RCEE & RHEd2010
Kuching,Sarawak
7 – 9 June 2010

# Virtualization Technology in Teaching Information Technology Security

Mohd Zaki M, Erman H., Nor Azman M. A., Mohd Faizal A. , Siti Rahayu S
*Faculty of Information and Communication Technology*
*Univeristi Teknikal Malaysia,*
*Karung Berkunci 1200,*
*75450 Ayer Keroh, Melaka.*

*{ zaki.masud, , erman, nazman, faizal.abdollah, sitirahayu }@utem.edu.my*

**Abstract**- The effective way to educate students on using technologies is through hands-on experience. Learning a subject by hands-on experience can synchronize their head and hands, making the subject matter easier to be absorbed as well as stimulating the mind of the students to be more creative and innovative. In teaching Information Technology Security, exposing the student to real-time scenario of threat and safeguarding network resources expose the student to the real danger of exploitation and the devastating effect of security breach on network infrastructure. Unfortunately this requires a huge amount of time and cost for preparing and setting up the equipment and software for the practical session. Moreover, most of the activity in a security subject can also jeopardize other devices in the real network, for instance simulating a worm attack or hijacking server attack might affect the whole network of the campus. Thus, 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. In order to alleviate this problem, this paper 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.

***Keywords-Virtual machine, Network Security, Information technology security, Laboratory***

## 1. Introduction

Information Technology (IT) Security is one of the important fields in the science and technology area especially with the current development in information and communication technology. The rapid growth of the Internet usage in the recent years, has make people nowadays more depending on the technology to help them with their daily task. Unfortunately, majority of the user does not realize how easy their information can be exposed if certain precaution is not taken to secure them. This is where subject like Information Technology Security is important where its expose user in particular on the knowledge of threat and method of safeguarding their network resources. The IT security subject contains the methods and challenges in achieving confidentiality, availability and integrity in information technology security. Every aspect of information technology security is being reviewed in this subject, including physical security, software security, database security, network security, cyber law and computer ethic. In understanding the subject there is needs to provide the students with hands on activity that give them the real experience on threat and vulnerabilities found in information technology. The activities include exploiting and safeguarding the vulnerabilities that exist in the information technology.

The hands-on activity can be done by implementing real time scenario on penetrating a machine and implementing the right safeguard method on the machine in order to prevent any exploitation that could jeopardize the services offered by the server. These activities need to be implemented on a control environment such as security laboratory so that it will not affect the existing IT resources but due to frequent exploitation activity and safeguarding implementation the security teaching laboratory resources must be maintained every time the hands-on activity is done. The equipment needs to be updated regularly and reset to the default setting for the students to be able to apply the skills they learn in the lecture class in the laboratary session. However, traditional networking labs has limited resources and do not have a flexible configurations. Besides that the equipment is normally shared between the students who take the course and if the session is one after another then this will add an extra burden for the laboratory personnel to set the equipment back to its default setting. Thus there is a need to have a special security teaching laboratory that is flexible to configure, easy to maintain and cost and time effective.

To address this challenge, this paper will present the implementation of Virtualization Technology in Information Technology Security laboratory. The laboratory task is done in a real scenario but using a simulation environment provided by virtualization technology through its virtual machine application. Virtualization technology provides compatibility, isolation, security and inspection to any machine. One of virtualization technology benefit is providing a virtual platform for another operating system (OS) called as guest OS to run on top of a running operating system called a host OS in a single machine [1]. By running two OS on one machine we can solve the limited resources problem and via this, one student can simulate an attack scenario between two machines on a single machine. With a very high processing power and huge amount of memory space in the computer nowadays, the virtual machine is the answer to overcome the said problem. The details of virtualization technology are discussed in section 2.

The rest of the paper is structured as follows, section 2 discusses the background and technologies of virtual machine, section 3 present the implementation of the laboratory activity in VM as well as the student acceptance in the teaching approach, section 4 discuss the conclusion and directions of this work.

## 2. Virtualization Technology

In the early day's software are made based on the hardware or platform it will be installed. One type of software can only be installed on one type of hardware since each type of hardware was specially designed with its own instruction set and developed with its own specific software. As Information technology evolves, users are insisting for a software that is compatible with any hardware, thus software and hardware manufacturer today has consider developing a new computer system to support the user's demand.

The constrain of hardware and software is eliminates by the introduction of virtualization technology, VM enabled a much higher degree of portability and flexibility. Software is now added to a running machine to provide a virtual platform that can give it the appearance of a different platform for another OS to run on it. Virtualization supports an operating system, instruction set, and computational resources which differ from those available on the underlying software. One of the software that provides virtualization is called virtual machine.

Virtual machine (VM) is defined as an efficient and isolated duplicate of a real machine [2]. This environment is created by using Virtual Machine Monitor (VMM) which provides a second layer on a machine for another operating system to run on it. VMM reproduces everything from the CPU instruction to the I/O devices in software of operating system which it run on. Virtualization in VM involves mapping of virtual resources, for example, the register and memory to real hardware resources and it also use the host machine instruction to carry out the actions specified by VMM. This is done by emulating the host hardware. Figure 1 illustrated the VM concept.

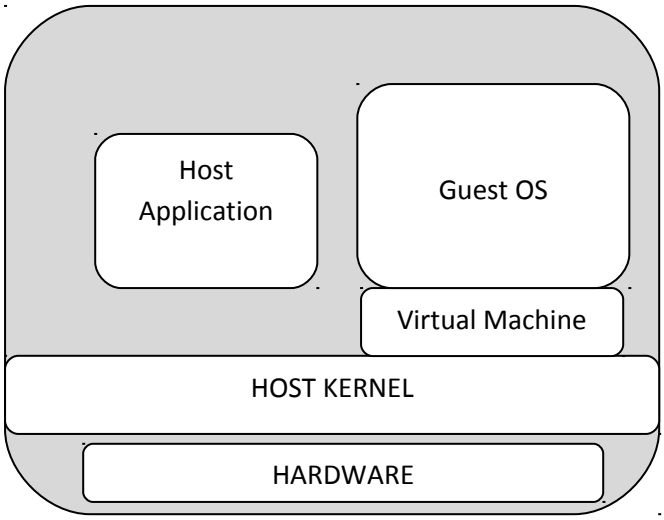


Figure 1. Virtual machine concept

When it was introduced in the 80's users are skeptic on the theory of running an OS on top of the OS, because in theory it will reduce the performance of the processor and the memory of the machine, VM requires a high computing resources and this would be a problem with the old machines which have a low computing resources. However, with the introduction of dual core and quad core processor in the market nowadays this would not be a problem anymore; moreover, today's machine can provide large memory and storage space which have change users to accept VM technology. To date there are many virtual machine solution available for personal computer and Macintosh computer such as VMware [3], Qemu[4], Xen [5], Virtual box[6] and Microsoft Virtual PC 2007.

### 2.1 *VM advantages*

As stated earlier VM is used to let user run more than one OS in a single machine by emulating the underlying hardware thus giving a student chance to create an attack scenario that normally involves more than one machine at one time. Other than that it also eases the teacher and laboratory personnel to do the maintenance. In summary implementing VM in a laboratory activity gives a lot of advantages to the teachers, technician and student, among the advantages are:-

Compatibility: VM let guest OS run on top a host OS without any changes or modification is done on it host OS. Its mean student can simply install a Windows OS on the

host and at the same time install a linux distribution OS on top the VM or vice versa. This shows the compatibility of VM to run on any OS platform and at the same time offering other windows OS or different types of OS on it [7].

Isolation: VM provide strong isolation between the host OS and guest OS, any error or malfunctions on the guest OS will not affect the host OS. This is because VM provides a complete layer of virtual hardware to the guest OS, the guest OS communicate directly to the hardware without going through host OS, thus providing a strong isolation between the host and guest operating system.

Security: among the activity in a security lab session will involved a simulation of virus outbreak, worm, Trojan or might be port scanning for a hacking activity that will affect other computer in the vicinity. By simulating the entire malicious code activity in a virtual environment which is isolated from the real network can prevent a major malicious code outbreak from corrupting other machine.

Ease of management: The management and maintenance of the guest OS will be done by the user who uses the VM, different user will have their own VM and if any problem occurs its only involve one particular user only. In particular, the users are able to restart their machines if they encounter any problem occurs, the snapshots features provided in some of the VM will let user to be backups or even reinstall a clean system image in case of a major miss configuration and these can be done without disturbing the host OS and other VM own by other user. Moreover it will release the teaching staff and laboratory administrators from that duty.

Save cost: Hands on activity for a security lab requires a lot of equipment, for instance an attack scenario might need two or more computers connected via router or switch, thus a high initial cost is needed to provide all the facilities needed in an experiment. VM let you create a Local Area Network within one host by running a multiple VM on top one host which eliminates the need of multiple machines.

Mobility: Once an image disk is created for VM it can be copy and moved to any host that contains VM, this let student who cannot finish their work in the laboratory session can continue the exercise at their own time and any place provided the VM is installed in the machine.

## 3. The Implementation

The following is a set of the security exercise that has been applied in our practical session. The computer has a specification of AMD Phenom 9600B with Quad-Core Processor 2.29 GHz, 2.00 GB RAM and 250 GB hard disk and the host OS is windows XP whereas the virtual machine used is VMware Workstation. VMware workstation is chosen because it is user friendly and easy to use.

### *3.1 Laboratory activity*

The total laboratory activity in IT security subject is 10 and for the initial implementation, the last 5 of the laboratory activities are choose to be using VMware Workstation whereas the first 5 laboratory activities is just a case study scenario on IT security issues. This is done purposely for studying the effectiveness of applying VM in the teaching of IT security. The 5 activities that implement VM in the activity are as follow:-

#### 3.1.1 *Introduction to Virtual machine and Operating system.*

Students are requires to create 4 VM and installed each of the VM with different type of Operating System. The OS installed are windows server 2003, windows XP, Ubuntu [8] and backtrack [9]. This activity is to train the student to be familiar with the VMware workstation. Practices include taking a snapshot of current setting and then delete several file systems to corrupt the OS, restart the OS with the snapshot. Setting a LAN environment among the VM is also done in this exercise.

#### *3.1.2 Port Scanning*

Two VMs is needed; one installed with windows server 2003 and configured to be a server that runs a web server as well as FTP server with the remote connection is enabled. The other VM is installed with backtrack 3 package which will become as the attacker machine. The two VMs are configured to host only network setting which will enable the LAN connectivity between the two VM. Students are then required to investigate the port scanning activity by issuing a NMAP command from the attacker VM. The server side of the VM is installed with Wireshark software to capture the network traffic activities. This will show the students how a scanning activities looks like.

#### 3.1.3 *Securing Files Transfer Protocol, FTP using IPSec*

FTP has be known as an unsecure ways to transfer file because the packet send to connect to server is not encrypted and can seen by using some network monitoring tool like Wireshark. In the exercise the student are required to set an FTP server and a client server connected in LAN environment. From the client server user are asked to login to the ftp server while at the ftp server user will captured the traffic using Wireshark. From the captured packet student can see the login info such as username and password, this prove that FTP is not secure. In order to secure the connection user can enable the IPSec option in

both client and server. Then student can prove the secure connection by repeating the same step in capturing packet for FTP.

#### *3.1.4 Installing Intrusion detection System, IDS*

Snort is an open source Intrusion detection system that is free to use. In this exercise student will used 2 VM that is set to be an attacker and target. The target will be installed with Ubuntu with web server and FTP server enable whereas the attacker VM is installed with backtrack 3 which is a linux distribution focused on penetration testing. Students are asked to installed snort and it rules before enable it a fast detection mode. On the attacker side student are asked to do port scanning activity using NMAP and monitor the alert created by snort in the target VM due to the scanning activity. This exercise provide student in configuring snort as an intrusion detection system.

#### 3.1.5 *Exploiting vulnerabilities in gaining access activity.*

In this activity student will do a hacking activity on exploiting vulnerabilities found on a victim computer. Two VM are needed, one is installed with windows XP service pack 1 and apache web server and another one is using backtrack 3. Both of the VM will be configured with host only network configuration in order to create a LAN environment. Student need to run NMAP in the backtrack 3 to scan the available port offered by the windows XP. Windows XP service pack 1 have vulnerability in its rpc dcom services and by using metasploit in backtrack 3 student gain access to the windows XP and deface the website offered by the apache web server.

### *3.2 Computer Utilization*

The laboratory activity was done to 2 groups of students taking this subject during their first trimester in the second year of their Bachelor of Science Computer (Software Engineering). In term of Computer performances, the implementation of VM does not give a significance effect on the overall performance of the computer table 1 shows the CPU utilization and memory utilization of the host OS during the lab implementation.

Table 1. Computer Performance

| Number Of VM Running | CPU utilization (%) | Memory Utilization (MByte) |
|---|---|---|
| No VM | 2% | 774 |
| One VM | 20% | 1123 |
| Two VM | 30% | 1512 |

From table 1 we can conclude that the CPU utilization only effected during the starting of VM but after the VM running and no activity involved the VM the CPU utilization is back to idle. Whereas the memory utilization is decreasing depending on the number of memory allocated to the VM RAM configuration.

### *3.3 Student Acceptance*

To evaluate the effectiveness of Virtualization technology in teaching IT Security, a voluntary survey study was made towards 78 students who take the IT Security subject for semester 1 session 2009/2010. These groups of students are taking Bachelor in computer science (software engineering). From the survey 74% of the students are not familiar with Virtualization technology. Additionally 94% of the student never used VM in their life and only 21% from them realize the impact of VM in helping them in understanding the subject.

The survey shows that before the introduction of the hands on activity with VM, only 19% of the respondents have a very good understanding on the concept of IT security subject but after the students are introduced to the activity in the laboratory, there is 36% increase in number of student having a very good understanding in the subject. These show that the implementation of hands on activity with VM really helps the student to have better understanding in the subject matter. Moreover, the questionnaire shows us that 90% of the student agrees that the hands on activity using VM really increase their interest in learning the subject.

## 4. Conclusion

According to the result of the survey, the implementation of virtualization technology creates interest among the student to learn this subject. The activities done in the hands-on session shows them how easy to exploit the vulnerabilities found in their system if the security measures are not taken. In term of the machine processing performance there is no much impact, running the VM is the same as running other application software on the machine. Besides that, the implementation also provide an ease of management for the teacher and laboratory personnel as well as cost saving since the lab exercise only requires only one computer installed with one OS and VMware workstation. The implementation of Virtual Machine in teaching Information Technology Security Lab is a success. More over the exercise also help the student to have a real experience of handling network securities issue without having to worries of the effect of their exploitation activity affecting other computer in the network and the mobility factor of the VM can help them in exploring the activity in their own time on different computer with the same computer setup that they have configured in the

Following the successful utilization of VM in our lab activity, in the near future we would like to adopt the same strategies on other Information technology subject such as operating system, system development and others networking subject. As VMware workstation is a protected with user license in our next project we will try open source VM such as QEMU or Virtual Box in our lab implementation.

**References**

[1] Dunlap, G. W., King, S. T., Cinar, S., Basrai, M. A. & Chen, P. M. 2002. ReVirt: Enabling Intrusion Analysis Through Virtual-Machine Logging and Replay. Proceeding of 2002 Symposium on Operating System Design and Implementation.

[2] Popek, G. & Goldberg, R. 1974. Formal Requirements for Virtualizable Third Generation Architectures. Communications of the ACM, 17(7): 412-421.

[3] VMware Inc. 2009. (2009, April 05). VMware Workstation. [Online]. Available : http://www.vmware.com/

[4] Bellard, F. 2009. (2009, January 1). QEMU CPU Emulator. [On-line]. Available: http://fabrice.bellard.free.fr/qemu/

[5] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, 2003, "Xen and the art of virtualization," in Proceedings of the nineteenth ACM symposium on Operating systems principles. pp. 164–177,.

[6] Sun Microsystem., 2009. (2009, April 05). Virtualbox. [Online]. Available: http://www.virtualbox.org/

[7] Garfinkel, T., Paff, B., Chow, J., Rosemblum, M. & Boneh, D. (2003). TERRA: A virtual Machine-Based Platform Trusted Computing. SOSP 2003: 193-205.

[8] Canonical Ltd., 2009 (2009, December 05). Ubuntu [Online]. Available: http://www.ubuntu.com/

[9] BackTrack Linux 2009. (2009, December 05). Backtrack [Online]. Available: http://www.backtrack-linux.org/