Volume-4, Issue-7, July-2015 • ISSN No 2277 - 8160

Research Paper | Engineering

Decentralized Virtual VAPT Laboratory Model

Parag Pravin Shimpi — Student, ME IT (Information Security), Department of Information Technology, K. J. Somaiya College of Engineering, Mumbai, India

Prof Mrs Sangeeta Nagpure — Faculty, Head of Department of Information Technology, K. J. Somaiya College of Engineering, Mumbai, India

ABSTRACT

Offering the students some hands-on experience, as well as the attacker's point of view is a novel approach to teach Information Systems Security. The students will discover how easy it is to exploit unsecured applications. The hands-on security lab assignments will help students to develop and test not only computer networking and security skills, but also much broader skills, such as creative and critical thinking, problem analysis and solving, accuracy and being attentive to details.

The distinctive feature of Decentralized Virtual VAPT Lab model is that it will actively uses highly efficient learning by doing paradigm of education and a 'playground' in which students and lecturers can experiment without fear of corrupting or attacking the network of the college without any additional cost.

KEYWORDS : Information Security, Penetration Testing, Virtualization, Laboratory

1. INTRODUCTION

"I hear and I forget. I see and I remember. I do and I understand." This famous saying of Confucius has been a motto for many educators, who firmly believe that learning must be grounded in experience [14]. The importance of practical work in science and engineering, supported by lab exercises, is widely known. It is well-known that factual knowledge is of little use without the ability to synthesize the information and demonstrate, through active problem solving, that one can apply the knowledge to real world problems. The traditional approach for such labs has been to set up physical infrastructure in which to build the labs. However, this kind of configuration typically requires a large monetary investment and is hampered by rapid technological obsolescence, time-consuming maintenance tasks, and limits on physical space. These constraints can make it difficult, if not impossible, for a majority of faculty to offer relevant laboratory exercises [20].

The most efficient approach to prevent security incidents is to attempt the same actions an attacker would try, and re-configure the security settings accordingly. This process is also known as penetration testing or ethical hacking. From the educational perspective, penetration testing is an activity composed from a set of complex skills combined with an extensive amount of domain-related conceptual knowledge, and is therefore most successfully mastered through learning sessions and practice [19]. Hence, teaching ethical hacking techniques is becoming a necessary component of computer security curriculum as it yields better security professionals than other curriculums teaching defensive techniques alone [17].

With the recent advances in technology, it has become possible to transform much of the computing infrastructure, as well as some computational engineering lab infrastructure, into a virtual environment, not only to avoid the pitfalls of the physical approach, but also to introduce a significant new development into the curriculum [20]. In this work, a virtualized infrastructure is designed to introduce an affordable implementation of a new paradigm in computing that facilitates an enhanced classroom experience with more hands-on, exciting, and relevant lab exercises [20].

2. LITERATURE REVIEW

The Tele-Lab project offers a system for hands-on IT security training in a remote virtual lab environment – on the web, accessible by everyone [2]. Also, The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) is a software engineering lab at the University of Idaho. RADICL allows virtual partitioning so disparate experiments and exercises can be run concurrently [4].

The Virtualization, Cloud, and Storage Technology Learning Environment (VCASTLE) platform at ECPI University offers network security, virtualization, and storage labs to inset and online students in Computer and Information Systems (CIS) programs. While a security lab at WMU is composed of desktops. Each desktop runs up to three virtual machines [8].

V-isoNet has enabled Dublin Institute of Technology to encourage student's innovation by giving the student the ability to in effect do or try 'anything' without consequences. It allows students to use their own laptops by installing openVPN client [10]. Similarly, LOST project developed by 'La Salle - Ramon Llull University' in collaboration with ISECOM, is an eLearning environment that helps security trainers to teach hands-on technological knowledge on security testing and auditing and engages students in the security world from the Ethical Hacking perspective [12]. SEED labs have also covered a spectrum of security topics like vulnerabilities, attacks, software security, system security, network security, Web security, access control, authentication, cryptography [14].

3. LABORATORY ARCHITECTURE DESIGN ANALYSIS

There are two main options regarding the laboratory that can be used for the training: It can be either real, or virtual.

1. Real (Physical) Lab
2. Virtual Lab

a. Centralized (Remote) Labs

b. De-centralized (Proposed) Lab Model

3.1. Traditional Physical Lab

One approach can be implementing real laboratories by using the available facilities and equipment. Nevertheless, such an approach will most probably require a reconfiguration of the existing equipment may cause disorders in the network's normal operation and may pose significant dangers when there is unrestricted operation of certain tools (e.g. sniffers) [3].

The second option is to use a dedicated lab that will be cut-off from the rest of the network. This will enable the easy restoration of its normal operation and will also prevent various security issues from affecting other parts of the network. The obvious drawback is the increased cost for obtaining the required equipment and the need for dedicated space within the facility. Moreover, students may need to invest a substantial amount of time in reading manuals, trying to figure out how to do certain things, which will certainly cause some disorientation and confusion regarding the aims and objectives of the

training [3]. Such labs are exposed to a number of drawbacks: they are immobile, expensive to purchase and maintain. Of course, students are not allowed to have Internet access on the lab computers. Hands-on exercises on network security topics even demand to provide more than one machine to each student, which have to be interconnected one being the one to be protected, and one being the 'external' one that implements an attacker. (E.g. a Man-in-the-Middle attack needs three computers: one for the attacker and two other machines as victims) [2].

As most of the tools in the lab course, such as IP filters, intrusion detection systems and the like, change machine configurations, machines cannot be shared between students although the machines run the multi-user operating system Linux. Also, the large number of machines not only has to be provided but also actively maintained. If a student, working with administrator rights, misconfigures some tool, he may destroy the whole machine configuration, so that it is necessary to get the system back in a stable state. This is difficult and sometimes impossible, as the only solution may be to install the new operating system. This can be is frustrating sometimes [1].

3.2. Centralized Remote Lab

In this approach, virtual laboratories can be accessed through a web browser, thus eliminating the need for set-up and maintenance. It does not require any hardware or physical space (apart from the host server) [3]. This advanced technology can be effective because it allows offering to students anywhere (as long as they have an Internet access) diverse lab setups [8]. Students log into the lab portal from a web browser, and schedule accesses to their own equipment topologies. Configurations defined by students are saved in a persistent environment. Remote and anytime access to labs maximizes the college's investment in equipment and software [8].

In this traditional model of centralized remote labs, physical machines and other physical equipment are needed for student's use. The computers in the lab are connected to concentrator/server. Remote users (students) connect to the server through Internet to conduct lab exercises. This setup has the following disadvantages:

- The centralized server is expensive as it requires very high processing power.
- The cost of maintaining this server can be very high.
- Remote access to these labs, even using broadband Internet connection, can be slow and unstable sometimes.
- The students are assigned certain lab time slots, or must use a scheduling system to reserve the lab time [9].

Although a powerful server is employed to host the virtual machines, the large number of participants prevents the students from all being active simultaneously, as the server can only run a restricted number of virtual machines simultaneously without being annoyingly slow [1].

4. DECENTRALIZED VIRTUAL VAPT LABORATORY MODEL

A proposed Decentralized Virtual VAPT lab model will be based upon an 'Isolated Virtual LAN of at least two to three machines'. This teaching laboratory model builds on the previously discussed methods of teaching and also adds unique elements that help build a teaching environment that approaches a real-world, hands-on laboratory that is both fun and inspiring to students [6].

To satisfy these teaching and technical requirements a computing environment can be devised to allow student the freedom to interact within a networked environment and to isolate this environment from the rest of the institute's actual network, therefore avoiding any issues regarding the compromising of the institute's back-bone network. The approach is decided to implement this isolated network to leverage the utilization of virtualization technologies to the utmost [10].

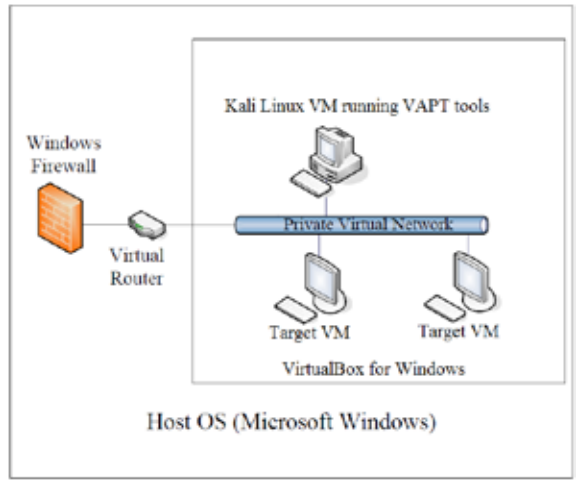

Fig.1 Decentralized Virtual VAPT Lab Model

In the decentralized virtual lab approach, pre-configured virtual machines and other lab materials can be prepared by the instructor and distributed to the students. The students then install the virtual machines on their computers and complete hands-on exercises using the virtual machines [9]. The students can install Virtual box and use it to run one or more virtual machines. The Virtual box virtual router acts as the DHCP server and the NAT gateway for the private virtual network. One virtual machine works as the server (target). The host machine or another virtual machine (preferably Kali Linux) can be used as the attacker [9]. This setup was closer to the configuration in the real world [9].

4.1. Concept of Virtualization

This lab model utilizes the virtualization technology to configure a computing environment needed for the hands-on laboratory exercises. The virtualization of a computer means to run emulator software on a computer (host computer or physical computer) to emulate another desired computer (virtual computer). The host computer and the virtual computer can run the same or different operating systems.

For users, a virtual computer looks just like an additional window on their computer desktop and functions like another physical computer. Users can switch back and forth between the virtual computer and the host computer. The host computer and the virtual computer can share both data and Internet access. Users can also conduct the same computing tasks, such as installing new software, on the virtual computer as if they would do on the host [18]. This lab model is developed on virtual computers using Virtual box but the virtual computers can be imported to other emulators if needed. In this project, a virtual computer can be implemented by a folder of 2-8 GB files and is based on Ubuntu Linux or Windows and can be run on top of any OS like Mac OS, Windows or Linux [18].

4.2. Virtualization Advantages over Traditional Lab Models

Virtualization technology enables multiple virtual machines and their applications to run simultaneously on a single physical computer. This eliminates the need to have multiple physical machines host diverse operating systems typically deployed in security labs. In preparation for this lab model, preconfigured virtual machines can be created for student's use. These virtual machines can also be installed by the students on their personal computers at home and used to conduct lab exercises. The virtual lab approach is different from the centralized remote laboratory because students run the lab on their own computers and do not depend on the remote servers. Additionally, the virtual environments allow rapid changes to be made to the lab exercises or environments thus allowing instruction with up-to-date technologies. Furthermore, the burden of maintaining centralized physical labs has been lifted from the institution's shoulders [9].

In the development of lab model, re-configurability is important. Virtual machines can be halted and saved, freeing machines for other uses, and quickly redeployed later. This rapid re-configurability allows

many students to use multiple virtual machines simultaneously and without interference. In this way lab maximizes machine use by minimizing the monopolization of hardware. In less than five minutes, this can make the transition from completely switched off machines, to fully configured and ready to run: The network is live, interfaces are up, and virtual machines can communicate. All of this is done with the click of a mouse [4].

Virtualization technology suits the purposes from two aspects. Firstly, virtualization allows the ad-hoc addition of virtual machines to the isolated network. Secondly and purely from a public relations aspect, having the 'playground' network physically limited to one machine adds to the level of trust. In other words Academic and Technical staff and students will have a greater perceived confidence in the isolated aspect of this security 'playground' as it is only located on one piece of hardware [10].

4.3. Actual design

To achieve our design goals, two types of OS can be run in the VAPT lab model environment as open source Linux and closed source Windows. It can be used primarily for exploration type labs, in which students play with a security system to learn how things work and how security breaches can occur. Students will create 'virtual computers' (guest computers) within a physical computer (host computer). The guest computers and the host computer can also form virtual networks. All of this can be accomplished using a hosted hypervisor called as virtual machine software, such as Virtual box, Xen, VMware or Virtual PC [16].

A hosted hypervisor is a software program that runs within an operating system environment and the guest or virtual machine is run at a third level above the hardware. This configuration will allow creating an entire individual and separate network for each student. This will allow students to run not just their own VM but a number of VM's to create their own individual network. This will allow the students to see interactions on both sides (Attacker System and Target System) [10]. Figure 2 shows the actual architectural design of decentralized virtual VAPT lab model.

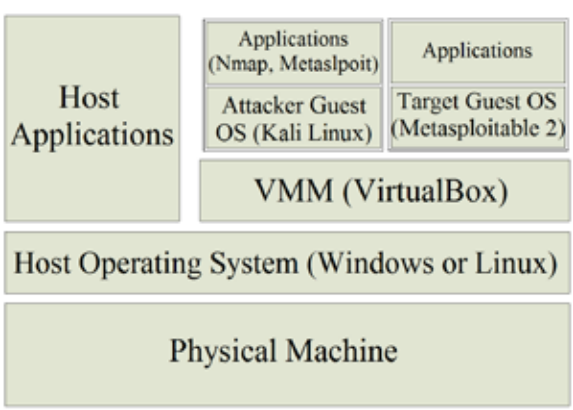

Fig.2 Actual Architecture of Decentralized Virtual VAPT Laboratory Model

Virtual box is selected over other virtualization products for three main reasons:

1. Virtual box can be installed under Windows or Linux operating systems, which are used by most of the people. The students can continue using their existing operating systems and applications without interruptions.
2. Virtual box is free and open source product. Thus no need to invest money.
3. Virtual box supports enough guest operating systems. Virtual box virtual machines were capable of running guest operating systems including DOS, Windows, many distributions of Linux, FreeBSD and Solaris. It was possible to emulate a diversified network environment using Virtual box virtual machines.
4. Virtual box is stable and user-friendly [9].

4.4. Virtual Machines

Now the task is to set up an attacker system and target system (vulnerable server) and be able to hack it. A server from scratch can be installed or a vulnerable software or application can be obtained and installed, or any vulnerable server available on the Internet can be downloaded and installed. Virtualization is again a great paradigm for this process because students can work on their vulnerable server using their own computer or laptop, without the need to have remote access to the test bed. Once the vulnerable virtual server is installed and up, it is ready to the assigned scenario of exercise [12].

4.4.1. Vulnerable Server (Metasploitable 2):

There are many vulnerable servers available on internet. They are open source and free to use. Metasploitable 2, Web for pentesters, Web goat, Game over, etc. Metasploitable 2 can be used for many of the VAPT exercises. The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. Version 2 of this virtual machine is available for download and ships with even more vulnerabilities. This virtual machine is compatible with VMware, Virtual Box, and other common virtualization platforms. It is designed for training, exploit testing, and general target practice. Unlike other vulnerable virtual machines, Metasploitable 2 focuses on vulnerabilities at the operating system and network services layer instead of custom, vulnerable applications. It is a great way to practice exploiting vulnerabilities that might be found in a production environment. Also, Metasploitable 2 has deliberately vulnerable web applications pre-installed. The web server starts automatically when Metasploitable 2 is booted. It contains the vulnerable web applications like mutillidae (NOWASP Mutillidae 2.1.19), dvwa (Damn Vulnerable Web Application), phpMyAdmin, tikiwiki (TWiki), tikiwiki-old, dav (WebDav).

4.4.2. Attacker System (Kali Linux):

Kali Linux is the Operating system that is dedicatedly made for hackers by the Offensive Security organization of Israel hackers. Kali Linux is a hacker's dream come true. The entire distribution is built from the ground up for penetration testers. The distribution comes preloaded with hundreds of security tools that are installed, configured, and ready to be used. Best of all, Kali Linux is free! It is nothing but the rebirth of Backtrack Linux. Backtrack Linux was the old distribution of Kali Linux in which many tools were out-dated [21].

Kali Linux machine has the latest tools required for penetration testing. Kali Linux itself includes information gathering tools, web crawlers, database analysis tools, tools for network mapping and operating system fingerprinting, vulnerability assessment and exploitation tools, as well as password cracking tools. Kali Linux also comes with Armitage—a front-end for the Metasploit penetration testing software. Nmap is the best known network mapping tool for scanning ports and determining the version of the operating system and applications running on the target computer.

4.5. Lab Exercises

Figure 3 shows the list of 40 Lab Exercises for Decentralized Virtual VAPT Laboratory.

Lab Exercises

1. Getting started with VAPT
2. VAPT fundamentals
3. Kali Linux command line
4. Reconnaissance
5. Fingerprinting using NMAP
6. Footprinting using WHOIS
7. Footprinting using DNS info
8. Google hacking
9. Social engineering using SEToolkit
10. Traffic capturing using Wireshark
11. ARP cache poisoning with IP forwarding
12. ARP cache poisoning to impersonate default gateway
13. Vulnerability discovery using Nessus
14. FTP anonymous login issue and smiley face attack
15. Netcat – A swiss army knife
16. Exploitation using Metasploit
17. Metasploiting the target
18. Exploiting Windows XP using Metasploit
19. Metasploit MSFCLI
20. Accessing Windows system by executable file in Metasploit
21. Metasploit Meterpreter
22. Bypassing antivirus using MSFVenom
23. Encoders to bypass antivirus
24. Custom cross compiling for antivirus evasion
25. Web based exploitation
26. SQL injection attack
27. Manual SQL injection
28. SQL injection using SQLMAP
29. Cross site scripting
30. XSS using BeEF
31. Password wordlist creation using ceWL and Crunch
32. Online password attack using Hydra
33. Offline password attack
34. Wireless hacking fundamentals
35. Cracking WEP access point
36. Cracking WPA / WPA2 access point
37. Blocking Wi-Fi access point
38. Study of OpenSSL heartbleed vulnerability
39. Study of Shellshock Bash injection vulnerability
40. Study of POODLE vulnerability

Fig.3 Lab Exercises

5. EXPECTED RESULTS

The advantages of using virtual machines emphasize their flexibility. It allows multiple operating systems to coexist on a single physical machine. It provides an insulated environment so that failure in one machine does not affect another. Network traffic or attacks generated within the virtual network have no impact on the public network. For instance, malware samples can be executed and studied inside the virtual machines. The malware-related traffic can be contained and captured inside the private network. After the work is done, the infected virtual machine(s) can be deleted and replaced with fresh virtual machine(s) fairly quickly. Isolated network will allow students and lecturers to interact without fear of compromising a production network. Because students could also access the web while still being isolated, it was possible to utilize traffic monitoring tools.

With VMs acting as the client, the virtual lab becomes more portable. Although the students can still use the host machine as the client, it is no longer required. If a student's computer is temporarily out of service, she/he can install the virtual box on her/his laptop or home computer if there was one. The student can also go to on-campus computer lab, launch Virtual box, and open the prebuilt virtual machines and perform the labs. There is no need to install any program on the host machine, which is not allowed in most student computer labs. The hands-on learning of Decentralized Virtual VAPT lab model is focused on proposed designed and developed learning framework for many types of computer attacks. This proposed Decentralized Virtual VAPT lab model will have many advantages.

Merits of learning framework:

- Analysis of relevant vulnerabilities in software/Web systems
- An overview of computer attack
- Demonstration of an attack in real time in lab environment
- Step-by-step procedure
- Software implementation of an attack
- Prevention of an attack and defense mechanisms
- Advanced types of an attack
- Relevant hands-on exercises

Also, it will provide students with a set of following advantages:

1. Deeper understanding of the subject.
2. Much better retention factor: The retention factor of learning by doing paradigm of education is higher than 80-85%.
3. Promotion of critical thinking.
4. Getting a 'feeling' and own experience.
5. Financial benefit: As this lab model is based on open source tools and techniques. There is no burden on college regarding the buying any new thing. Thus students can learn in the college itself. There is no need to go to private institutes to learn hands-on practical and spend high amount.

The premise is that the proposed learning framework will provide students with deep knowledge and excellent technical hands-on skills for each type of computer attack discussed in a class, and will prepare students to deal with advanced computer attacks in real-world environment. Thus, students can experience the benefit of starting from identical setups, the ability to reset their machines when something goes wrong, the freedom from outside interference, and the ability to use greater numbers of machines for exercises. They also get the further benefit of being able to actually do all the work on their own, which is not always possible in a physical lab.

6. CONCLUSION

This project is conceived out of a practical requirement, therefore requiring a practical solution. The benefit of this practicality is that tangible or actual implementation can be expected as a result of the research. Essentially for students, a practical demonstration of attacks and vulnerabilities is of benefit to help to reinforce and extend concepts conveyed in lectures. And a 'playground' in which students and lecturers can experiment without fear of corrupting or attacking the production network of the college.

REFERENCES

1. Jorg Keller, Ralf Naues, "A Collaborative Virtual Computer Security Lab", Proceedings of the Second IEEE International Conference on e-Science and Grid Computing (e-Science'06) 0-7695-2734-5/06 © 2006 IEEE | | 2. Christian Willems, Thomas Klingbeil, Lukas Radvilavicius, Antanas Cenys, Christoph Meinel, "A Distributed Virtual Laboratory Architecture for Cybersecurity Training", 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates, 978-1-908320-00-1/11/ © 2011 IEEE | | 3. Alexandros Papanikolaou, Vassilios Karakoidas, Vasileios Vlachos, Andreas Venieris, Christos Ilioudis, Georgios Zouganelis, "A Hacker's Perspective on Educating Future Security Experts", 2011 Panhellenic Conference on Informatics, 978-0-7695-4389-5/11 © 2011 IEEE | | 4. Kyle King, David Manz, Paul Ortman, Doug Shikashio, and Paul Oman, "A Rapidly Reconfigurable Computer Lab for Software Engineering Security Experiments and Exercises", Proceedings of the 19th Conference on Software Engineering Education and Training Workshops (CSEETW'06) 0-7695-2647-0/06 © 2006 IEEE | | 5. Prof. Siddeeq Y. Ameen, Ibraim M. Ahmed, "Design and Implementation of E-Laboratory for Information Security Training", 2013 Fourth International Conference on e-Learning "Best Practices in Management, Design and Development of e-Courses: Standards of Excellence and Creativity", 978-0-7695-5036-7/13 © 2013 IEEE | | 6. Randal T. Abler, Didier Contis, Julian B. Grizzard, Henry L. Owen, "Georgia Tech Information Security Center Hands-On Network Security Laboratory", IEEE TRANSACTIONS ON EDUCATION, VOL. 49, NO.1, FEBRUARY 2006, 0018-9359 © 2006 IEEE | | 7. Dr. Alexander V. Uskov, "Hands-On Teaching of Software and Web Applications Security", Interdisciplinary Engineering Design Education Conference, 978-1-4673-5112-6/13 ©2013 IEEE | | 8. Lotfi ben Othmane, Vijay Bhuse, Leszek T. Lilien, "Incorporating Lab Experience into Computer Security Courses", 978-1-4799-0462-4/13/$31.00 ©2013 IEEE | | 9. Peng Li, Tijjani Mohammed, "Integration of Virtualization Technology into Network Security Laboratory", 38th ASEE/IEEE Frontiers in Education Conference NY, 978-1-4244-1970-8/08 ©2008 IEEE | | 10. Michael Gleeson, David Markey, Dr. Fred Mtenzi, "Investigation and Development of a Security and Forensic Analysis Teaching Environment", 978-1-4244-4615-5/09 © 2009 IEEE | | 11. Marco Anisetti, Valerio Bellandi, Alberto Colombo, Marco Cremonini, Ernesto Damiani Fulvio Frati, Joël T. Hounsou, Davide Rebeccani, "Learning Computer Networking on Open Paravirtual Laboratories", IEEE TRANSACTIONS ON EDUCATION, VOL. 50, NO. 4, NOVEMBER 2007, 0018-9359 © 2007 IEEE | | 12. Jaume Abella, Guiomar Corral, Agustin Zaballos, "LOST Project, a Learning platfOrm for Security Training", Computers in Education (SIIE), 2012 International Symposium Andorra la Vella, 978-1-4673-4743-3 © 2012 IEEE | | 13. Kai Qian, Chia-Tien Dan Lo, Minzhe Guo, Prabir Bhattacharya, Li Yang, "Mobile Security Labware with Smart Devices for Cybersecurity Education", Integrated STEM Education Conference NJ, 978-1-4673-1097-0 ©2012 IEEE | | 14. Wenliang Du, "SEED: Hands-On Lab Exercises for Computer Security Education", Security & Privacy, IEEE (Volume: 9 , Issue: 5 , 1540-7993/11 © 2011 IEEE | | 15. Dr. Alexander V. Uskov, "Software and Web Application Security: State of the Art Courseware and Learning Paradigm", 2013 IEEE Global Engineering Education Conference (EDUCON) Berlin, Germany, 978-1-4673-6110-1/13 ©2013 IEEE | | 16. Dong Hu, YuYan Wang, "Teaching Computer Security using Xen in a Virtual Environment", 2008 International Conference on Information Security and Assurance, 978-0-7695-3126-7/08 © 2008 IEEE | | 17. Zouheir Trabelsi and Walid Ibrahim, "Teaching Ethical Hacking in Information Security Curriculum: A Case Study", 2013 IEEE Global Engineering Education Conference (EDUCON) Berlin, Germany, 978-1-4673-6110-1/13 ©2013 IEEE | | 18. Li-Chiou Chen, Lixin Tao, "Teaching Web Security using Portable Virtual Labs", 2011 11th IEEE International Conference on Advanced Learning Technologies, 978-0-7695-4346-8/11 $26.00 © 2011 IEEE | | 19. Kristian Skracic, Juraj Petrovic, Predrag Pale, Dijana Tralic, "Virtual wireless penetration testing laboratory model", 56th International Symposium ELMAR-2014, 10-12 September 2014, Zadar, Croatia, 10.1109/ELMAR.2014.6923370 © 2014 IEEE | | 20. Evrim Guler, Suleyman Uludag, Murat Karakus, Stephen W. Turner, "Virtualized Lab Infrastructure on a Budget for Various Computing and Engineering Courses", 978-1-4673-2334-5/12 ©2012 IEEE | | 21. Parag Shimpi, Sangeeta Nagpure, "Penetration Testing: An Ethical Way of Hacking", Global Journal For Research Analysis, 10.15373/22778160 | | 22. paragtailor.wix.com/infosec |