TEST Engineering & Management

*January - February 2020*
*ISSN: 0193 - 4120 Page No. 6003 - 6010*

# Designing Damn Vulnerable Operating System (DVOS) for Cyber Security Teaching & Learning

Muhammad Nabil bin Zainuddin Universiti Kuala Lumpur
Malaysian Institute of Information Technology Kuala Lumpur, Malaysia aklahnabil@gmail.com

Shafiza Mohd Shariff Universiti Kuala Lumpur Malaysian Institute of Information Technology Kuala Lumpur, Malaysia shafiza@unikl.edu.my

***Article Info***
***Volume 82***
***Page Number: 6003 - 6010***
***Publication Issue:***
***January-February 2020***

***Article History***
***Article Received****: 18 May 2019*
***Revised****: 14 July 2019*
***Accepted****: 22 December 2019*
***Publication****: 29 January 2020*

***Abstract:***
Educators teaching computer system security students are often faced with finding a suitable environment to test their student's skills and knowledge without breaching any law or misconduct security ethics. Students normally have no problem in understanding the theory part of a syllabus but when it comes to practical part, as there is no single environment that can be used for all type of attacks. Security students had to setup a multiple environment for all these different types of attacks, which can become troublesome as some environment is not easy to setup. In this study, we have designed a machine, Damn Vulnerable Operating System (DVOS), that focus on preparing a defensive cyber security testing environment. The DVOS is an environment that are intentionally vulnerable and can handle multiple type of common security attacks that covers from web application attack, network attack and open service port attack. Other than that, DVOS is also developed in the form of an ISO image file that can be bootable from a USB drive. By using DVOS, computer system security students can now own a defensive testing environment to apply what they have learn in class.

***Keywords:*** *Operating System; System Vulnerabilities; Web Vulnerabilities;*

## I. INTRODUCTION

Nowadays, the evolution of technology is growing rapidly and part of it came from the impact of industry stated that revolution of industrial are triggered by the internet, which allows user and machines communicate through the internet and open a hole in a security section. As a computer system security student, it is a challenge for us to keep up with the rapid development of the technology as most of the time we are only taught the theoretical part of a philosophy. Thus, we do normally have the knowledge when it comes to case discussion or analysis but when it comes to solving it in real time basis, not many are capable to achieve it.

The root of this problem is that most computer system security student are well exposed to the theoretical part of a knowledge, but they do not have much exposure on the practical part. [2] stated that practical learning will empowers learners to integrate theory and practice and apply their skills to solve any problem. Therefore, lacks legal environment for security trainers to do testing will make it harder for them to test their skills and knowledge on practical over theory. Most security lab's environment nowadays only has forensic and attacking tools, but they do not have a defensive testing environment. Hence, when It comes to a real time case basis situation not many of the computer system security student are able to apply what they have learned in classes.

Thus, we do need a change in the academic syllabus by adding up a reliable security lab environment that consist of all three elements that

January - February 2020
ISSN: 0193 - 4120 Page No. 6003 - 6010

are the forensic environment, attacking basis environment and defensive basis environment. Forensic environment is including collecting and analysing physical and logical evidence, by providing corresponding tools and guided. Attacking basis environment is an environment aimed for advanced penetration testing and security auditing by providing tools which are geared towards various information security tasks. Lastly, defensive basis environment is a vulnerable environment for defending an attack. Therefore, a defensive testing environment is required as a safe place for security students to demonstrate their security knowledge, without disturbing a real live network environment.

The problem is, computer system security practitioner does not have a suitable environment to test out their skills and knowledge without breaching any law or misconduct security ethics. They normally have no problem in understanding the theory part of a syllabus but when it comes to practical part, they will normally have trouble with it as no defensive testing environment are available for them to test out their knowledge without breaching any law or misconduct security ethics.

Currently, there are some developer has released an environment for attack, but specific for one type of attack only such as Damn Vulnerable Web Application (DVWA), an open-source web applications attacks platform and Kioptrix VM, a virtual machines environment with system vulnerability. There is no single environment that can be used for all type of attacks. Security students had to setup a multiple environment for all these different types of attacks, which can become troublesome as some environment is not easy to setup.

## II. LITERATURE REVIEW

In literature, operating system in education has common vulnerabilities for security applications. In this section, we will start with usage of operating system in higher education environment and Linux as an operating system. Then proceed with the common vulnerabilities for security applications and finally the discussion on project related work.

### *A.* Operating System

An operating system is the most essential program that allows a computer's hardware to communicate with the software in order to allow the computer to run smoothly. According to "An operating system is defined as a program that acts as an intermediary between user of a computer and the computer hardware". concludes that a client application software requires a collection of system programs, tools and utilities that offer them general services and help to handle thecommunication between the application and the computer hardware. When an operating system (OS) is prompt first to boot the computer,the computer will manage tests to make sure all the computer hardware is working properly, check for new updates for the applications and software, and then the OS can focus to handle specific task.

It is important for a student to understand the importance of an operating system in the computerized system. However, it has been reported in previous studythat basic operating system skills are increasingly taken for granted. As argues that in education institutes, students are not taught on the practical fundamental of the computer system, whereby even in installing any additional software in the provided computer at institutes, the students must make a formal request to the IT department. Therefore, we see the need of having a free operating system for education purpose so that students in higher education can practice their knowledge without having to rely to the institute.

One of the free and flexible operating system available is Linux. Linux operating system has increasingly been used in education institution. Linux is an "open-source" software, in which the source code is freely available on the Internet and allows their user to personalize the OS to fit their requirement, unlike the other commercial OS. Based on [9], open source software is free to be obtained

*January - February 2020*
*ISSN: 0193 - 4120 Page No. 6003 - 6010*

and users can modify it, but with limitation to the kind of modification permissible. This shows that Linux OS can bethe best platform for both educators and students due to its combination of reliability and solution for desktop platform.

There has been some distribution of Linux that already cater the needs of students in higher education learning. The Linux distributions are Debian, Kali Linux and Ubuntu Operating System.

• Debian.This OS uses the Linux Kernel or the FreeBSD kernel. It uses deb package format and DPKG package manager to support many types of hardware platforms.

• Kali Linux.This OS is Debian-based Linux distribution. It has a particular usage compared to the Linux distributions. It is aimed for the use of Penetration Testing and Security Auditing. Several hundred tools for various information security related tasks are embedded in the OS. The tools are useful to perform penetration testing, do security research, executecomputer forensics tasks and to execute reverse engineering. Users can also customize the tools and the OS to fit to their needs.

• Ubuntu.This operating system is also based on the Debian GNU/Linux distribution focusing on the personal computer needs, although the server edition is also made available. Since Ubuntu are mainly designed for personal computers, their Graphical User Interaction (GUI)is customizable, making them popular among higher education students and researchers. With the use ofGNU General Public License, users can copy, change, develop and redistribute their own version of Ubuntu's software programs.

Based on the comparisons of Linux operating systems, we find Ubuntu OS is the perfect platform for this project that targeted students in higher education. Furthermore, previous studyhas also reported that some organizations develop free operating system's distributions based on Linux for students due to limitation access of the commercial OS, specifically the Window's Operating System.

### *B.* Common Vulnerabilities for Security Applications

An application vulnerability is a system flaw or weakness in an application that could be exploited to compromise the security of the application. Once an attacker has found a flaw, or application vulnerability, and determined how to access it, the attacker has the potential to exploit the application vulnerability to facilitate a cybercrime. These crimes target the confidentiality, integrity, or availability of resources possessed by an application, its creators, and its users. Attackers typically rely on specific tools or methods to perform application vulnerability discovery and compromise.

Based on Open Web Application Security Project (OWASP), an organization focused on improving the security of software, has release a top 10 vulnerability list on web applications in the past few years is included cross site scripting (XSS), command injections and file inclusion. stated that cross site scripting (XSS) is one of the most common application layer attack technique used by attacker to deface the website, manipulate or delete the content through inputting unwanted command strings.

A cyber-attack is any type of offensive action that targets computer information systems, infrastructures, computer networks or personal computer devices, using various methods to steal, alter or destroy data or information systems. A denial-of-service (DOS) attack is one of the cyber-attacks, it overwhelms a system's resources so that it cannot respond to service requests. A distributed denial-of-service (DDOS) attack is also an attack on system's resources, but it is launched from many other host machines that are infected by malicious software controlled by the attacker. stated that DOS attacks can come in many difference forms, by reducing system availability to the users.

TEST Engineering & Management

*January - February 2020*
*ISSN: 0193 - 4120 Page No. 6003 - 6010*

### *C.* Operating System as Learning Platform in Higher Education Environment

Many approaches have been explored for providing operating system as learning platform. Some of it is a project based on NetzTrack OS Project in German-Malaysian Institute. This is Linux Operating system which enhanced with advanced security features and all learning syllabus. This operating system is can be secured from any "silent" virus or other threats. It works well with security features combination of snort and other security features. All learning syllabus includes means it will save some students time to separately downloads these on their own. This project is dedicated to the students and lecturers in higher education.

According to research project of [10], they analysesSilverOS which is Silverlight operating system known as Web OS. It brings the convenience and comfort from classical desktop application into the browser. System host all the data and applications on the web, so they can get access from internet browser and not locally to anyone. In addition, the applications can do without installation and will be executed in draggable and resizable windows.

Other related work is by [5], they are created an education operating system based on Linux platform for the students of Coimbra College of Education. This project is based on Linux Ubuntu Operating system. This project also has pre-installed the necessary software needed through the course, new Graphical User Interface, and has developed USB and Live-CD distributions to simplify the installation process. In addition, it serves as an alternative so that the students can develop their assignments and projects.

All the related works show that the operating system tried to help the students in providing the tools for organization, storage as well as entertainment. Some effort needed to develop the operating system and facilitate the adaption of common users, students and lecturers to the Linux Operating System.

## III. METHODOLOGY

This section describes the methods and the methodology that have been using to implement in this project. The primary data sources and data collected will describe how the methods being used and how they were structured. This chapter shows how the project is fully developed starting from the first step such as data collection to the final touch of the project. The understandings of all the activity and process that involve in the development of this project will help to build a good project. Choosing the right application development model could help in ensuring the success of an application development project.

### *A.* Research Methodology Model

Rapid Application Development (RAD) model to complete the project. RAD methodology is a type of software development that does not spend a lot of time or resources on planning and instead uses a method of prototyping to introduce the product. A prototype is a version of the product that mimics what that actual product will look like, and it can complete the same functions. This allows for a faster output of the element being created.

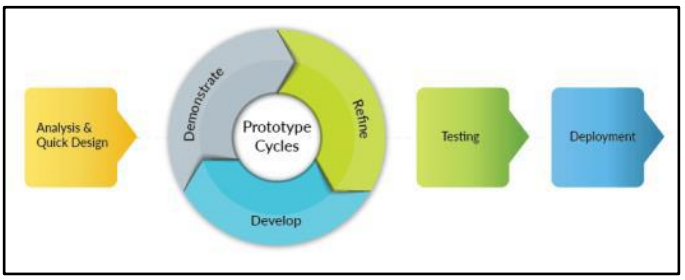


Figure 1 RAD Model

Without a plenty of preplanning in the development stage, the prototype can easily be altered to quickly make changes throughout the testing stages. The team of experts involved in the testing of the application prototype including the developers, customer service representatives, and IT

January - February 2020
ISSN: 0193 - 4120 Page No. 6003 - 6010

professionals need to work together in a forward motion to get the best version possible of the prototype. Then, a final product can be introduced to the customer much more quickly.

### B. Project Development

The main objective in developing this operating system is to provide a legal hacking environment for computer system security students training. It is focusing on preparing a defensive testing environment to test out the practical security knowledge. This operating system will be made intentionally vulnerable by including several types of system and web vulnerabilities into a single operating system. The type of Attacks the students can perform in this vulnerable operating system:

1. Web application attack such as cross site scripting, command execution and file inclusion.
2. Network attack such as Wi-Fi cracking, denial of service and buffer overflow.
3. Open service port such as SSH and Telnet service

We will now show the interface for each of the attack scope covered for this project. Figure 2 shows the interface of DVOS login screen. The default login credential for DVOS is “dvos” as username and “dvos” as password. Login credential is required to be able to enter the system.

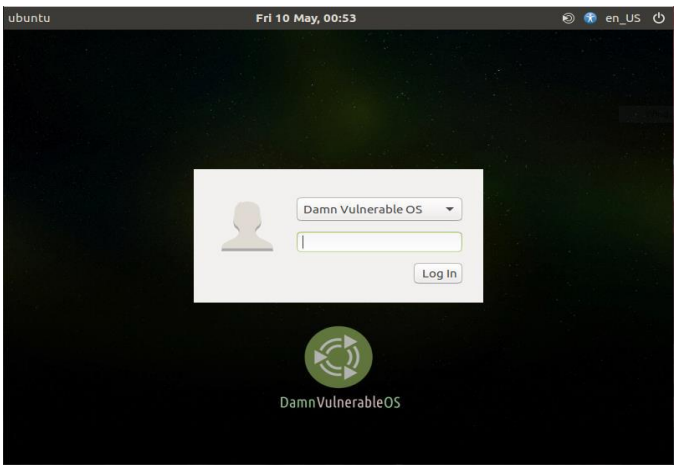


Figure 2 DVOS Login Screen


Figure 3 Welcome Panel

Figure 3 shows the interface of DVOS welcome panel. This panel will pop up every time user login into the system. From this panel, user can choose type of attack they want to practice. Figure 4 shows the interface of web attack panel. This panel will pop up when user click on web attack button on welcome panel. From this panel, user can check the web hosting status, restart and stop web server on DVOS.


Figure 4 Web Attack Panel

Figure 5 shows the interface of network attack panel. This panel will pop up when user click on network attack button on welcome panel. From this panel, user can start Wi-Fi cracking attack, detecting DOS attack and start buffer overflow attack. Lastly, in Figure 6 the interface of open services panel in shown. This panel will pop up when user click on open services button on welcome panel. From this panel, user can check the telnet and SSH server status.

January - February 2020
ISSN: 0193 - 4120 Page No. 6003 - 6010


Figure 5 Network Attack Panel

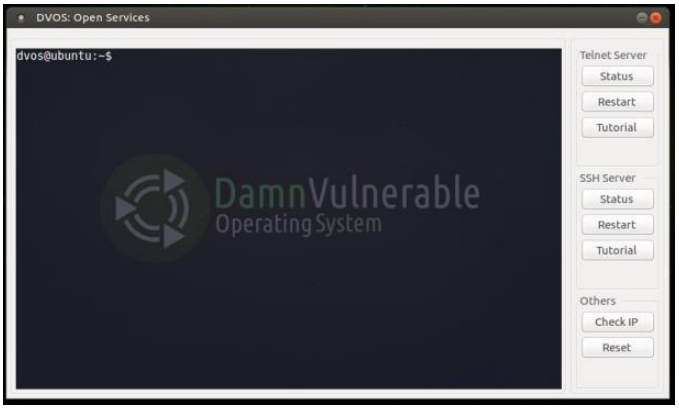


Figure 6 Open Services Panel

## IV. TESTING AND RESULT

The test results are described in this section. We conducted functional testing to check whether the vulnerable include in this operating system can handle an actual attack. In this section we will show the result of each functional testing.

Functional testing verifies the system's input-output behaviour. The black box testing method are used in functional testing. It is testing that ignore the internal mechanism of a system or component and focuses solely on the outputs generated in response to selected inputs and execution conditions.

All vulnerabilities process will be tested including web vulnerability Wi-Fi hotspot, detecting DOS attack and open services. This test involves by testingto make sure that each service is up and running. Table 1 to 4 shows the test case for each of the web vulnerability mentioned earlier. All of the tests are successful in achieving the expected results.

Table 1 Test Case for Starting Wi-Fi Hotspot

| | Details |
|---|---|
| Test Case ID | T01_NA_WC |
| Test Case Name | Testing Wi-Fi hotspot |
| Purpose | To test if the script can create a Wi-Fi hotspot for wireless cracking attack. |
| Initial Criteria | • User must make sure their devicenetwork adapter is supported for Wi-Fihotspot.<br>• User must specify their network adapter interface inLinux. |
| Execution Steps | 1. Launch DVOS welcome panelprogram.<br>2. Click on network attack button to open network attackspanel.<br>3. Click on start Wi-Fi Cracking button to enable the Wi-Fi hotspot. |
| Execution Results | The script will create a Wi-Fi hotspot with weak password, enable user to do a wireless cracking attack. |

Table 2 Test Case for Detecting DOS Attack

| | Details |
|---|---|
| Test Case ID | T02_NA_DD |
| Test Case Name | Detecting DOS attack using DOS detector |
| Purpose | To test if the script can detect a DOS attack on the server network. |
| Initial Criteria | User must have the DVOS IP address to send DOS attack. |
| Execution Steps | 1. Launch DVOS welcome panel program on DVOS computer.<br>2. Click on network attack button to open network attacks panel. |

January - February 2020
ISSN: 0193 - 4120 Page No. 6003 - 6010

| | |
|---|---|
| | 3. Click on start DOS detector button to start DOS detector program.<br>4. Launch LOIC, a network stress tools on another computer.<br>5. Enter DVOS IP address on LOIC, then click start attack. |
| Expected Results | The script will detect the DOS attack with an alert that indicate they are under attack. |

Table 3 Test Case for Telnet Service Status

| | Details |
|---|---|
| Test Case ID | T03_OS_T |
| Test Case Name | Testing Telnet Service |
| Purpose | To test if telnet service is running on server. |
| Initial Criteria | User must connect to any internet connection. |
| Execution Steps | 1. Launch DVOS welcome panel program.<br>2. Click on open services button to open services panel.<br>3. Click on telnet status button to check current telnet service status. |
| Execution Results | The terminal will show that the service is up and running, indicate that the server will accepting any incoming telnet connection. |

Table 4 Test Case for SSH Service Status

| | Details |
|---|---|
| Test Case ID | T04_OS_SSH |
| Test Case Name | Testing SSH Service |
| Purpose | To test if SSH service is running on server. |
| Initial Criteria | User must connect to any internet connection |
| Execution Steps | 1. Launch DVOS welcome panel program.<br>2. Click on open services button to open services panel.<br>3. Click on SSH status button to check current SSH service status. |
| Execution Results | The terminal will show that the service is up and running, indicate that the server will accepting any incoming SSH connection |

## V. CONCLUSION AND RECOMMENDATION

Based on this research, testing and comparison made with existing projects, this project has accomplished all the objective. The first objective is to study about common vulnerabilities for security applications. This objective has been achieved by studying the past journals and articles that related to Linux operating system and common vulnerabilities for security applications.

The second objective is to develop an operating system that intentionally vulnerable. There are three major types of attacks covered in this Damn Vulnerable Operating System(DVOS): web applications, open ports and network attacks. The attacks are based on the OWASP Top 10 vulnerability list for web application system. Testing on the functionality of each of the attack has been carried out and the DVOS was able to function accordingly. From the result, it shows that the operating system can handle all the vulnerabilities provided as discussed.

However, we have also found a limitation in the system. During the conversion of the operating system into an ISO image, the system file is limited to less 4GB of size only. This is because the

*January - February 2020*
*ISSN: 0193 - 4120 Page No. 6003 - 6010*

conversion will include all user data files, which including system cache created during development process. To solve this problem, all cache and junk file will be cleared before conversion process occurred.

For the future implementation, it is recommended the vulnerabilities provide in several difficulties. Currently, DVOS only provide an easy level of vulnerabilities only. Therefore, an addition of medium and hard level is highly recommended in future updates. Besides that, a support of 32-bit system type is also recommended in next updates. Currently, DVOS development only releasing a support of 64-bit system file only which is cannot run on outdated device with old CPU processor. If support for 32-bit device is developed, more devices will be able to run DVOS.

## VI. REFERENCES

[1] Brettel, M., Friederichsen, N., Keller, M., & Rosenberg, M. (2014). How virtualization, decentralization and network building change the manufacturing landscape: An Industry 4.0 Perspective. International Journal of Mechanical, Industrial Science and Engineering, 8(1), 37-44.

[2] Savery, J. R. (2015). Overview of problem-based learning: Definitions and distinctions. Essential readings in problem-based learning: Exploring and extending the legacy of Howard S. Barrows, 9, 5-15.

[3] Silberschatz, A., Gagne, G., & Galvin, P. B. (2018). Operating system concepts: 9th Edition. Wiley Publishing.

[4] Bassil, Y. (2012). Windows and Linux operating systems from a security perspective.arXiv:1204.0197, April 2012

[5] Dias, J., Tavares, S., Carvas, A., & Silva, P. S. (2012, June). Open source operating system for students: EOS Project. In Proceedings of the Workshop on Open Source and Design of Communication (pp. 79-83). ACM.

[6] Carl, G., Kesidis, G., Brooks, R. R., & Rai, S. (2006). Denial-of-service attackdetection techniques. IEEE Internet computing, 10(1), 82-89.

[7] Kiryakova, G. (2017). Application of cloud services in education. Trakia Journal of Sciences, 15(4), 277.

[8] Dawson, M., DeWalt, B., & Cleveland, S. (2016). The case for UBUNTU Linux operating system performance and usability for use in higher education in a virtualized environment.

[9] MacKinnon, J. G. (1999). The Linux Operating System: Debian GNU/Linux. Journal of Applied Econometrics, 14(4), 443-452.

[10] Garmpis, A., & Gouvatsos, N. (2012). Innovative teaching methods in operating systems: the Linux case. Innovative approaches in Education: Design and Networking.

[11] Johari, R., & Sharma, P. (2012, May). A survey on web application vulnerabilities (SQLIA, XSS) exploitation and security engine for SQL injection. In 2012 International Conference on Communication Systems and Network Technologies (pp. 453-458). IEEE.