

# A Web-based E-Learning Environment for Information Security

Alok Tripathi  
IT Division

DOEACC Society, Gorakhpur Centre  
Gorakhpur, India

Abhinav Mishra  
IT Division

DOEACC Society, Gorakhpur Centre  
Gorakhpur, India

## ABSTRACT

In last decade there is enormous development in the field of E-Learning. Through E-learning computer education can be imparted effectively and efficiently. Information security is an important field in computer education as large number of security attacks are coming into picture. Hence there is need of trained manpower in Information Security to design countermeasures against such type attacks. This paper discusses a web based e-learning environment where participants can learn the anatomy of hack attacks and then learn to design countermeasures against such type of attacks. This web based E-learning in Information Security is being imparted through a scenario based Virtual Training Environment to teach the Information Security concepts to participants by following a practical approach.

## Keywords

E-learning, Information Security, Virtual Training Environment, Attacks

## 1. INTRODUCTION

E-Learning is a rapidly growing field. This has necessitated the development of E-Learning environments. Through E-Learning, education can be imparted in a convenient way. It also reduces the resources and cost required for training. If compared with a traditional learning environment there is greater flexibility with E-learning environments and also it provides user oriented learning where more user interaction is involved. In E-Learning all the resources are provided to students through internet and students can learn any time any where.

Researches and Educators have been proposing lots of innovative designs for the development of E-Learning environments. The focus of these designs is to improve the quality of learning and provide personalization and convenience to users. Every researcher, educator believes that there should be major difference between the conventional learning and E-Learning.

This Paper discusses about an E-Learning environment for Information Security where users can learn at their own pace. This environment provides a simulated environment through virtual machines where user can perform actual network security attacks and then can learn to design effective countermeasures against such type of attacks. This environment provides a nondestructive type of learning environment where machines or network can be collapsed by performing security attacks and then the networks can be recovered and new countermeasures against security attacks can be implemented and attacks can again be performed to test the effectiveness of countermeasures.

In this environment, learners can improve their Information Security skills through self paced learning by performing scenario based experiments and after that assessing their knowledge through an online assessment test.

This paper is organized as follows; section 2 introduces the related work. The section 3, discusses software architecture of E-learning environment. The section 4 discusses the network architecture of the E-Learning environment. The section 5 lists the modules developed in this E-learning environment. In Section 6 evaluation of results of the proposed design has been done. The section 7 gives the conclusion and possible future work.

## 2. RELATED WORK

Sandy Britain et al [1] have introduced the viable systems Model (VSM) and have shown how the model can be adapted for use in an educational context. One of the most important factors in their study is that students should have the capacity to organize themselves so that all the study is not solely tutored.

Another important feature that emerges from their analysis is that students should be able to contribute their own resources and materials to the group. This means that the responsibility for the shaping of learning content shifts from the tutor to the students. The third key feature of their discussion is that it should be easy to continuously adapt and individualize the structures, content and activities it contains as the course progress. In their solution it should be possible to archive completed learning activities for future reuse.

Sevgiozkam et al [2] have attempted to propose an E-Learning evaluation model comprising a collective set of measures associated with an E-learning System. The research in this paper sought to empirically test the constructs of this proposed conceptual model via a survey instrument and to demonstrate which were critical for e-learning systems effectiveness, particularly when implementing a Computer Education course. This study contributes to the E-learning literature with an instrument providing a roadmap for practitioners and researchers to better understand how E-learner's perceived satisfaction can be increased and how the use of Learning Management System can be improved.

Weiltu et al [3] have shown that E-learning environments are different from the classical education. In this paper, the design is presented from a different point of view. It has constructed a curriculum-specific E-learning environment. It focuses on not only how to teach the students but also how to prompt the interaction between the teachers and the students according to the features of the curriculum. They conclude that student interaction and collaboration has also played an important role in their E-learning environment. So their E-learning environment provides sufficient interactive and collaborative methods to the students.

As information security is becoming more and more important there are also many E-learning Systems developed for information Security Education.

[4] Presents remote hands on network laboratory and relative comprehensive open courseware.

[5] [6] also describes the remote networking labs for information security to improve the learning effects.

[7] Utilizes the digital radio, Internet protocol (IPTV) and Multimedia Technology in E-learning environments for information Security Education.

[8-11] discusses on the development of E-learning environments for information Security Education from a different point of view.

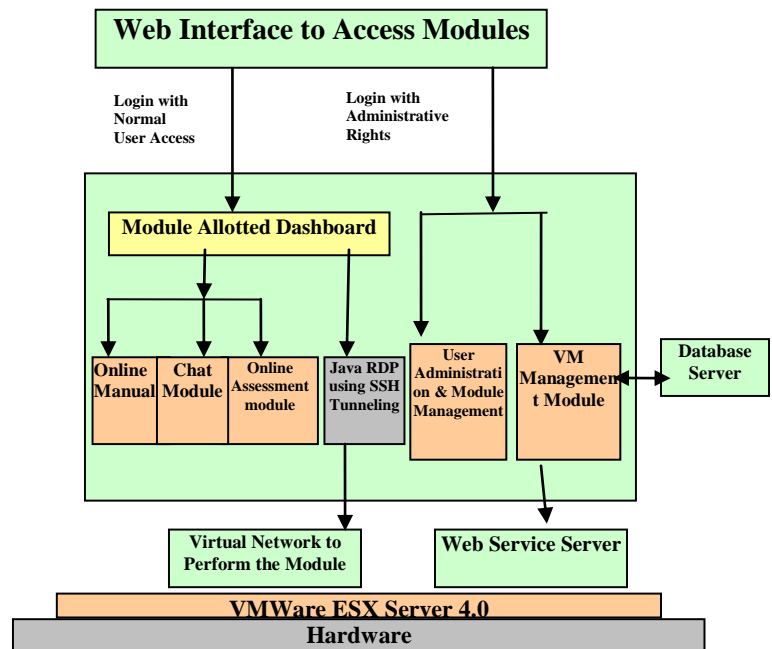
This paper discusses a totally different design from the above researchers to develop a web-based E-learning environment. It uses virtual technology to develop a virtual lab which is remotely available via web browser using which participants can learn information security concepts by performing hands on lab using latest tools and technologies currently available for information Security. Thus this paper discusses a totally new paradigm towards Information Security education.

### 3. SOFTWARE ARCHITECTURE OF THE E-LEARNING ENVIRONMENT

The software architecture of the E-learning environment is shown in Fig. 1. There is a web interface designed to access the modules. There are two modes of login through the web-Interface. In first mode, the user login 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 assess 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 server using SSH tunneling. The Virtual Network, the online manuals, chat modules and online assessment modules are tightly integrated in to the system and GUI Interface is available to access these components.

When the user login 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.



**Fig 1: Software Architecture of the E-learning Environment**

#### 3.1 Description of Software Components of Web based E-learning Environment

As discussed in software architecture following software components have been developed to support the E-learning Environment.

- Web Interface to the Modules
- 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 web based e-learning environment.

##### 3.1.1. Web Interface to the Modules

- Language used (front-end) : PHP, Java Script & Ajax
- Back End Tools : MySQL
- Lines of Code : 20,000(approx.)

##### 3.1.2. VM-Management module, Module allocation and User Management module

- Scripting Language Used : Perl-script and Shell Script
- Front-End Tool Used (for Interface) : PHP
- Back-End Tool Used : MySQL
- Lines of Code : 15,000(approx.)

### 3.1.3. RDP Solution to access the modules behind Proxy on Client Side

- Language Used for Front-End : PHP(for Interface)
- Language used for Background : Java Programming
- Lines of Code : 20,000(approx.)

### 3.1.4. Online Assessment module

- Language Used : PHP, JavaScript
- Backend User : MySQL
- Course Lab IFrame is used for dynamic Interfacing
- Lines of Code : 1000 (approx)

### 3.1.5. Chat Module

- Language Used : PHP
- Back-end : MySQL
- JSON is used for serialization of data
- JQuery and JavaScript are also used.
- Lines of Code : 1000(approx.)

## 4. NETWORK ARCHITECTURE OF THE E-LEARNING ENVIRONMENT

The Network Architecture for the e-learning environment is shown in Fig. 2. There is a Server hosting ESX 4.0 Virtualization software. This ESX 4.0 virtualization software is being used for hosting virtual machines and virtual networks. Firewall is used to create demilitarized zone (DMZ) and port mapping to provide online access to the virtual machines. The Web Server is used for providing online access to instruction manual and virtual machines through the web based interface from remote locations using Internet. The SSH server is being used to tunnel the connection with the remote machine for accessing modules behind proxy server and NAT. Web Service server is used here to manage the virtual machines used for performing information security lab assignment. The Router is being used to provide the link to internet service provider (ISP). The architecture being shown here shows how internal and external users are accessing the web based e-learning environment through Internet.

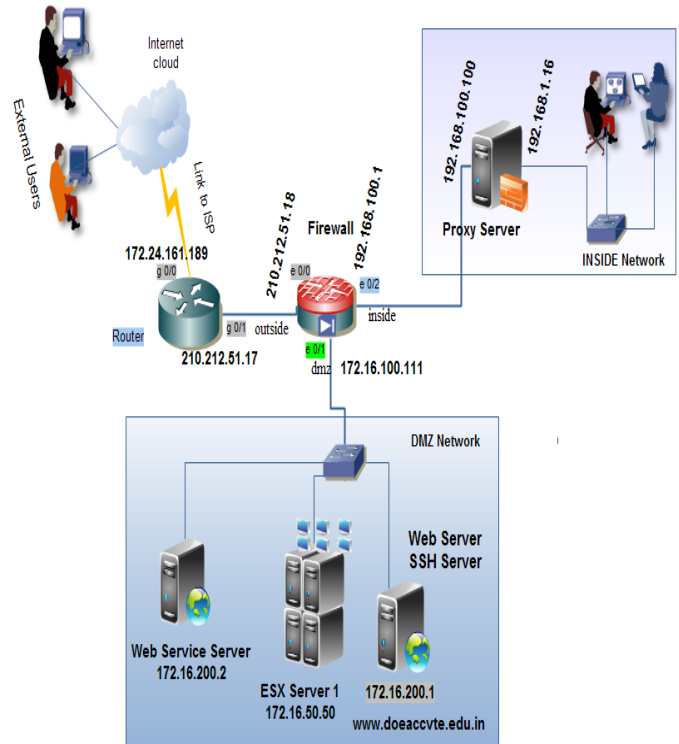


Fig 2: Network Architecture of the E-learning Environment.

## 5. LIST OF THE MODULES DEVELOPED FOR E-LEARNING ENVIRONMENT

The module list developed for the E-learning environment is as follows:

### 5.1 Group A (Information Gathering & Countermeasures)

- Network Discovery & Scanning
- Target Enumeration
- Vulnerability Assessment

### 5.2 Group B (Ethical Hacking & Countermeasures)

- Sniffing & Countermeasures
- Brute Force Attack & Countermeasures
- IP Spoofing with 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

### 5.3 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

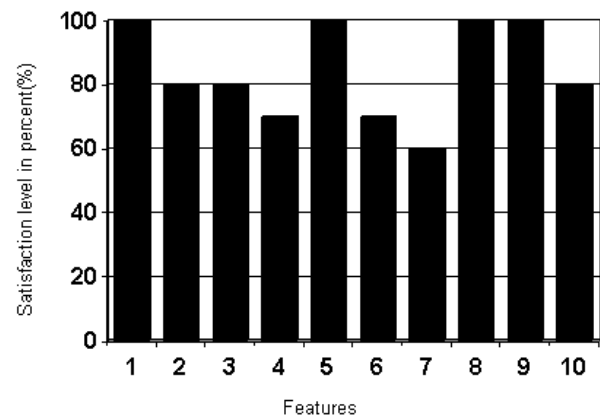
So from the module list it is clear that the modules are categorized in to three categories. The categorization of the modules is done considering the normal attack scenario in which the attackers first gathers information about the network, and then the attack is done. The first two sections teach the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

## 6. EVALUATION OF RESULT OF THE PROPOSED DESIGN

The web based E-learning environment for Information Security has been evaluated from ten different features as listed below.

1. Whether the interface to access modules in E-learning environment is user friendly.
2. Whether the Technical quality of modules developed is good.
3. Whether the Technical quality of manuals developed is good.
4. Whether sufficient theory concepts are included in the environment.
5. Whether the environment provides sufficient practical concepts to participants.
6. Whether the environment is suitable for interactive teaching and learning.
7. Whether the environment provides self pace learning abilities
8. Whether the environment provides self evaluation methods to the participants
9. Whether the E-learning environment developed is better than physical environment.
10. Overall evaluation.

The design was evaluated by providing online access to the modules deployed in the environment. The suggestions and feedbacks were taken on the above features and results are shown in Fig. 3. The results show that most of the participants are satisfied with the web based E-learning environment for information security.



**Fig 3: Evaluation Results**

## 7. CONCLUSION

The E-learning environment can be constructed in many ways. Different researchers have explored different ways to construct the E-learning environment. This paper has presented a totally different approach by utilizing the latest technology the virtualization. This environment gives the feel to the participants that they are working in a real environment. It also focuses on interaction between instructor and learner by incorporating chat modules etc. Most of the scenarios here are taken from real scenario which the user faces day today.

Although the design discussed here is fully successful but it could be further improved by simulation of attacks in a Wide Area Network (WAN) scenario. Also presenting the E-learning environment is primarily focused on practical oriented approach but in future the curriculum could be improved by enriching theoretical concepts also so that the E-learning environment meets the objective of full information security curriculum.

## 8. 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.

## 9. REFERENCES

- [1] Sandy Britain et al., "A Framework for Pedagogical Evaluation of Virtual Learning Environments." JISC Technology Application Programme University of Wales-Bangor.
- [2] Sevgiozkan et al. "Multi-Dimensional Evaluation of E-Learning Systems in the Higher Education Context: An Empirical Investigation of a Computer Literacy Course." 39th ASEE/IEEE Frontiers in Education Conference W1C-1.
- [3] We Hu et al. "Collaborative Web -Based E-Learning Environment for Information Security Curriculum." World Academy of Science Engineering and Technology 53 2009.
- [4] D.Q. Yuand et al. "Designing a Comprehensive Open Network Laboratory CourseWare", Journal of computing sciences in colleges, Volume 24, Issue 1 (October 2008), 2008, PP 174-181.
- [5] C.C. Li, J. Pickard et al., "A Practical Study on Networking Equipment Emulation", Journal of computing sciences in colleges, Volume 24, Issue 2 (December 2008), 2008, PP. 137-143.

- [6] H.A. lahoud,X. Tang “ Information Security Labs in IDS/IPS for Distance Education”,Proceeding of the 7th conference on Information technology education , 2006 ,Minneapolis , Minnesota ,USA,PP 47-52
- [7] Z. Xiao, F.Ye,”New Insights on Internet Streaming and IPTV” Proceedings of the 2008 international conference on content-based image and video retrieval,2008,Niagara Falls,canada,PP 645-654.
- [8] S.Rigby,M.Dark,” Designing a Flexible,Multipurpose Remote Lab for the IT Curriculum”,Proceedings of the 7th conference on Information technology education 2006,Minneapolis,Minnesota,USA,PP. 161-164.
- [9] Eli J. Weissman, ”An Evaluation of Online Learning Environment(OLE) on the Adult at-risk Population” ,Journal of computing sciences in colleges,2003,volume 18,Issue 3, PP. 142-154.
- [10] W.D. Armitage et al ,”Remotely Accessible Sandboxed Environment with Application to a laboratory course in Networking”,Proceedings of the 8th ACM SIGITE conference on Information Technology Education 2007,Destin,Florida,USA,PP. 83-90.
- [11] Aboutabl, M.S. “ The Cyber Defense Laboratory: A Framework for Information security Education” Information Assurance workshop, IEEE, 2006.