Guide for Designing Cyber Security Exercises

VICTOR-VALERIU PATRICIU
Computer Science Department
Military Technical Academy
Bucharest, Bd. George Cosbuc, no. 81-83
ROMANIA
victorpatriciu@yahoo.com

ADRIAN CONSTANTIN FURTUNA
Computer Science Department
Military Technical Academy
Bucharest, Bd. George Cosbuc, no. 81-83
ROMANIA
adif2k8@gmail.com

Abstract: - Cyber security exercises are a very effective way of learning the practical aspects of information security. But designing such exercises is not an easy task and requires the work of several people. This paper presents a number of steps and guidelines that should be followed when designing a new cyber security exercise. The steps include: defining the objectives, choosing an approach, designing network topology, creating a scenario, establishing a set of rules, choosing appropriate metrics and learning lessons. The intended audience of this paper is persons who are in charge with design and organization of a new cyber security exercise and do not have the experience of previous exercises.

Key-Words: - cyber security exercise, cyber defense exercise, security education, design guide

1. Introduction

Cyber security exercises have been for a long time the ultimate learning experience for many students in some universities, especially from United States [1]. Periodical competitions are organized between universities or inside one university where students play the roles of attackers or defenders in a controlled and well defined environment.

The whole purpose of these exercises is educational, to ensure that students have an experiential training in information security – a process described in Kolb's Experiential Learning Theory [2].

This paper is meant to be a guide that can be used by universities or other organizations to prepare a cyber security exercise. The steps needed to do that were synthesized from a series of academic papers written after various cyber security exercises. The guide describes seven steps that should be taken when organizing such an exercise. Each step is presented in detail and some options for implementation are also given.

The contribution this paper brings is a general method to organize a cyber security exercise that can be customized to the organizer's needs and objectives. The previous work in this area consists in some efforts to document a framework for cyber security education [3] and a series of analysis, overview opinions and questions about generalization of cyber security exercises [1].

2. The Need for a Uniform Structure

There is a great diversity among the cyber security exercises organized until now regarding their structure, objectives and approach.

For instance, the Cyber Defense Exercise (CDX) is an inter-academy competition [4] in which teams design, implement, manage and defend a network of computers. The attacker role is played by a team of security professionals from various government agencies. In this exercise students are focusing on defensive tasks in network security, and spend a lot

of time conducting forensic analysis and making security configurations.

An opposite approach is taken by the organizers of the International Capture The Flag (also known as the iCTF) form University of California, Santa Barbara. The iCTF contest is a distributed, wide-area security exercise, whose goal is to test the security skills of the participants. It is held once a year and it is a multi-site, multi-team hacking contest in which a number of teams compete independently against each other. The exercises are based on the DEFCON Capture the Flag contest [6].

To address this diversity, this guide can be used as a starting point for any university that wishes to organize its own cyber security exercise / competition. In this case, the exercise would best fit as a capstone project for last year students, which already have an Information Assurance background. But the guide does not apply only to university environment; it can be used also by other organizations with the purpose of training their employees in Information Assurance field.

3. Design Steps

Designing a cyber security exercise requires careful planning by multiple persons involved in this activity. As we can see from the papers written as feedback for various cyber security exercises, a cyber defense exercise can have many forms but all of them share some common characteristics that we use to build this template. We have identified seven steps necessary for building a cyber security exercise – Figure 1.

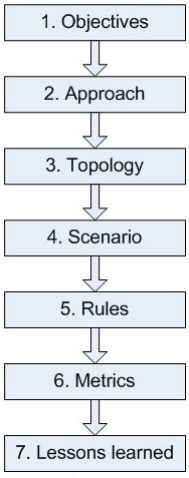

Figure 1 – Design Steps for a Cyber Security Exercise

First of all, the exercise must have a set of *objectives*. Based on these objectives, we take a specific *approach* in designing the exercise. Also based on the objectives, we decide which specific hardware and software equipment shall be used in the exercise and what will be their overall *topology*. Based on the topology and the objectives we build the *scenario* of the exercise – the story. The set of *rules* derive from the scenario and from the objectives. The *metrics* necessary for measuring the efficiency of the exercise shall be based also on the established objectives. Finally, the exercise should have a method of gathering the *lessons learned* by the participants and also by the organizers. All of these template steps will be described in the following paragraphs of this paper.

Another important aspect of the exercise is to define the entities that will compose it. In a general cyber security exercise there are mainly two sides: the *attacker side* and the *defender side*. On each side there are computer systems that are managed by teams of participants. Each side must have at least one system to participate to the exercise and the maximum number of participating systems is theoretically infinite. The components of the exercise are represented in Figure 2.

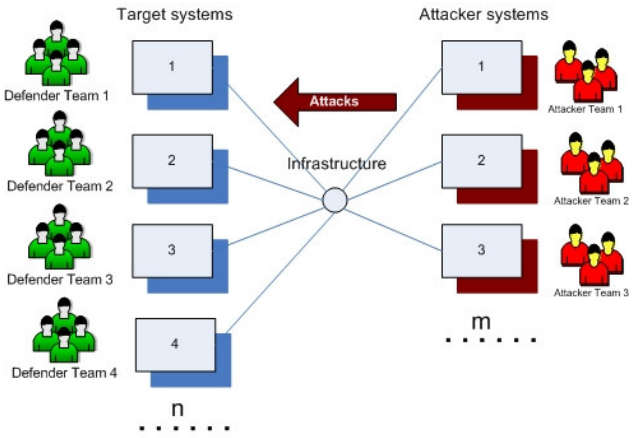

Figure 2 – The Components of a Cyber Defense Exercise

As we can see, the cyber security exercise contains five main components that must be defined in the following steps of the guide:

- Defender team
- Target system
- Infrastructure
- Attacker team

- Attacker system

4. Define Exercise Objectives

Defining the exercise objectives is the starting point for the design of the cyber security exercise. All of the following steps of the exercise design depend on the chosen objectives and are influenced by them.

The objectives for a cyber security exercise can be split in two main categories, according to the type of security training desired – offensive security or defensive security.

The defensive security training prepares the participants for the generic job of security administrator. Their main goal is to be experts in configuring and managing various security equipments. The best example for this kind of practical training is the annual "Cyber Defense Exercise" organized by the US Military Academy at Westpoint [4].

On the other side, the offensive security training is also an effective way to learn information security, as discussed by Vigna [7] and Mink [8]. This type of training prepares the participants for the generic job of penetration tester and helps them "think like the enemy", in a proactive manner.

But these training directions should not be seen as completely separated from each other. In order to implement effective defense mechanisms, a very good knowledge of the attack methods is needed. So a security administrator needs to know what are the attacks a penetration tester could implement in order to prepare defense mechanisms against them and also a penetration tester must know what defense methods a security administrator might implement in order to prepare attacks that try to bypass them.

In Table 1 there are some common learning objectives for a cyber security exercise according to the participants' specialization:

Learning objective	Participant specialization: Security administrator (SA) or Penetration tester (PT)
- implement security configurations	SA
- monitor systems' activity	SA
- test / harden the administered system	SA
- security configuration fine tuning / improvement	SA
- incident handling / response	SA
- analyze logs and do forensics	SA
- hands-on experience with various attack tools	PT
- perform reconnaissance and gather information	PT
- perform scanning and enumeration	PT
- gain access	PT
- perform DDoS	PT
- escalate privileges	PT
- maintain access	PT
- cover tracks and place backdoors	PT
- write and test new tools	SA+PT
- understand the defense techniques according to the attack methods	SA+PT

Table 1 – Cyber Security Exercise Objectives

5. Choose the Approach

The approach chosen for the exercise shall be directly derived from its objectives. Generally, a cyber defense exercise intended to train security administrators would adopt a defense oriented approach while an exercise for penetration testers would take an offense oriented approach. Comprehensive security training should adopt a mixed approach, as described below.

5.1. Defense Oriented Approach

When using this approach, the goals of the exercise are to study and practice the defense methods that can be used during a cybernetic attack. These methods are more related to system administration and forensics tasks. The defenders should know that the defense is a continuous process that can be split into the following actions:

- Create a security policy
- Implement security measures
- Monitor the security state

- Test your own security state
- Improve the security

These actions constitute the well known "Security Wheel" – Figure 3 – and should be used in order to secure the defended asset, monitor its activity in order to detect any attacks and mitigate them by improving the configurations.

In a defense oriented approach, there are at least three ways of organizing the exercise.

- The participants receive the requirements and services they should provide and they must develop their own computer systems to provide them
- The participants receive default installations for specific systems and services to provide and they must configure them in order to be protected
- The participants receive already installed and configured systems and they must protect them

In this approach, the attacker can be the instructor or an external party.

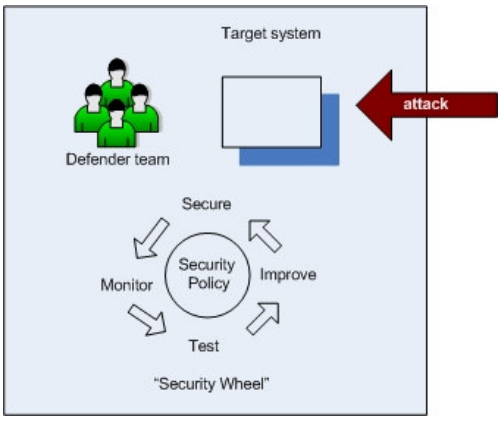

Figure 3 – Defender Actions

5.2. Offense Oriented Approach

The participants need to learn also the offensive component of a cyber defense exercise because this helps them better understand how to defend against attacks. There is a need for deep understanding of the attack methodologies in order to know how to efficiently mitigate them.

So an offence oriented approach would place the participants into the attacker's position. They will have to perform attacks against various targets. In order to simulate a real life attack, the participants should follow the next steps of a regular attack (Figure 4):

- perform reconnaissance
- scanning and enumeration
- gain access or perform DoS
- escalation of privileges
- maintain access
- cover tracks and place backdoors

In an offence oriented approach, the target can be a system preconfigured with known vulnerabilities and most not necessarily be administered by someone during the attack.

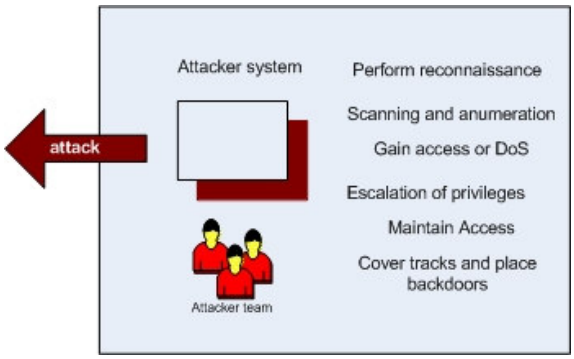

Figure 4 – Attacker Actions

5.3. Mixed Approach

The mixed approach combines the defensive approach with the offensive approach and is the most comprehensive method to perform a cyber defense exercise. In this case the participants to the exercise will be split in two parts, the ones who will play the defender role and the ones who will be the attackers – Figure 5.

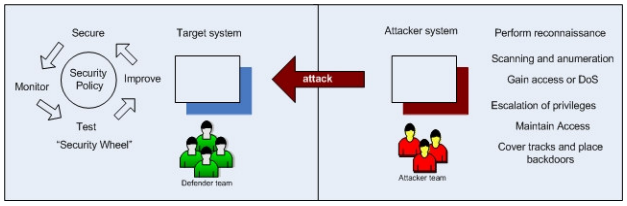

Figure 5 – Mixed Approach

6. Design Network Topology

At this stage, the organizers should define the infrastructure, what systems will be used during the exercise and how they will be interconnected in order to support the exercise objectives.

For instance, if one of the exercise objectives is to train the participants in defending a local area network with a Windows Active Directory infrastructure, the topology should reflect that.

The topology should also be according to the number of participants to the exercise, to ensure no bottlenecks and best communication between systems.

7. Create Exercise Scenario

Until now, we have established what we want to do from the technical point of view. Now it's the time to give the exercise a shape that can be presented to the participants. This is the scenario and it should put the participants in a realistic situation in which they must defend or attack a target system. The scenario describes the situation that the exercise is trying to simulate and the logical flow of events that will be happening. It should also contain an intriguing story in order to increase the participants' degree of interest. As part of the scenario, the participants could be asked to perform business related tasks during the exercise, in order to simulate a real working environment.

The realism of the scenario is also given by the attacker's goals. In general, the cybernetic attack goals fall into the following categories:

- access confidential data (read/write)
- disrupt services
- control machines

These are the things that the defenders must not allow to happen.

From the logical point of view, the targets of the attacks can be:

- public services
- computer networks
- humans
- trust relationships

8. Establish a Set of Rules

The rules and guidelines for a cyber defense exercise should address the following topics:

- **General rules**

These rules should express clearly how the exercise is supposed to run and how the participant should be organized. They should also address problems like: equity between team resources, what tools are allowed to use, team responsibilities, each team's role in the competition, communication between participants, competition timing, etc.

Another thing that these rules should specify is what happens if one participant breaks one rule (e.g. disqualification, penalty).

- **Scoring engine**

This set of rules must express the way the teams obtain points, what are the winning conditions, what are the actions for which teams lose points and which actions will not get them any points. The scoring method should be transparent to all participants to the exercise.

- **Eligibility**

There should be well defined criteria for the participation at the exercise. For instance, if the exercise was organized by a university, the participants would be eligible if they were students at that university and if they had passed successfully all their information security related exams. Other criteria could be: age, study year, clean background, etc.

- **Legal issues**

From the legal point of view, the set of rules must express the limitations imposed by the state law and local law from where the exercise will be organized. Exercise organizers should check law related aspects for: unauthorized intrusion, unauthorized access to data in transmission, unauthorized access to stored data, individual privacy rights, contractual obligations.

For instance, the usage of some attack tools might be interdicted – like in Germany [9].

- **Limitations**

The rules should also establish what are strategies and practices that are and the ones that are not allowed during the exercise. They should be divided in rules for defenders and rules for attackers (e.g. DoS attacks are not allowed). The persons who arbitrate the competition should also know what are their limitations (e.g. they must not influence any of the teams).

9. Choose Appropriate Metrics

To measure the effectiveness of the cyber security exercise, a set of metrics is needed. The effectiveness of the exercise expresses how well the objectives have been achieved. So the chosen metrics should be tightly related to the objectives. On the other side, the objectives should be expressed in measurable terms.

In Table 2 there are some examples of objectives for a cyber security exercise and the associated metrics:

Learning objective	Metric for effectiveness
- implement security configurations on a specific system	- number of successful attacks performed by the attacker teams on that system
- monitor systems' security	- number of detected attacks from the total number of attacks performed
- incident handling / response	- the time taken to recover from a successful attack
- analyze logs and do forensics	- the number of attacks correctly identified
- perform scanning and enumeration	- the number of open ports/services detected compared to the total number of open ports (pre-configured)
- perform DDoS	- the downtime of the attacked service compared to attack duration
- cover tracks and place backdoors	- number of successful accesses to target systems kept until the end of the exercise

Table 2: Sample Metrics for Exercise Effectiveness

10. Don't Forget the Lessons Learned

This step is very important for the effectiveness of the cyber security exercise. The organizers should find an appropriate mechanism for gathering feedback from the participants (e.g. evaluation forms at the end of the exercise). A very useful information would be the techniques and tools that each party had used in order to accomplish the scenario objectives. After centralization and analysis, this information should be made public because it will help the participants realize what was really going on during the exercise and will help the organizers improve other editions of the exercise.

11. Conclusions

Designing a cyber security exercise is not an easy task and requires the work of several people. When organizing such an exercise it is always best to learn from the past experience of the ones who already did it.

This paper presented a number of steps and guidelines that should be followed when designing a new cyber security exercise. The guidelines have been crystallized from the analysis of a number of papers written after various cyber security exercises.

The ideas presented in this paper can be used by anyone who wants to organize a cyber security exercise for an educational purpose (e.g. universities, companies, governmental institutions, etc).

References:

[1] Lance J. Hoffman, Daniel Ragsdale: *Exploring a National Cyber Security Exercise for Colleges and Universities*, IEEE Security and Privacy, Volume 3, Issue 5 (September 2005)

[2] D.A. Kolb, *Experiential Learning: Experience as the Source of Learning and Development*. Prentice-Hall, Inc., Englewood Cliffs, N.J. 1984.

[3] Thomas Augustine, Ronald C. Dodge, *Cyber Defense Exercise:Meeting Learning Objectives thru Competition,* IEEE Security and Privacy, Volume 5, Issue 5 (September 2007)

[4] Wayne Schepens, Daniel Ragsdale, John Surdu, *The Cyber Defence Exercise: An Evaluation of the Effectiveness of Information Assurance Education*, The Journal of Information Security, Volume 1, Number 2. July, 2002

[5] The UCSB iCTF contest, http://ictf.cs.ucsb.edu/index.php

[6] Defcon hacking event, Las Vegas. http://www.defcon.org

[7] G. Vigna, *Teaching network security through live exercises*. Security education and critical infrastructures**,** Pages: 3 – 18, 2003

[8] Martin Mink and Felix C. Freiling, *Is Attack Better Than Defense?Teaching Information Security the Right Way,* Proceedings of the 3rd annual conference on Information security curriculum development, Kennesaw, Georgia, 2006

[9] http://www.theregister.co.uk/2007/08/13/german_anti-hacker_law/