Cyber Defense Exercises and their Role in Cyber Warfare

Bogdan-Alexandru BRATOSIN
IT&C Security Master
The Bucharest University of Economic Studies
ROMANIA
axelbrato@yahoo.com

Abstract: The threat of cyber-attacks is increasing with the access to PC's and Internet of a larger number of people around the world. Although the Internet provides a large number of advantages, it can also be used as a cyber-weapon in order to serve the interests of counties, political and economic groups or individual. The cyber-attacks of today are capable to disable the manufacturing of nuclear bombs of a country. Thus, there is an increasing demand for IT security specialists. Cyber-defense exercises (CDX) are by far the most complex and up to date methods of training the next generation of IT security specialists.

Key-Words: cyber defense exercises, cyber-attack, cyber terrorism, cyber warfare, cyber espionage, information assurance.

1. Introduction

After the 20th century technology developed at an astonishing rate. From the first hard disk developed by IBM in 1956, the IBM 350 with a storage capacity of 3.75 Megabytes, till today when we can access hard disks with capacities of 4 Terabytes, and furthermore in the next years to come the capacity will reach an astonishing capacity of 60 Terabytes.
Our society has become, over the years, technologically dependent. As individual computers play a significant role in our lives, every day we use computers to communicate with each other, to shop, to read the latest news, to create. While as a society, over the years, we have become dependent on computers, because they are integrated in our water supply systems, power supply systems, economical-financial systems, healthcare systems, transportation and ultimately military defense systems. All the systems are software dependent and interconnected, meaning they are vulnerable to cybernetic attacks. A cyber-attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber-attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.
The downside of our society's dependence, created a new environment – the cyberspace. New vulnerabilities are discovered, new tools for the attackers to use are available and ultimately the physical location of the attackers is no longer a limit. This new environment has led to the creation of new concepts – cyber terrorism and cyber warfare – both concepts at the core represent the same idea, only the actors are different. As a consequence, all politically and military conflicts now have a "cyber dimension", which size and impact are difficult to predict.
The Internet is an international entity and because of that, the law cannot be fully enforced. The anonymity is one of the greatest "benefits" that the attackers still reside on, is very difficult to wage a war against an unknown threat or attacker, weather that attacker is a single person, an army or even a state. Finally, cyber defense suffers from the fact that there is little moral inhibition to computer hacking, which relates primarily to the use and abuse of computer code. All things considered, the current balance of cyber power favors, so far, the attacker.
Cyber security has quickly evolved from a technical discipline to a strategic concept.

ISSN 2067 – 4074

Therefore cyber defense is a major concern for states and organizations. Many states and organizations have made cyber defense one of the national security objectives. The implementations, maintenance and improvement of national cyber security comprise a range of elements. These are comprised of strategic documents of political nature, laws, regulations, organizational and administrative measures, such as crisis management within a State, and also technical protection measures. Furthermore, awareness raising, training, education, exercises and international cooperation are important features of national cyber security. Thus, the aspects to be considered reach from strategic through the administrative to the technical level.

2. Cyber terrorism, Cyber warfare and Cyber espionage – history and theory

2.1 Cyber-attacks – a growing threat

Conducting an "information operation" of strategic significance is not easy, but neither is it impossible. During World War II, the Allies after having deciphered the Enigma disseminated false information to Adolf Hitler, signaling that the D-Day invasion would take place at Pas-de-Calais and not Normandy. This gave Allied forces critical time to establish a foothold on the continent and change the course of history.

Nowadays, information security plays a vaster and more important role in a state's defense.

In 2006, during the war between Israel and Gaza, Palestinian hackers successfully denied service to almost 700 Israeli internet domains, thus rendering tension in the Middle East accompanied by cyber-attacks. [1]

In 2007, a cyber-attack demonstrated us that air defense plays a significant role in national defense when the air defense of a Syrian nuclear reactor was, presumably, hacked before it was ultimately destroyed by Israeli's air force. [2]

In 2009, the president of the United States announced that the electrical grid of the country has been probed and that also in other country cyber-attacks have plunged cities into darkness. [3]

Furthermore, security specialist that plans the National Security of a state should regard the power grid, water supply, healthcare system and transportation as primary objectives when planning.

The most complex cyber-attack discovered so far is – Stuxnet. The worm Stuxnet was discovered by a Belarusian antivirus firm in the year of 2010. The worm is believed to have been active on the internet for at least one year prior its discovery. According to Falkenrath, the worm succeeded what five years of United Nations Security Council resolution could not: prevent Iran in building a nuclear bomb. [4] If we agree with the above statement, then half-megabyte of computer code that infected the software of at least 14 industrial sites in Iran, including the uranium-enrichment plat, thus substituted air strikes which should have been conducted by the Israeli's Air Force. [5] To some degree, it is believed that Stuxnet may have been more effective than a conventional military attack and may have avoided major collateral damage.

2.2 National Security Planning

National security planners should take into account 3 basic types of cyber-attacks that target: [6]

- the *confidentiality* of data;
- the *integrity* of information;
- the *availability* of computer information and resources;

Attacks that target *confidentiality* of data encompasses any unauthorized "acquisition" of information, in which the attacker acts only as an observer, without tampering the information. For example, in the year 2009, a research group called Information Warfare Monitor discovered the existence of "GhostNet", a network dedicated to cyber espionage that targeted political, military, diplomatic and economic information. [7]

The second type of attacks targets *integrity* of information, this means the sabotage of data for criminal, political or

military purposes. Cyber criminals have been known to encrypt data on the victim's hard drive and then demand a ransom in exchange for the decryption key. [8]
The last type of attacks targets the *availability* of computer information and resources. The goal of this type of attacks seeks to prevent authorized users to access information or resources which they require to perform certain tasks. This is commonly known as denial-of-service (DoS). In 2001, a 15 year-old student in Montreal, conducted a DoS attack against some of the world's biggest online companies. The resulted financial lose was reported being over $ 1 billion.

3. U.S. National Cyber Defense Strategy

United States' Department of Defense (DoD) elaborated 5 initiatives: [10]

Initiative 1 – Treating cyberspace as an operational domain to organize, train and equip.
DoD must ensure that it has the necessary capabilities to operate effectively in all domains – air, land, maritime, space and cyberspace. DoD must organize, train and equip for the challenges and opportunities of cyberspace. Because of the risk implied in cases of cyber-attacks, DoD will integrate scenarios into exercises and training to prepare U.S. Armed Forces for a wide variety of contingencies.
Initiative 2 – Employment of new defense operating concepts to protect DoD networks and systems.
DoD implemented a four step strategy:

- enhancing its cyber "hygiene"
- deter and mitigate insider threats
- employ an active cyber defense
- developing new defense operating

Initiative 3 – Partnership with U.S government departments and agencies and the private sector.
DoD will work with the Department of Homeland Security and Defense Industrial Base to mitigate risk effectively.
Initiative 4 – Building relationships with U.S. allies and international partners.
DoD seeks to create a strong partnerships with U.S. allies and international partners to timely share information about malicious code, emerging actors to increase collective cyber defense.
Initiative 5 – Leverage the nation's ingenuity through cyber workforce and technological innovation.
In order to train the future IT security specialist to achieve its goals, DoD will use scientific, academic and economic resources to create the next generation of civilian and military security specialized personnel.
In the first initiative, the DoD proposes the idea of "war games", which, in essence, are cyber defense exercises.

4. Cyber Defense Exercises (CDX)

Almost in any domain practice and experience will outperform theory. Cyber defense is one of those domains.
Cyber defense exercises are conducted annually by various organizations, like NATO, National Security Agency (NSA), Department of Defense (DoD), etc.
CDX can be regarded as a computer security competition that was design to foster education and awareness among future security specialist and military personnel about the role of Information Assurance in protecting the nation's information system.
NSA and DoD conducts annual exercises with various academies: U.S. Military Academy, U.S. Naval Academy, U.S. Air Force Academy, U.S. Coast Guard Academy, U.S. Merchant Marine Academy, Air Force Institute of Technology, Royal Military College of Canada.
The main goal of these exercises is to asses' students' abilities to maintain network services while detecting and responding to network security intrusions.
During the course of four days three teams take part in a CDX: the Blue Team (comprised of students from each academy that participates in this competition), the Red Team (NSA/DoD specialists that act as "hackers" performing cyber-attacks) and a White Team (a representative from NSA sent to

ISSN 2067 – 4074

each academy to act as a liaison between the school and the exercises headquarters).
Each Blue Team is given control of a poorly managed enterprise system. The student's first task is to identify vulnerabilities and mitigate the problems. The teams must redesign and reconfigure the network and services to be more secure, but also staying within a certain specific budget.
Students are graded on their abilities to maintain the enterprise systems including: messaging, domain controller, web and database servers, file servers and workstations. They also must submit timely report on Red Team activity and respond to their attacks.
CDX offers a real world scenario for preparing students in designing, building and successfully defend a real world network against simulated attacks conducted by the Red Team.
The Red Team employs various technics when conducting cyber-attacks. Technics like: [11]

- *Credential hijacking* – stealing administrative credentials.
- *Credential replay* – replay hashed administrative credentials or cookies, gaining control of web servers.
- *Cross-site scripting* – introduction of cross-site scripting vulnerability to a compromised web server.
- *Malware callbacks* – malware designed to open contacts from within the victim's network.
- *OpenFire remote access* – remote access vulnerability in OpenFire instant messaging server.
- *SQL injections* – the use of SQL injections on databases to obtain administrative passwords.
- *SSH reverse tunnel* – set up a reverse SSH tunnel from a compromised workstation to the site's servers with the purpose of gaining unauthorized access.
- *Windows DNS stack overflow* – vulnerability exploited in Windows domain controller, thus gaining access to the domain controller.
- *Weak passwords* – because of the weak level of passwords, some of them were guessed by the attackers.

5. Creating a CDX

5.1 Types of CDX

Cyber defense exercises are hands-on information assurance exercises. The main purpose of these exercises is to train the participants into various aspects of information security.
There are many types of cyber-defense exercises. Some of them include:

- *"Capture the Flag"* where a system contains various pieces of information scattered across multiple workstations. In this contest, there are two or more teams participating. The goal of each team is to recover all the pieces of information. Because there is only one target system, the teams will intersect each other, thus they will need to conduct offensive and defensive actions against the opposing teams. The goal of the exercise is which team recovers the information fastest.
- *"Race to Finish"*. This type of exercise is designed in the same manner as "capture the flag" exercise, the same goal, with only one little difference. The difference is that there is not only one target system, but the number of target systems is equal to the number of team participating in the exercise. The goal of the exercise remains the same, each team gathers the fastest the information, but there will be no need for offensive actions against the other participants.
- The last type but not the least, is *"Tower Defense"*. This type of exercise involves two different types of teams. In comparison to the above two types of exercises, in this exercise participate two types of teams: Blue team and Red team. The Blue teams purpose is to defend the "tower", while the Red team's goal is to attack the "tower" to achieve various tasks. Here the set of rules is a little bit more complex, because the metrics needed to verify the results of the exercise are vast and complex.

5.2 Case Study – "Knight and Day"

SkyNet Technologies developed a battery that is 2000 times more durable, 1000 times more powerful and 10 times smaller than the average Li-Ion battery. The discovery has not been yet patented. A rival company Krypton Technologies is on the verge of discovering the same technology. Because the discovery has not yet been patented, and the technology is so revolutionizing Krypton Tech hires a group of hackers to infiltrate Sky Net systems and retrieve the blue print. The hackers were given the following information, from a mole placed in SkyNet Company:

- the blue print is an AutoCAD file. This means the file has a DXF extension.
- the file was split into five pieces. The software used for splitting the file is a well-known, commercial used archiver, meaning that the software could be 7ZIP, WinZip, WinRar, or WinAce.
- the last piece of information gives hints about the possible location of the pieces. The first piece is stored on the CEO's station and the rest four pieces will surely not be found on the employees workstations, meaning that the last four pieces resides on the company servers.

Because it's a race to finish cyber defense exercise type and uses an offensive approach, there is no need for a defender team. The target system will be replicated for each attacking team. The target system will be comprised of several virtual machines emulated on a single physical machine. These virtual machines are grouped in a local area network which is connected to the outside world through a gateway machine. The system is composed of a demilitarized zone and an internal network, thus the computers in DMZ will be accessible from the Internet, while the internal network can only be accessed through the gateway machine. The following configuration will be used for the target network:

- The Gateway machine is a Linux based system. The vulnerable service is SSH, which has a weak SSH password: user "skynet" /password: "skynet1234". This machine contains a piece of the blueprint.
- Database server (www.skynet.hk) is a Linux based system. Its vulnerable service is web, while the site battery.skynet.org is vulnerable to SQL injection. The database server is MySQL and it runs as root. This machine also contains a piece of the blueprint.
- The DNS server (ns.skynet.hk) is a Linux based system and its vulnerable service is DNS, because it allows DNS zone transfer from any IP address, thus uncovering the other hosts.
- The FTP server (ftp.skynet.hk) is a Linux based system. Its vulnerable service is FTP (Port 21212) and this vulnerability allows anonymous access. This machine contains a piece of the blueprint.
- The CEO's machine is a Linux based system. Its vulnerable service is SMB, because it enables file sharing. This machine contains a piece of the blueprint.
- The Intranet hosting server (intranet.skynet.hk) it a Linux based system. Its vulnerable service is web, because it allows arbitrary file download. This machine contains the last piece of the blueprint.

The Target Network Topology can be observed in Figure 1 below.

ISSN 2067 – 4074

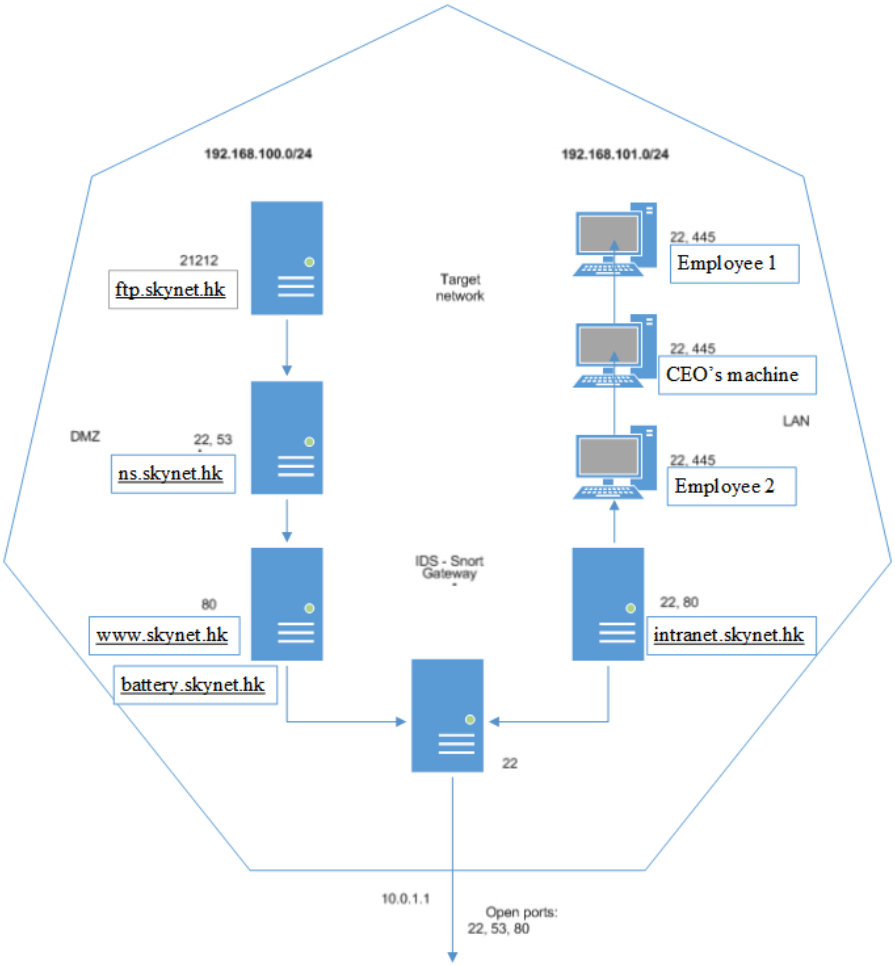

Figure. 1 Target Network Topology

In order to accomplish the objectives of this exercise, the participants must perform a series of logical steps and attack the target systems:

- Scan for open ports and find port 22, 53 and 80 open on the Gateway machine
- Do a zone transfer on the DNS server and discover all the hostnames inside the target network (including www.skynet.hk and battery.skynet.hk which are pointing to the same internal physical machine)
- Perform a brute force attack against the SSH server on the Gateway utilizing all the information received in the scenario description. The word "skynet" should be included as username and should be mangled in order to obtain his simple password: skynet1234.
- Scan the internal network for finding live hosts and open ports. A complete scan should reveal port 21212 used by the FTP server. By trying anonymous login, the participants should easily gain access to the blueprint piece.
- Exploit SQL injection vulnerability from battery.skynet.hk. This is a virtual host accessible only by this name, which should have been discovered in the DNS zone transfer attempt. Since the server runs a MySQL database (as root) the attacker can create a user defined function (UDF) and execute system commands as root. Upload a shell and execute it.
- Test for unprotected network shares. This will offer an easy artifact to the participants who will test all the machines from inside the target network.

6. Conclusions

As stated earlier practice outperforms theory, practices makes perfect.
Exercises, such as the CDX, provide the much needed hands-on experience. The

practical aspects of risk mitigation are strengthened by the incorporation of team building, management, communication and budget management.

During the exercises, students not only develop the technical skills required to successfully and securely manage systems, but also they develop leadership skills needed to manage systems in a hostile environment.

A system can be managed securely only when all administrative processes, all configurations and communication channels are understood.

Acknowledgment

Parts of this research have been published in the Proceedings of the 6th International Conference on Security for Information Technology and Communications, SECITC 2013.

References

[1] Stoil, R.A. & Goldstein, J. (28 Jun 2006) "One if by Land, Two if by Modem," The Jerusalem Post.

[2] Fulghum, D.A., Wall, R. & Butler, A. (26 Nov 2007) "Cyber-Combat's First Shot," Aviation Week & Space Technology 167(21) 28.

[3] "Remarks by the President on Securing our Nation's Cyber Infrastructure," (29 May 2009) The White House: Office of the Press Secretary: www.whitehouse.gov.

[4] Falkenrath, R.A. (26 Jan 2011) "From Bullets to Megabytes," The New York Times.

[5] Kushner David - The Real Story of Stuxnet (26 Feb 2013)

[6] Strategic Cyber Security – Kenneth Geers – 2011 CCD COE

[7] "Tracking GhostNet: Investigating a Cyber Espionage Network," (29 Mar 2009) Information Warfare Monitor.

[8] Geers K. (2007a) "Greetz from Room 101," DEF CON, Black Hat 1-24.

[9] Verton, D. (2002) The Hacker Diaries: Confessions of Teenage Hackers (NY: McGraw-Hill/Osborne).

[10] Department of Defense Strategy for Operating in Cyberspace – July 2011

[11] William J. Adams et al. - Collective Views of the NSA/CSS Cyber Defense Exercises on Curricula and Learning Objectives.