A Test Bed for Information Security Skill Development with Virtual Training Environment

Alok Tripathi, Abhinav Mishra
IT Division
DOEACC Society, Gorakhpur Centre
Gorakhpur, India
atripathi@doeaccgkp.edu.in, amishra@doeaccgkp.edu.in

G.V. Raghunathan
HRD Division
Department of Information Technology
New Delhi, India
raghu@mit.gov.in

***Abstract*— New attacks are emerging rapidly in Information Security; hence the tools and technologies available for securing the information needs substantial upgradation as well as skills for operationlization to mitigate these attacks. It requires creation of practical training environment with tools and technologies available for Information Security. The design of Information Security courses involves scenario based hands-on-labs with real time security incidents and problems with global reach which could be customized quickly as per the scenario and user's requirement. In order to understand the underlying concepts as well as to learn the practical aspects of network and system security environment, an initiative has been taken and a Virtual Test-Bed has been developed to meet the above objectives. It is an essential component in Information Security training concept which could be used to perform actual security attacks and remedial measures as well as to test the effectiveness of protection mechanisms and help in handling the security incidents effectively. This paper discusses the development of this test bed for Information Security skill development with virtual training environment using which Information Security concepts, attacks on networks/systems and practical scenarios are simulated for imparting hands on training to participants.**

Keywords- Attacks,Information Security,Test-Bed,Virtual Training Environment,Simulation

I. INTRODUCTION

Need of the Test Bed:

The design of Information Security Courses involves group and role playing activities and scenario based hands-on sessions to achieve the objectives of providing the participants practical training with real time security incidents. Participants require a lab set up with Virtual Training Environment (VTE) to simulate actual security attacks and remedial measures to test the effectiveness of protection or to handle the incidents effectively. The scenarios need to be designed depending on subjects like incident handling, Operating System (OS) hardening, forensics, etc. For each lab session a manual also need to be prepared that includes the context for the topics, network of machines with which the participants interact and step-by-step instructions with screen shots. The Virtual Training facility needs to be established in such a way that participant can attend the lab sessions at convenient time and solve the prescribed lab assignments/exercise using the manual. This way using Virtual Training Environment participants get the opportunity to solve the problems in real networked systems. Establishing Virtual Training Environment (VTE) based set up facility is very helpful to train the system administrators and information security officers who manage the organization networks. The lab consists of various heterogeneous platforms, open source tools, firewalls, intrusion detection system, honey pot, etc which can be accessed by a user from any remote location.

Based on the effectiveness and advantages of such facility, a test-bed with virtual training based environment has been setup which help in creating right kind of manpower equipped with adequate practical expertise in the area of Information security.

II. TECHNOLOGY BEHIND THE TEST BED

Virtual Lab Environment is generally created using the virtualization technology. Virtualization Technology enables one computer to run multiple operating systems simultaneously in simulation mode.

There are various virtualization software packages available from various vendors now a day. For e.g. Virtual Server from Microsoft, VMware ESX Server from VMware Inc., Zen from Citrix. These software packages could be used for simulating Personal Computer (PC) virtual environment. Various operating systems like Windows, Linux can be installed on top of the virtualization software. The operating systems can be configured like normal PC and if accessed from different physical system across networks, it appears to be accessing different systems. This way a local area network (LAN) scenario can be configured using the virtualization technique.

The virtualization software comes with a managerial console which can be used to control and configure the virtual machine. Virtual Machine Remote Control service provides the management of the virtual server from the remote machine, which has remote control client installed on it. The Virtual Environment in the server can be accessed using the web browser from the remote system. Based on one's credentials, the user can choose and access the virtual environment as per the need. Virtual machine network can be configured to access only the virtual machines on the same server. This enables an environment for analyzing malware. In this case, the virtual machine cannot be accessed from the other physical machines. Each Virtual Machine consists of two files—one for keeping configuration details related to the Virtual machine and the other for the Virtual hard disk management. Such a setup is shown in Fig. 1.

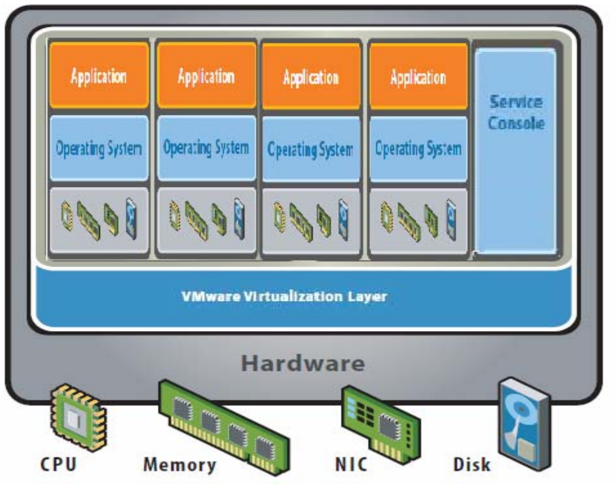

Figure 1. VMware Virtualization Setup

III. DESIGN OF THE TEST BED

A. Design Constraints

The following Design Constraints have been taken in to consideration while designing the required Test Bed.

- The Test Bed should be designed in such a way that it facilitates self paced learning. This implies that users should be able to perform lab modules just by following the instruction given in instructional manual without the help of the instructor.
- Some times the user may require making changes to configuration of the setup. The changes should be such that it should not affect the other users performing the lab hence it implies separate network has to be provided to each of the user to perform lab concurrently.
- Some times the user may do mistake and may crash the environment this means that quick restoring facility to the initial state of the environment should be there.
- The Test Bed should facilitate the user to learn network security design also. For this the network can be collapsed by network attacks and after that it can be quickly be restored to its initial state, so that design could be further tested by making modifications to the initial design.
- The Test-Bed should facilitate the user to learn artifacts analysis for malware. So that the malware can run in an isolated environment provided by the Test-Bed and its actual effect on the environment, in which it is running could be studied so that effective counter measures can be designed against the malware.

B. Selection of Virtualization Software to be used for Test Bed

For setting up the Test-Bed virtualization software is required. The aim of the Test-Bed is to provide a complete lab for Information Security Skill Development. This lab contains a number of different types of operating system and multiple security tools running on them. Therefore the following issues needs to be kept in view for the selection of virtualization software:

Most of the popular operating systems (32 Bit/ 64 Bit) should be supported by the virtualization software. Virtualization software should be robust and must have stability, while running in a production environment. Online Vendor support in the form of online manuals, advisories, telephonic, email should be available for administrating the product as well as API(Application programming Interface) libraries and packages should used for supporting the developmental effort also.

As the test-bed is to be accessed remotely through web browser hence feature in the virtualization software should be that to manage it remotely. The Virtualization software should be hardware independent as far as possible. Special features like Dynamic Resource Management, Live Migration and High Availability should be supported by Virtualization software for expansion of Test Bed in future. The VMware ESX Server 4.0 chosen as virtualization software on the basis of comparison given in Table 1.

TABLE 1: VIRTUALIZATION SERVER COMPARISON

Area of comparison	**VMware ESX Server 4.0**	**Xen Server (4.1)**	**Hyper-V**
Vendor	VMware Inc.	Citrix Systems Inc.	Microsoft Corp.
Primary usage	Production Environment and Testing	Testing & Development Environment	Testing & Development Environment
Required Host OS (if any)	Infra v3:Bare-Metal	Xen: Bare -Metal	Windows 2008 x64
Management tools	Virtual Center	XenCenter Administrator Console	Microsoft Virtual Machine Manager
Supported Guest OS	Almost all are supported	Quite a few are supported like MS 2003 Server, XP, 2K, RHEL (all versions), SUSE& Debian Linux	MS Server 2008 & 2003 and SUSE Enterprise Linux Server 10 SP1 are supported
Performance	Higher Performance More virtual Machines per hardware	Almost as high performance in most for Linux. A bit slower performance for Windows.	Slower Performance Fewer Virtual Machines per hardware

Live Migration (VMotion/ XenMotion)	Supported	Supported	Quick Migration (not real Live migration)
High Availability (HA)	Supported	Not Supported	Quick Migration (Host Clustering)
Dynamic Resources (DRS)	Supported	Not Supported	NLB is a Windows Server 2008 feature
Max. no. of CPUs per Virtual Machine	8 Processors	8 Processors	Depends on Windows Server 2008
Max Memory per Virtual Machine	255GB	32GB	Depends on Windows Server 2008
Max Memory per Host	1 TB	128GB	Depends on Windows Server 2008
Virtualization Approach	Emulation, Paravirtualisation and binary translation	Paravirtualisation	API based
Special Hardware Requirement	Require supported SCSI or SATA controllers.	Require Intel-VT or AMD-V	x64 based processor (Intel VT or AMD-V)

C. *Selection of Operating System for Test Bed*

For Operating Systems selection for the Test Bed following considerations have been taken.

- The popular operating systems which are in common use should be selected as the user community targets common attacks against these operating systems because they are in use.
- Server Side as well as client side operating system must be included.
- One of the selected operating system should be from the open source community, as these are emerging operating systems which are most likely to be used for critical deployment as well as in common use in future.
- The open source security tools available should be supported by the operating system as the test-bed would deploy open source security tools.
- Security exploits are available for the operating system so that they can be demonstrated and countermeasures can be suggested for information security skill development of the user.
- The networking protocol TCP/IP (Transmission Control Protocol/Internet Protocol) should be supported by the operating system.
- Operating system should be stable so that it should not crash while performing labs.

Taking into above considerations following operating systems have been chosen for the Information Security Skill development modules.

- Microsoft Windows XP Professional
- Microsoft Windows Server 2003 Standard edition
- Red Hat Enterprise Linux 4.0

IV. SOFTWARE ARCHITECTURE OF THE TEST BED

The software architecture of the Test bed is shown in Fig. 2. There is a web-Interface designed to access the Test-Bed. There are two modes of login through the web-Interface. In first mode, the user login in to the system with normal user privileges. In this mode of login the user first gets a Dash Board of Modules Developed. From here the user clicks the allotted module and after clicking he gets the virtual Network to perform the module, online manual (by reading which the user can perform the module step-by-step), Chat Module through which the user can chat with the administrator in case of technical problems and online assessment module through which user can access his knowledge after performing the module. The Java RDP (Remote Desktop Protocol) solution is designed to provide the user to access the Virtual Machine behind proxy using SSH (Secure Shell) tunneling. The Virtual Network, the online manuals, chat modules and online assessment modules are tightly integrated in to the system and Graphical User Interface (GUI) is available to access these components.

When the user logins with the administrative rights (which is second mode of login) he gets the User Administration and Module Management module and VM Management module. Through the User Administration and Module Management module, the administrator can perform the Module Allocation, Module Reallocation, and Activating User, Deactivating User and other Module Monitoring and User Monitoring activities.

Through the VM Management module the administrator can perform the administrative tasks and management tasks on virtual machine, inventory available in VMware ESX-4.0.

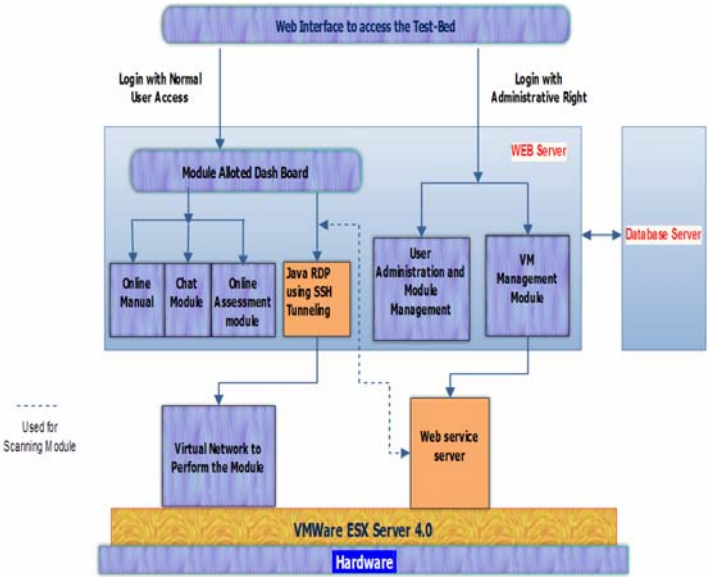
Web Interface to access the Test-Bed
Login with Normal User Access
Login with Administrative Right
WEB Server
Module Alloted Dash Board
Online Manual
Chat Module
Online Assessment module
Java RDP using SSH Tunneling
User Administration and Module Management
VM Management Module
Database Server
Used for Scanning Module
Virtual Network to Perform the Module
Web service server
VMWare ESX Server 4.0
Hardware

Figure 2. Software Architecture of the Test Bed

A. *Description of Software Components of the Test-Bed*

As discussed in software architecture following software components have been developed to support the Test-Bed.

- Web Interface to the Modules
- Central VM Management module.
- Module allocation and User Management modules.
- RDP Solution to access the modules behind the proxy and NAT on client side.
- Online Assessment module
- Chat module

The following is the detailed technical information about the above software components of the Test-Bed.

1) Web Interface to the Modules

a) Language used (front-end) : PHP, Java Script & Ajax

b) Back End Tools : MySQL

c) Lines of Code : 20,000(approx.)

2) Central VM-Management module , Module allocation and User Management module

a) Scripting Language Used : Perl-script and Shell Script

b) Front-End Tool Used : PHP (for Interface)

c) Back-End Tool Used : MySQL

d) Lines of Code : 15,000(approx.)

3) RDP Solution to access the modules behind Proxy on Client Side

a) Language Used for Front-End : PHP (for Interface)

b) Language used for Background : Java Programming

c) Lines of Code : 20,000(approx.)

4) Online Assessment module

a) Language Used : PHP, JavaScript

b) Backend User : MySQL

c) Course Lab IFrame is used for dynamic Interfacing

d) Lines of Code : 1000 (approx)

5) Chat Module

a) Language Used : PHP

b) Back-end : MySQL

c) JSON is used for serialization of data

d) JQuery and JavaScript are also used.

e) Lines of Code : 1000(approx.)

B. *Justifications of Tools used for software components of Module*

- Why PHP is used?

PHP is used as front-end tool to maintain the session state of web pages and for taking input from server side. It is much faster than other scripting languages (like JSP or ASP etc.) because PHP parser is written in 'C' programming language.

- Why MySQL is used?

MySQL is used because database to be handled is not very large and also it is an open source technology. The performance of the system with PHP as front end and MySQL as back-end is far better than other combinations of front-end and back-end used currently.

- Why Java is used?

Java is a cross platform & machine independent language. However it is not faster like C/C++, but it provides more secure solution. So the Java is used for software components discussed above.

- Why VM Perl and Shell Script are used?

VmPerl is an API that can be utilized through the Perl scripting Language. VmPerl API allows one's to write code to simplify the administration and management of the virtual infrastructure in VMware ESX Server. Shell script is used as ESX Server is Linux based hence some times it is easier to automate administrative jobs using shell scripts.

V. NETWORK ARCHITECTURE OF THE TEST BED

The Network Architecture for this Test-Bed is shown in Fig. 3. There is a Server hosting VMWare ESX 4.0 Virtualization software. This ESX 4.0 virtualization software is being used for hosting virtual machines and virtual networks. NAT (Network Address Translation) is used for port mapping to provide online access to the virtual machines. Ethernet switch is used for connecting Virtual Network to the Physical Network. Web Server is used for online access to the Test-Bed from remote locations using Internet. SSH (Secure Shell) server is being used to tunnel the connection with the remote machine for accessing modules behind proxy server and NAT (Network Address Translation). Router with Firewall is being used to protect the virtual Test-Bed from external attacks. The architecture being shown here shows online access of Test-Bed through Internet where user is sitting behind a proxy server.

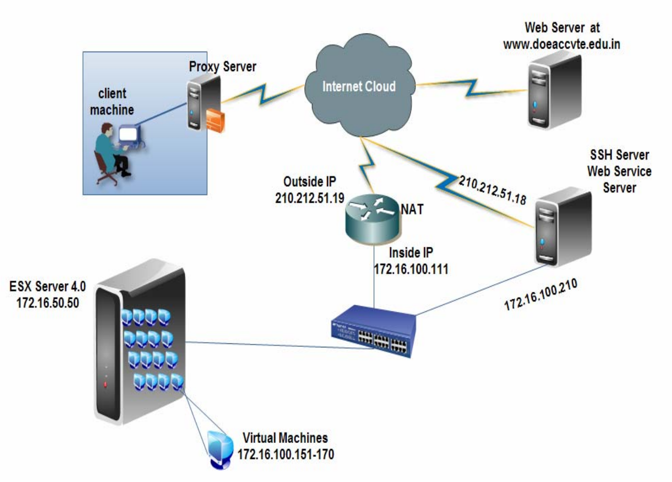

Figure 3. Architecture of the Test Bed.

VI. Detailed Description of the Test-Bed

The module list developed for the Virtual Test Bed is as follows:

Group A (Information Gathering)

- Network Discovery & Scanning
- Target Enumeration
- Vulnerability Assessment

Group B (Ethical Hacking & Countermeasures)

- Sniffing & Countermeasures
- Brute Force Attack & Countermeasures
- IP Spoofing with Denial of Service(DoS) & Countermeasures
- Trojan, Backdoor & Virus & Countermeasures
- Bypassing Proxy & Countermeasures
- SQL Injection Attack & Countermeasures
- Code Injection & Countermeasures
- E-mail Spoofing, Phishing & Countermeasures
- Hacking Wireless Network & Countermeasure

Group C (Hardening, Perimeter Security & Evaluating Security)

- E-mail Security
- Network Traffic Analysis
- Network Traffic Encryption
- Installing & Configuring Intrusion Detection System
- Configuring Host Based Firewall
- Host System Hardening (Windows)
- Host System Hardening (Linux)
- Evaluating Security

So from the module list it is clear that the modules are categorized into three categories. The categorization of the modules is done considering the normal attack scenario in which the attackers first gathers information about the network, then the attack is done. The first two sections teach the user about anatomy of Information Gathering and Ethical Hacking. After learning the anatomy of Information Gathering and Ethical Hacking, in the third section the user learns configuring firewall and Intrusion detection system, Hardening of the System and Evaluating Security to implement protection against attacks.

VII. Conclusion

The Test-Bed for Information Security Skill Development with Virtual Training Environment so developed is being used for imparting hands on training on Information Security to System Administrators, Government Officers and Information Security Professionals. The Test-Bed is being further improved with the users feedback received. As it can be accessed online through web-browser hence this Test-bed is being used for providing Information Security training to participants at remote locations where physical setup of complete Information Security lab is not there. Therefore this Test-Bed is reducing training costs by reducing logistical costs and physical setup cost and users are likely to perform the lab at their convenient time at their preferred locations.

Efforts are on to enhance this Test bed by including the modules on Cyber Forensics also. It is also planned to increase the effectiveness of this Test-Bed further by simulating modules for complex Network Security Design of a real WAN scenario.

Acknowledgment

The authors are thankful to the E-Security Division of DIT (Department of Information Technology, under Ministry of Communications & Information Technology, Government of India) for sponsoring the activity.

References

[1] Old field B "strengthening the security workforce: A competency and functional frame work for Information Technology security professionals", 11th Annual colloquium for Information system security Education, MA:IEEE, 2007.

[2] Conklin A. and G. While, "A Graduate Level Assessment Course: A module for safe vulnerability Assessments", proceedings of the 9th colloquium for Information system security Education, Atlanta GA,2005.

[3] Conklin W.A., "Cyber Defense competitions and Information security Education: An active learning solution for a capstone course", proceedings of the 39th Hawaii International Conference on system sciences, Waikoloa, H A: IEEE,2006.

[4] Information Technology (IT) Security Essential Body of knowledge (EBK): A competency and Functional frame work. Department of Homeland Security National Cyber Security Division working Draft Vo.5 (Pre-Publication draft),2007.

[5] Aboutabl, M.S. " The Cyber Defense Laboratory: A Framework for Information security Education" Information Assurance workshop, IEEE, 2006.

[6] Chris Heien, Ric Massengale Ningning Wu.,"Building a Network Test Bed for Internet Security Research" proceeding Journal of computing science in colleges volume 23, Issue 4 PP 73-79 ISSN: 1937-477, April 2008.

[7] Lincke, S.J. ; Holland, A, "Frontiers in Education Conference Global Engineering: knowledge without Borders, opportunities without passports" , FIE'07, 37th Annual,2007.

[8] Keith A. Morneau, " Designing an Information Security Program as a core competency of network technologists" Proceedings of the 5th conference on Information Technology Education Salt lake city, UT, USA 2004:ACM