. This node maintains data about the sandbox, raw data from measurements, and access to network configuration. Every sandbox is isolated in a separate virtual network, so none of the sandbox activity can affect other sandboxes or outside world. Every sandbox has ability of network and host monitoring.

2.3 Implementation

KYPO is implemented in a cloud operated by Masaryk University and CESNET [13], the Czech National Research and Education Network. The MetaCloud [14] is an Infrastructure as a Service computing cloud built using OpenNebula 4.10 [15] with KVM hypervisor. The cloud solution is similar to Amazon Elastic Compute Cloud (EC2) [16] or Google Compute Engine [17]. Detailed hardware specification can be found on the MetaCloud homepage [14]. Even though this cluster is shared among other users, it allows us to deploy hundreds of nodes [12].

To make access to cloud resources easier we have implemented interface that simplifies deployment of virtual machines and network connections. The interface uses a REST-base architecture. This allows users to create sandboxes according to configuration file in JSON format or modify deployed sandboxes using available functions. The configuration file defines all attributes of sandbox, e.g., number of Local Area Networks, their addressing, number of hosts, routing between LANs, network link properties. This helps users to focus on the sandbox itself without taking care of how it will be deployed. Every node used in sandbox is described with its name, IP address, physical role, and virtual image ID. Users can create their own images or they can make use of our library of images with preconfigured common services, e.g. FTP, HTTP, DNS.

Users' access to KYPO and sandboxes is realized through one entry point provided by web application developed on Liferay [18] portal technology. According to the users' authorization they are allowed to access deployed sandboxes, manage deployed sandboxes (all or only part), and deploy new sandboxes. Nodes in sandbox are accessible through VNC console. This simulates physical access to the computer. User can reboot the computer or disconnect the computer from sandbox' network without losing access to the system.

3 Training and Exercise Use Case Evaluation

We developed training scenarios in KYPO environment to improve learning process of our students and participants of our workshops. This practice follows the trend of active learning, which is basis of new learning methodologies [19]. In fact students retain 90% of actively used knowledge compared to only 5% of only passively consumed knowledge [20]. Therefore our trainings consists from talk, game where knowledge is actively used, and feedback based on measured data which is given by lecturer.

3.1 Training Scenario Description

Our training scenario, deployed in KYPO Cyber Exercise & Research Platform, is called Capture the Flag Game (CtF Game). It is designed as a multi-level game focused on teaching of basics of penetration testing. This game concept is similar with AEC games [21],[22], D-CTF game [23], SANS NetWars [24], and other cyber security games developed in the world. Game participant plays role of a hacker (cracker), which goal is to take over a server and exploit it for an NTP-based DDoS attack against victim machine. Goal of our CtF Game is to teach participants basic techniques of penetration testing of computer network and its services. In accordance with ENISA practice guide [19] it is also desirable to teach participants these techniques in the most interactive way.

CtF Game consists from simple network infrastructure with three machines. The network topology is depicted in Figure 3. The game contains four levels with increasing difficulty. The First level is focused on a network exploration with common tools. Goal of the second level is exfiltration of an important data through on of server vulnerabilities. The third level is focused on a takeover of the server through other vulnerability using well-known Metasploit tool. Goal of the last level is preparation of the server as an attacking machine and execution of the final attack against victim server. For correct solution of each level player gains score. Maximum score is 600 and is reduced by using hints. Hints penalty varies with importance of the hint. Expected time of solution is between 30 and 120 minutes and it heavily depends on skills of the player.

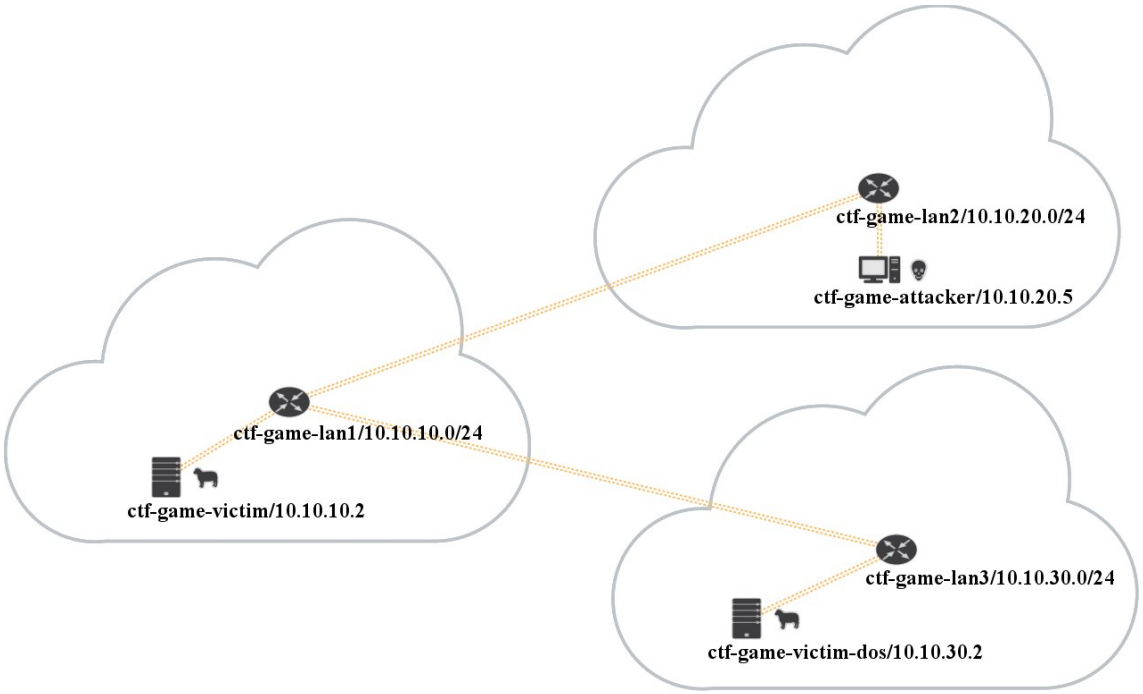

Figure 3: Capture the Flag Game network schema. Users control attacker node via VNC.

3.2 Participants

CtF Game participants came from different organizations and have various sets of skills in area of Information and Communication Technologies and especially a computer security. For our purposes we split participants into three groups defined by skills. Each of these groups is also defined by set of difficulties during CtF Game.

First group called beginners are people with low skills in computer security and ICT in general. Beginners are slow but conscientious players. They have problems with the most basic actions like changing keyboard layout, typing special characters, or logging into KYPO portal. They carefully follow instructions and they do not hesitate to ask for a help.

Second group are experienced users. These users have solid background in computer security and in ICT in general. Experienced users are comfortable with terms like special characters, correct software version, work with console, etc. The biggest pain of these users is their know-how. Experienced users simply do not read manuals. So they do not read our CtF Game instructions either. Experienced users therefore stop in dead end looking for overcomplicated solutions for simple tasks.

Third group are advanced users, which are experts in computer security and in ICT in general. Advanced users have almost same strengths and weaknesses as experienced users. Moreover, they use heavily customized or own compiled browsers, ssh clients, and other programs. These programs are often source of serious complications, if they use own computer.

3.3 Evaluation and Experience

We collect statistical data about our trainings, where CtF Game was used. Most important indicators as level difficulty denoted by a participant, time of completion of the game, and amount of scored points during game are displayed in Table 1. All indicators were divided up by above mentioned groups. As we mentioned before maximum score is 600 and time of solution varies from 30 to 120 minutes. Level difficulty is measured on a scale from 0 to 5, where 0 means very easy level and 5 means extremely hard level. Grading of difficulty do not have strict methodology and it is left up to the user.

	Average Scoring	Average Time	Average Difficulty Level 1	Average Difficulty Level 2	Average Difficulty Level 3	Average Difficulty Level 4
Beginners	431	89	1	3	2	3
Experienced	515	58	0	2	2	3
Advanced	538	45	0	1	1	2

Table 1: Average values of game indicators. Maximum score is 600. Level difficulty is on scale from 0 – very easy to 5 – extremely hard.

We find out two expected trends related to skills of a user. Least experienced users gain fewer points and solve levels longer than more experienced players. Average values are presented in the Table 1. Beginners are further divided into two groups. Those who use Google for looking for answers and those who prefer do task themselves. First group has always shorter time of solution of CtF Game, but score variance is not so obvious. Further we expected that game was designed with increasing level difficulty. All three group show us that this expectation is wrong. Most difficult level is fourth (last) and second level instead of expected last fourth and third level. This may be a consequence of tools or techniques used in the third level. Both causes have similar probability. Technique used in the level is simple SQL Injection into a form in a PHP website. Complication is not understanding of SQL injection, but typo probability is very high. Also tool used in the level is cURL, which is a command-line tool for transferring data via various protocols. CURL is not as well known as other command-line tools like WGET, and web browsers links, and lynx. Further automatic SQL injection is much more common in these days [25]. So users can be frustrated very quickly. The last level discovered unexpected fact that users are too dependent on an interactive shell. Users became confused very quickly after connecting into the machine via telnet terminal, which does not support command completion.

3.4 Lessons Learned

From collected data and our observations during workshops we summarized following lessons learned.

- Users, especially experienced and advanced ones, do not read information, manuals, and texts in game. It is necessary to explicitly tell them the most important facts.
- Unexpected things can be a serious complication. For the example “exotic” keyboard layouts like French or Spanish layout can complicate typing of special characters.
- Unfamiliar operating systems can confuse inexperienced lecturer.
- Experienced and advanced users require copy & paste functionality of VNC console.
- Users from advanced group often require SSH connection to their machine instead of VNC connection.
- Advanced users can find unintentional vulnerabilities and try to use them to complete game levels.
- Always group similar advanced users into same groups. One advanced user in group of beginners can finish too early and he will get bored. In the other hand beginner in group of advanced people will be frustrated from his relatively slow progress.

4 Future Work

In our future work, we will focus on the improvement of user interface, more cost-effective simulation of critical information infrastructures, and implementation of more advanced tools for cyber security trainings and exercises management, execution and evaluation. Simultaneously, we will be active in development of other useful features such as a KYPO Connection Point.

We will improve user interface for players and also for lecturers. User interface for players will be updated to provide better experience during trainings and exercises. New features will also provide support for remote attendance on trainings and exercises and remote communication with lecturer. User interface for lecturers will be updated to provide automatic processes for training use case preparation and deployment. New tools will provide

advanced management of training and effective evaluation of participants' actions and therefore more valuable feedback.

KYPO Cyber Exercise & Research Platform back end will be updated to provide more cost-effective deployment of very large infrastructures. This goal will be achieved by advanced cloud resources planning (RAM, CPU, bandwidth, storage) and better resource utilization. Measuring and support infrastructure will be also updated to be more effective in work with cloud resources.

We will also develop KYPO Connection Point, which will provide remote connection of physical piece of hardware to KYPO environment. These pieces of hardware can be subsequently embedded into scenarios for testing, evaluating, or used for training purposes. It is especially useful for hardware, which cannot be emulated like SCADA systems, Base Station Subsystems, industrial computers, and other parts of Critical Information Infrastructure.

References

[1] White B., et al. An integrated experimental environment for distributed systems and networks. *ACM SIGOPS Operating Systems Review*, 2002, 36.SI: 255-270.

[2] Enisa.europa.eu, 2014, Cyber Europe 2014 Information — ENISA. [online]. 2014. [Accessed 13 April 2015]. Available from: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information

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

[4] CCDCOE, 2015, Locked Shields 2015. [online]. 2015. [Accessed 13 April 2015]. Available from: https://ccdcoe.org/locked-shields-2015.html

[5] Drašar M., et al. Similarity as a central approach to flow-based anomaly detection. *International Journal of Network Management*, 2014, 24.4: 318-336.

[6] Claise B. "Cisco Systems NetFlow Services Export Version 9," RFC3954 (Informational), Internet Engineering Task Force, 2004.

[7] Paterva.com, 2015, Paterva / Maltego. [online]. 2015. [Accessed 13 April 2015]. Available from: https://www.paterva.com/web6/products/maltego.php

[8] Benzel, T., et al. Experience with DETER: a testbed for security research. In: *Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006. 2nd International Conference on*. IEEE, 2006. p. 10 pp.-388.

[9] Chen L. Construction of the New Generation Network Security Testbed-Testbed@ TWISC: Integration and Implementation on Software Aspect. *Institute of Computer & Communication, National Cheng Kung University, Tainan, Taiwan*, 2008.

[10] Årnes A., et al. Using a virtual security testbed for digital forensic reconstruction. *Journal in Computer Virology*, 2007, 2.4: 275-289.

[11] Krishna K., et al. V-NetLab: a cost-effective platform to support course projects in computer security. In: *Proceedings of 9th Colloquium for Information Systems Security Education*. 2005.

[12] Kouřil D., et. al. Cloud-based Testbed for Simulation of Cyber Attacks. In Hanan Lutfiyya and Piotr Cholda. *Proceedings of the Network Operations and Management Symposium (NOMS 2014)*. Krakow, Poland: IEEE Xplore Digital Library, 2014. ISBN 978-1-4799-0913-1.

[13] Cesnet.cz, 2015, CESNET | CESNET, zájmové sdružení právnických osob. [online]. 2015. [Accessed 13 April 2015]. Available from: http://www.cesnet.cz

[14] Metavo.metacentrum.cz, 2015, MetaCentrum - Virtual Organization. [online]. 2015. [Accessed 13 April 2015]. Available from: http://metavo.metacentrum.cz/en/index.html

[15] Opennebula.org, 2015, OpenNebula | Flexible Enterprise Cloud Made Simple. [online]. 2015. [Accessed 13 April 2015]. Available from: http://opennebula.org/

[16] Amazon Web Services, Inc., 2015, AWS | Amazon Elastic Compute Cloud (EC2) - Scalable Cloud Hosting. [online]. 2015. [Accessed 13 April 2015]. Available from: http://aws.amazon.com/ec2/

[17] Google Developers, 2015, Google Cloud Computing, Hosting Services & Cloud Support. [online]. 2015. [Accessed 13 April 2015]. Available from: https://cloud.google.com/

[18] Liferay.com, 2015, Liferay - Enterprise open source portal and collaboration software - Liferay.com. [online]. 2015. [Accessed 13 April 2015]. Available from: http://www.liferay.com/

[19] Good Practice Guide On Training Methodologies: How to Become an Effective and Inspirational Trainer. Heraklion: ENISA, 2014, 2014. Accessed April 9, 2015. http://dx.publications.europa.eu/10.2824/33183.

[20] LALLEY, J.; MILLER, R. The learning pyramid: Does it point teachers in the right direction. *Education*, 2007, 128.1: 16.

[21] Tresner M. 2015, Hacking Competition - hackerská soutěž. Aec.pentest.cz. [online]. 2015. [Accessed 13 April 2015]. Available from: http://aec.pentest.cz/

[22] Tresner, M, 2015, SafeWeb.cz / CTF Hacking Competition. Safeweb.cz. [online]. 2015. [Accessed 13 April 2015]. Available from: http://www.safeweb.cz/

[23] Dctf.defcamp.ro, 2015, D-CTF 2014 - DefCamp Capture the Flag. [online]. 2015. [Accessed 13 April 2015]. Available from: http://dctf.defcamp.ro/

[24] SANS Institute, 2013, SANS NETWARS, [online]. 2013. [Accessed 13 April 2015]. Available from: http://www.sans.org/media/netwars/brochure-netwars-2013.pdf

[25] Sqlmap.org, 2015, sqlmap: automatic SQL injection and database takeover tool. [online]. 2015. [Accessed 13 April 2015]. Available from: http://sqlmap.org/