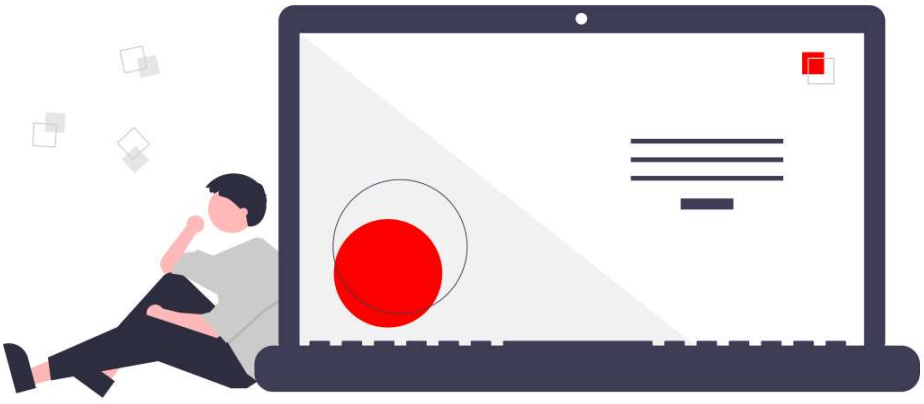
Secure IDE for Red Teaming



COMPX576 – Programming project

Venkatasubramanian Sankaranarayanan

Student ID: 1649356

Table of contents

Project proposal

Introduction

We all know that there are Integrated Development Environment customized testing environment for Software Development. What about Security testing? Here I have proposed a secure environment for practicing various attacking skills for Red teaming with few challenges. It can help attackers enhance their skills in various attacking methodologies inside a secure environment without disturbing the real world devices.

Methodology

I am including the methodologies, which include developing the environment, customization, deployment and testing.

1. Choosing suitable Operating system for the room (environment)
2. Setting up server
3. Installation of LAMP stack architecture
4. Building CMS (Content Management System) on top of LAMP stack
5. Creating custom plugin for CMS
6. Implementing Access management to make privilege escalation attack more challenging
7. Creating and hiding relevant ‘flags’ as a part of the challenge
8. Deployment and testing
9. Final product submission

Requirements

1. Hypervisor – Oracle VirtualBox
2. Operating System – Debian Based architecture
3. Attacking machine (another os in the hypervisor within the NAT network)

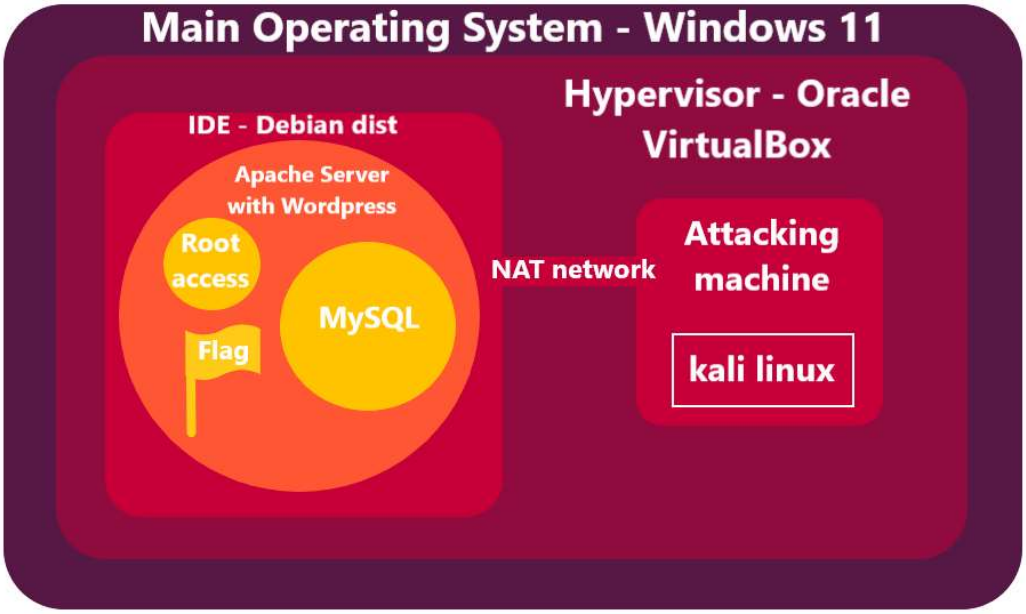
Technologies

1. Hypervisor – Oracle VirtualBox
2. Operating System (Debian based OS)
3. Webserver – Apache/Ubuntu
4. Database – MySQL
5. Scripting Language – PHP/Bash
6. Content management System – Wordpress
7. Secure Shell with RSA/passwd login
8. Networking - TCP/IP and NAT
9. IDE (Code) – nano/Vim

What I am learning for this project?

1. Server configuration
2. Custom CMS plugin development
3. PHP – Server side programming language
4. Access level definition – Custom Linux automations

Architecture



Conclusion

This project helps in Cybersecurity training bridging the gap between theoretical and practical implementations especially designed for the Red team. This allows people who have keen interest on red teaming and are ready to take up tough challenges without disturbing the real world entities. Ultimately, it contributes to the Cybersecurity community who are ethically bound to the compliances.