Journal of Scientific Research & Reports
11(4): 1-14, 2016; Article no.JSRR.27572
ISSN: 2320-0227

SCIENCEDOMAIN *international*
www.sciencedomain.org

Simulation-based Learning Utilizing Virtualization Technology and Backtrack in Teaching Information Assurance and Security: Case in Haramaya University

Patrick D. Cerna[1*]

[1]Department of Information Technology, College of Computing and Informatics, Haramaya University, P.O.Box 335, Haramaya, Ethiopia.

Author's contribution

The sole author designed, analyzed, interpreted and prepared the manuscript.

Article Information

DOI: 10.9734/JSRR/2016/27572
Editor(s):
(1) Grigorios L. Kyriakopoulos, School of Electrical and Computer Engineering, National Technical University of Athens (NTUA), Greece.
Reviewers:
(1) Manish Mahajan, Punjab Technical University, India.
(2) Rupali Warkar, Pune University, India.
Complete Peer review History: http://sciencedomain.org/review-history/15313

Original Research Article

Received 8th June 2016
Accepted 1st July 2016
Published 7th July 2016

ABSTRACT

Simulation-based training techniques, tools, and strategies can be applied in designing structured learning experiences, as well as be used as a measurement tool linked to targeted teamwork competencies and learning objectives. An adequate computing lab support for advanced computer courses that needs practical understanding and hands-on approach is a perennial challenge for most higher educational in Ethiopia. The study presents a model of using dedicated and flexible lab support information security and assurance courses as part of the curriculum of Bachelor of Science in Information Technology in Haramaya University, Ethiopia. Using virtualization technology different laboratory setup on a single computer machine has been implemented using one of the well-known operation system for penetration testing called backtrack. Information Security topics like Port Scanning and Service Identity Determination, Password Cracking, Trojan Attacks, Steganography, Man-in-the-middle attacks, and Web SQL injection were able to learn and simulate by students under this virtualization setup. A self-administered survey questionnaire has been employed to assess the class service quality and perception of the students on this matter. The result shows that after the students are introduced to the activity in the laboratory using virtual

**Corresponding author: E-mail: p.cerna.1978@ieee.org;*

machine in simulating topics in information security, there is 83% increase in number of student having a very good understanding in the subject. Moreover, the table shows us that 90% of the student agrees that the hands on activity using VM really increase their interesting learning the course. Moreover, the table shows us that 90% of the student agrees that the hands on activity using VM really increase their interesting learning the course. These show that the implementation of hands on activity with VM really helps the student to have better understanding in the subject matter. In conclusion, virtualization technology is not only limited to industry utilizing them to improve their servers and network services, but also has been effective as innovative teaching strategy in the laboratory practical session in the academe. Thus, it was found that the students are accepting the challenge to learn information security using virtualization and are benefiting greatly from their experiences.

Keywords: Virtualization; information security; man-in-the-middle attack; steganography; SQL web injection; password cracking.

1. INTRODUCTION

With rapid advances in the virtualization technology, laboratories leveraging virtual machines, or Virtual Hands-on Laboratories, have become one of the key education resources in computing field Glantz [1]. For higher educational institution with limited number of computing resources, a computer virtualization technology becomes more mature, leveraging in a virtual simulation laboratories. Apart from this concerns and issues on practical security attack and defense tools for educational purpose can be mitigated with simulation laboratories.

Virtual computer networks are wide-spreading along researchers, administrators and teachers all around the world Gurgel et al. [2]. These kinds of tools provide a solution for creating low-cost experiments that students can run in their personal computer, even if they have a modest configuration Fuertes and Vergara [3]. According to Gercek and Saleem [4], the network lab is a multipurpose open lab where different course experiments can be conducted simultaneously, policies, guidelines and operational procedures need to be clearly stated at the technical as well as at the procedural level.

One of the innovative approaches in teaching is Simulation-based learning, it offers the opportunity for information technology students to practice skills, techniques, communication, problem solving and critical thinking in a replica of working environment. According to Webster [5], simulation offers innovative ways of teaching students about real situation in a controlled environment. According to Rhodes and Curran [6], an interactive environment that permits learning through hands on experience is possible with high fidelity simulation experiences in nursing education. Lateef [7] explain that simulation is a technique for practice and learning that can be applied to many different disciplines and trainees. Furthermore, Lateef [8] emphasize that it is a technique (not a technology) to replace and amplify real experiences with guided ones, often “immersive” in nature, that evoke or replicate substantial aspects of the real world in a fully interactive fashion.

An adequate computing lab support for advanced computer courses that needs practical understanding and hands-on approach is a perennial challenge for most higher educational in Ethiopia. Factors, such as lack of physical space, budgetary constraints, conflicting needs of different courses, and rapid obsolescence of computing technology, precipitate this challenge. Thus advanced computer courses needed dedicated simulation laboratory with diverse support requirements to improve student performance and well-equipped in changing world of working environment. Other than that, there exist some difficulties in teaching Information Security course in Haramaya University. The problems arise from three different aspects; Pedagogical and Management Issues, Laboratory Structure and Content of Exercise.

In this research, the author presents a model of using dedicated and flexible lab support information security and assurance courses as part of the curriculum of Bachelor of Science in Information Technology Program under the College of Computing and Informatics in Haramaya University, Ethiopia.

2. RELATED WORK

According to Jha [9], simulation is a technique for practice and learning that can be applied to many different disciplines and types of trainees. It is a technique (not a technology) to replace and amplify real experiences with guided ones, often “immersive” in nature, that evoke or replicate substantial aspects of the real world in a fully interactive fashion Jha [9]. “Immersive” here implies that participants are immersed in a task or setting as if it were the real world Jha [9].

Lateef [7] explains that simulation has also begun to change much of the ways in which medicine is taught and how trainees and junior doctors acquire the relevant skills. Medical, nursing, and other health care staff also have the opportunity to develop and refine their skills, repeatedly if necessary, using simulation technology without putting patients at risk Lateef [7].

According to Lateef [7], simulation training centers, with their new techniques and equipment, offer unique opportunities for dynamic, complex, and unanticipated medical situations to be practiced and managed. She emphasize Lateef [7] that in both aviation and health care domains, human performance is strongly influenced by the situational context, i.e., the interaction between the task, the environment, and the behavior of team members. Lateef [7] arque that in aviation, more than 50 years of research has shown that superior cognitive and technical skills are not enough to ensure safety: effective teamwork skill is a must Similar observations are also now being made in the practice of medicine Lateef [7].

Agarwal et al. [10] explains that a dedicated computer lab for a course is warranted when a general lab cannot provide adequate computing support for the course. According to Belles, Gorka and Miller [11], a dedicated lab is designed to support a specific course; normally, however, such labs support multiple courses.

Consequently, it is imperative that the design and configuration of an under-development lab must be (1) versatile – to accommodate diverse and conflicting computing needs, (2) flexible – to efficiently support different courses, and (3) modular – to easily incorporate new technologies or allow lab reconfiguration Wilson [12].

Gadelha et al. [13] present the OS Simulator, which consists of a simulator file system to support the teaching and learning of operating systems. The authors' work describes the tool and analyzes the students positive attitude feedback obtained through questionnaires Gadelha et al. [13]. Fuertes and Vergara [3] present the VNUML, a virtualization tool similar to *Netkit* for virtualization of computer networks, VNUML has very similar features and based on UML as well. The authors show a comparison of performance among the VNUML, Netkit and other similar tools Fuertes and Vergara [3].

Barbosa et al. [14] presented a evaluation of apprenticeship in computer networks through Netkit virtualization tool, and what strategies can be used to improve learning, proposing a working method that can be used in the classroom, or even in the students’ homes in case of distance education courses disciplines.

Yang [15] describes the laboratory projects developed for system and network administration course sequence offered in an Applied Computer Science Master’s program in the spring of 2006. The first course focused on system administration, while the second course focused on network part. In each course, theoretical aspects were covered in class, while projects were assigned to teach students the practical application. University of Milan within the course of Security of Informatics Systems and Networks has designed and developed a complete training environment using Xen platform on top of Gentoo Linux Damiani et al. [16]. Chen and Tao [17] have developed a tool called Secure WEb development Teaching (SWEET) to introduce security concepts and practices for web application development. The tool provides introductory tutorials, teaching modules utilizing virtualized hands-on exercises, and project ideas in web application security Chen and Tao [17]. In addition, the tool provides pre-configured virtual computer for laboratory exercises Chen and Tao [17]. Zaki et al. [18] presents an implementation of Virtualization Technology in teaching Information Technology Security which allows labs to progress in a secure and portable manner while providing additional protection for the real systems. In this study, a special laboratory environment that can be set up with minimal cost, is easy to manage and can isolate the hazardous activities from the real environment is needed Zaki et al. [18].

In the light of the above literature, the research identifies gaps and found some limitation of the previous conducted study on this topic. Most of the empirical study conducted in the past had now fully simulated the all important topic in information security such as password cracking, web sql injection, steganography, man-in-the-middle attacks, among others. With this, the researcher was motivated to present a model of using dedicated and flexible lab support using virtualization technology and backtrack operation system for penetration testing in order to successfully implement most if not all topics in information security and assurance.

3. METHODOLOGY

3.1 Virtual Lab Setup

The lab exercises are written for both a Windows and Linux environment. It was setup using Virtual Machine software called VM Ware Player. Hassell [19] explains that Virtualization, the move from real, physical hardware to virtual hardware is being seen as one of the next big things in IT. There are more virtualization options for IT departments than ever before, including Xen SourceInc's and Virtual Iron Software Inc's open-source applications, Microsoft Corp's Virtual Server and VMware Inc's venerable products Hassell [19]. But if you are new to this party, you might not know how to get started Hassell [19].

There are several lab exercises in which both environments are required so it is recommended that you set up all 4 virtual machines. Thus there are 4 lab setup which are windows, linux, mixed or internet designate the lab environment required for each lab exercise in the title. The first windows labs designated with the letter ‘w’ consists of 2 Virtual PCs, one with Windows 7 Professional and one with Windows 2008 Server. In general, the Windows 7 PC will be the client/attacking machine and the Windows 2008 Server will be the server/target machine while the second linux labs designated with the letter ‘l’ consists of 2 Virtual PCs, one with Backtrack (client/attack) and the other with Metasploitable (server/target).

In general, the Backtrack will be the attacking machine and the Metasploitable will be the target machine. The third lab setup is a mixed environment designated with the letter ‘m’ will have Virtual PCs from both environments. Usually this environment uses the Linux server as an SSH, DNS or mail server while the fourth lab is a host setup designated with the letter ‘h’ with interconnectivity lab that can be done from the PC that is hosting the Virtual Machines or they can be done from any PC that has Internet access.

3.2 Activity 1: Penetration Testing: IP Address and Port Scanning, Service Identity Determination

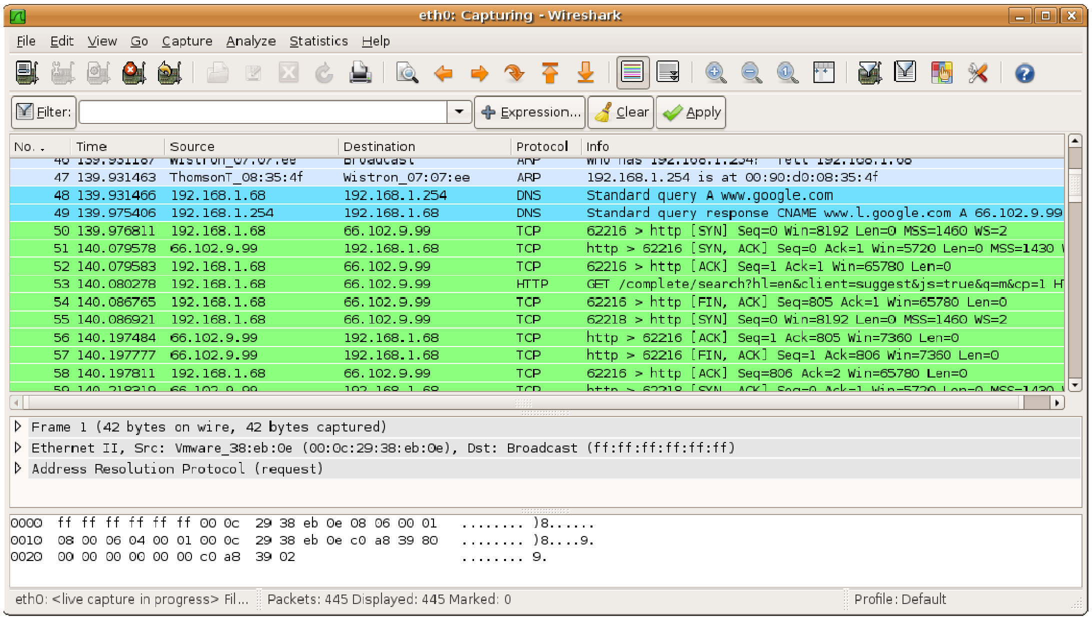
Penetration Testing or Ethical hacking attempt to break into systems and networks to find weaknesses that might be exploited by criminals Ke et al. [20]. According to Conklin et al. [21], penetration testing is a method of testing a network’s security by using various tools and techniques common to attackers. The methodology used is similar to that of an attacker: enumerate the network, assess vulnerabilities, research vulnerabilities for known exploits, and then use tools available to penetrate the network Conklin et al. [21]. Enumerating a network to discover what machines are attached and operating is a useful task for both an intruder and a system administrator Conklin et al. [21]. Bacudio et al. [22] and, penetration testing is a series of undertaken activities to identify and exploit security weaknesses. It is security testing which attempts to circumvent security features of a system Wack et al. [23]. Osborne [24] defines a penetration test as “a test to ensure that gateways, firewalls, and systems are appropriately designed and configured to protect against unauthorized access or attempts to disrupt services.

In simulating this topic in the laboratory, the first lab ‘w’ or windows lab has been adapted. To simulate this lab the author used Nmap to identify the computers that are on the network, enumerate the ports on the computers that were located, and then look at the network traffic generated by these actions. Nmap is also a well-known tool amongst penetration testers for general purpose network scanning Alder et al. [25]. Nmap is compatible with various operating systems like Windows, Linux, Mac OS X, Sun Solaris, and several other platforms.

It was then used to scan the ports stealthily and compare the method to the previous scan. To observe service banners, Telnet will be used to obtain the banners from IP/port combinations obtained from Nmap scans.

3.2.1 Procedure

Step 1: Start the Windows 2008 Server and Window 7 Professional machines. Only log on to the Windows 7 machine.
Step 2: Start Wireshark.
Step 3: Use Nmap to scan the network.
Step 4: Analyze the output from Wireshark.
Step 5: Use Nmap to scan open TCP ports.
Step 6: Use Wireshark to analyze the scan.
Step 7: Use Nmap to do a stealth scan on the computer.
Step 8: Use Wireshark to analyze the scan.
Step 9: Use Nmap to enumerate the operating system of the target computer.
Step 10: Use Telnet to connect to the web server, FTP server, and SMTP banner.
Step 11: Log off from the Windows 7 Professional PC.


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

```
No. .  Time        Source              Destination         Protocol  Info
   46 139.931187  Wistron_07:07:ee    Broadcast           ARP       Who has 192.168.1.254?  Tell 192.168.1.68
   47 139.931463  ThomsonT_08:35:4f   Wistron_07:07:ee    ARP       192.168.1.254 is at 00:90:d0:08:35:4f
   48 139.931466  192.168.1.68        192.168.1.254       DNS       Standard query A www.google.com
   49 139.975406  192.168.1.254       192.168.1.68        DNS       Standard query response CNAME www.l.google.com A 66.102.9.99
   50 139.976811  192.168.1.68        66.102.9.99         TCP       62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
   51 140.079578  66.102.9.99         192.168.1.68        TCP       http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 W
   52 140.079583  192.168.1.68        66.102.9.99         TCP       62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
   53 140.080278  192.168.1.68        66.102.9.99         HTTP      GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
   54 140.086765  192.168.1.68        66.102.9.99         TCP       62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
   55 140.086921  192.168.1.68        66.102.9.99         TCP       62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
   56 140.197484  66.102.9.99         192.168.1.68        TCP       http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
   57 140.197777  66.102.9.99         192.168.1.68        TCP       http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
   58 140.197811  192.168.1.68        66.102.9.99         TCP       62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
   59 140.218319  66.102.9.99         192.168.1.68        TCP       http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 W

▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.

eth0: <live capture in progress> Fil...   Packets: 445 Displayed: 445 Marked: 0   Profile: Default
```

Fig. 1. Traffic generated by Nmapscan
(Source: Nmap Software in windows server)

3.3 Activity 2: Password Cracking

In cryptanalysis and computer security, password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system Lundin [26]. A common approach (brute-force attack) is to try guesses repeatedly for the password and check them against an available cryptographic hash of the password. The time to crack a password is related to bit strength (see password strength), which is a measure of the password's information entropy, and the details of how the password is stored. Most methods of password cracking require the computer to produce many candidate passwords, each of which is checked. One example is brute-force cracking, in which a computer tries every possible key or password until it succeeds Ethical Hacking Central [27]. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be attempted before brute force. Higher password bit strength exponentially increases the number of candidate passwords that must be checked, on average, to recover the password and reduces the likelihood that the password will be found in any cracking dictionary Montoro [28].

According to Lundin [26], the time to crack a password is related to bit strength, which is a measure of the password's information entropy, and the details of how the password is stored.

Most methods of password cracking require the computer to produce many candidate passwords, each of which is checked. One example is brute-force cracking, in which a computer tries every possible key or password until it succeeds. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be attempted before brute force. Higher password bit strength exponentially increases the number of candidate passwords that must be checked, on average, to recover the password and reduces the likelihood that the password will be found in any cracking dictionary.

To simulate this topic in the laboratory, the author adapted the second lab setup or 'l' linux lab. It uses the build in program called John the Ripper installed by default in the backtrack machine, which serves as the attacker. According to Ethical Hacking Central [27], John the Ripper is a free password cracking tool that runs on a large number of different platforms. It is one of the most used password cracking tools because it combines several other password crackers into a single package and has a number of handy features such as automatic hash type detection. In this post I will present a simple John the Ripper tutorial to get you started.

John the Ripper is a fast password cracker, currently available for many flavors of Unix, Windows, DOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt (3) password hash types most commonly found on various Unix systems, supported out of the box are Windows LM hashes, plus lots of other hashes and ciphers in the community-enhanced version openwall [29].

3.3.1 Procedure

Step 1: Create Some User Accounts. Let's create user1 with password "flower" and user2 with a password of "hacker".

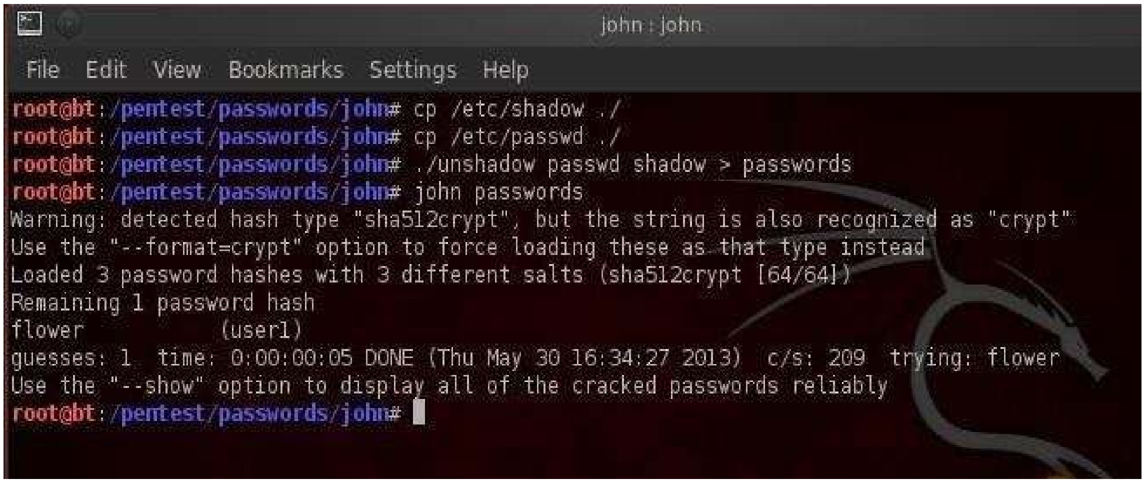
Step 2: Open John the Ripper. We can access it from BackTrack by going to the BackTrack button on the bottom left, then Backtrack, Privilege Escalation, Password Attacks, Offline Attacks, and finally select John the Ripper from the multiple password cracking tools available.

Step 3: Test John the Ripper. At the prompt, type: bt> john -test

Step 4: Copy the Password Files to Our Current Directory
Linux stores its passwords in /etc/shadow

Step 5: Unshadow. Next we need to combine the information in the /etc/shadow and the /etc/passwd files, so that John can do its magic

Step 6: Crack. Now that we have unshadowed the critical files, we can simply let John run on our password file using the command bt> john passwords



```
root@bt:/pentest/passwords/john# cp /etc/shadow ./
root@bt:/pentest/passwords/john# cp /etc/passwd ./
root@bt:/pentest/passwords/john# ./unshadow passwd shadow > passwords
root@bt:/pentest/passwords/john# john passwords
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 3 password hashes with 3 different salts (sha512crypt [64/64])
Remaining 1 password hash
flower           (user1)
guesses: 1  time: 0:00:00:05 DONE (Thu May 30 16:34:27 2013)  c/s: 209  trying: flower
Use the "--show" option to display all of the cracked passwords reliably
root@bt:/pentest/passwords/john# 
```

Fig. 2. Cracking password using John the ripper
(Source: Terminal in BackTrack OS)

3.4 Activity 3: Trojan Horse Attacks

Trojans are pieces of malware allowing a hacker to remote access a computer system Conklin et al. [21]. They are not self-replicating and are not automated in that they need direction interaction with a hacker to fulfill their purpose Landwehr [30]. Trojans need to be installed from an executable file or a compiler. Sometimes Trojans exploit flaws in a browser, messenger program, or media player. Once installed, the hacker can use the Trojan to access sensitive information. SolidPass protects you from Trojans with powerful two-factor authentication Solidpass [31]. According to Landwehr et al. [30], Trojan horse, or Trojan, is any malicious computer program which is used to hack into a computer by misleading users of its true intent. The term is derived from the Ancient Greek story of the wooden horse that was used to help Greek troops invade the city of Troy by stealth.

Trojans are a common way that attackers attempt to exploit a computer. There are many different types of Trojans with different degrees of functionality. The infamous Back Orifice is a Microsoft Windows– based Trojan that allows complete remote administrative control over a client machine. NetBus and SubSeven were also two popular Trojans used to compromise target systems Conklin et al. [21].

To simulate this topic in the laboratory, the author adapted the first lab setup or ‘w’ windows lab. It uses the build in program called spy net installed by default in the backtrack windows client machine, which serves as the attacker. Spy Net 2.6 the ultimate combination network monitoring and administration software tool suite. SPY NET 2.6 monitors activity such as keystrokes typed on your network, web sites visited and more. Thus far, a single interface to a PC , application launching, screenshot viewing and sending a message to more than one PC to existing desktop computer functions as the main client controls Conklin et al. [21].

3.4.1 Procedure

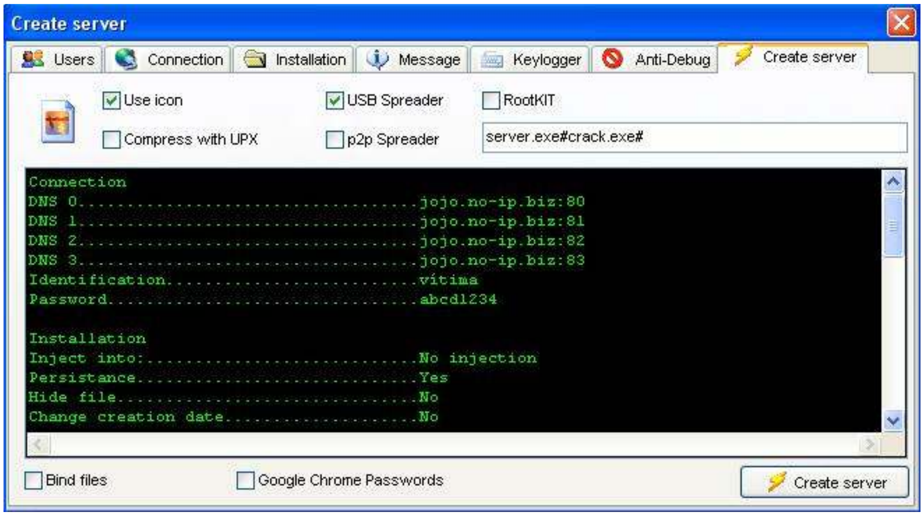
Step 1: Log on to the Windows 7 Professional and Windows 2008 Server PCs.
Step 2: Install Spy-net on the Windows 7 Professional PC.
Step 3: Configure the server and Trojan file

Beta Testers:
Viotto (opensc.ws)
kMr (Good friend)
ECko (indetectables.net)
Dea7h
krizhiel

spynetcoder@gmail.com

Fig. 3. Spy net main interface
(Source: SPYnet software in windows server)

Step 4: Deploy and run the Trojan.



☑ Use icon ☑ USB Spreader □ RootKIT
□ Compress with UPX □ p2p Spreader server.exe#crack.exe#

```
Connection
DNS 0...................................jojo.no-ip.biz:80
DNS 1...................................jojo.no-ip.biz:81
DNS 2...................................jojo.no-ip.biz:82
DNS 3...................................jojo.no-ip.biz:83
Identification..........................vítima
Password................................abcd1234

Installation
Inject into:............................No injection
Persistance.............................Yes
Hide file...............................No
Change creation date....................No
```

□ Bind files □ Google Chrome Passwords

Fig. 4. Spy net Trojan options
(Source: SPYnet software in windows server)

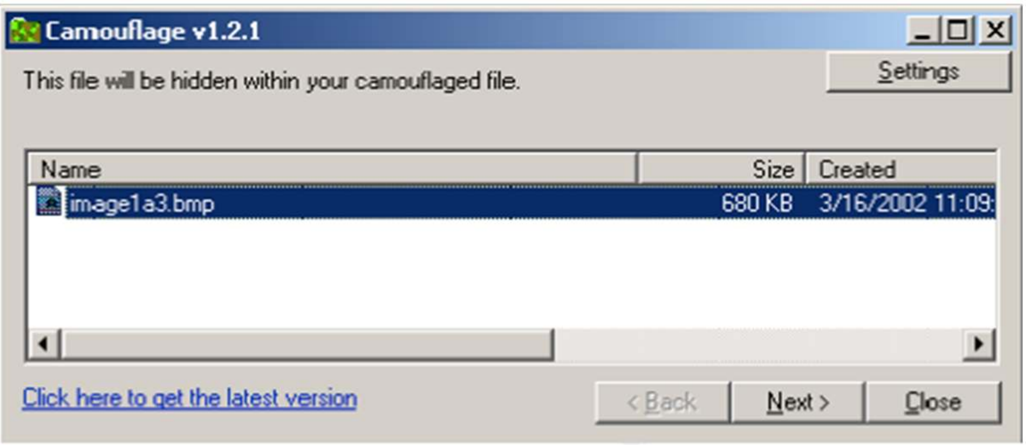
3.5 Activity 4: Steganography

The word “steganography” is derived from the Greek words stegos meaning cover and grafia meaning writing defining it as covered writing Soni et al. [32]. According to Akhtar et al. [33], steganography is the art and science of secret communication. It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The actual files can be referred to as cover text, the cover image, or cover audio message. After inserting the secret message it is referred to as stego medium. A stego-key has been used for hiding encoding process to restrict detection or extraction of the embedded data Akhtar et al. [33].

To simulate this topic in the laboratory, the author adapted the first lab setup or ‘w’ windows lab. It uses the build in program called camouflage installed by default in the backtrack windows client machine, which serves as the attacker. Camouflage Software is easy to use, install, and a very versatile steganography tool that is free of charge and available for download to anyone Sans [34].

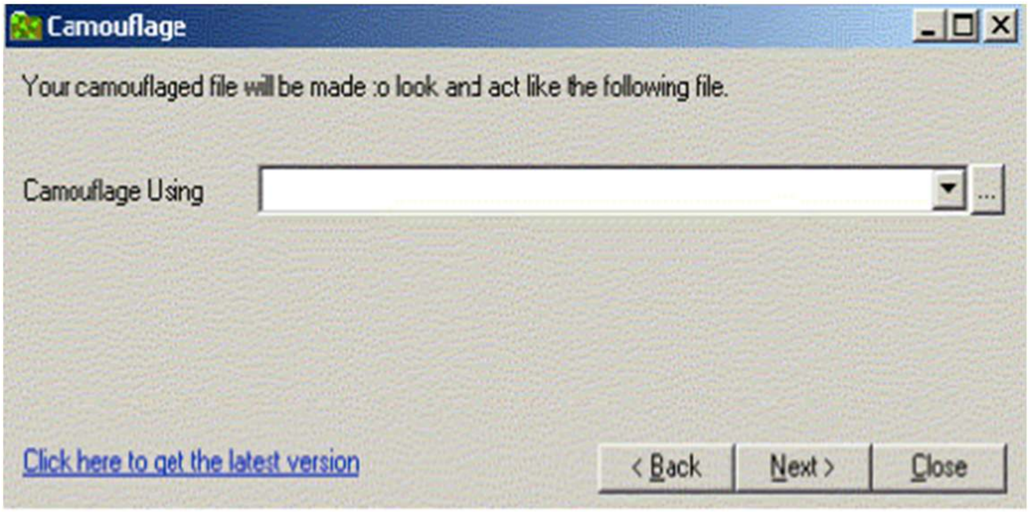
3.5.1 Procedure

Step 1: Log on to the Windows 7 Professional and Windows 2008 Server PCs.
Step 2: Install Camouflage on the Windows 7 Professional and Windows 2008 Server PCs.
Step 3: Create and hide a message.



This file will be hidden within your camouflaged file.

Name	Size	Created
image1a3.bmp	680 KB	3/16/2002 11:09:



Your camouflaged file will be made :o look and act like the following file.

Fig. 5. Camouflage program for creating and hide a message on an image

(Source: Camouflage software running in windows server)

Step 4: Upload the message to the web server.

Step 5: Retrieve the message from the Windows 2008 Server PC.

Step 6: Log off from the Windows 7 Professional and Windows 2008 Server PCs.

3.6 Activity 5: Man in the Middle Attack

Man in the middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker. A man-in-the-middle attack can only be successful when the attacker can impersonate each endpoint to the satisfaction of the other Patange [35].

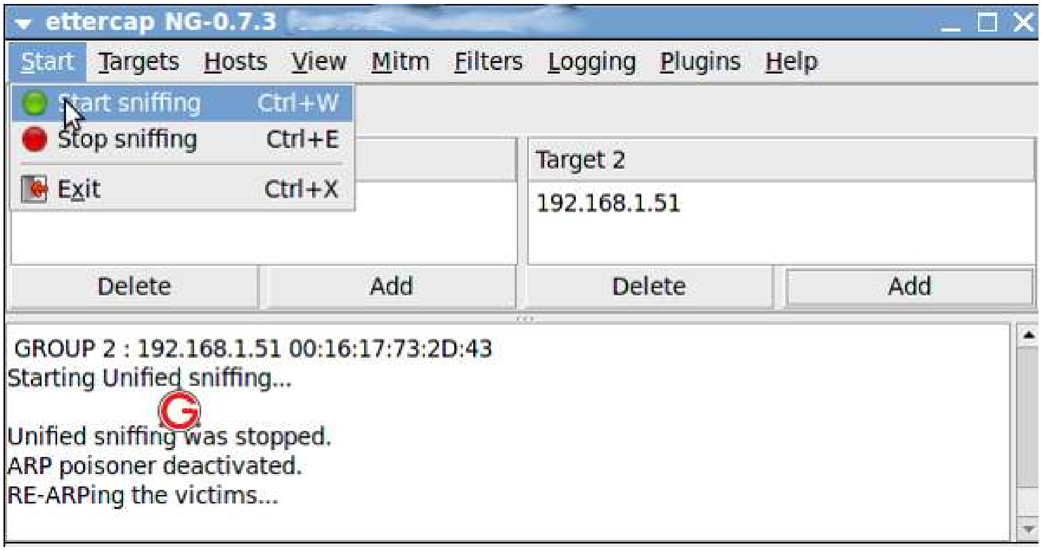
Man in the middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. Man-in-the-middle attacks can be thought about through a chess analogy. Mallory, who barely knows how to play chess, claims that she can play two grandmasters simultaneously and either win one game or draw both. She waits for the first grandmaster to make a move and then makes this same move against the second grandmaster. When the second grandmaster responds, Mallory makes the same play against the first. She plays the entire game this way and cannot lose. A man-in-the-middle attack is a similar strategy and can be used against many cryptographic protocols Trappe [36].

To simulate this topic in the laboratory, the author adapted the third lab setup or ‘m’ mix windows and linux lab. It uses the build in program called wireshark and ettercap installed by default in the backtrack client machine, which serves as the attacker. Wireshark is a Free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education Wireshark [37].

Step 1: Log on to the Windows 7 Professional, Windows 2008 Server, and BackTrack PCs.

Step 2: Document the IP and MAC addresses of the three PCs.

Step 3: Start Wireshark and run Ettercap on the BackTrack PC.



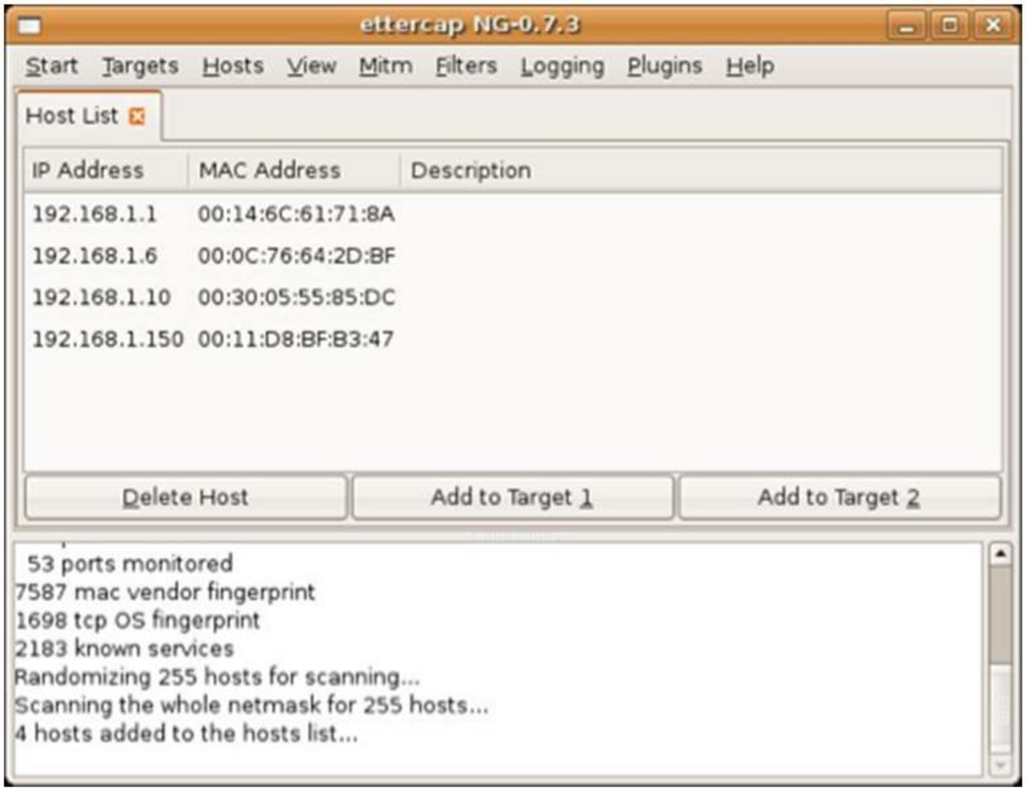
Target 2

192.168.1.51

```
GROUP 2 : 192.168.1.51 00:16:17:73:2D:43
Starting Unified sniffing...

Unified sniffing was stopped.
ARP poisoner deactivated.
RE-ARPing the victims...
```

Fig. 6. Ettercap interface starting sniffing
(Source: Ettercap running in BackTrack O.S)



IP Address	MAC Address	Description
192.168.1.1	00:14:6C:61:71:8A	
192.168.1.6	00:0C:76:64:2D:BF	
192.168.1.10	00:30:05:55:85:DC	
192.168.1.150	00:11:D8:BF:B3:47	

```
 53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
```

Fig. 7. Ettercap interface performing man-in-the-middle attack
(Source: Ettercap running in BackTrack OS)

Step 4: Capture an FTP session.
Step 5: View the Ettercap output and analyze the Wireshark capture.
Step 6: Log off from all PCs.

3.7 Activity 6: Web SQL Injection

According to Acunetix [38], SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements (also commonly referred to as a malicious payload) that control a web application's database server (also commonly referred to as a Relational Database Management System – RDBMS). Since an SQL injection vulnerability could possibly affect any website or web application that makes use of an SQL-based database, the vulnerability is one of the oldest, most prevalent and most dangerous of web application vulnerabilities. By leveraging an SQL injection vulnerability, given the right circumstances, an attacker can use it to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQL injection can also be used to add, modify and delete records in a database, affecting data integrity Acunetix [38].

Sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections sqlmap [39].

To simulate this topic in the laboratory, the author adapted the fourth lab setup or 'h' host lab setup. The client attacking machine is a backtrack with a built in program called sqlmap to perform SQL injection to a Windows server machine hosting a website application.

3.7.1 Procedure

Step 1: Go To Applications>BackTrack>Exploitation Tools>DataBase Exploitation Tools>MySQL Exploitation Tools>sqlmap.

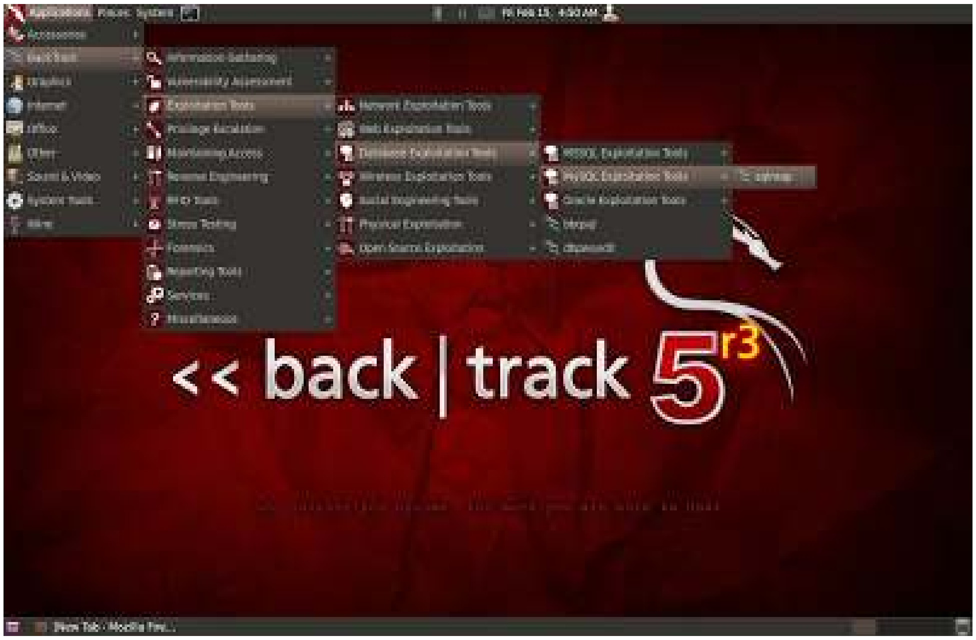
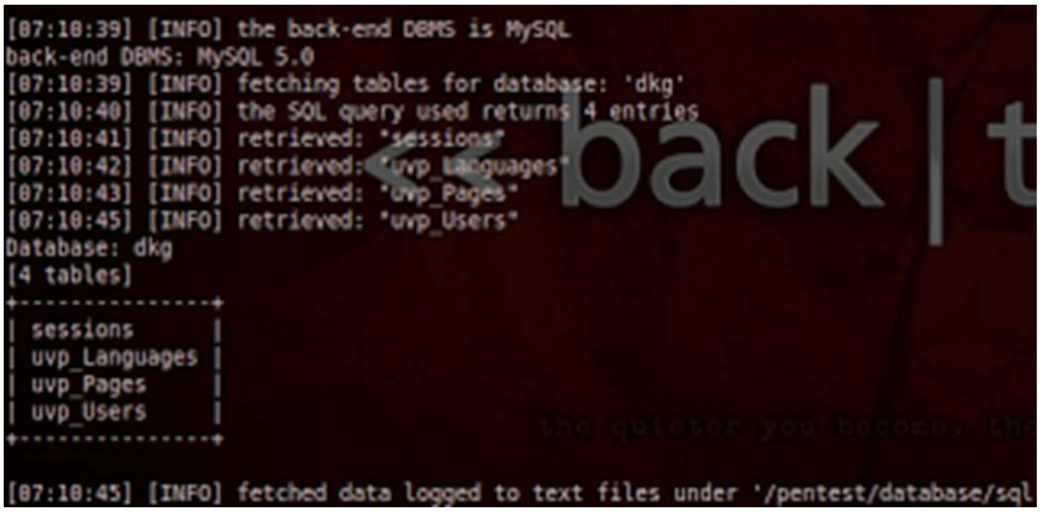


Fig. 8. Backtrack and Sqlmap short location
(Source: SqlMap in backtrack OS)

Step 2: Open Sqlmap and type Following Command: python sqlmap.py -u http://www.haramaya.com –dbs.

Step 3: Now Choose Any of The Database From Result. For Example: in this case dkg. Type the Following Command: python sqlmap.py -u http://www.vulnerablewebsite.com -D dkg –tables.



```
[07:10:39] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 5.0
[07:10:39] [INFO] fetching tables for database: 'dkg'
[07:10:40] [INFO] the SQL query used returns 4 entries
[07:10:41] [INFO] retrieved: "sessions"
[07:10:42] [INFO] retrieved: "uvp_Languages"
[07:10:43] [INFO] retrieved: "uvp_Pages"
[07:10:45] [INFO] retrieved: "uvp_Users"
Database: dkg
[4 tables]
+---------------+
| sessions      |
| uvp_Languages |
| uvp_Pages     |
| uvp_Users     |
+---------------+

[07:10:45] [INFO] fetched data logged to text files under '/pentest/database/sql
```

Fig. 9. Sql map interface retrieving web database password
(Source: SqlMap in backtrack OS)

Step 4: Now we have got tables of database. Choose any of the table from the result for getting information from it. hacker's need username and password to login the victim site. So, in this case. the attacker should choose uvp_users table. It may contain information about the users of website. It maybe username, password in this table.

Step 5: After finishing the cracking process, the username and password of the database will reveal. The attacker can then change the content of the database and web sql injection has been successfully implemented.

4. STUDENT ACCEPTANCE

To evaluate the effectiveness of Virtualization technology in teaching Information Security and Assurance, a self-administered survey questionnaire was conducted towards 85 students who take the Information Security and Assurance course in Semester II Academic Year 2014/2015. These groups of students are taking Bachelor in Science in Information Technology program.

From Table 1, it implies that 93% of the students are not familiar with Virtualization technology while only 7% of them are familiar in using this technology. In addition, the survey shows that after the students are introduced to the activity in the laboratory using virtual machine in simulating topics in information security, there is 83% increase in number of student having a very good understanding in the subject. Moreover, the table shows us that 90% of the student agrees that the hands on activity using VM really increase their interesting learning the course. These show that the implementation of hands on activity with VM really helps the student to have better understanding in the subject matter.

Table 1. Familiarity and understanding of virtualization technology in information security course

S. no	Variables	Category of variables	Frequency	Percentage
	Virtualization orientation (before)	Familiar Not familiar Total	6 79 85	7% 93% 100.0%
	Virtualization understanding (after)	Increase understanding	77	90%
		Unable to understand Total	8 85	10% 100.0%

5. CONCLUSION

Teaching courses and simulating it in the lab is very challenging to any teaching professional in a University. Especially if there are factors that serves as barrier in putting it in place like physical space, budgetary constraints, conflicting needs of different courses, rapid obsolescence of computing technology so as treats to internal network security. This research had tried to eliminate these barriers by introducing a mechanisms and innovative teaching strategy to utilize existing facilities and introduce the virtualization technology. Using a virtual machine like VM Ware, configure with the different lab setup using tools like backtrack and its necessary software, the researcher were able to simulate different information security topics and activity. Virtualization technology is not only limited to industry utilizing them to improve their servers and network services, but also has been effective in the laboratory practical session in the academe. Thus, it was found that the students are accepting the challenge to learn virtualization and are benefiting greatly from their experiences.

COMPETING INTERESTS

Author has declared that no competing interests exist.

REFERENCES

1. Glantz EJ. Innovative practices in teaching information sciences and technology. Innovative Practices in Teaching Information Sciences and Technology: Experience Reports and Reflections. 2014;53–62. Available:http://doi.org/10.1007/978-3-319-03656-4
2. Gurgel PHM, Branco LHC, Barbosa EF, Branco KRLJC. Development of a practical computer network course through netkit virtualization tool. Procedia Computer Science. 2013;18:2583–2586. Available:http://doi.org/10.1016/j.procs.2013.05.445
3. Fuertes VM, Vergara JEL. A quantitative comparison of virtual network environments based on performance measurements. 14th Workshop of the HP Software University Association, Munique; 2007.
4. Gercek G, Saleem N. Designing a versatile dedicated computing lab to support computer network courses : Insights from a case study physical layout of the lab. Journal of Information Technology Education. 2006;5:1.
5. Webster MR. An innovative faculty toolkit simulation success. Nurse Educator. 2009; 34:148-149
6. Rhodes ML, Curran C. Use of the human patient simulator to teach clinical judgment skills in a baccalaureate nursing program. CIN: Computers, Informatics, Nursing. 2005;23(5):256-262.
7. Lateef F. What's new in emergencies, trauma, and shock? Role of simulation and ultrasound in acute care. Journal of Emerging Trauma. 2008;1:3–5.
8. Lateef F. Simulation-based learning: Just like the real thing. Journal of Emerging Trauma Shock. 2010;1:3–5. DOI: 10.4103/0974-2700.70743
9. Jha AK, Duncan BW, Bates DW. Simulator based training and patient safety in: Making health care safer: A critical analysis of patient safety practices. Agency for Health care, Research and Quality, US dept of Health and Human Services. 2001;511–8.
10. Agarwal KK, Critcher A, Foley D, Santi R, Sigle J. Setting up a classroom lab. The Journal of Computing in Small Colleges. 2001;16(3):281-286.
11. Belles R, Gorka S, Miller JR. Flexible network topologies for your computing lab: VLAN and router technology at work in the classroom. The Journal of Computing in Small Colleges. 2002;17(3):53–59.
12. Wilson JH. Recipe to lab management or the cookie cutter approach to building labs. Proceedings of the 30th Annual ACM SIGUCCS Conference on User Services, Providence, Rhode Islands. 2002;298-300.
13. Gadelha RNS, Azevedo RR, Oliveira HTA. OS Simulator: Um simulador de sistemas de arquivos para apoiar o ensino/ aprendizagem de sistemas operacionais. In: Proceedings of XXI Education Informatic Brazilian Symposium, João Pessoa, in Portuguese; 2010. Portuguese
14. Barbosa EF, Gurgel M, Regina K, Jaquie L, Branco C, Paulo S. Teaching computer networks: A practical approach using virtualization tools. IEEE; 2013.
15. Yang L. Teaching system and network administration using virtual pc. Journal of the Consortium for Computing Sciences in Colleges; 2007.
16. Damiani E, Frati F, Rebeccani D. The open source virtual lab: a case study; 2004.

17. Chen L, Tao L. Teaching web security using portable virtual labs the development of SWEET. 2012;15:39–46.
18. Zaki MM, Erman H, Azman NA, Faizal MA, Rahayy SS. Virtualization technology in teaching information technology security; 2010
19. Hassell J. Server virtualization: Getting started. Computerworld. 2007;41(22):31-31.
(Accessed 2 March 2016)
Available:http://search.proquest.com/docview/216090475? accountid=27965
20. Ke JK, Yang CH, Ahn TN. Using w3af to achieve automatedpenetration testing by live DVD/live USB. presented at the meeting of the Proceedings of the 2009 International Conference on Hybrid Information Technology, Daejeon, Korea; 2009.
DOI: 10.1145/1644993.1645078
21. Conklin WM, Nestler V, White G. Principles of computer security. McGraw Hill; 2011.
22. Bacudio AG, Yan X, Chu BB, Jones M. An overview of penetration testing. International Journal of Network Security & Its Applications. 2011;3(6):19.
23. Wack J, Tracy M, Souppaya M. Guideline on network security testing. Nist Special Publication. 2003;800:42.
24. Osborne M. How to cheat at managing information security. Scitech Book News. 2016;30:4.
(Accessed on 2 March 2016)
Available:http://ezproxy.aut.ac.nz/login?url=http://search.proquest.com/docview/200176483?accountid=8440
25. Alder V, Burke J, Keefer C, Orebaugh A, Pesce L, Seagren ES. How to cheat at configuring open source security tools. n.d.
26. Lundin Leigh. PINs and passwords, part 2. Passwords. Orlando: SleuthSayers; 2016.
(Accessed 5 March 2016)
Available:http://www.sleuthsayers.org/2013/08/pins-and-passwords-part-2.html
27. Ethical Hacking Central. John the Ripper; 2016.
(Accessed 3 April 2016)
Available: http://ethicalhackingcentral.com/tutorials/john-the-ripper-tutorial/
28. Montoro Massimiliano. Brute-Force Password Cracker. Oxid.it; 2016.
(Accessed 4 April 2016)
Available:http://www.oxid.it/ca_um/topics/brute-force_password_cracker.htm
29. Openwall. John the Ripper Password. Cracker; 2016.
(Accessed 7 April 2016)
Available: http://www.openwall.com/john/
30. Landwehr CE, Bull AR, McDermott JP, Choi WS. A taxonomy of computer program security flaws, with examples; 1993.
31. Solidpass. Trojan Attacks; 2016.
(Accessed in 4 April 2016)
Available:http://www.solidpass.com/threats/trojan-attacks.html
32. Soni A, Jain J, Roshan R. Image steganography using discretefractional Fourier transform. Intelligent Systems and Signal Processing (ISSP). 2013;97:1-3.
33. Akhtar N, Johri P, Khan S. Enhancing the security and quality of LSB based image steganography. Computational Intelligence and Communication Networks (CICN). 2013;385:390.
34. Sans. The ease of steganography and camouflage. Sans Institute; 2002.
35. Patange Tanmay. How to defend yourself against MITM or Man-in-the-middle attack; 2013.
36. Trappe Wade. Introduction to cryptography with coding theory. New York: Pearson; 2005
37. Wireshar. Wireshark FAQ; 2016.
(Accessed 5 April 2016)
Available: www.wireshark.org
38. Acunetix. SQL Injection (SQLi); 2016.
(Accessed 5 April 2016)
Available: http://www.acunetix.com/websitesecurity/sql-injection/
39. Sqlmap. Sql Map Introduction; 2016.
(Accessed 6 March 2016)
Available: http://sqlmap.org/

Peer-review history:
The peer review history for this paper can be accessed here:
http://sciencedomain.org/review-history/15313