Modern Applied Science; Vol. 10, No. 11; 2016
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

A CTF-Based Approach in Information Security Education: An Extracurricular Activity in Teaching Students at Altai State University, Russia

Alexander Mansurov[1]

[1] Altai State University (ASU), Barnaul, Russia

Correspondence: Alexander Mansurov, Faculty of Physics and Technics, Altai State University (ASU), Barnaul, 656049, Russia. E-mail: mansurov.alex@gmail.com

Received: June 18, 2016 Accepted: July 18, 2016 Online Published: August 17, 2016

doi:10.5539/mas.v10n11p159 URL: http://dx.doi.org/10.5539/mas.v10n11p159

Abstract

Capture the Flag (CTF) competitions are the most popular events in cybersecurity conferences where participants can demonstrate their skills. Also, the CTF is widely acknowledged as a valuable pedagogical tool for providing the students with real life problems in computer security area when dealing with CTF tasks. However, there is the possibility to go beyond treating CTF tasks only. The paper presents an approach to establish a CTF-based educational framework that allows students to gain more practical skills, knowledge and expertise in information security and related areas. The framework is implemented in Altai State University (Barnaul, Russia) in 2014 as an extracurricular club activity, and the club runs successfully up till now. Pedagogical benefits, learning methodology and educational aspects are discussed, and positive feedback shows the success of the proposed approach.

Keywords: information security, capture the flag, active learning, lab workshop, vulnerabilities

1. Introduction

Capture the Flag (CTF) exercises and competitions nowadays are regular and well-known events in various semi-professional information security conferences. Everyone can demonstrate his or her skills in practical cyber security tasks and problems. Tasks for Jeopardy-type CTFs often deal with various practical aspects of information security like stego, reverse engineering, cryptography, binary analysis, etc. Attack-Defense type CTFs require knowledge and experience with developing exploits, using hacking tools and patching vulnerabilities. These simulated real-life problems set an extremely high knowledge barrier for CTF participants. To be successful, they have to be proficient in numerous topics and possess hands-on experience. Otherwise, dealing with almost real-life problems (CTF tasks) can be "frustrating and bewildering" (Werther, Zhivich, Leek, & Zeldovich, 2011) due to complexity of problems.

In Russian Federation, higher education (and information security education is no exception) is governed by Federal State Educational Standards (FSES) – a set of mandatory requirements for a defined level of education and (or) field of study. The standards are approved by the federal executive branch responsible for public policy and legal regulation in the sphere of education. FSES regulate time limits of major and minor courses and contain requirements for implementation and results that should be achieved afterward (FSES, 2010). Following FSES, Altai State University offers a traditional curriculum in information security that is mostly aimed at providing a general scope of knowledge and basic practical experience in respective areas due to a limitation of academic hours in courses. Workshops and labs deal with pre-organized assignments that aimed at specific aspects of problem areas and understanding of principles. Thus, experience and critical skills needed for cybersecurity, such as script programming, system administration, networking, web-programming, besides many others, are often left out of consideration (Cheung, Cohen, Lo, Elia, & Carrillo, 2012). In this case, self-study and peer instruction are the only options left for students, and it requires motivation to learn and practice on their own.

Another shortcoming is that there is a regular course load for students with scheduled increase in school work. Without a thorough supervision, there is a high chance that students would quit self-studying due to the lack of extra time, and further focus on something else more interesting and important for them. Thus, they may not

retain the knowledge they gained without its regular refreshment and application.

Several papers (Werther et al., 2011; Eagle & Clark, 2004; Irvine, 2011) state that a CTF event 'as-is' offers limited educational opportunities since *a priori* knowledge and experience should already be available at hand. However, it is still possible to use them as a pedagogical tool for teaching computer security. CTF tasks are widely used to teach students to solve them directly as examples of real life problems, and specially arranged introductory lectures and classes are offered to cover task-related problems and backgrounds (Werther et al., 2011; Eagle & Clark, 2004; Ho, Mallesh & Wright, 2009). Workshops are organized to build up teamwork and provide a hands-on experience. Still, the CTF remains just a 'tool' linked to a real life-like practice.

In this paper, an approach to developing a CTF-based educational framework to provide students with knowledge and practical experience they are lacking is presented. The framework is implemented in Altai State University (Barnaul, Russia) in a form of an extracurricular activity. The proposed approach allows covering blind spots in students' knowledge, coordinating the learning process, and utilizing all steps of the CTF for educational purposes.

2. Pedagogical Aspects

To exploit the CTF to its full potential with further benefits, a form of extracurricular activities is the most advantageous one. There are several aspects that have been considered beforehand:

1) Teamwork / Group working. Application of teamwork is not limited to curriculum and management functions in education. It is a well-known approach to tackling difficult problems as well as the basis for various educational techniques (Sallis, 2002). For the CTF, to be able to work as a group in a team is crucial for students to achieve something. Since most tasks are complex, it is necessary to share the load and responsibility. Firstly, working in a team allows students to hone their good communication skills for successful interaction with other members of a group. Also, it is a way for students to compare their knowledge and skills with each other and to point out what should be learned further to be successful.

2) Active and collaborative learning. Today's working environment often includes team activities and collaborative working. Therefore, it is appropriate for students to learn how to build a team with members of different skills and work together on a common problem, utilizing each member's strength effectively. Sharing information and discussing problems, learning something together and from each other proves to be very advantageous in computer security management and provides valuable experience (Conklin, 2006).

3) Challenge based learning. This framework focuses on increasing student engagement in addressing issues and proposing solutions. It is a student-centered approach with its roots in problem-based learning technique. Challenge based learning is ideally suited for tackling cybersecurity problems. Students gather around a certain problem and try to find a way to solve it. This stimulates the development of problem-solving skills and cognitive process. Since there could be a variety of proposed solutions, students need to obtain more knowledge to provide a better one. The role of a teacher here is gradually shifted to coaching and assisting students with guiding activities and resources (Cheung et al., 2011).

4) No strict curriculum. Extracurricular activities are not regulated by educational standards and do not have to follow certain plan and schedule. There are no limitations to forms of educational activities and techniques. Therefore, it allows some liberty in providing the most effective solution and guidance to cover certain areas of knowledge for students when needed. For example, some topics are better delivered in lectures, while the others are required practical experience and workshop participation. Also, the role of a tutor for those cases is assigned to the most capable and experienced person – a student with profound knowledge and experience on the subject, a professional who deals with the subject on a regular basis, or a faculty teacher.

3. Educational Design

To exploit the CTF to its full potential, an extracurricular 'free to join' club "CTF Club" for students interested in deep knowledge and real-life experience in various areas of information security and communication technologies was established. The club has been supported by faculty administration and provides three supervised sessions per week (16 weeks in a semester). All sessions are hosted in a teaching lab equipped with switches, routers, servers, and workstations. Lab vacant hours are available for students for their self-study activities. The first session is usually a lecture or an overview of content that is necessary for dealing with the next two workshop sessions. If several problems arise during workshops, or some aspects are needed to be discussed more thoroughly, then the third workshop includes the required coverage and case studies. However, the order could be changed freely according to the particular situation.

Since every step in a CTF competition could be treated as a source of valuable knowledge and experience, it is

wise to identify primary CTF 'elements' that should be covered by the "CTF Club" in its educational framework (Fig. 1).

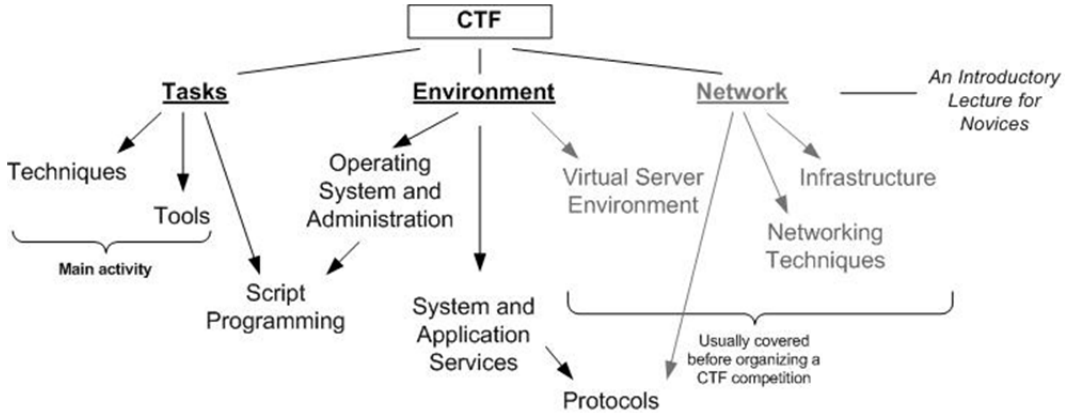

Figure 1. CTF-based framework structure

Usually, an introductory lecture is delivered for novices on their first session. It provides an overview of the CTF events and what the CTF is 'made of', i.e. kinds of CTF competitions, types of tasks, working environment, and networking. This session allows novices to understand better what it is expected them to do and what knowledge and skills are required.

Several topics related to networking and setting up the working environment are covered separately when students decide to organize their own CTF competitions. Since most of the content is not about the cybersecurity problems, it is not on the main club agenda. Still, it helps students to brush up their skills on deploying network configurations and managing virtual servers and services.

Dealing with tasks, performing attacks and providing defensive measures are the most interesting activities, and a major amount of time is devoted to these problems. To successfully solve a CTF task and to learn something from it, a lot of additional areas of expertise should be involved. They are placed within the scope of the '*Environment*' section on Fig.1. Here, the '*Environment*' means not only the working environment of CTF competitions like scoreboards or a group of virtual servers, but the environment for the task or the real life-like problem that introduced to students. Therefore, it is necessary to understand 'how it works' and 'why it is happening.' Covering the mentioned areas and choosing the most suitable form for it (a self-study, a study in a group, a case study, or a lecture) depend on a particular problem and are completely up to the students. Since different tasks can bring up the same areas of expertise repeatedly, it significantly contributes to mastering these areas by students and retaining their knowledge and skills.

3.1 CTF Tasks

There is a variety of CTF tasks, and each task is linked with a certain area of knowledge, skills, and expertise. Schematically, this can be illustrated as follows (Fig. 2):

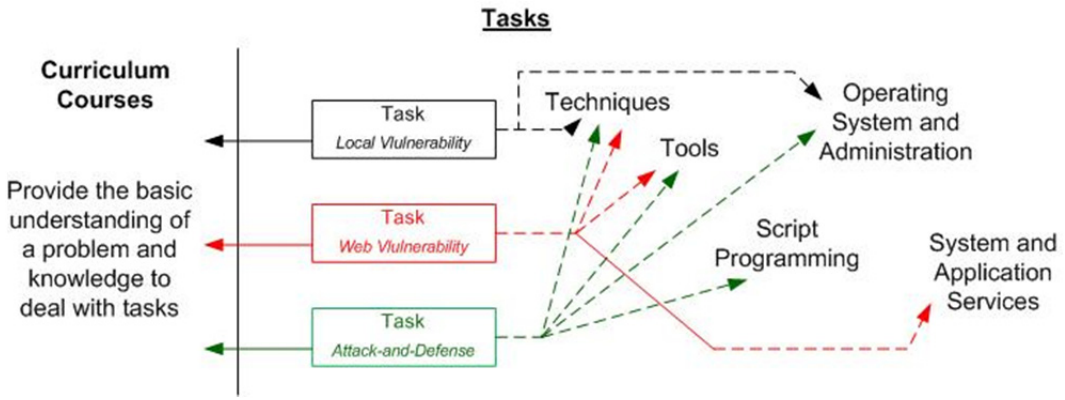

Figure 2. CTF tasks linked with respective areas of knowledge and expertise

Generally, a solution for a task is vastly based on *a technique* that should be applied and *a tool* to execute the technique. However, applying a technique or using a tool require knowledge and skills to back up the actions. Since the goal of the club is to provide knowledge and skills, task solving procedure needs to be analyzed for what knowledge and skills are exactly required and to which area they belong. The next step is to clarify whether students / club members are familiar with what required or not. When this step is covered, and blind spots are revealed, the next action is to get rid of the blind spots by providing the necessary teaching and explanation. Thus, each task appears to be linked with more than just techniques and tools and carries a lot more than just practical experience. Students learn not just how to deal with a problem, but what stands behind it and how it could be prevented. Additionally, they get insights on how to use tools better and how their work can be improved.

Local vulnerability tasks often exploit workarounds and malfunctions in elements and system services of operating systems (OS) that lead to violation of access rights policies. They are directly linked to *aspects of OS functioning and OS administration*. Besides the 'know-how', *a tool* or an exploit might be needed to successfully exploit the vulnerability. Also, it is important to understand what steps should be done to prevent someone from exploiting it in the future.

Web vulnerability tasks originate in misprogrammed Web-based applications and misconfigured Web-services. Often they rely on SQL injections, cross-site referencing and code injection. Obviously, much attention should be paid to the functioning of *system and application services*, as well as aspects of safe *programming* and source code analysis.

Attack and defense tasks deal with protecting your own services while exploiting the vulnerabilities of the services of others. Thus, besides aspects of *system administration*, source code analysis and patching rely heavily on *programming* skills, and effective use of *tools* (exploits, scanners, etc.) includes *script programming*. All of this is governed by a set of techniques for effective discovery of vulnerabilities and matching them with respective tools.

Binary exploit and reversing tasks are based on deep understanding of how compiled code executes and performs. Those are the most difficult tasks for students because they address to skills of low-level programming, disassembling and program tracing. Unfortunately, a lot of self-study and self-devotion that is needed is not admired by students, and those tasks are not very popular in the club.

Forensic, steganography and cryptography tasks require the knowledge of techniques, algorithms, and protocols. This knowledge is usually provided by curriculum courses and exploited during club sessions.

Naturally, dealing with all tasks is mandatorily linked with the knowledge that students get from their curriculum courses. It greatly helps to keep their knowledge at hand and to revisit parts of courses that have already been forgotten. If some course yet to be studied, students are advised to learn what they need to solve the task either on their own or in one of the club session that provides teaching and explanation. In the future, it allows students to reduce the course load and to improve greatly while studying the mentioned course in their curriculum. What is not covered in curriculum courses (like, for example, aspects of *OS administration* and *script programming*) can be mastered during the club sessions.

Tasks for club sessions are obtained from the Internet. There are many Web resources about CTF activities (e.g., '*The Practice CTF List*' - *http://captf.com/practice-ctf/*) where anyone can find a set of pre-arranged tasks for their liking. Students who are already experienced in the CTF try to develop their own tasks for club sessions and their own CTF competitions. This requires good programming skills and essential knowledge about security aspects that should be incorporated in self-made tasks.

Quests are also very popular among club members. The quest includes a set of tasks linked with each other with a clearly defined final goal. A great source of ready to use quests is the '*Vulnerable by Design*' resource (*https://www.vulnhub.com/*). An already prepared virtual machine (VM) image can be downloaded and run during club sessions or by students individually for their self-study. Additionally, there are 'walkthroughs' - step by step guides on how to solve all the tasks, what techniques and tools should be used for each step. They are of great importance for educational process of the "CTF Club". Each step can be analyzed and explained besides being simply repeated in practice. Repeating the steps of a 'walkthrough' allows students to gain practical skills, while analyzing and explaining of what have been done and what have been used allow to obtain the knowledge necessary to back up skills and build up the experience.

There are no strict regulations on what tools (exploits, libraries, scanners, traffic analyzers, etc.) should have been used. The main goal of club sessions is to provide education while tools are just necessities that may come,

evolve and go. Also, club sessions do not teach programming languages since these details could be mastered by students in self-study.

3.2 CTF Environment

Typical CTF working environment should be scalable, manageable and reliable. The most common approach that meets those criteria is the Virtual Server Environment. Virtualization is quite handy for workshops and practices. Students use freeware products *VMware Workstation Player* (*http://www.vmware.com/products/player/*) and *Oracle VM VirtualBox* (*http://www.virtualbox.org/*) for running and working with already prepared VMs or their own Linux server. However, production virtualization solutions are more complex, and many questions should be addressed concerning their security, management, and reliable operations. Students can practice and get additional expertise on:

- hypervisors and aspects of their functioning;
- aspects of security and reliability of virtual servers;
- configuration and management of virtual servers in a virtualization environment;
- providing security and reliability for services and applications running on a virtual server.

For educational purposes, freeware solutions like *KVM* (*http://www.linux-kvm.org/*), *OpenVZ* (*http://openvz.org/*) and *vSphere Hypervisor* (*http://www.vmware.com/products/vsphere-hypervisor/*) are used and studied in club sessions. Students also work with *Docker* containers (*http://www.docker.com/*) to get familiar with another architectural approach for resource isolation and investigate matters of security and protection of applications.

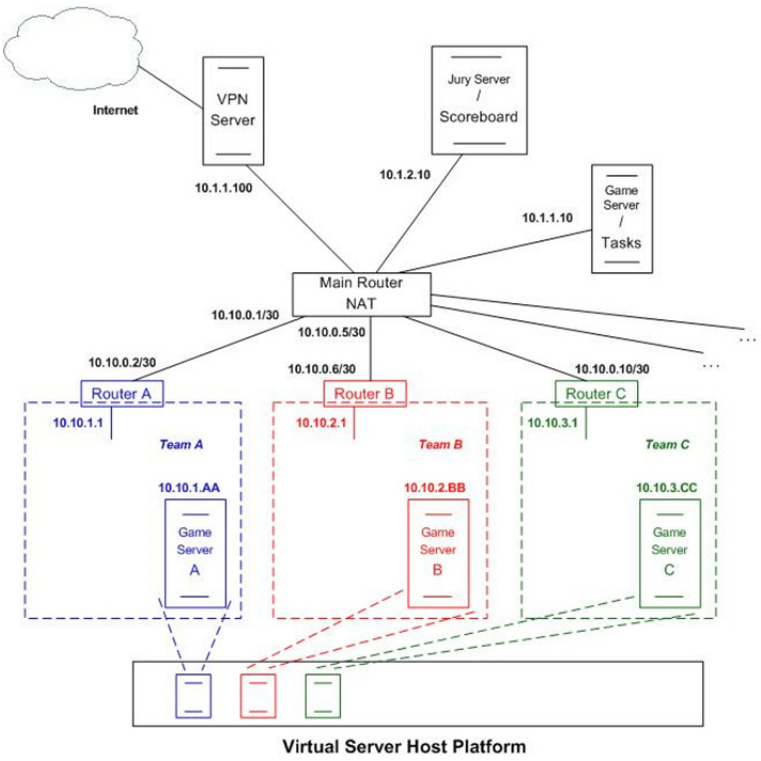

Figure 3. Typical network configuration for CTF events

3.3 Networking

A typical network configuration for CTF events is presented on Fig. 3. Networks of each team are connected through respective routers to the Main router that enables overall connectivity. There is a separate game server for each team for Attack and Defense CTFs. The main router in Attack and Defense CTFs also performs NAT on team network links to prevent players from identifying the source of attacks. The game server with tasks is deployed for task/quest based CTF events. There is the Jury Server that monitors the event and displays the scoreboard with points. The virtual private network (VPN) server is needed for external players that wish to join

the action. Thus, an isolated network is created, and aspects of security for global and corporate university network are ensured.

There are also many opportunities for students to become more proficient in networking. Setting up the network configuration in Fig.3 requires an understanding of networking technologies, routing, and configuration of network equipment like switches and routers. Most of these aspects are usually covered in respected curriculum courses, but here is a real network that should be deployed and maintained in operation. Thus, it becomes handy for students to refresh their knowledge and gain practical experience. For advanced steps, technologies like VRF (Virtual Routing and Forwarding) or problems like route leaking can be studied and discussed.

3.4 OS Administration

There are many things that need to be studied and experienced in practice in *OS administration*, especially in administration of Unix-like OSes. Dealing with tasks, deploying servers and configuring services allows to enhance the students' knowledge in this area and to develop quite a number of skills. Also, many aspects of OS security mechanisms are studied thoroughly (for example, behavior of suid programs or SELinux configuration) and kept within reach. Besides, the use of services and applications that run on OS like proxies, firewalls and scanners for border control and inspection of traffic is quite beneficial for future computer security specialists.

Another point in studying *OS administration* more deeply is *script programming*. It is required for convenience and work automation. Since it deals with programming, a teaching of writing scripts is usually omitted from curriculum courses. However, it is widely used in real life practice, and students have to use scripts to develop their own tasks and improve their performance when solving tasks. Basic aspects of shell programming and usage of Perl, Python, and other script languages are generally covered in one of the club sessions and are further mastered by students in their self-study.

4. Operating the Club

The "CTF Club" in Altai State University started its work in 2014. At first, there were only a handful of people enough to form a single team. The club got more popular in the next year, and it was possible to start running own CTF competitions and participate in others due to a number of students who already have an experience and those who have a desire to test their skills. Nowadays, there is a group of students who are closely engaged in club activities while other students prefer to attend only those sessions that they are interested in. However, a brief survey conducted in March 2016 shows the following results:

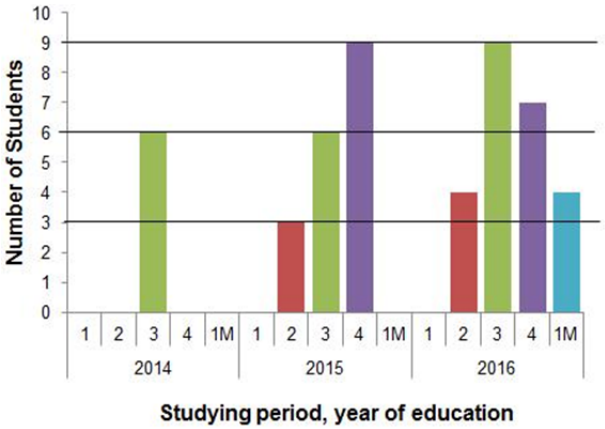

Figure 4. Number of student members of the club

Figure 4 shows the increase of interest in club activities among students. From six students at the beginning in 2014, there are students of almost all years of education who joined the club activities. In 2016, four first-year master's students who were formerly graduate bachelor students decide to stay in the club and continue to participate in club sessions. Being the most experienced ones they provide the assistance and coaching in various aspects to other students as well as sharing their experience.

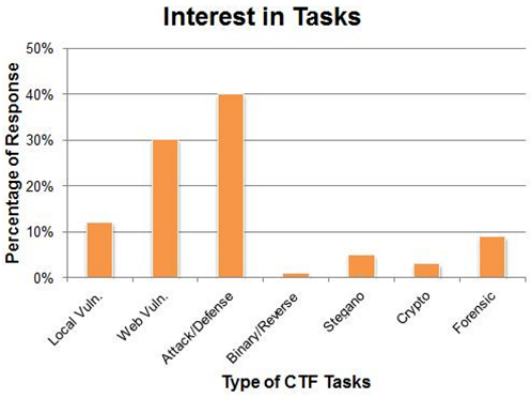

Figure 5. Students interest in CTF tasks

Figure 5 demonstrates the interest in CTF tasks among students. As it was mentioned earlier, the most popular are tasks of 'Attack and Defense' type. Naturally, they are the most realistic and competitive ones and require good teamwork and offensive/defensive skills. Next in popularity are tasks dealing with Web and local vulnerabilities. They offer an immediate satisfaction by displaying the results of work and can be done both in teams or singlehandedly. The least popular are binary reversing and cryptography tasks due to their complexity and a huge amount of meticulous work.

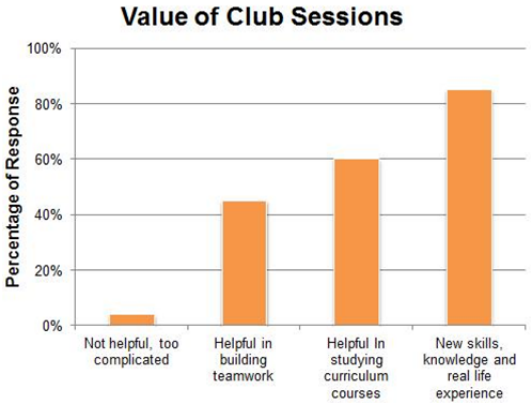

Figure 6. The value of club sessions for students

Figure 6 shows the results of a multiple choice question about the value of club sessions for students. Almost all of the student members believe that the most valuable thing for them is the opportunity to get news skills, knowledge and real life experience in cybersecurity problems. Also, they praise club activities for being helpful in building teamwork and studying their curriculum courses. Obviously, dealing with tasks and catching up with others were quite overwhelming for someone. However, the overall results clearly demonstrate the successfulness of club sessions and students appreciation for usefulness of club activities.

4. Conclusion

This paper presented the CTF-based educational framework to provide students studying information security with additional skills, knowledge and real life experience. The proposed framework is implemented in Altai State University in 2014 in a form of an extracurricular activity that coexists well with the curriculum and has several pedagogical benefits. Being student-centered and allowing the liberty in acquiring the needed knowledge and skills 'on demand' are of great advantage for the proposed framework. Besides, there are no limitations to dealing with CTF tasks only, so, other aspects concerning system administration, script programming, virtualization environment, networking, and protocols are studied and practiced. This also helps students a lot with studying their curriculum courses and getting more proficient in practical aspects of their future work. There is a clearly demonstrated interest among students and positive feedback that shows the success and

usefulness of the proposed approach.

References

Werther, J., Zhivich, M., Leek, T., & Zeldovich, N. (2011). Experiences in cyber security education: The MIT Lincoln laboratory capture-the-flag exercise. *Proceedings of the 4th Cyber Security Experimentation and Test* (pp. 12-12). Retrieved from https://www.ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/2011_08_08_Werther_CSET_FP.pdf

Eagle, C., & Clark, J. L. (2004). Capture-the-Flag: Learning Computer Security Under Fire. *Proceedings of the Sixth Workshop on Education in Computer Security (WECS)* (pp. 17-21). Monterey, CA. Retrieved from http://calhoun.nps.edu/bitstream/handle/10945/7203/wecs6_ch04.pdf

Irvine, C. (2011). The value of capture-the-flag exercises in education: An interview with Chris Eeagle. *IEEE Security & Privacy*, *9*(6), 58–60. http://doi.ieeecomputersociety.org/10.1109/MSP.2011.177

Cheung, R., Cohen, J., Lo, H., Elia, F., & Carrillo Marquez Veronica (2012). Effectiveness of Cybersecurity Competitions. *Proceedings of International Conference on Security and Management*. Las Vegas, Nevada. Retrieved from http://josephpcohen.com/papers/seccomp.pdf

Cheung, R., Cohen, J., Lo, H., & Elia, F. (2011). Challenge based learning in cybersecurity education. *Proceedings of the 2011 International Conference on Security & Management*. Las Vegas, Nevada, USA. Retrieved from http://josephpcohen.com/papers/cbl.pdf

FSES for Information Security. (2010). *Higher Education FSES Portal* (in Russian). Retrieved from http://fgosvo.ru/fgosvpo/7/6/1/9

Ho, J. W., Mallesh, N., & Wright, M. (2009). The Design and Lessons of the ASCENT Security Teaching Lab. *Proceedings of the 13th Colloquium for Information Systems Security Education* (pp.124-132). Seattle, WA. Retrieved from https://www.asee.org/public/conferences/8/papers/4887/download

Sallis, E. (2002). *Total Quality Management in Education*. Psychology Press.

Conklin, A. (2006). Cyber Defense Competition and Information Security Education: An Active Learning Solution for a Capstone Course. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*. http://dx.doi.org/10.1109/HICSS.2006.110

Copyrights