IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

Cyber-X: Own Server Based Platform for Pentesting

Dr. Mrs. Anuradha Kondelwar[1], Nikhil Hingawe[2], Ankit Bachar[3], Greenkumar Bisen[4], Karan Bhosale[5], Gajendra Tandekar[6]
Assistant Professor, Department of Computer Engineering[1]
B.E Students, Department of Computer Engineering[2,3,4,5,6]
Priyadarshini College of Engineering, Nagpur, Maharashtra, India

Abstract: *Security technology is important to security, but the practices of the people who develop, integrate, evaluate, configure, maintain, and use that technology are more important; indeed, these practices are the foundation of technical security. We argue that the flexibility of virtual environments will play a critical role in many cyber security related aspects. Problems like the assessment of newly devised intrusion detection techniques, the evaluation of skills of cyber defense team members, the evaluation of the disruptive effects caused by the diffusion of new malware, are just few examples of issues that cannot be directly addressed in production systems even though they require realistic operating environments in order to be suitably performed.*

Keywords: Virtual Environment, Cyber Attack, Security, Threats, Web Application Penetration Testing

I. INTRODUCTION

Virtual Machine technology applies the concept of virtualization to an entire machine, circumventing real machine compatibility constraints and hardware resource constraints to enable a higher degree of software portability and flexibility. Virtual machines are rapidly becoming an essential element in computer system design. They provide system security, flexibility, cross-platform compatibility, reliability, and resource efficiency. Designed to solve problems in combining and using major computer system components, virtual machine technologies play a key role in many disciplines, including operating systems, programming languages, and computer architecture. For example, at the process level, virtualizing technologies support dynamic program translation and platform-independent network computing. At the system level, they support multiple operating system environments on the same hardware platform and in servers.[1][7] 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.[3]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.[4][5]

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.[6] So firstly we have installed Virtual box and then Windows, Sql server, Apache Server, Wordpress,

2.1 Setup of Machine

A. 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. The first step in our project is installation of virtual box as we need to install Os and various types of software's which will make our machine penetrable and vulnerable.[2]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

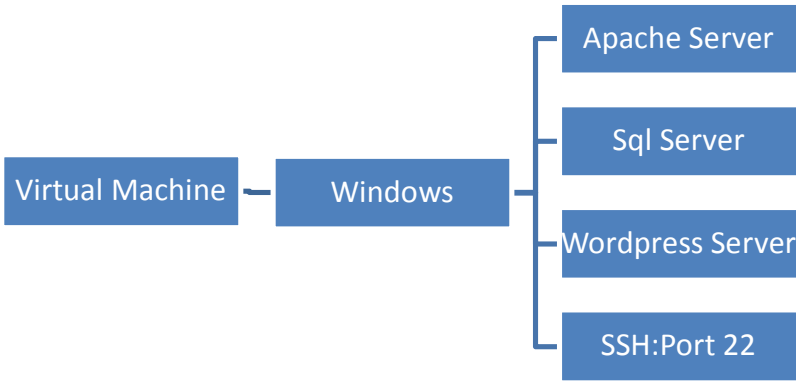

Figure 1: Design Flowchart.

B. 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 virtual box, we will assign all the required network and hardware configuration in the virtual box.[4]

C. 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.

D. 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.

E. 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.

F. 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.[1][7][3] 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).[7][5][2]

2.2 Penetration Testing.

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.[5][6][7] 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.[4][7] 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.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

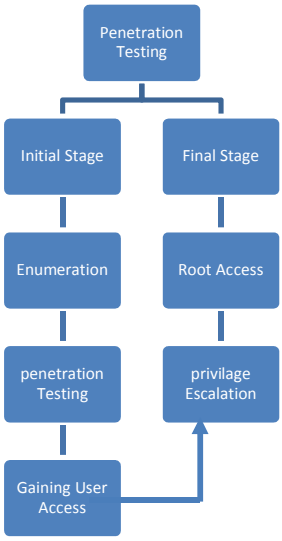

Figure 2: Penetration Testing

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.

III. Modelling and Analysis

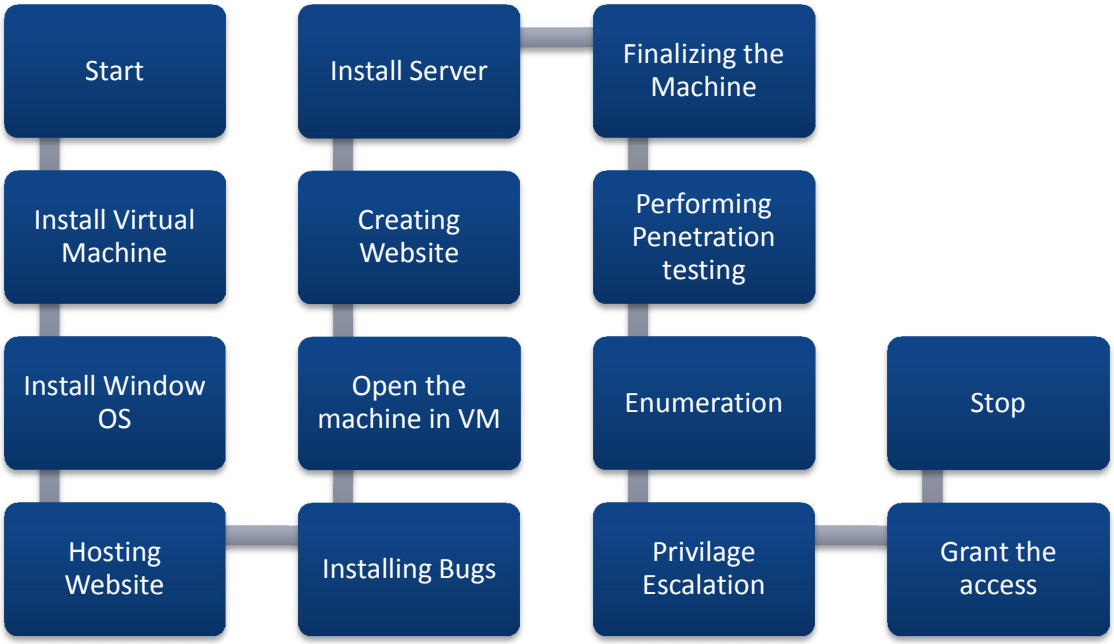

Figure 3: Flowchart.

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.[1][7][6][8] Then, we installed Microsoft Windows Os, commonly referred to as Windows, is a group of several proprietary graphical operating

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

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.

V. 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][7] 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.

VI. CONCLUSION

We have seen how the bug can lead to hacking of our website. Avoiding this mistake 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 testing is an effective testing process that helps to uncover the critical security issues of your system to check for exploitable vulnerabilities to their IT Infrastructure, or web applications. Penetration Test is a vital service that levers on an established methodology, that uses a variety tool 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. As cyber threats continue to increase, it has become essential for companies to keep their IT infrastructure, web apps and systems safe and secure from any possible threats and vulnerabilities. In this context, all actors of virtualization can profit from PTaaS and from the cloud provider to the system owner, also including the ethical hacker, promoting the global security of virtualized environments. Therefore, penetration testing has become so important in today's digital world with rampant cyber-attacks on the go. Testing Parts with its team of highly skilled security and pen testers ensures the best pen testing services to give you the complete benefit and helps to identify any possible vulnerabilities within your systems or IT infrastructure or web apps. 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.

REFERENCES

[1]. Authors: Jim Smith, Ravi Nair, Virtual Machines. Versatile Platform for systems and Processes, 1st Edition - June 3, 2005.
[2]. Hale, K. S. and Stanney, K. M. Handbook of virtual environments: Design, implementation, and applications. CRC Press, 2014.
[3]. 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)
[4]. "Penetraion Testing Guide", http://www.penetration-testing.com
[5]. iVolution Security Technologies, "Benefits of Penetration Testing," http://www.ivolutionsecurity.com/pen_ testing/benefits.php, accessed on Nov. 23, 2011.
[6]. Shewmaker, J. (2008). "Introduction to Penetration Testing," http://www.dts.ca.gov/pdf/news_events/SANS_ InstituteIntroduction_to_Network_Penetration_Testing.pdf, accessed on Nov. 23, 2011.
[7]. Penetration Testing on Virtual Environments, guarda2016.
[8]. J. Michael Butler; Rob Vandenbrink. IT Audit for the Virtual Environment. SNAS, 2009.