i-tee: A fully automated Cyber Defense Competition for Students

Margus Ernits
Tallinn University of Technology
Akadeemia tee 15a, Tallinn,
Estonia
margus.ernits@gmail.com

Johannes Tammekänd
Estonian IT College
Raja 4C, Tallinn,
Estonia
johannes.tammekand@gmail.com

Olaf Maennel
Tallinn University of Technology
Akadeemia tee 15a, Tallinn,
Estonia
olaf.maennel@ttu.ee

Abstract

We present an *Intelligent Training Exercise Environment* (*i-tee*[1]), a fully automated Cyber Defense Competition platform. The main features of i-tee are: automated attacks, automated scoring with immediate feedback using a scoreboard, and background traffic generation. The main advantage of the platform is easy integration into existing curricula and suitability for continuous education as well as on-site training at companies. The platform implements a modular approach called *learning spaces* for implementing different competitions and hands-on labs. The platform is highly automated to enable execution with up to 30 teams by one person using a single server.

The platform is publicly available under MIT license[2].

Categories and Subject Descriptors

C.2.4 [**Computer Systems Organization**]: Distributed Systems—*Client/server*

Keywords

Cyber Security Exercises; auto-configuration; Virtual Networks

1. INTRODUCTION

Practical hands-on and problem-based learning is an efficient way to study Information and Communications Technology (ICT) subjects, as it provides a playful and exciting learning experience [1]. Therefore, Cyber Defense Exercises (CDX) are used to give a realistic, intensive learning experience for students [1].

Given the huge and proven benefits of such learning events, one might ask: Why are CDX-s not integrated into every ICT curriculum?

The problem: Although a CDX is an effective learning method it is rarely used because designing a new cyber competition is a complex and time consuming task that contains many design steps such as: Objectives, Approach, Topology, Scenario, Rules, Metrics and Lessons Learned [2].

Creating a new CDX demands a huge amount of effort from the organizer—well beyond that of designing a new course. In addition, one may not have all the competences needed for developing a new CDX.

To the best of our knowledge there are no defense oriented CDX platforms publicly available that are open source, easily integrated into existing curriculum, provide modular learning spaces, and can be executed by one instructor alone.

2. EXAMPLE OF A LEARNING SPACE

Our platform consist of an underlying framework on which several learning spaces can be hosted. We will discuss an example of one learning space, "CyberOlympics 2015". This event was held in Estonia on February 14, 2015[3].

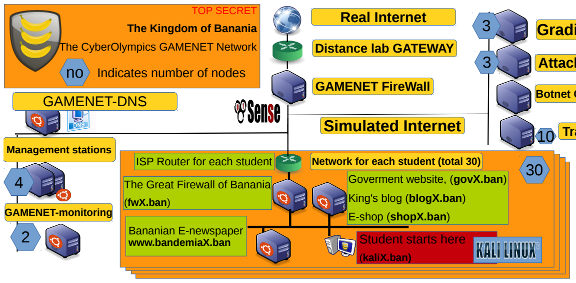

Figure 1: The GameNet

The Scenario brings the participant to a role-play in the *Kingdom of Banania* as intern for system administration of Bananian e-Government[4]. The task is to ensure the availability and functionality of the websites such as: Governmental site govX.ban (where X represents the No of participant/team), King's Blog blogX.ban and e-shop shopX.ban as shown in Figure 1.

Several events emerge, such as: defacement of government's website, threatening video from Hacker group Acronymous #OP Banania followed by intensive attacks.

The full scenario can be found from competition's website[5]. We are using Blue team type CDX [3], where the defending (Blue) teams compete with each other and against automated attacks performed by the system.

[1] **i-tee** — In Estonian "tee" means way/path/street. So i-tee can be understood as "Information-way".

[2] https://github.com/magavdraakon/i-tee

[3] http://www.kmin.ee/en/news/unique-student-cyberwar-games-be-held-estonia

[4] https://www.youtube.com/watch?v=-nzMTk0Nkbw

[5] http://www.kyberolympia.ee/competition

SIGCOMM '15 August 17-21, 2015, London, United Kingdom
© 2015 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-3542-3/15/08.
DOI: http://dx.doi.org/10.1145/2785956.2790033

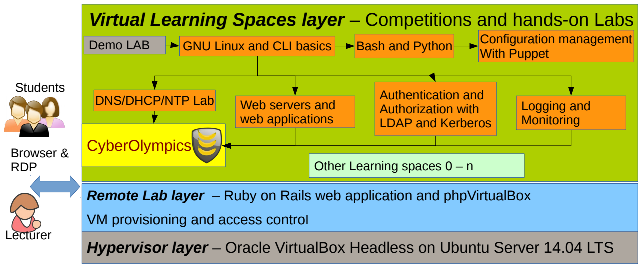
Virtual Learning Spaces layer – Competitions and hands-on Labs
Demo LAB
GNU Linux and CLI basics
Bash and Python
Configuration management With Puppet
DNS/DHCP/NTP Lab
Web servers and web applications
Authentication and Authorization with LDAP and Kerberos
Logging and Monitoring
CyberOlympics
Other Learning spaces 0 – n
Students
Browser & RDP
Lecturer
Remote Lab layer – Ruby on Rails web application and phpVirtualBox
VM provisioning and access control
Hypervisor layer – Oracle VirtualBox Headless on Ubuntu Server 14.04 LTS

Figure 2: The architecture of the system

The students are in the role of defenders and after completing the tasks they are able to recognize common attacks against web applications, install different application level firewalls such as web application firewalls, SQL firewalls, intrusion detection and prevention systems. For each student the scoring system assesses the availability and functionality of the websites, attack-proofing, and the time to recover. This provides valuable feedback to the learners during and after the execution.

3. ARCHITECTURE OVERVIEW

Our proposed framework is an open source platform that enables an easy creation of a new cyber security competition with up-to-date content and resource-friendly execution. The game environment is accessible over the Internet using a web browser and a Remote Desktop Protocol (RDP) client. Each team or participant operates in the game environment their own isolated network and virtual machines, see Figure 1.

The automation includes the setup of Virtual Machines (VM's) for each participant, configuring private and shared networks and most crucially, performing malicious attacks against each team, providing automated scoring of objectives.

The platform has three layers as seen in Figure 2. First, the **Virtualization Layer** runs the VM's and is driven by upper layers. Second, the **Virtual Lab Layer** provides Remote Access (web, RDP) and Control functions for the VM's (start, stop, pause, console access) and for executions (start, stop, pause, attack, open objective, end). Third, the **Virtual Learning Space Layer** provides the scenario, objectives, automated scoring and automated attacks for objectives. Immediate feedback for competitors shows the progress and score using the scoreboard. The automated traffic generator provides smoke cover for automated attacks and hides scoring traffic as well, therefore making the cyber event more realistic and difficult. Some key functions are:

Automated VM provisioning is template-based and on demand when a new student starts their own learning space or joins the competition. Particular VMs are built using *Puppet* configuration manager, shell and Python scripts to customize the VM and networks based on the VM's role, student and the learning space. In addition, all virtual networks needed for new students are generated on the fly. For example, when a new VM starts, the configuration of network interfaces and networks are automatic based on template name, username and learning space name.

Automated attacks are executed after opening the corresponding objective. Attacks are generated by attack bots residing in simulated Internet subnet as shown in Figure 1. Attacks currently available in *i-tee* include: Distributed Denial of Service DDOS, shellshock, Heartbleed, SQL injections, Command injections, cross site scripting (XSS) and several attacks against security misconfigurations, outdated software and cookie security. More attacks will be added in the future and can also be shared among all contributors. Attack bots have functionality to change the attackers' IP address on the fly, making blocking harder. For example, an attack using SQL injection logs into a web-shop, manipulates with prices and buys items.

Automated scoring is performed for each objective and gives visualized feedback for students using the scoreboard[6]. Scoring is done by scoring-bots which are located in the same IP space as attack-bots (Figure 1). When one particular IP is used by attack bots then the scoring-bot will not reuse this IP and vice versa, because a student can block attackers but is not allowed to block scoring as non malicious traffic.

Noise generation: When students investigate the attacks and try to separate an attacker's traffic from legitimate traffic, such as scoring, the attacks could easily be distinguished without background noise. The platform provides a responsive customizable application level traffic generator that simulates real users and hides the attacks. The traffic generators are controlled by the central control server (CnC) and the amount of traffic is tunable during the execution.

Hardware used to run CDX learning space was: HP ProLiant DL380 G7, 2CPU total 12 core (24 threads). RAID 10 2TB disk, 148GB RAM. Actual resources required for a competition depend on the number of participants and complexity of team networks. In the CyberOlymics each student required about 4GB RAM and less than 20GB HDD.

4. CONCLUSIONS

The main contribution is the open source framework *i-tee* itself, which provides automation for cyber defense exercises and training. It allows running different types of complex exercises with little preparation by the facilitators. The *i-tee* platform was successfully tested during a live CDX and has proven useful during several hands-on classes in the context of a university curriculum. The platform is able to run several learning spaces in parallel and has modular architecture enabling reuse of fragments from different learning spaces. We hope that this platform will be used by the community to develop and share new learning spaces and improve the quality of studies by providing a hands-on playful learning experience.

5. REFERENCES

[1] C. Eagle. Computer security competitions: Expanding educational outcomes. *IEEE Security and Privacy*, 11(4):69–71, 2013.

[2] A. FurtunaÌĘ, V.-V. Patriciu, and I. Bica. A structured approach for implementing cyber security exercises. In *Communications (COMM), 2010 8th International Conference on*, pages 415–418, June 2010.

[3] J. Rursch and D. Jacobson. When a testbed does more than testing: The internet-scale event attack and generation environment (iseage) - providing learning and synthesizing experiences for cyber security students. In *Frontiers in Education Conference, 2013 IEEE*, pages 1267–1272, Oct 2013.

[6] Scoreboard 2015 – http://scoring.kyberolympia.ee/