iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** III **Month of publication:** March 2022

DOI: https://doi.org/10.22214/ijraset.2022.40917

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

CyberX: Own Server Based Windows OS and Penetration Testing

Dr. Mrs. Anuradha Kondelwar[1], Nikhil Hingawe[2], Ankit Bachar[3], Greenkumar Bisen[4], Karan Bhosale[5], Gajendra Tandekar[6]

[1] *Assistant Professor,* [2, 3, 4, 5, 6] *Ug Students, Department of Computer Technology, Priyadarshini College of Engineering Nagpur, Maharashtra, India*

Abstract: ***Computer systems have faced the difficulty of protecting the data with which they work since the beginning, and as technology has advanced, computational security measures have become increasingly complex to counter potential threats. We're currently engaged in a war game with the traditional attackers and defenders. The attackers desire complete control of the systems. Defenders, on the other hand, virtualized systems to ensure the resources' safety in the event of an assault. Attackers have also developed increasingly complex strategies to circumvent such safeguards, necessitating the need to predict such events, which can be accomplished through the use of preventative measures. Simulating Penetration Testing is one way to accomplish this (PT). PT is a computer system attack that employs a series of specialized tools to search for security flaws. These tools may finally get access to the computer's features and data, allowing the finding of evidence of vulnerability. Cyber-attacks are more likely in virtual environments. The purpose of this paper is to present a framework for performing penetration testing in virtual environments.***

Keywords: Security, Penetration Testing (PT), Vulnerability, Virtual Environments, Cyber-attack.

I. INTRODUCTION

Virtualization or emulation of a computer system is called as virtual machine (VM). Virtual machines are computer architectures that give similar functionality as given by physical computer. Specialized hardware, software, or a combination of both hardware and software are used in for their implementations. The mix of hardware, software, and networking is required in the building of a virtual machine since hardware, software, and the network must all work together at the same time in order for the machine's output or result to be correct. We created our own virtual penetration testing lab at home because many of the pupils desire to study ethical hacking. Creating a pentesting lab is essential for learning various testing techniques and staying out of legal issues, as hacking is illegal.It's crime to break into anyone's computers and networks when you don't have permission, so establishing your own lab that is similar to someone else's environment is a must for learning different testing tools and hacks while staying out of legal trouble.[2]While performing security testing on a system, there is a risk of severe damage that could result in the permanent deletion of the data on the targeted device or the destruction of the target computer or network; however, in our own pentesting lab, we will have complete control over the environment for testing and can also configure the target to the exact specifications needed for the test.[1]

Basically, in this project, we will build our own server using Oracle Virtual Box, and we will design our own website using html, CSS, and javascript, with all of the data being stored on our server machine. We'll do some penetration testing with a variety of tools and methodologies.

Sophistication of cyber-attacks has accompanied the rapid technological evolution. Many cyber-attacks can be avoided, and for that it is necessary to use appropriate security strategies. Therefore we can perform penetration testing as it is a preventive method which will be best defense. Penetration Testing allows testing computer security, to assess the level of security of the technological infrastructure and make the necessary corrections.[8]

For several years, it has been found that with this type of testing, it's possible to discover security weaknesses that compromise critical assets of organizations.

The depth of penetration study can be applied even in equipment for personal use, and will depend on the required needs in respect of security controls to prevent unauthorized access. To face the scaling of applications and services required, organizations have focused on virtualization to optimize computing resources, and according to safeguarding the security, it is necessary to investigate penetration testing targeted for virtual environments, and this concern seeks to fulfill this research.

©IJRASET: All Rights are Reserved

In this paper, we assume the perspective of the defender, who is trying to defend the virtual environment from the attackers wishing to execute malicious code.[3] In the 2nd section a global exposure of virtual environments. The 3th section describes the penetration testing and their use. Finally, in the 4th section we propose a framework for penetration testing in virtual environments, which we hope will be an aid to help the defenders protect virtual systems from the attacks to which they are exposed. In the last section, the final considerations are presented.[11][8]

II. METHODOLOGY

As we know virtual machines are computer architectures that give the similar functionality as given by physical computer. Various types of hardware, software, or a combination of both hardware and software are used in for it's implementations. So firstly we have installed Virtualbox and then Windows, Sql server, Apache Server, Wordpress, SSH inside it.[8]

A. *Development of the Machine*

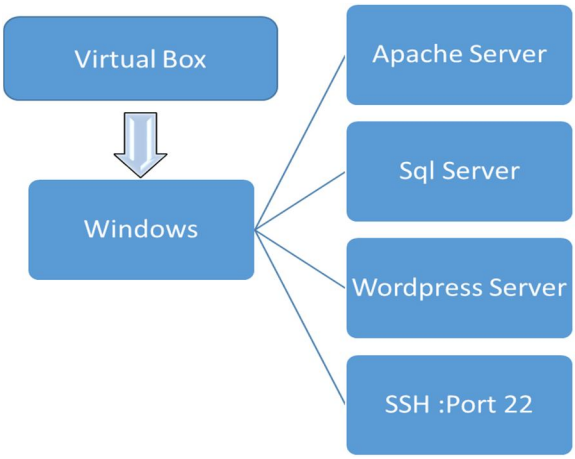


Figure 1: Design Flowchart.

1) *Virtualbox:* It is an open source software , which has cross-platform, virtualization software access enabling developers to deliver output faster by running multiple OS on a single device. The aim of our project is to create a web application based virtual machine which is penetrable and vulnerable to achieve this aim we need a virtualized environment where we can install Os and create a virtual machine for this purpose we are using virtualbox software developed by Oracle corporation.[4][10] The first step in our project is installation of virtualbox as we need to install Os and various types of softwares which will make our machine penetrable and vulnerable.
2) *Windows:* The next step of our project is installation of windows. We have used Windows7 version for our project. After installing the Windows7 successfully in the virtualbox , we will assign all the required network and hardware configuration in the virtualbox .
3) *MySQL Server:* The next step of our project is installation of MySQL Server. We are using MySQL server for creating database with the proper details and the configuration to create a WordPress server locally in our machine.
4) *Apache Server:* The next step of our project is installation of Apache HTTP Server. It is an open-source cross-platform web server software. The web application or the website which we have created will be hosted and installed on this server with all the required directories and repositories.
5) *Wordpress:* The next step of our project is installation of WordPress .It is a free and open-source content management system written in PHP and paired with a MySQL or MariaDB database. Features include a plugin architecture and a template system, referred to within WordPress as Themes .
6) *SSH Port 22:* The Secure Shell Protocol is a cryptographic network protocol for operating network services securely over an unsecured network. Its most notable applications are remote login and command-line execution. SSH applications are based on a client–server architecture, connecting an SSH client instance with an SSH server. All the above following steps are related to the installation and creation of the virtual machine with desired configuration and settings. This was initial stage of our project in which we have successfully executed all the steps and developed virtual machine with all the required bugs and exploits. Next Stage or the final stage of our project will deal with the penetration testing with various types of tools in Os(kali linux)

B. Penetration Testing

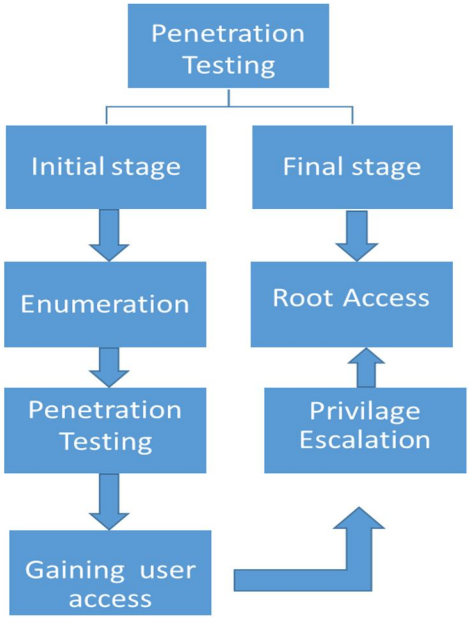


Figure 2: Pentesting

Penetration testing is the process of gaining access by finding a loophole in the system in order to gain and stealing the credential of the users.
Penetration is done in the manner mentioned in the above figure which is as follows

Penetration is done in two stages:

1) *Initial Stage:* In the initial stage we will perform basic enumeration on the web application in which we will find out the loopholes available on the web application. After finding all the loopholes and exploits we will exploit or attack the target machine and try to gain user access or user shell of the operating system. [6][9][1]
2) *Final Stage:* After gaining the user access we further have to gain the administrator rights access of the target machine in order to achieve that we need to perform privilege escalation. After performing privilege escalation if we get the administrator access or the root access to the target machine we can say that we have successfully gain the access into the machine.[1]

III. MODELING AND ANALYSIS

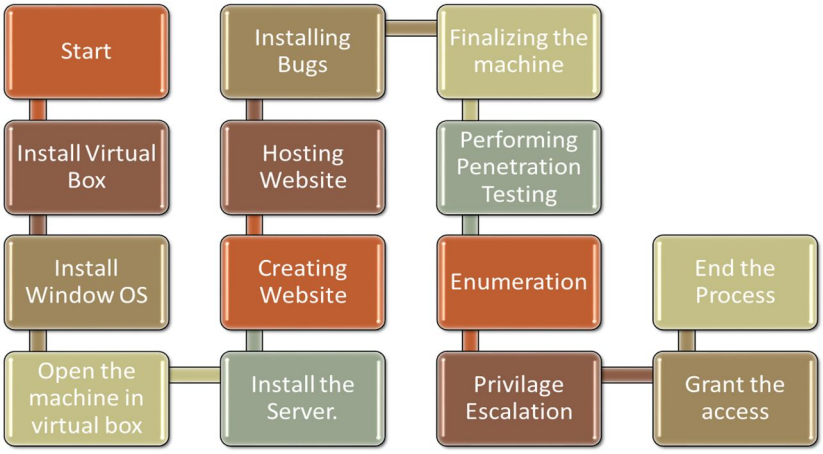


Figure 3: Model Flowchart.

Above Flow Diagram shows the designing of the machine and the various steps involved in the project.We have used virtual box. Oracle VM VirtualBox enables you to run more than one OS at a time. This way, you can run software written for one OS on another, such as Windows software on Linux or a Mac, without having to reboot to use it.
Then, we installed Microsoft Windows Os, commonly referred to as Windows, is a group of several proprietary graphical operating system families, all of which are developed and marketed by Microsoft.
Installed Server on the virtual machine ,then created an index page hosting on Server ,Installed Bugs in the server and thus finalised the machine.[1]

IV. RESULT

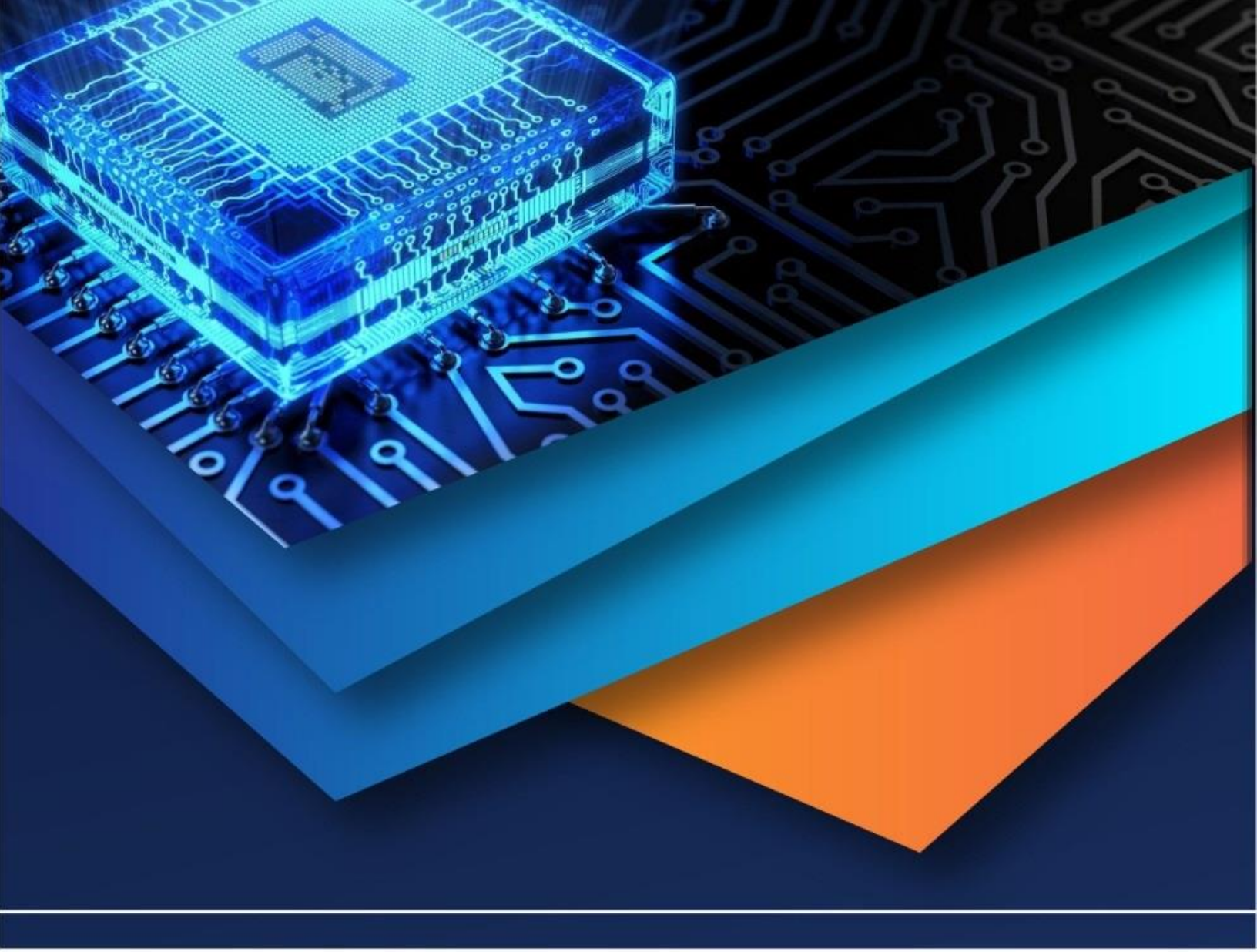
We have successfully created our own virtual vulnerable machine by installing the apache server in it and hosting it with the live webpage, setting up the bugs and making an environment which is liable for pentesting.[3][11]
After the machine was ready, we successfully tested it with the various types of tools and successfully rooted and gained all the access of the machine. We obtained both the flags hidden inside the servers of the machine. It means that our machine is successfully working.

V. CONCLUSIONS

Thus we conclude that our project is done successfully. we have design ,implemented, tested the machine. We have seen how the bug can lead to hacking of our website. Avoiding this mistakes can help us to keep our system safe. Virtualization with regard to security, if well implemented, deployed, monitored, and managed can offer security advantages, but a failure in any one of these can lead to disastrous results. Penetration Test is a vital service that levers on an established methodology, that uses a variety tools to systematically identify system vulnerabilities and weaknesses, analyzing breaches and mapping solutions, allowing mitigate attack vectors in a more effective way. The value of penetration testing depends from the use of the latest threat information and contextualization of these with the business. Penetration testing is particularly valuable for the maintenance of security of the virtual environments. There are several security considerations to keep in mind in virtual environments, ranging from the hypervisor configuration, to the security measures and network storage, without neglecting the virtual machines. The naturally mobile nature of the virtualized environment requires security to travel with the virtual machine. Encryption and access control are of the greatest importance to protecting the VM and its data inside the datacenter. To expedite this situation at preventive level, and consequently at the security level, in the very near future PT should be made available as a service. In this context, all actors of virtualization can profit from PTaaS, from the cloud provider to the system owner, also including the ethical hacker, promoting the global security of virtualized environments.

REFERENCES

[1] Penetration Testing on Virtual Environments, guarda2016.
[2] Furfaro, A., Piccolo, A., and Saccà, D. SmallWorld: A Test and Training System for the Cyber-Security. European Scientific Journal, ESJ, 12(10) (2016), 130-145.
[3] Mihai, I. C. Penetration Tests on Virtual Environment. Int'l J. Info. Sec. & Cybercrime, 1(37) (2012).
[4] J. MICHAEL BUTLER;ROB VANDENBRINK. IT Audit for the Virtual Environment. SNAS, 2009.
[5] Morariu, O., Borangiu, T., and Raileanu, S. vMES: virtualization aware manufacturing execution system. Computers in Industry, 67 (2015), 27-37.
[6] Shkurkin, D., Novikov, V., Kobersy, I., Kobersy, I., and Borisova, A. Investigation of the scope of intellectual services in the aspect of virtualization and information economy of modern Russia. Mediterranean Journal of Social Sciences, 6(5 S3) (2015), 21-29.
[7] Ying-chun, Z. H. A. O. Application of Desktop Virtualization in the Library [J]. Information Science 2, 016 (2012).
[8] Hale, K. S. and Stanney, K. M. Handbook of virtual environments: Design, implementation, and applications. CRC Press, 2014.
[9] Halfond, W. G., Choudhary, S. R., and Orso, A. Penetration testing with improved input vector identification. In In 2009 International Conference on Software Testing Verification and Validation (2009), IEEE, 346-355.
[10] Krutz, R. L. and Vines, R. D. The CISSP and CAP Prep guide. Wiley, 2007.[11] [ACM Press the 4th International Conference - Kuala Lumpur, Malaysia (2016.12.28-2016.12.31)
[11] [ACM Press the 4th International Conference - Kuala Lumpur, Malaysia (2016.12.28-2016.12.31)] Proceedings of the 4th International Conference on Information and Network Security - ICINS '16 - Penetration Testing on Virtual Environments



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)