ISSN: 2321-7782 (Online)
e-ISJN: A4372-3114
Impact Factor: 7.327

Volume 6, Issue 5, May 2018

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Designing a Cloud-Based Virtual Lab as a Service

Smeet Palkar[1]
BE Student,
Computer Department,
Marathwada Mitra Mandal's College of Engineering,
Pune, India

Yashodhan Vaidya[2]
BE Student,
Computer Department,
Marathwada Mitra Mandal's College of Engineering,
Pune, India

Shailaja Jadhav[3]
Assistant Professor,
Computer Department,
Marathwada Mitra Mandal's College of Engineering
Pune, India

Abstract: Hands-on experiments are essential for Cyber security education. Legacy laboratory solutions usually requires significant efforts to build, configure,maintain, and scale the infrastructure. However, with the advent of cloud computing technology, it is now become convenient to build learning environments that follow the constructive view of learning, supporting on demand and self-controlled learning environments and skill based assessments. This project focuses on building and integrating virtualised labs for Cyber security to an innovative and competitive cloud-based virtualised learning platform.

Keywords: Virtual Machine, Hypervisor, Remote-access, Cyber security, Thin-clones.

I. Introduction

Cloud computing provides its users with more convenient ways to use the resources and with a model where the users are charged as per the usage of their resources. The model is known as "pay-as-per-usage". Users can access the cloud services from anywhere at any time. They only need a working Internet connection. We are of the opinion that teaching must reach as much students as possible. Thus, cloud provides the best solution to our aim. Training developers can be done easily and efficiently from a cloud service as the teacher would have at-most control of the whole teaching process. We came across teaching methods where the theoretical part is very well explained and understood but it is impossible to gain experience due to the lack of resources. Thus, we focused on creating virtual environments equipped with the tools for a specific use case in order to help students across the world gain hands-on experience.

Cyber security is one of the most important requirements in any business logic. Thus we have decided upon a few most common cyber-attacks to take as a base for the visualized lab. This will help all kinds of clients learn to recover from such attacks. We have also included a functionality to learn to do these attacks as that is best way for coming up with preventive measures on the field. We have also planned on adding a skill based assessment at the end of every use-case in order to help student know how well they have learnt it.

The work done in this project is divided up into the following. Section II provides the related work the we referred while completing different steps in this project. Section III gives a brief description about the Use-Cases chosen for the Virtual Lab. Section IV gives an insight on the environment used to manage, configure and propagate the virtual machines. Finally, section V contains the conclusion and future scope.

II. Related Work

Virtual environments are mainly used for services. Thus, we merged a few concepts used by multinational firms and chose only those modules which help to make teaching efficient.

Every branch in computer engineering comes down the same objective- efficiency. Therefore we worked hard to find the most efficient ways to perform the attacks. This does not mean they may be the best methods but definitely the easiest and ones which are able to teach the concept faster and better.

III. Cyber Attacks

We chose only the most common attacks as our working space for this project. They are:

1. *Ddos*

Denial of Service attacks are aggressive attacks on an individual computer or website with intent to deny service to intended users. DoS attacks can target end-user systems, servers, routers and Network links. The victim computer or system cannot handle data larger than a fixed size. A ping of death packet is sent from a source computer to target computer, it then gets fragmented into smaller group of packets. One fragment is of 8 octet size. When these packets reach the target computer, they arrive in fragments. The fragmented packets are reassembled as a packet which are received as chunks. But the whole assembled packet causes buffer overflow at the target machine.[1] This is denial of service attack. When this attack is performed on the target machine by a number of computers, it is called Distributed Denial of Service attack.

Distributed Denial of Service attack is well known attack responsible for many service outages around the globe. We have included the easiest way to simulate this attack on a virtual server by virtual clients.

2. *SQLi*

It is an application security weakness that allows attacker to control an application's database- letting the attacker access or delete data from the victim's database- by tricking the application into sending unexpected SQL commands. When a victim computer is attacked with SQL injection, the database of the victim is under threat and necessary information can be altered or deleted by the attacker. Important information can be accessed and the security of the database is compromised.

SQL injection and another well known attack where unsanitized codes on the internet are an easy target for these attacks.[2] We have included a tool called sqlmap in order to discover exploits in the system.

3. *XSS*

Cross Site Scripting is an attack which allows the attacker to inject malicious code on a website. Once this malicious code is injected on the website, the services of this website are made unavailable to any other user accessing it. The attack can also redirect the users to any other website which the attacker wants. The malicious code is injected by commenting the malicious code on the website. The malicious script which persists on the website is called Persistent XSS. Persistent XSS makes the website unavailable for the users. This attack does not compromise the victim's personal information or does not gain access to the victim's system.

Cross-site Scripting is very easy to learn and recover form. However, a very small mistake while programming can cause heavy losses just by XSS. This attack is demonstrated by setting up a LAMP server.

4. *Session Hijacking*

Cookies are very important and one must make sure its not possible to be stolen.[3] Session hijacking uses the same LAMP server to demonstrate cookie stealing and reloading to educate the client about such a scenario.

5. *Phishing*

In this attack, the attacker sends a link to the victim which redirects the victim to a login page of a trusted site. The page script of this trusted site is tampered with the attackers similar looking site. When the victim puts his/her login credentials in the login tab (thinking it is the actual site), the information is received by the attacker and an error is shown to the victim. Personal information of the victim is compromised. By accessing this personal information the bank details or personal accounts of the victim can be accessed. To prevent this attack, users need to be aware about such false emails which may lead to loss of personal information. Fake websites are very common nowadays. Phishing takes the clients to the core of how it works by creating a free website.

6. *Insecure Direct Object Reference*

Insecure Direct Object References occur when an application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources in the system directly, for example database records or files.

IV. Working Environment

It takes very powerful resources to host services for learning as the host system requires to take the load of managing the packages and processing power for every application that the client requires.

1. The Virtual Lab is hosted on the hypervisor, VMware ESXi 6.5. It provides a very good user interface for manipulating virtual machines and the networks between them.
2. Network between the virtual machines is isolated and controlled by a custom virtual router known as the transit router which runs a special operating system known as the VYOS.
3. The last data storage runs the VMs via thin clones so that the admin has at-most control.
4. These virtual machines can be remotely accessed by clients through a protocol called VNC which has similar functionality to RDP.
5. Clients only require login credentials in order to get access to the machines and there is no special UI. Just the feel of looking at physical systems in the same network.

V. Architectural Design

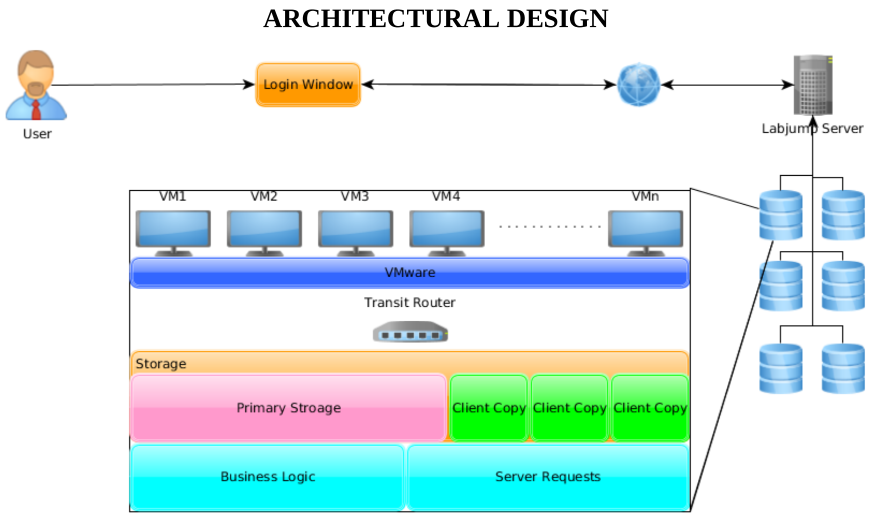


Fig. 1 Architectural design of virtual lab set-up

A good system architecture always works towards abstraction. Here, the user sees nothing but a login window which hides all the complexities of the system. The sever hosts the service of our labs which are designed to teach students about cyber security. Inside the server is the actual logic of virtualization. It contains a request handler and the business logic section which helps to automate the process as users can be multiple. Moreover, we are talking about security and we must not leave out the security of this system itself. Thus, client copies are made of the storage for different users which store only the changes instead of writing the changes in the primary memory. This helps to keep their workspace different and also keeps our storage safe from cyber attacks and accidental data loss or overwrite. We designed a virtual transit router using VYOS which helps to handle fenceing of the VMs. Fencing is the process of isolating the network of our VMs from that of the outside world. This step was very important as we do not want cyber security students interacting with the outside world until the have the full knowledge of the capabilities and posibilities of the tools used. On top of all this are the actual VMs which are usually configured to include the attacker- victim arrangement for the different attacks.

VI. Conclusion and Future Scope

A decrease in the quality of practical sessions and students, IT/ non-IT professionals not being able to gain first hand experience in the field of cyber security by actually implementing the cyber attacks and recovering the systems from these attacks made us work to create a cloud based visualized lab which provides first hand experience and knowledge in detail about various cyber attacks. The cyber attacks like DoS (Denial Of Service) attack, XSS (Cross Site Scripting), Session Hijacking, SQL Injection, Phishing and IDOR have been covered by these virtual labs. User will be given a guide with the knowledge about these attacks which include the steps to implement these attacks and to recover the system from these attacks. The attacks will be performed virtually by remotely accessing the virtual machine from the cloud with an unique Username and Password. The virtual machines provided to the user will be as per the requirement of the user and all the tools needed to implement these cyber attacks will be already installed. In this way we have made an extensive effort to reach out to maximum number of people and helping them acquire hands on experience about the cyber attacks which are just heard about from the world, with very few people actually being able to prevent their devices or recover their devices from such attacks. With the world turning to technology as an alternative to real time jobs, the need of security is increasing to prevent data theft and loss of important information.

References

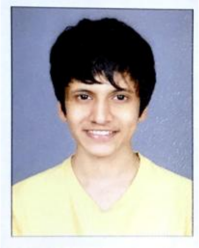
1. Preeti Daffu, Amanpreet Kaur “Mitigation of DDoS attacks in cloud computing” Published in 2016 at the 5th International Conference on Wireless Networks and Embedded Systems (WECON) pp. 1-5 , 2016
2. J. BV.K. Gudipati, Trinadh Venna, Soundarya Subburaj “Advanced Automated SQL Injection Attacks and Defensive Mechanisms.” 2016 Annual Connecticut Conference on Industrial Electronics, Technology and Automation (CT-IETA) pp. 1-6 , 2016
3. S. ZhanJoshua Pauli, Patrick Engebretson, Michael J. Ham “Cookie Monster: Automated Session Hijacking Archival and Analysis” 2011 Eighth International Conference on Information Technology: New Generations (ITNG) pp. 403-407 , 2011
4. M.Pezhman Sheinidashtegol, Michael Galloway “Performance Impact Of DdoS Attacks on Three Virtual Machine Hypervisors” 2017 IEEE International Conference on Cloud Engineering (ICCE) pp. 204-214 , 2017
5. huopeng Li, Ken Chen, Mohand Yazid Saidi “A failure avoidance oriented approach for virtual network reliability” 2017, IEEE International Conference on Communications (ICC) pp. 1-6 , 2017
6. Zhenhua Li, Yuanyuan Yang “Virtual Network Embedding in Hybrid Data Centers” 2017, ACM/IEEE Symposium on Architectures for Networking and Commu- nications Systems (ANCS) pp. 99-100 , 2017
7. Taurin Tan-atichat, Joseph Pasquale “VNC in High-Latency Environments and Techniques for Improvement” 2010 IEEE Global Telecommunications Conference GLOBECOM 2010 pp. 1-5 , 2010
8. Louis Casanova, Marcel, Edy Kristianto “Comparing RDP and PcoIP protocols for desktop virtualization inVMware enviroment” 2017 5th International Conference on Cyber and IT Service Management (CITSM) pp. 1-4 , 2017
9. R. Mohtasin, P. W. C. Prasad, Abeer Alsadoon, G. Zajko, A. Elchouemi, Ashutosh Kumar Singh “Development of a virtualized networking lab using GNS3 and Vmware workstation” 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) pp. 603-609, 2016

10. You Yu, Yuanyuan Yang, Jian Gu, Liang Shen "Analysis and suggestions for the security of web applications" Proceedings of 2011 International Conference on Computer Science and Network Technology vol. 1, pp. 236-240 , 2011

11. Engin Kirda, Christopher Kruegel "Protecting Users against Phishing Attacks" The Computer Journal vol. 49, no. 5, pp. 554-561 , 2006

AUTHOR(S) PROFILE

Smeet Palkar, pursuing the B.E. degree in Computer Engineering from Marathwada Mitra Mandal's College of Engineering due to be completed in 2018. He is now working with Labjump Services Pvt. Ltd. as an intern.



Yashodhan Vaidya, pursuing the B.E. degree in Computer Engineering from Marathwada Mitra Mandal's College of Engineering due to be completed in 2018. He is now working with Labjump Services Pvt. Ltd. as an intern.

Shailaja Jadhav, received the M.E. degree and B.E. degree in the field of Computer Engineeing. She has total 13 years of teaching experience and is currently working as an assistant professor with Marathwada Mitra Mandal's College of Engineering.