KARYA ILHAM PUBLISHING
CONNECTING MINDS, BRIDGING IDEAS, INSPIRING READERS

Journal of Advanced Research in Computing and Applications

Journal homepage:
https://karyailham.com.my/index.php/arca
ISSN: 2462-1927

OSSTMM-Based Information Technology Security Testing Information System

Firkhan Ali bin Hamid Ali[1,*], M. Tarmizi Abd Wahab[1], Zubaile Abdullah[1], Kamaruddin Malik Mohamad[1]

[1] Faculty of Computer Science & Information Technology, Universiti Tun Hussein Onn, Malaysia

ARTICLE INFO

Article history:
Received 10 March 2025
Received in revised form 20 April 2025
Accepted 10 May 2025
Available online 3 June 2025

Keywords:
OSSTMM; security testing; information security

ABSTRACT

This Information Technology Security Testing Information System is developed based on the manual modules found in the Open-Source Security Testing Methodology Manual (OSSTMM). OSSTMM uses manual forms to enter information from security testing and observation for an information technology infrastructure. Methodology used in this study is Prototype Development Model. The study had produce information system for information security testing based on OSSTMM. The computerized information system will make it easier for users to enter, edit and view data and information that has been obtained from the information technology security testing system.

1. Introduction

The issue of security in the world of information technology is a very important matter and it is often discussed by information technology experts around the globe. Therefore, a process of testing the level of security for an information technology implementation needs to be done to meet the set security standards at least at a minimum level [1].

Therefore, a non-profit organization, the Institute for Security and Open Methodology (ISECOM) have taken a good initiative by developing a standard manual for testing security levels in the implementation of information technology. The manual is the Open Source Security Testing Methodology Manual (OSSTMM) [2].

OSSTMM is an evaluation manual to test the level of security for an information technology implementation, especially in its physical infrastructure [3]. It contains detailed guidance on practical testing and evaluation of test results reports.

This OSSTMM manual is in the form of forms and guides that can be printed or used digitally. The implementation of information technology implementation security testing can be done based on

[*] *Corresponding author.*
E-mail address: firkhan1977@yahoo.com

https://doi.org/10.37934/arca.39.1.2835

the guidelines contained therein [4]. Then some forms can be used to record and store information regarding the results of the tests that have been made.

The system developed is an OSSTMM-based Information Technology Security Testing Information System that can be accessed through a web browser and has its database to store the information from the security testing that has been done. OSSTMM was chosen as an information technology security testing methodology because it is based on open source and is still in manual form.

2. Methodology

The development of this information system is made using the System Development Life Cycle (SDLC) methodology. The use of SDLC can ensure that the system developed for an organization is able to meet the set objectives and comply with the planned current requirements.

The prototype model is used in the development of this system as shown in Figure 1. This prototype model has five implementation phases namely planning, analysis, design, implementation and prototype and; implementation and testing.

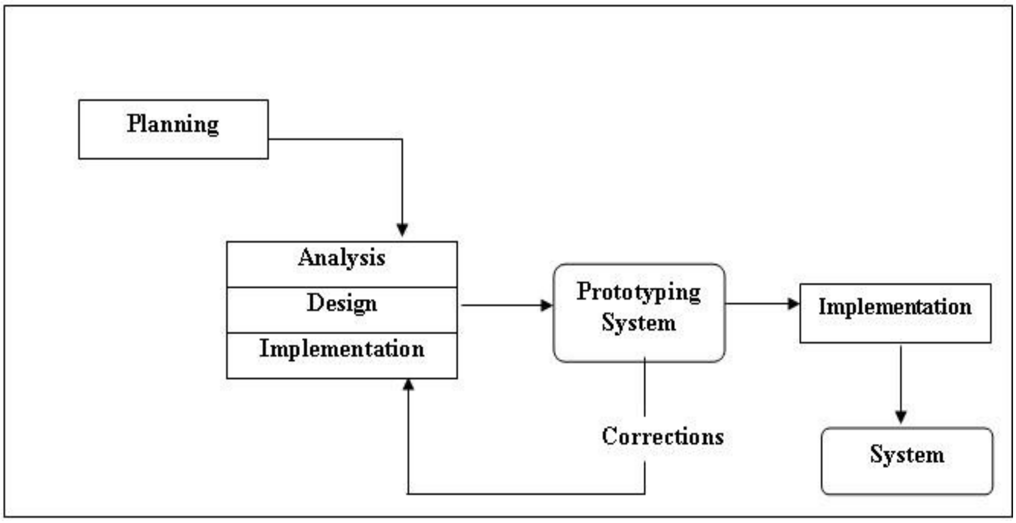


Fig. 1. Prototype development model

2.1 Planning phase

In this phase, the manual system found in OSSTMM information technology security testing needs to be studied more carefully and in detail. A planning schedule is also developed to facilitate the subsequent phases until this information system is successfully developed.

In addition, requirements such as hardware, software, work resources, and so on need to be determined immediately and accurately. It must be in accordance with the requirements of the information technology environment of the organization. In this project, a laboratory at the selected public university has been identified for the implementation of this project.

2.2 Analysis phase

All information related to the developed information system is collected and analyzed in more detail. The information system development strategy is also carefully studied so that it is compatible with the OSSTMM manual system. All hardware and software requirements are detailed more thoroughly.

In addition, the requirements in the OSSTMM information system are also identified so that it is developed in accordance with the needs of users and the OSSTMM manual. It also involves processes in identifying the programming language used, modules for users, and system requirements in the implementation of OSSTMM processes.

2.3 Design phase

The entire OSSTMM information system design is produced based on the results of a detailed analysis of the system and user requirements in the analysis phase. It involves the processes of designing user displays such as the system's user interface, the basic structures of the system, output design, and the identification of program codes for the system interface.

2.4 Design prototype and implementation

In this phase, all code programming processes are implemented based on the previous phases. Next, a prototype OSSTMM information system will be produced. However, in this phase, if there is a need or weakness, it will be repeated back to the analysis and design phase until the OSSTMM information system is able to function well and is accepted by users.

The database that has been designed in the previous phase will be developed along with the information system interface that has been identified. The process of repeating the previous phases will happen after the OSSTMM information system prototype is tested by developers and users.

2.5 Design testing and implementation

In this phase, the OSSTMM information technology security testing information system prototype model has been transformed into an information system that is ready to be fully implemented and adopted for real. The modules in the OSSTMM information system have been tested and run well in this phase. Next is testing acceptance by users to ensure that it coincides with the wishes and needs of users who will use it. Full testing will be done to this OSSTMM information system for the latest before it can be used by users. If it is successfully tested without errors and meets the wishes and needs of users, it will be implemented in the place where its use has been proposed.

3. System Design

This OSSTMM information technology security testing information system has been developed based on a web-based application that requires a web server in addition to a database to run it. It makes it easier for users to access this system because it can be accessed through any web browser in any operating system and anywhere through the network and the Internet [5].

The context diagram as shown in Figure 2 is developed to show how the developed OSSTMM information technology security testing information system interacts with end users and system administrators. It is a general overview of the entire OSSTMM information system and shows the relationship between entities and systems and inputs and outputs.

There are three entities that interact with this OSSTMM information system which are normal users, security analysts, and system administrators. Normal users are like superiors or certain people who need access only to reports of security testing results that have been made. Security analysts use it to see the guidelines in the implementation of security testing, enter test result information, update information, and see reports of security testing results that have been made [6].

While the system administrator acts as a coordinator for the OSSTMM information system such as verifying user status, adding items or attributes to the system, system maintenance, and so on. All users need to obtain confirmation from the system administrator first before being able to use this OSSTM information system.

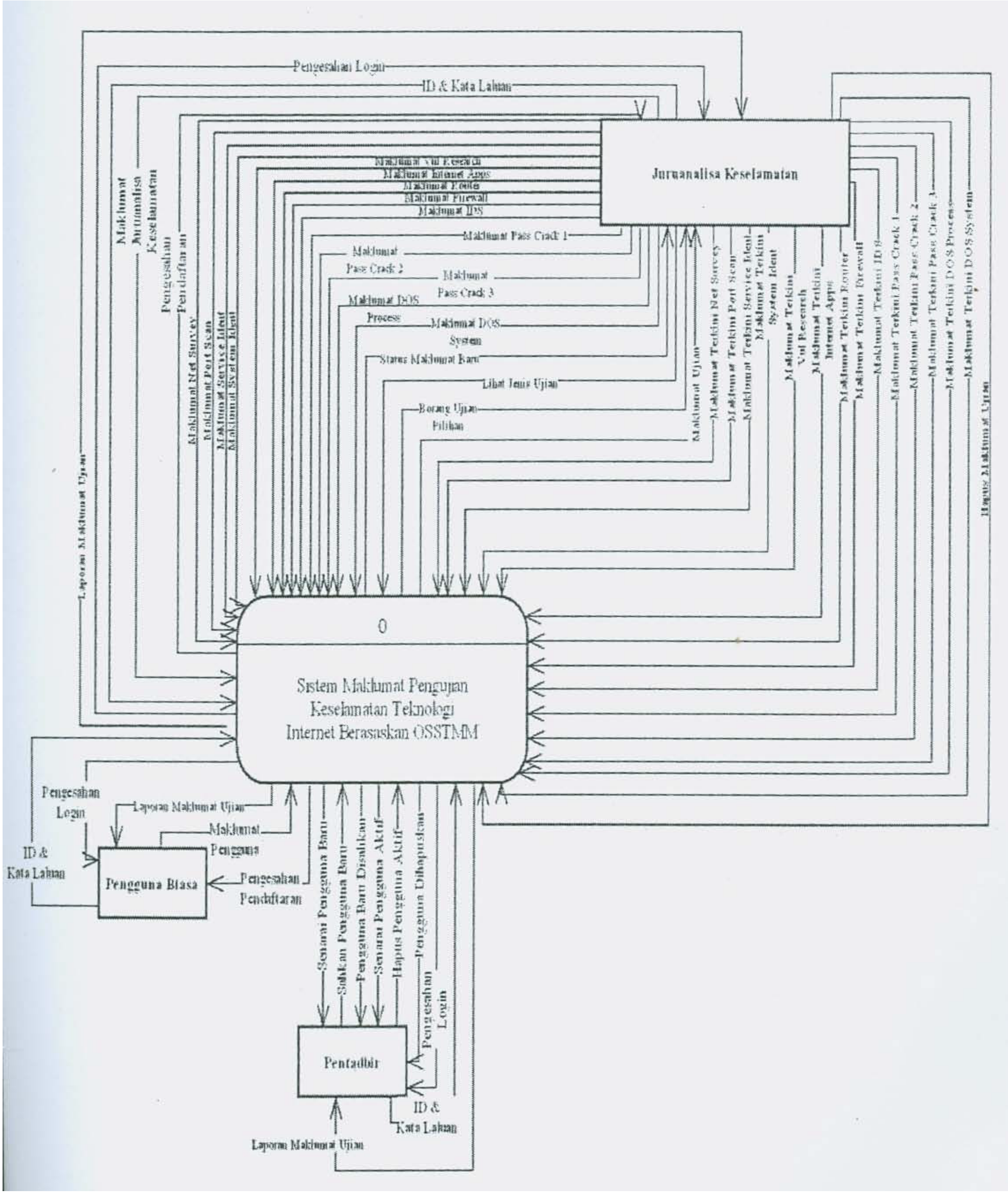


Fig. 2. Context Diagram

4. Results and Implementation

The OSSTMM information technology security testing information system has been developed in this study giving its main focus on developing the automation aspect of the computerized information system from the manual form system for OSSTMM-based information technology security testing.

One of its functions is to fill in, access and update information as a result of information technology security testing based on the OSSTMM method.

Users of this system must first register through the form provided on the website provided. Personal information as required must be registered first. In addition, registered passwords will be encrypted for security. Figure 3 is shown the entry menu into the system which is registration and entry for normal users, administrators, or security analysts.

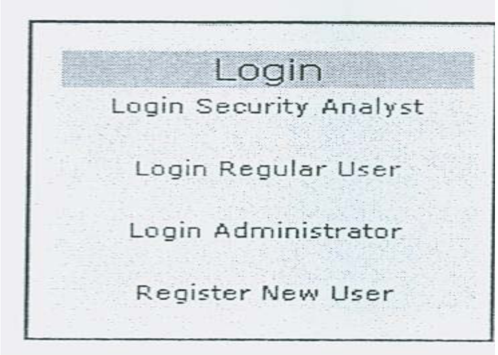


Fig. 3. Main menu

Once the registration is successful, the user can enter the system as shown in Figure 4.

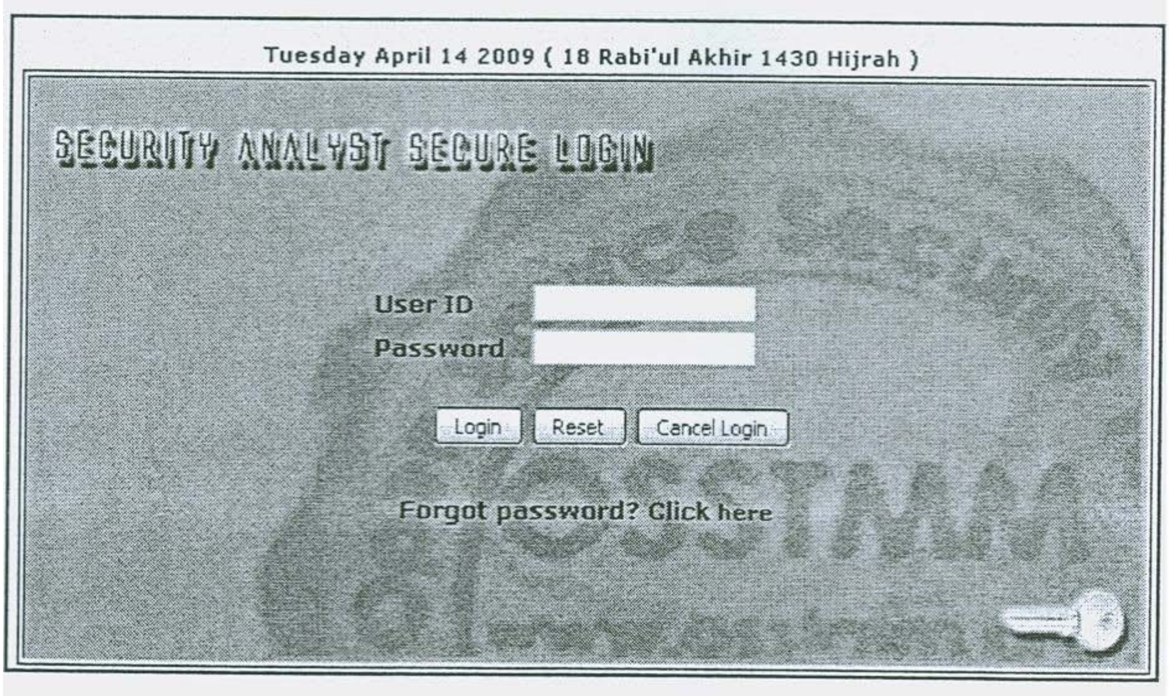
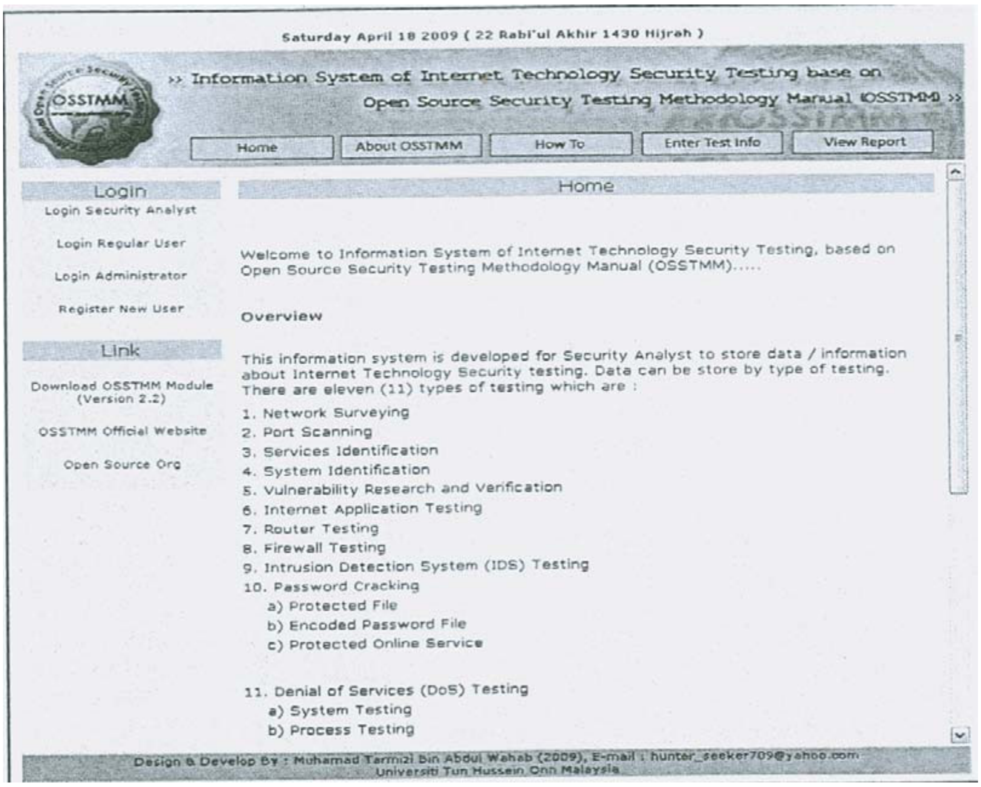

Tuesday April 14 2009 (18 Rabi'ul Akhir 1430 Hijrah)
SECURITY ANALYST SECURE LOGIN
User ID
Password
Login
Reset
Cancel Login
Forgot password? Click here
OSSTMM

Fig. 4. Login and password

Next is the main page for the OSSTMM information technology security testing information system as shown in Figure 5. The following Figure 6 is a homepage for security analysts to select the type of testing to be done. Figure 7 is the system page with one of the forms to enter information about a certain type of testing that has been done.



Saturday April 18 2009 (22 Rabi'ul Akhir 1430 Hijrah)

>> Information System of Internet Technology Security Testing base on Open Source Security Testing Methodology Manual (OSSTMM) >>

Home

Welcome to Information System of Internet Technology Security Testing, based on Open Source Security Testing Methodology Manual (OSSTMM).....

Overview

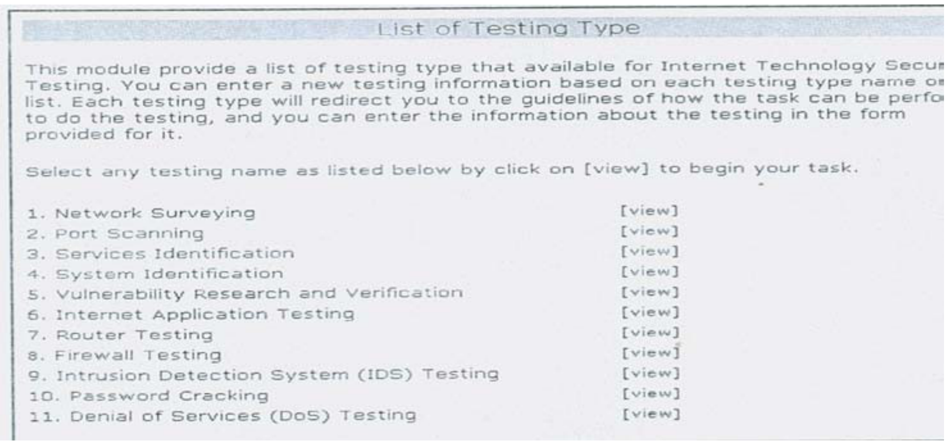
This information system is developed for Security Analyst to store data / information about Internet Technology Security testing. Data can be store by type of testing. There are eleven (11) types of testing which are :

1. Network Surveying
2. Port Scanning
3. Services Identification
4. System Identification
5. Vulnerability Research and Verification
6. Internet Application Testing
7. Router Testing
8. Firewall Testing
9. Intrusion Detection System (IDS) Testing
10. Password Cracking
    a) Protected File
    b) Encoded Password File
    c) Protected Online Service

11. Denial of Services (DoS) Testing
    a) System Testing
    b) Process Testing

Design & Develop By : Muhamad Tarmizi Bin Abdul Wahab (2009), E-mail : hunter_seeker709@yahoo.com
Universiti Tun Hussein Onn Malaysia

Fig. 5. Main page



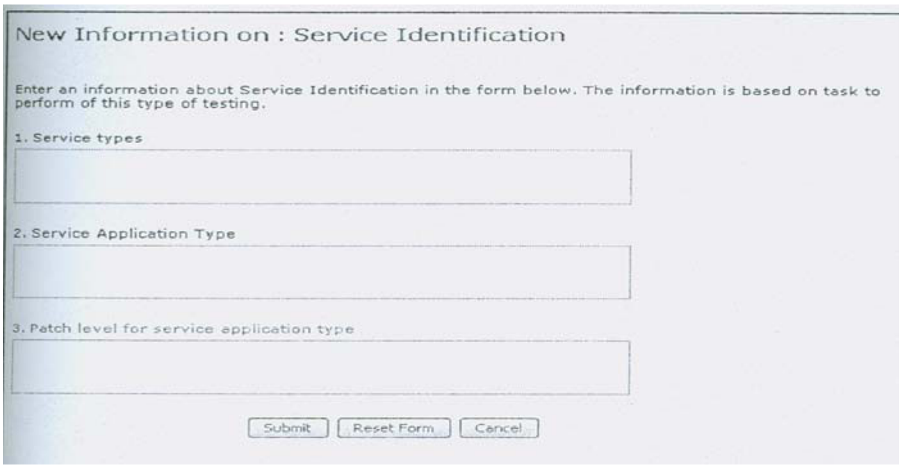
List of Testing Type

This module provide a list of testing type that available for Internet Technology Secur Testing. You can enter a new testing information based on each testing type name o list. Each testing type will redirect you to the guidelines of how the task can be perfo to do the testing, and you can enter the information about the testing in the form provided for it.

Select any testing name as listed below by click on [view] to begin your task.

1. Network Surveying	[view]
2. Port Scanning	[view]
3. Services Identification	[view]
4. System Identification	[view]
5. Vulnerability Research and Verification	[view]
6. Internet Application Testing	[view]
7. Router Testing	[view]
8. Firewall Testing	[view]
9. Intrusion Detection System (IDS) Testing	[view]
10. Password Cracking	[view]
11. Denial of Services (DoS) Testing	[view]

Fig. 6. Types of security testing



New Information on : Service Identification

Enter an information about Service Identification in the form below. The information is based on task to perform of this type of testing.

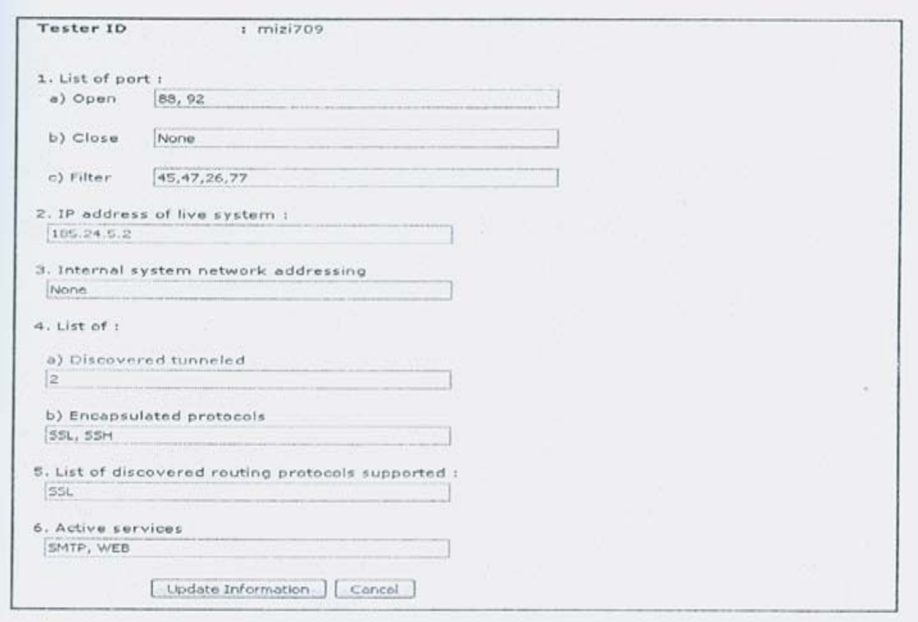
1. Service types

2. Service Application Type

3. Patch level for service application type

Fig. 7. Example of test information filling form

Figure 8 also shows examples of information technology security testing that has been entered and is ready to be updated if necessary.

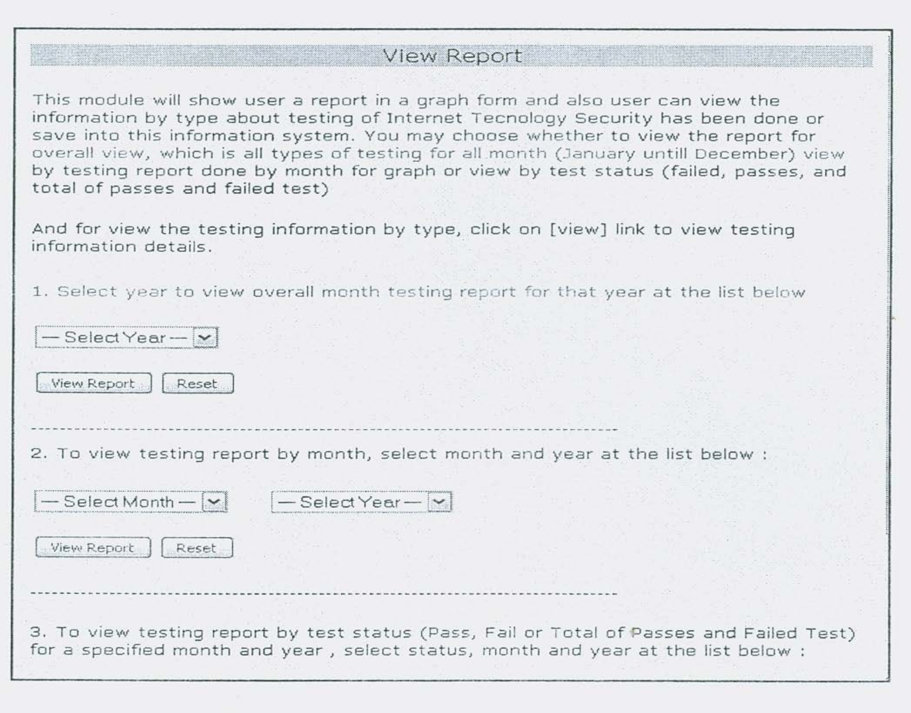


Tester ID : mizi709

1. List of port :
   a) Open 88, 92
   b) Close None
   c) Filter 45,47,26,77
2. IP address of live system :
   185.24.5.2
3. Internal system network addressing
   None
4. List of :
   a) Discovered tunneled
   2
   b) Encapsulated protocols
   SSL, SSH
5. List of discovered routing protocols supported :
   SSL
6. Active services
   SMTP, WEB

Fig. 8. Example of test result information

Figure 9 shows an example of a system page for generating a report on the results of the tests that have been carried out in the information system that has been developed.



View Report

This module will show user a report in a graph form and also user can view the information by type about testing of Internet Tecnology Security has been done or save into this information system. You may choose whether to view the report for overall view, which is all types of testing for all month (January untill December) view by testing report done by month for graph or view by test status (failed, passes, and total of passes and failed test)

And for view the testing information by type, click on [view] link to view testing information details.

1. Select year to view overall month testing report for that year at the list below

2. To view testing report by month, select month and year at the list below :

3. To view testing report by test status (Pass, Fail or Total of Passes and Failed Test) for a specified month and year , select status, month and year at the list below :

Figure 9. An example of a test result report generation form

That is the result of the implementation that has been developed OSSTMM information technology security testing information system that has been computerized from OSSTMM testing manual forms.

5. Conclusions

The development of OSSTMM's information technology security testing information system is to facilitate the process of maintenance and management of test information and information technology security testing results that have been made [7]. It facilitates the process of accessing, entering, and updating relevant information quickly, regularly, and easily. This OSSTMM testing method was taken because it has gone through a mature evaluation process by information technology security experts through the ISECOM organization and it is a testing technique based on open source.

However, the implementation scope is small in the implementation of this information system which is a laboratory at the selected public university. This is due to time and effort constraints in the development of this information system. The automatically generated report module in the form of a graph makes it easier for the management of an organization to see the information that is needed collectively and organized in order to make a decision.

The same is the case with web-based systems that allow it to be accessed easily and on various platforms through a web browser. However, there are some web browsers that display their interface in a messy form but the functions can operate well. Finally, this information technology security testing information system based on OSSTMM techniques can facilitate information technology security experts in handling testing information and test result information for the benefit of a company or organization in order to be able to operate better.

Acknowledgement
This research was funded by Universiti Tun Hussein Onn Malaysia.

References

[1] Falcón, Francisco Manuel Hilario, Milner David Liendo Arévalo, Giancarlo Sanchez Atuncar, and Ivan Crispin Sanchez. "Comparative study of computer security methodologies for countering cyber attacks." In *AIP Conference Proceedings*, vol. 2816, no. 1. AIP Publishing, 2024. https://doi.org/10.1063/5.0177434

[2] Nabila, Muhammad Alif, Putri Elfa Mas' udia, and Rachmad Saptono. "Analysis and Implementation of the ISSAF Framework on OSSTMM on Website Security Vulnerabilities Testing in Polinema." *Journal of Telecommunication Network (Jurnal Jaringan Telekomunikasi)* 13, no. 1 (2023): 87-94. https://doi.org/10.33795/jartel.v13i1.511

[3] Giuseppi, Alessandro, Andrea Tortorelli, Roberto Germanà, Francesco Liberati, and Andrea Fiaschetti. "Securing cyber-physical systems: an optimization framework based on OSSTMM and genetic algorithms." In *2019 27th Mediterranean Conference on Control and Automation (MED)*, pp. 50-56. IEEE, 2019. https://doi.org/10.1109/MED.2019.8798506

[4] Setiawan, Eko Budi, and Angga Setiyadi. "Web vulnerability analysis and implementation." In *IOP conference series: materials science and engineering*, vol. 407, no. 1, p. 012081. IOP Publishing, 2018. https://doi.org/10.1088/1757-899X/407/1/012081

[5] Ali, Firkhan Ali Bin Hamid, and Mohd Zalisham Jali. "Human-technology centric in cyber security maintenance for digital transformation era." In *Journal of Physics: Conference Series*, vol. 1018, no. 1, p. 012012. IOP Publishing, 2018. https://doi.org/10.1088/1742-6596/1018/1/012012

[6] Hamid Ali, Firkhan Ali, Mohd Khairul Amin Mohd Sukri, Mohd Zalisham Jali, Muhammad AlFatih Muhammad AlFatih, and Mohd Azhari Mohd Yusof. "Web-Based Reporting Vulnerabilities System for Cyber Security Maintenance." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 29, no. 3 (2023): 1-8. https://doi.org/10.37934/araset.29.3.198205

[7] Bin Hamid Ali, Firkhan Ali, Mohd Zalisham Jali, and Mohd Norazmi bin Nordin. "Preliminary Study on IT Security Maintenance Management in Malaysia Organizations." *PalArch's Journal of Archaeology of Egypt/Egyptology* 18, no. 1 (2021).