A Method for the Penetration Testing in IT Environment

Ivona ZAKARIJA, Vedran BATOS and Tomislav DOMIC
Department of Electrical Engineering and Computing, University of Dubrovnik
Cira Carica 4, Dubrovnik, Croatia
ivona.zakarija@unidu.hr, vedran.batos@unidu.hr,tomislav.domic@hi.t-com.hr

ABSTRACT

This presents an application of the selected procedure for penetration testing (pentesting) process based on *Black box* method. The phased approached has been implemented starting with analysis session of basic computer security issues, using freeware tools, and leading to the final (4th) phase to achieve the testing results and reporting lists to minimize and avoid possible security breaches. Paper presents analysis of potential vulnerabilities in order to provide practical explanation and guidelines for their removal. The testing processes has been done within real time IT environment to achieve the practical results.

Keywords: penetration testing, pentesting, black box, computer, security, vulnerabilities, software

1. INTRODUCTION

In modern era, more and more activities are processed through machines and man relies on their help in the execution of daily tasks. Although the machines are not prone to errors while processing data, their physical behaviour is often predictable and thus can be manipulated. Knowing that no system is 100% secure, the attacker chooses various vectors to subtly cause security breach.

It usually leads to data theft, modification of security and configuration settings, and in the worst cases of disabling operations and a complete loss of data. Therefore, in order to prevent these and similar incidents arose the need to conduct standardized testing security. Recognizing this fact in practice, a new branch of computer security developed, which is called penetration testing. This paper describes an approach to testing methodology and shows the most effective ways to check the security of computer systems.

2. SECURITY DEMANDS

The system is considered safe if it meets the criteria that guarantee confidentiality, availability and data integrity [1]. Data confidentiality standard is defined through information access for authorized users only. Availability ensures control and ability to use data while the data integrity ensures processing consistency and information validity within the system. Integrity is secured in such a way that the control processes can run only users who have the given privileges. It is essential that all three criteria are ensured since system security depends on their cohesion.

Generally, attackers exploit vulnerabilities in computer systems which allow them to successfully breach security. Vulnerabilities are divided into those in the programming code, configuration, network protocols, and physical vulnerability [2]. The most common vulnerabilities lay in the programming code while the successful attacks are carried out using physical vulnerability. This is clearly shown by cyber attacks statistics (Fig 1.).

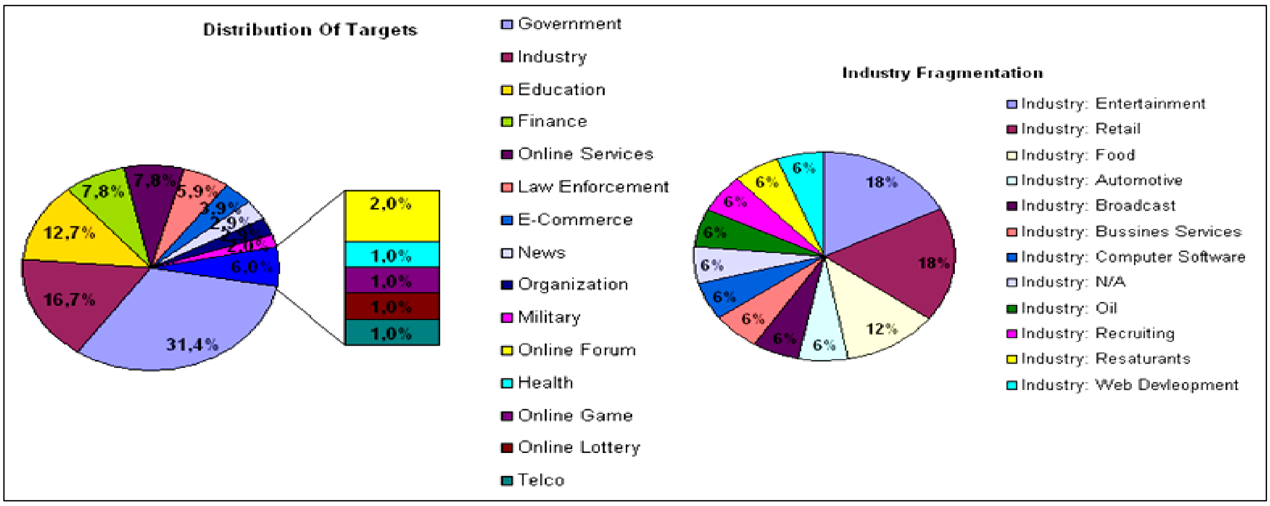


Figure 1. Cyber attacks statistics for october 2012. [3]

3. PENETRATION TESTING PROCEDURE

Penetration Testing - Pentest is a standardized procedure for checking the security of a computer system. Ideal conducting of pentest simulates ventures that would have made a malicious striker during execution attacks. In this way, possible security breaches in the computer system are identified using controlled procedures which also provide useful guidelines for their correction.

In principle, pentest uses one of the following three main methodologies, white, black or gray box [4]. Black box assumes that the attacker does not know anything about his target. That fact explains a large expenditure of time and effort in data collected in determining a potential attack vector. The entire testing process is carried out through four stages, with the possibility of iterations in waterfall sequence (Fig. 2).

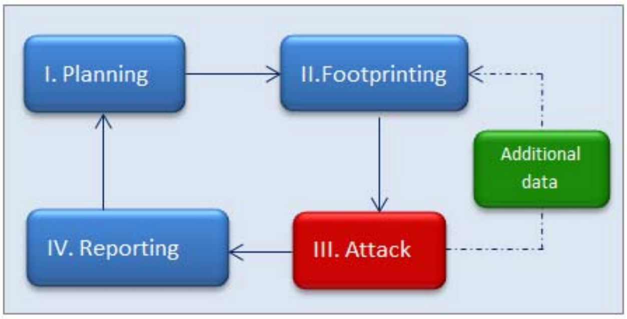


Figure 2. Penetration testing sequence of execution

Planning phase defines the scope and conducting method pentest in consultation with the client. After this official pentester prepares an action strategy, contractor is insured of possible negative consequences of testing. The next phase is the most comprehensive according to the number of procedures that should be implemented because it concerns with data collecting.

Reconnaissance phase is divided into fingerprinting, scanning and enumeration, and vulnerability analysis [5]. After carefully selecting the processed information attack vector must be designated, to explain the nature of found or targeted vulnerabilities.

Attack phase constitutes the core of each penetration test, which however does not always achieve success whereupon penetration tester selects new vectors of attack in the event of failure. After a successful attack, the entire process is documented and key vulnerabilities are identified as those that need to be repaired.

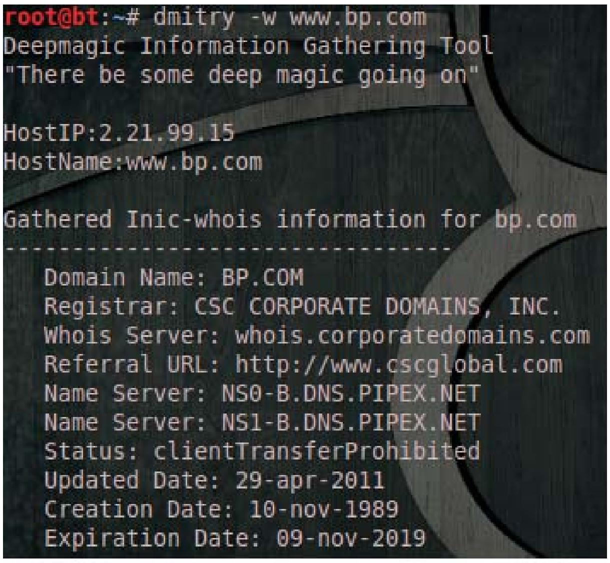
Reporting phase should provide categorized vulnerability information about targeted computer system, and to provide guidelines for its improvement if there contractor agrees. After penetration testing finishes, it is necessary to restore the initial state of computer system so organization can freely continue with their work.

4. THE USE OF PENETRATION TESTING TOOLS IN PRACTISE

For testing purposes, using a programming environment based largely on the Linux platform is considered a standard because Linux based machines faster and efficient approach in data processing. Backtrack OS represent a platform with such features. It is consisted of a number of preinstalled tools required to conduct safety tests.

Footprinting phase

The basic method for collecting information about the logical infrastructure of a computer network is done by WHOIS querying of Internet registries. For this purpose is used DMitry tool that provides information about the used block of IP address, organization name, email contacts, ASN number, ISP details, DNS servers with information about technical and administrative staff. The results from DMitry scan are shown in the report (Fig 3.).



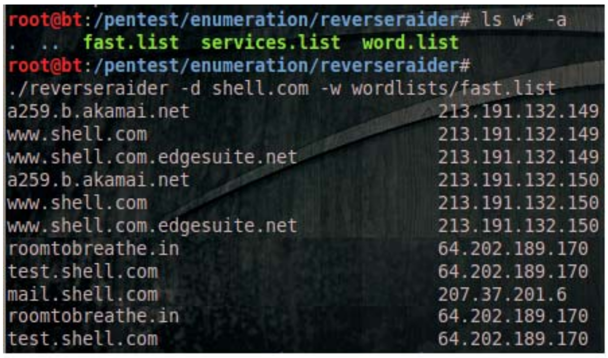
```
root@bt:~# dmitry -w www.bp.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:2.21.99.15
HostName:www.bp.com

Gathered Inic-whois information for bp.com
---------------------------------
   Domain Name: BP.COM
   Registrar: CSC CORPORATE DOMAINS, INC.
   Whois Server: whois.corporatedomains.com
   Referral URL: http://www.cscglobal.com
   Name Server: NS0-B.DNS.PIPEX.NET
   Name Server: NS1-B.DNS.PIPEX.NET
   Status: clientTransferProhibited
   Updated Date: 29-apr-2011
   Creation Date: 10-nov-1989
   Expiration Date: 09-nov-2019
```

Figure 3. Report shows DMitry scan results

As additional data collection method, Metagoofil is used to search relevant content associated with the target. It uses the API of a web search engines such as Google and retrieves files with relative paths on the network, author names, the installed applications specifications and network resources for sharing purposes. This type of information can be used for social engineering and staff deception. In order to obtain a complete list of available computers on a network domain, Reverseraider script is used. The screen excerpt from Reverseraider tool is shown in (Fig 4.).

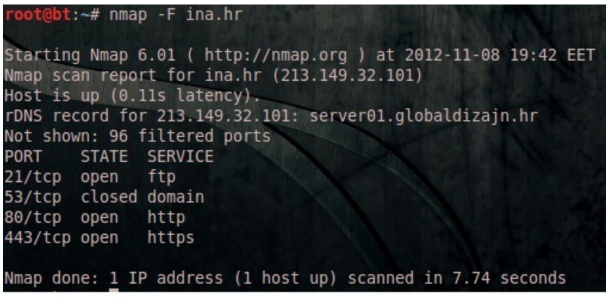


```
root@bt:/pentest/enumeration/reverseraider# ls w* -a
.  ..  fast.list  services.list  word.list
root@bt:/pentest/enumeration/reverseraider#
./reverseraider -d shell.com -w wordlists/fast.list
a259.b.akamai.net                       213.191.132.149
www.shell.com                           213.191.132.149
www.shell.com.edgesuite.net             213.191.132.149
a259.b.akamai.net                       213.191.132.150
www.shell.com                           213.191.132.150
www.shell.com.edgesuite.net             213.191.132.150
roomtobreathe.in                        64.202.189.170
test.shell.com                          64.202.189.170
mail.shell.com                          207.37.201.6
roomtobreathe.in                        64.202.189.170
test.shell.com                          64.202.189.170
```

Figure 4. Screen excerpt from reverseraider tool

Script takes solid files with lists of possible DNS names, and in combination with the name of the network domain actively checks computers using PING method. Collected information serve for scanning purposes against all the available resources to target, and their analysis in terms of finding potential security vulnerabilities. For the purposes of online scan using nmap, that is also an indispensable tool for many penetration testers.

Its activity is focused on the individual computers. Information as OS version, the number and types of ports are open, their specifications, the network protocols, encryption methods and such can be retrieved using various nmap probes. The screen excerpt from nmap tool is shown in (Fig. 5). Communication with the target is based on sending different types of IP packets (TCP Null, SYN, ACK, FIN, UDP) [6] where's the attacker interest that this procedure is carried out quietly to not start the automatic alarms from devices that block such activities (firewall, IDS, etc.) To reduce exposure of network and human resources, it is necessary to determine what information really needs to be available to the public.



```
root@bt:~# nmap -F ina.hr

Starting Nmap 6.01 ( http://nmap.org ) at 2012-11-08 19:42 EET
Nmap scan report for ina.hr (213.149.32.101)
Host is up (0.11s latency).
rDNS record for 213.149.32.101: server01.globaldizajn.hr
Not shown: 96 filtered ports
PORT    STATE  SERVICE
21/tcp  open   ftp
53/tcp  closed domain
80/tcp  open   http
443/tcp open   https

Nmap done: 1 IP address (1 host up) scanned in 7.74 seconds
```

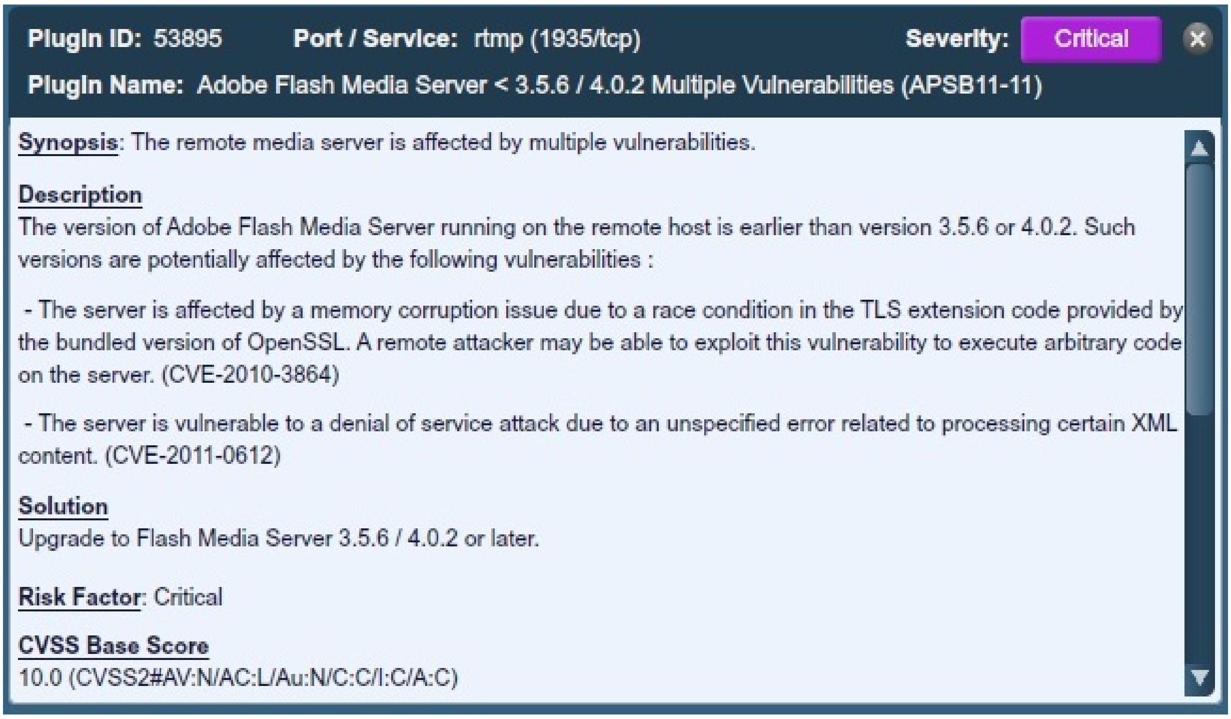
Figure 5. Screen excerpt from nmap tool

Taking this into account, the following steps should be done: shut down network services and ports that are not being used, provide a detailed inspection of packets on firewall, restrict employee activity on social networks and implement security policies within the organization to access data and start the processes.

Vulnerability analysis

Once the basic computing resources have been identified along with access points and methods of communication the process of examining vulnerabilities can start. This process includes searching databases for known vulnerabilities (*exploit database*) by default specifications and even writing custom scripts that are able to exploit the exposed vulnerability. Scripts that are able to take advantage of yet undiscovered vulnerabilities (*0Day Exploits*) are highly sought after on the black market today. One of the best vulnerability scanners is the Nessus. It is very efficient in scanning active applications, DNS servers, unprotected shared resources, factory computer settings, etc. It Uses ICMP and TCP ping methods of sending packets that are inherited from Nmap's arsenal. Nessus is able to generate detailed reports of discovered vulnerabilities and offer practical solutions for their removal. The results of Nessus vulnerability scanning are shown in (Fig. 6). A good example of a Web based scanner is Nikto which along of known vulnerabilities provides descriptions of improperly configured resources that can be successfully exploited in the attack.

Useful measures that can be taken to prevent vulnerability exploit are upgrading or installing applications with the latest version, removing the header information from the active devices and services, and ensuring traffic encryption using SSH and VPN methods.



Plugin ID: 53895 **Port / Service:** rtmp (1935/tcp) **Severity:** Critical

Plugin Name: Adobe Flash Media Server < 3.5.6 / 4.0.2 Multiple Vulnerabilities (APSB11-11)

Synopsis: The remote media server is affected by multiple vulnerabilities.

Description

The version of Adobe Flash Media Server running on the remote host is earlier than version 3.5.6 or 4.0.2. Such versions are potentially affected by the following vulnerabilities :

- The server is affected by a memory corruption issue due to a race condition in the TLS extension code provided by the bundled version of OpenSSL. A remote attacker may be able to exploit this vulnerability to execute arbitrary code on the server. (CVE-2010-3864)

- The server is vulnerable to a denial of service attack due to an unspecified error related to processing certain XML content. (CVE-2011-0612)

Solution

Upgrade to Flash Media Server 3.5.6 / 4.0.2 or later.

Risk Factor: Critical

CVSS Base Score

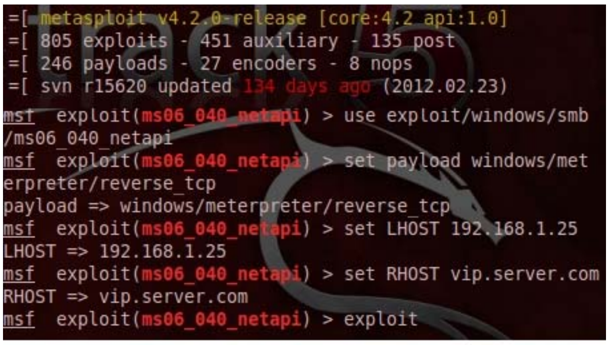
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Figure 6. Nessus vulnerability scanning report

Attacking Phase

After successful attack execution in the process of exploitation, the attacker will gain certain privileges over the system, which is then used in the stage of privilege escalation in order to seize as much control over computing resources and ultimately accomplish its goal.

This phase is the core of any penetration test and each time the most interesting and challenging that is not always successful and requires a wide knowledge and precision for successful execution. In the initial stage of exploitation (*exploitation phase*) penetration tester performs a security breach attempts using a custom composed pieces of program code (*exploits*). They are in most cases useful if the system has not been upgraded or has default settings or configured incorrectly. After successful execution of the attack in the exploitation phase, the real attacker would gain certain privileges over the system, which is then used in the privilege escalation phase. His ultimate goal is attain as much privileges as he can over computing resources to fulfill his intents.



```
 =[ metasploit v4.2.0-release [core:4.2 api:1.0]
 =[ 805 exploits - 451 auxiliary - 135 post
 =[ 246 payloads - 27 encoders - 8 nops
 =[ svn r15620 updated 134 days ago (2012.02.23)
msf  exploit(ms06_040_netapi) > use exploit/windows/smb
/ms06_040_netapi
msf  exploit(ms06_040_netapi) > set payload windows/met
erpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(ms06_040_netapi) > set LHOST 192.168.1.25
LHOST => 192.168.1.25
msf  exploit(ms06_040_netapi) > set RHOST vip.server.com
RHOST => vip.server.com
msf  exploit(ms06_040_netapi) > exploit
```

Figure 7. Exploit parameters configuration for Metasploit

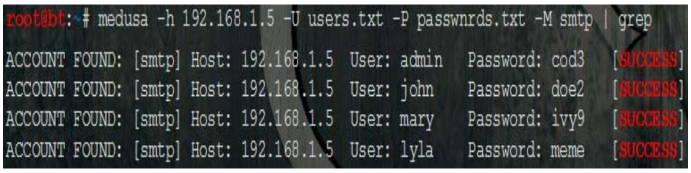
The best known software platform to execute attack is Metasploit which gained its popularity due to the possibility of using the immense library exploits for multiple operating platforms and networking protocols. The program also offers the possibility of encoding data (payloads) so the malicious code can seamlessly pass through the firewall and IDS devices [7]. The configuration of exploit parameters for Metaspolit is shown in (Fig. 7). In addition, the database also represents an important strategic point of each organization. For its testing purposes penetration testers use DarkMySQLi application which takes advantage of bad structured data in databases in order to effectively change its user permissions so in the end attacker can read, modify and execute data. Prior to its use, tester should check whether the web interface parses the input characters. Manually, it can be done by adding characters to the original URL (highlighted in red).

URL: http://www.newscoorporation/popup_news.php?id=”22

If the server sends error message using this syntax, it means that it is vulnerable against SQL Inject technique.

Warning: mysql_fetch_row(): supplied argument is not a valid MySQL result

During attack phase, brute force tools for password cracking are also used

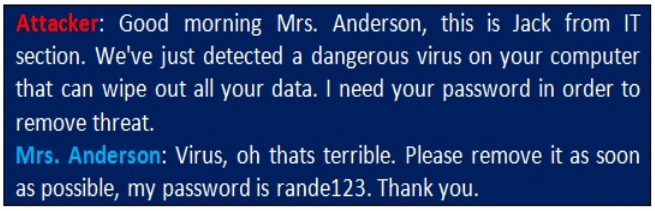


```
root@bt:~# medusa -h 192.168.1.5 -U users.txt -P passwnrds.txt -M smtp | grep
ACCOUNT FOUND: [smtp] Host: 192.168.1.5  User: admin   Password: cod3   [SUCCESS]
ACCOUNT FOUND: [smtp] Host: 192.168.1.5  User: john    Password: doe2   [SUCCESS]
ACCOUNT FOUND: [smtp] Host: 192.168.1.5  User: mary    Password: ivy9   [SUCCESS]
ACCOUNT FOUND: [smtp] Host: 192.168.1.5  User: lyla    Password: meme   [SUCCESS]
```

Figure 8. Brute force passwords lookup with Medusa tool

Medusa is an example of such a tool that is designed for fast and parallel testing of login information services. Using a parallel process allows testing on multiple host computers at once. It is possible to use several different files to test values versus number of services that are defined by modules (FTP, HTTP, IMAP, RSH, etc.). (Fig. 8) shows brute force passwords lookup with Medusa tool. Despite all the technological advances of displayed attack tools, social engineering has proved as the most effective method that deals with the prediction of human behavior based on the information in their environment [8]. An example of social engineering is shown in (Fig. 9).

Trained attacker can seize valuable information using employee disinformation which allows access to otherwise protected network resources. To ensure the system against attacks quality insurance policies must take place.



Attacker: Good morning Mrs. Anderson, this is Jack from IT section. We've just detected a dangerous virus on your computer that can wipe out all your data. I need your password in order to remove threat.

Mrs. Anderson: Virus, oh thats terrible. Please remove it as soon as possible, my password is rande123. Thank you.

Figure 9. Social engineering example

While logging for service or computer, it is advisable to use complex passwords with a random sequence of characters. Next, the user should be limited with the number of login attempts because an attacker can use brute-force tool for recurrent logging. Because of that logging forms are additionally supplied with logical queries (*captcha*) to verify that the human executes request. It is impossible to predict all attack vectors but in most cases the attackers use the fact that administrators do not change the default settings for activated service or application [9, 10, 11].

5. CONCLUSION

The increase in cyber threats and frequent attacks on computer systems is increasing day by day. By using black box methods, the attacker does not need to have physical access to the network as it makes him more efficient and provides a great deal of anonymity. We have seen how easy it is for attacker once he has collected the required data on the target, to perform fast and accurate attack. Taking into account that the majority of attacks happen due to data theft, the trading companies should be particularly vigilant as the majority of transactions take place online using credit card payments. Therefore, in order to avoid business losses, organizations must ensure proactive monitoring system to its upgrading and training of the staff, which guarantees a sturdy integrity and quality business.

6. REFERENCES

[1] J. Andress, **The Basics of Information Security**, Elsevier, 2011

[2] J. Ericson, **The Art of Exploitation**, 2nd Edition, No Starch Press, 2008

[3] P. Passeri, **October 2012 Cyber Attacks Statistics**, http://hackmageddon.com/2012/11/06/october-2012-cyber-attacks-statistics/, (December 2012)

[4] Ec-Council, **Ethical Hacking and Countermeasures**, Cenglage Learning, 2009

[5] J. Faircloth, **Penetration Tester's Open Source Toolkit**, Elsevier, 2011

[6] C. Hurley, **Penetration Tester's Open Source Toolkit**, Syngress, 2007

[7] A. Singh, **Metasploit Penetration Testing Cookbook**, Packt Publishing Ltd, 2012

[8] C. Hadnagy, **The Art of Human Hacking**, John Wiley & Sons, 2010

[9] W. Pritchett, D. De Smet, **BackTrack 5 Cookbook**, PACKT Publications 2012

[10] A. Gupta, S. Laliberte, **Defend I.T.: Security by Example**, Addison-Wesley Professional, 2004

[11] D. Stuttard, M. Pinto, **The Web Application Hacker's Handbook**, Wiley, 2011