Research Project Report

Cyber Range

Sergey Grebennikov
Innopolis University
s.grebennikov@innopolis.ru

Vadim Rashitov
Innopolis University
v.rashitov@innopolis.ru

Saif Saad
Innopolis University
s.s.mohammed@innopolis.ru

Dmitry Fofanov
Innopolis University
d.fofanov@innopolis.ru

August 5, 2018

Abstract

The corporate systems and applications require regular security tests. In the same time, no less important is a qualification of specialists in the company according to aspects of information security. All of these questions need a universal solution to make it fast, qualitatively and timely. In this project, we develop the platform for deploying and testing infrastructures based on different systems. Also, there are several types of training models in the Cyber Range that aimed at getting the best practice in information security.

I. Introduction

Most of the companies face the problem of testing security the growing corporate systems. A problem is a large number of different applications inside a corporate network and low qualification of security specialists in the company. According to corporate applications, It requires regular security tests and proper environment for these tasks. But as for specialist, the problem is outdated knowledge. The maintaining of the appropriate level of competency becomes harder and critical with the development and integration of new technologies in the company. The approach for solving these problems is using a special platform for deploying and testing infrastructure and teaching employees.

There are requirements for this platform. One of them is a separate environment. The purpose of an "environment" is to support an isolated and repeatable deployment of a known configuration of the system. This includes a particular version of each component, third-party library, configuration file, set of users, permissions, etc. There is a difficulty of deploying various hosts with different configurations on the systems. It is better to use a pre-defined configuration and orchestration tool for creating and managing environments.

Another requirement to the platform is the scalability. The platform must quickly grow and expand. Also, It follows the property of independence. One infrastructure should not be dependent on another. Shared environments that are used by multiple developers and often comprise multiple physical and/or virtual machines and must be managed more carefully.

The primary part of the Cyber Range is an educational module. Users should be provided by various labs and tests with different levels of complexities. The tests are more interesting for users if they are close to reality. Various types of training allow achieving the best results. This module must have the user-friendly interface, the features of monitoring, analyzing and reporting all activities of users. No less important regular updating the repository of the labs.

In this paper, we develop the Cyber Range that has to satisfy all the requirements mentioned before. We describe the architecture, module and the idea behind cyber range and how it can improve the reconnaissance and skills of cybersecurity expert by providing a training platform that can allow them to practice on some of the real scenarios that had lead to a data breach in some companies, Also we wanted to provide a tool that can be used to teach everyone how wants to join the cybersecurity field by allowing them to practice on friendly and easy challenges, And the trainer can solve these challenges and make his way to the hardest one. We use the procedure of continuous integration and continuous delivery for developing the educational module that consists of the web application. There is used API between modules of the Cyber Range to communicate with each other. All documentation and code are presented.

II. Research goals

- Develop the platform for deploying multiple types of infrastructure.
- Develop the methodology and training for practical security tests.

III. Methodology

The project is divided into the following stages:

1. Develop a functional model according to requirements. It allows us to describe and understand the specification and whole conception of the Cyber Range.

2. Design the architecture of the platform. There is a description of hardware, open source applications that are used for developing Cyber Range. Also, there is the scheme of modules in the platform. How all parts of the Cyber Range communicate with each other.

3. Deploy the virtualization platform based on XEN hypervisor. Preparation the environment for Cyber Range.

4. Create a repository for OS images and applications. It requires a lot of memories to store various images. It is better to store images on different machines for high availability.

5. Develop WEB application and orchestration tools. This stage comprises a web interface for users, API functions, scripts, dockers.

6. The final step is deploying and testing first test labs, gather statistics and improving functionality.

IV. Related work

Different types of cyber ranges are used for the military, academic and commercial purposes. Whereas the most of the military researches in this field usually are not public, some good surveys are available. An informative document by Royal Military College, Canada [1] provides the topic of simulation and modeling describing near thirteen simulation-type cyber ranges and categorizing it. In [2] the authors demonstrate the history, classification, functionality, and purposes of cyber ranges. Also, the review [3] covers the analysis of the software tools underpinning network testbeds. From the recent work of 2017 [4] the authors Masaryk University, Brno, describe the designing and execution of a cyber defense exercise to validate the KYPO cyber range prototype. The global scope of the cyber ranges role in the NATO - EU infrastructure is shown in [5]. The paper demonstrates how the knowledge of cyber threats evolved over the last decade the vector of the system evolution.

V. Cyber Range Architecture

In this section, we describe the architecture of the Cyber Range. The main parts of the platform, their features, and roles.

A. *The main conception*

The are five essential modules in the platform (Figure 1). The Virtualization, Core, Storage, Containerization and Network modules. The Core module that consists of the WEB application is described in the next section. The functions of other modules are represented below.

All modules communicate with each other using API functions.

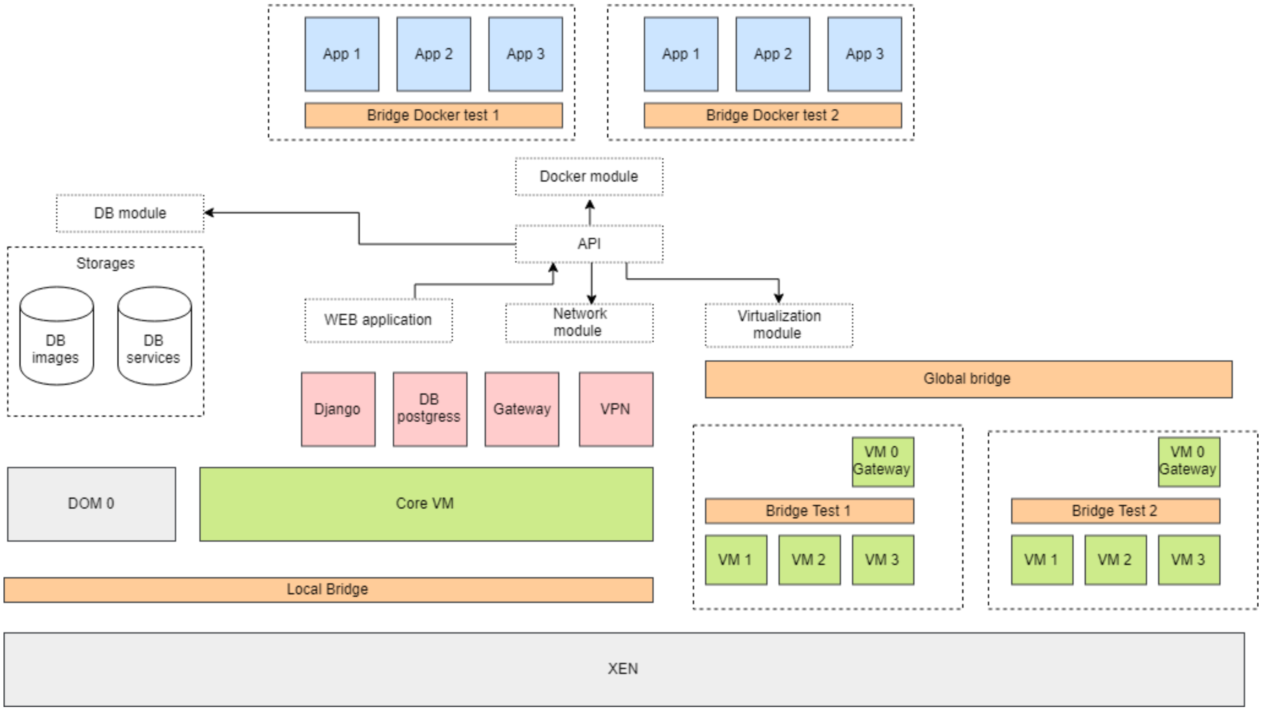


Figure 1: *Architecture of Cyber Range*

B. Virtualization

The Hypervisor XEN is used for managing virtual machines in the Cyber Range. It plays two roles. The first is the platform for deploying system virtual machines. The system virtual machine means an instance that necessary for the functioning of Cyber Range. There are the following system virtual machines: Core VM, Docker VM, Gateway VM. Also, Dom0 - the only virtual machine which by default has direct access to hardware. There are installed oVswitch and xentools utilities in Dom0. Ubuntu server 16.04 is used as the operating system for Dom0. The second role of the virtualization module is the managing of temporary virtual machines. These machines are deployed while creating infrastructure.

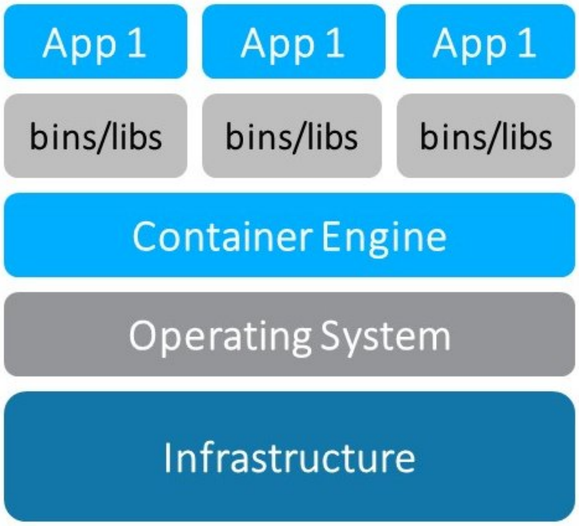
There are two types of deploying VM and preparing services on it. The first type is the copying template of a VM with a pre-installed application on it. On the one hand, this approach is fast and easy but on the other hand, it requires a large storage space. The second type is the deploying empty VM and further installation services on this VM by scripts. This approach does not require a lot of space in a storage. But the time of deploying increases.

C. Containerization

Docker Figure 2, Which is a operating-system-level virtualization that can run lightweight Linux images (called containers) with few resources, this engine is heavily used in our solution to run any web-app/app for the trainer to practice. Docker consist of three parts:

- Docker engine: is the part of Docker which creates and runs Docker containers.
- Docker container: is a live running instance of a Docker image.
- Docker image: is a file that contains a specific web-app/app to run.

Using this way we can have an isolated environment for each web-app/app and also preventing the trainer/team from corrupting other trainers/teams web-app/app.



https://rancher.com/playing-catch-docker-containers/

Figure 2: *Docker engine*

Using the Docker engine gave us the ability to deploy our solution two way:

- A completely offline deployment: by using a local registry to store the docker images, This registry is called docker hub, The only disadvantage is storage, as every image have to be stored in the installation media or provided separately.
- A lightweight deployment: where are the image will be stored online on docker hub, The disadvantage is the delay, As every image need to be downloaded in order to use it, And this will cause a lot of delays especially if there are a lot of docker images to be downloaded.

By default for stages mode, Only two containers are running for each trainer/team, the current one that they are solving, And the next one, This allows us to remove any delay that may happen in the startup of a docker container when the trainer/team finish the current challenge.

D. Network

Hypervisors need the ability to bridge traffic between VMs.On Linux-based hypervisors, this used to mean using the built-in L2 switch. For this reason, openVswitch is used in the hypervisor. It divides one domain into several domains. The control of an access between domains is performed by the utility Iptables. There is a problem with assigning the IP address to VMs. In this case, we use DHCP server to do it automatically.

VI. Application

The Cyber Range platform was developed for the following roles: trainer (or operator) and trainee (or user). The platform provides different features for each. For example, the operator is able to create new or deploy existing virtual infrastructure with any services in it using virtualization technology. The virtual infrastructure might be the same as any original physical one. In addition, using containerization technology the operator can develop new or deploy existing tasks to be used by users. Each task should consist of scenarios and levels of difficulty. From the user point of view, he is able to see the virtual infrastructures or assignments that was deployed for him. All user actions are monitored by the operator panel.

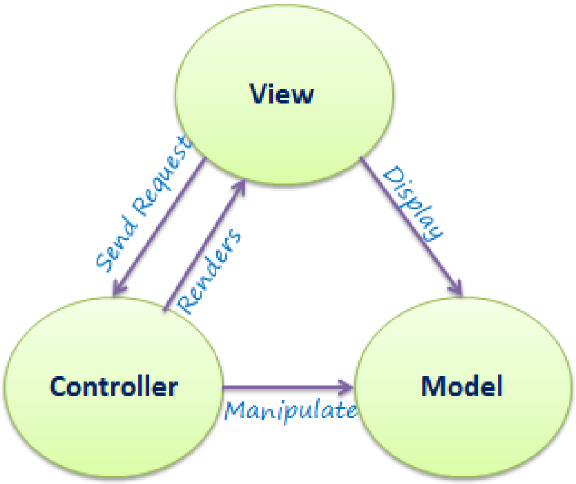
Between the end user and platform, the application is required to manage the whole logical processes in the system. This application represents web application that was build using MVC architecture. The MVC architectural pattern has existed for a long time in software engineering. MVC separates an application into three components - Model, View, and Controller. (Figure 3)

Model: Model represents the shape of the data and business logic. It maintains the data of the application. Model objects retrieve and store model state in a database. Model is a data and business logic.

View: View is a user interface. View display data using the model to the user and also enables them to modify the data. View is a User Interface.

Controller: Controller handles the user request. Typically, users interact with View, which in-turn raises appropriate URL request, this request will be handled by a controller. The controller renders the appropriate view with the model data as a response. Controller is a request handler.

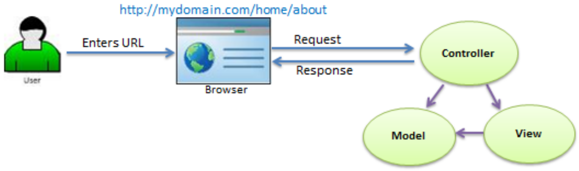
When the user enters a URL in the browser, it goes to the server and calls appropriate controller. Then, the Controller uses the appropriate View and Model and creates the response and sends it back to



http://www.tutorialsteacher.com/mvc/mvc-architecture

Figure 3: *MVC Architecture*

the user (Figure 4).



http://www.tutorialsteacher.com/mvc/mvc-architecture

Figure 4: *Request/Response*

This architecture provides a convenient environment to interact with the user and platform. Django framework was taken as a base environment to develop web-application. The application deploys on any web-server and uses a PostgreSQL database management system to process data. The web-server is deployed as a dedicated virtual machine on the hypervisor.

VII. Training models

In this section, we will describe the training modes that will be provided by our solution.

A. *Stages*

In this training mode, The trainer will start with a challenge, This challenge is called **stage**, If the trainer solved this stage he will get access to the next stage, And the flag of the previous stage is the password of the next stage, So that the trainer will not be able to access any stage unless he solved the previous one. This is demonstrated in Figure 5

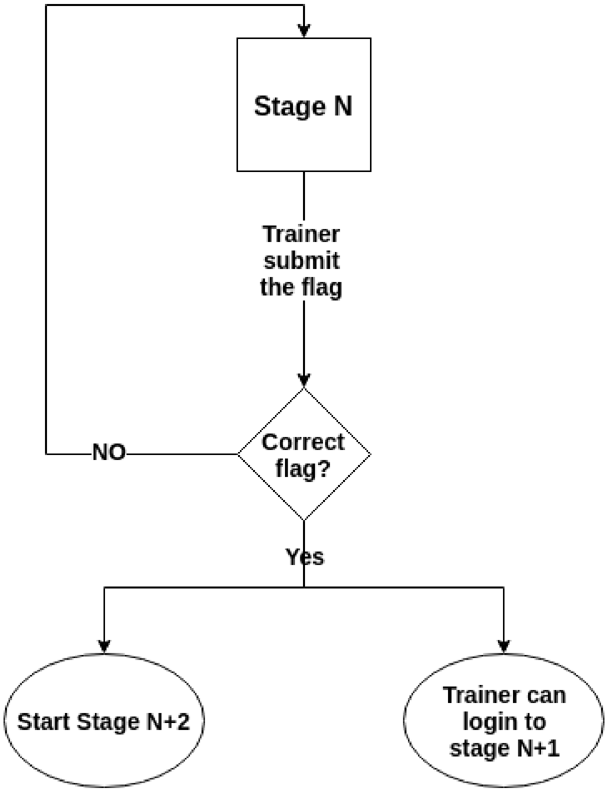


Figure 5: *The flow of solving stage training mode*

Also, This mode of training has 4 difficulty levels:

- Easy: in this level the trainer will try to solve a very basic tasks and gain experience and knowledge in how to approach the stages, What type of scan has to be done, How to discover the vulnerability and will Learn the basic steps of exploiting that vulnerability, Also this level does not apply any method of exploitation mitigation technique to the vulnerable stage.
- Medium: In this level, the trainer will try to solve some stages with an easy to bypass exploiting mitigation technique and there will be advance exploitation requirements.
- Hard: In this level the trainer will have to solve harder stages with more advance exploitation mitigation technique and in some stages the

trainer might need to write hit own exploit to solve some of the tasks, Also in this level the trainer will have to solve a simulation of a real exploitation scenarios that led to a data breach in sole companies.
- Mix: This mode used the above level to generate a random sequence of the level that needs to be solved by the trainer, And each trainer will get his unique sequence of levels.

B. *Attack vs defense*

The attack-defense mode assumes a team working and simulation of a practice closer to a realistic situation. There is an infrastructure in the lab with predefined topology and applications. One team attacks the base while another tries to defend it.

C. *AD vs AD*

The difference from the previous type of training is that each team has their own infrastructure. Also, the team‘s members consist of attackers and defenders. Defenders of the team try to find weak points in the infrastructure and patch them. In the same time, another part of team attacks applications and services of command number two.

VIII. Ethical issues

This project will have to comply with all ethical standards of morality and in its research will not be violated any laws concerning the exploitation of found vulnerabilities in real life.

IX. Conclusions and suggestion for further research

During the work, we examined a lot of potential configurations and scenarios for the implementation of the cyber range. The developed configuration, preliminary implemented as a functional model IDEF0, proved to be the most applicable and flexible for the further open source implementation with own solution. The core concept was built for the further development and it has a great potential for the scaling and logical complexity increasing In the future, attention should be paid to improving the storage of virtual infrastructure, improving the deployment of virtual images through the use of ensemble tools and the development of new learning scenarios.

References

[1] I. Chapman S. P. Leblanc A. Partington and l. Bernier. “An overview of cyber attack and computer network operations simulation”. In: *Military Modeling Simulation Symposium Boston, Massachusetts: Society for Computer Simulation International* (2011).

[2] S. Magrath J. Davis. “A Survey of Cyber Ranges and Testbeds”. In: *Cyber Electronic Warfare Division* (2013).

[3] C. Siaterlis and M. Masera. “A survey of software tools for the creation of networked testbeds”. In: *International Journal On Advances in Security* (2010).

[4] P. Celeda J. Vykopal R. Oslejsek. “KYPO Cyber Range: Design and Use Cases”. In: *Conference: 12th International Conference on Software Technologies* (2017).

[5] P. Pernik. “Improving Cyber Security: NATO and the EU”. In: *International Centre for Defence Studies, Tallin, Estonia* (2014).