Portable Penetration Testing and Firewall Configuration Toolkit

Megat Ahmad Izzat Megat Ahmad Kamil
Malaysia Institute of Information Technology (MIIT), Universiti
Kuala Lumpur1016 Jalan Sultan Ismail, 50250 Kuala Lumpur
megatahmadizzat@me.com herny@unikl.edu.my
norhaizaya@unikl.edu.my

Norhaiza Ya Abdullah
Malaysia Institute of Information Technology (MIIT), Universiti
Kuala Lumpur1016 Jalan Sultan Ismail, 50250 Kuala Lumpur
megatahmadizzat@me.com herny@unikl.edu.my
norhaizaya@unikl.edu.my

Herny Ramadhani Mohd Husny
Malaysia Institute of Information Technology (MIIT), Universiti
Kuala Lumpur1016 Jalan Sultan Ismail, 50250 Kuala Lumpur
megatahmadizzat@me.com herny@unikl.edu.my
norhaizaya@unikl.edu.my

Abstract - **In the domain of security, a security officer must be offensive and also defensive. Being attack by attacker is not an option. They need to be creative, they have to think like them, and then only they can beat them. That is why leaning the arts of penetration testing is crucial in education level. On the other hand, let's not forget about the basic fortress off all time that is a must to protect a network, the firewall. To possess knowledge in security, early exposure must be nurtured from undergraduate level to ease the development of knowledge and learning process for a scholar. Current scholars who are studying in security field seldom have the opportunity to exercise hands-on activity in class due to time constraint and lack of infrastructure in an educational organization. To support the initiative of providing exposure among the scholars and to overcome the aforementioned problems, an approach to develop a portable penetration testing and firewall configuration toolkit has been proposed as a learning aid for the students to perform simulation on conducting penetration testing and configuring firewall for beginners. The scholars will be able to use this proposed toolkits to perform hands-on activity at anywhere and anytime. From the proposed toolkit, scholars are able to execute basic penetration testing, network monitoring, port scanning, firewall configuration, and web and filtering. By having this proposed toolkit, the teaching and learning process will be much easier, efficient and time saving compared to conventional methods of teaching. As a conclusion, the proposed plug-and-play toolkit implements benefit user in terms of time saving, early exposure and facilitate teaching and learning session effectively**

Keyword--security, penetration testing, firewall, it audit, information security, network security, system security.

1 INTRODUCTION

Portable Penetration Testing and Firewall Configuration Toolkit is a portable device that allows students to perform penetration testing and configuring firewall in a portable device. It will only be the size of a credit card can be plugged in into any HDMI monitor or TV. The idea of developing the Portable Penetration Testing and Firewall Configuration Toolkit is because the equipment in UniKL computer lab does not suffice to accommodate Bachelor of Information Technology (Hons) in Computer System Security (BCSS) degree programme students to exercise penetration testing and firewall configuration hands on during lab. Apart from that, the device is aim to provide exposure towards BCSS students on how to configure firewall on physical device.

2 RELATED WORK

The proposed toolkit is implemented with two (2) modules, penetration testing and firewall configuration. The related work will cover both aspects.

2.1 **Penetration Testing Distribution**

There are several Linux operating system distributions that are geared up to suit penetration testing requirement. The operating system distribution is preconfigured and packaged with the tools needed by the penetration tester to perform penetration testing.

Kali Linux is a successor to BackTrack, which underwent a massive architecture restructuring. It was build based on Debian based architecture. Unlike BackTrack, all the tools in Kali was selected according to most relevant and most updated specifically for suitability according to today's security threat and exploit. Rapid7 re-engineered its Metasploit framework to be compatible with Debian's packaging requirements making Metasploit is now more deeply integrated into the system, making it more stable and robust. Kali is also available to ARM based device. This allows users to implement Kali on the Raspberry Pi minicomputer or Samsung's ARM Chromebook and other ARM based device.

2.2 Firewall

IPFire is an Open Source firewall distribution for x86 and ARM based systems. It turns the Raspberry Pi computer into a configurable firewall for home networks and very small businesses. As the Raspberry Pi computer comes natively with only one network interface card, it works perfectly as a 3G router without plugging in additional hardware. By using the IPfire Linux distribution, user are able to have their own portable physical firewall connected between their router and computer.

2.3 Existing Tools

Electronic lock is a locking device, which operated by means of electric current. Nowadays, there are many types of electronic locks and authentication methods. The general brief for each authentication method for electronic lock verification and electronic lock with biometric base that available in market as listed in Table 1.

TABLE 1 : COMPARISON OF EXISTING PORTABLE PENETRATION TESTING TOOLKIT

Product	**PWNIE EXPRESS**	**Integrated Penetration Testing Platform**
Processer	**2core Intel i5 processor (4 cores w/HT), 2.66GHz**	**1.2 GHz Armada-370 CPU**
Memory	**8GB DDR3 memory**	**1GB DDR3**
Storage	**60GB internal solid-state storage**	**32GB microSDHC (Class 10)**
Network	**Onboard high-gain 802.11 a/b/g/n wireless supporting packet injection & monitor mode**	**High-gain 802.11b/g/n, packet injection & monitor mode, 8” External antenna**
	Onboard high-gain Bluetooth (up to 1000’ range) supporting packet injection & monitor mode	**External wireless 802.11b/g/n & Bluetooth adapters supporting packet injection**
	External 6-band (worldwide) 4G GSM cellular USB adapter	**2x Gigabit Ethernet**
	External 10/100 USB Ethernet Adapter (for 2nd wired network interface)	**External high-gain Bluetooth adapter (up to 1000’ range) supporting packet injection & monitor mode**
Power Output	**15 watts**	**5 watts idle, 15 watts max**
Dimension	**21.59cm x 19.05cm x 6.35cm**	**11.4cm x 20cm x 0.865cm**
Price	**$USD3,895.00 (RM12534,11)**	**$USDI, 095.00 (RM 3523,71)**

3. THE PROPOSED SYSTEM

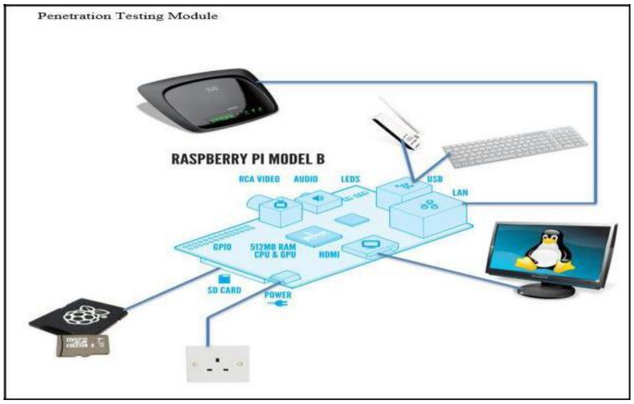

Figure 1 ; Initial sketch of penetration testing module

The Raspberry Pi will act as the main body of the penetration testing distribution. The monitor, keyboard, and mouse will be connected to it and act as input and output device. User can choose either to use LAN port or wireless adapter to establish network on the penetration testing distribution. The SD Card will store the operating system for penetration testing. The configuration for hardware is shown as in Figure 2.

.

Fig. 2: Main Interface of penetration testing module

As the distribution is based on Linux and the device that runs it is resource limited, most of the tools are in command line interface (CLI). The main screen for the penetration testing distribution is plain and simple as the Raspberry Pi has limited specification and will need more resource to display more graphics. But the statistics for each main function of the machine are visible in the left top corner of the screen to acknowledge user about real-time hardware condition

4. RESULT AND CONCLUSION

The testing phase includes User Acceptance Testing, Unit Testing and Integration Testing. Details of each testing are listed in Figure 3, Table 2 and Table 3.

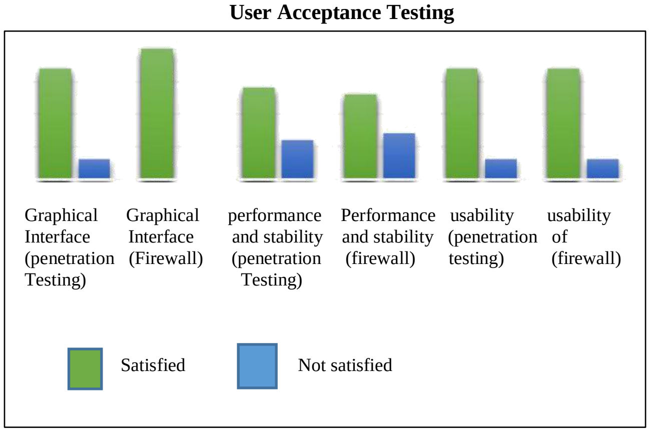

Fig. 3: Result of User Acceptance Testing

As summary, most of the user satisfied with the Graphical Interface, Performance and Stability and Usability of both subsystems.

4.2 Unit Testing

TABLE 2 : RESULT OF UNIT TESTING

No	Test Case	Description	Subsystem	Result
1.	Booting up the device	Perform testing on booting up and operating the device	Penetration Testing Distribution	The device passed all three tests and are ready for next testing phase
			Firewall Distribution	The device passed all tests and are ready for next testing phase

4.3 Integration Testing

TABLE 3 : RESULT OF INTEGRATION TESTING

No.	Test Case	Description	Subsystem	Result
1.	Booting up the device with keyboard, mouse, and wireless adapter attached	Perform testing on booting up and operating the device with keyboard, mouse, and wireless adapter attached to the device	Penetration Testing Distribution	The device with keyboard, mouse, and wireless adapter attached passed all three test and are ready for next testing phase
2.	Testing the capability of TP-Link WN722N Wireless Adapter to perform network monitoring and packet injection	Perform testing on the capability of TP-Link WN722N to perform packet injection	Penetration Testing Distribution	The device can integrate and work without problem with TP-Link WN722N Wireless Adapter
3.	Booting up the device with keyboard, mouse, and Ethernet adapter attached	Perform testing on booting up and operating the device with keyboard, mouse, and Ethernet adapter attached to the device	Firewall Distribution	The device with keyboard, mouse, and Ethernet adapter attached passed all three test and are ready for deployment phase

Result from Unit Testing and Integration Testing shows that both subsystem which is Penetration Testing Distribution and Firewall Distribution are ready for deployment and fulfill the system specification and requirement.

4.4 Conclusion and Future Enhancement

Portable Penetration Testing and Firewall Configuration Toolkit is a project that can be useful to be used as a teaching aid to BCSS students to perform simulation on penetration testing and hands-on on firewall configuration. The device will provide students with benefits in terms of reducing time constraint, with its plug n play features and small form factor. Apart from being portable and time saving, the device is very affordable.

For future improvement, resizing the device with a built-in 5-inch monitor is an ease towards user. Hence the user will not require a HDMI monitor every time they want to use the Portable Penetration Testing and Firewall Configuration Toolkit.

4.5 Acknowledgments

We would like to acknowledge and express our gratitude to Universiti of Kuala Lumpur for funding our final year project.

4 REFERENCES

[1] Wack, J., Tracy, M., & Souppaya, M. (2003). Guideline on Network Security Testing. Nist special publication, 800, 42.

[2] Duan, B., Zhang, Y., & Gu, D. (2008, November). An Easy-to-Deploy Penetration Testing Platform. In Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for (pp. 2314-2318). IEEE.

[3] Upton, E., & Halfacree, G. (2012). Raspberry Pi User Guide. John Wiley & Sons.

[4] Kubitza, T., Pohl, N., Dingler, T., Schneega B. S., Weichel, C., & Schmidt, A. (2009). One Size Doesn't Fit All.

[5] Jyoti Sharma. (2012). Software Prototyping, Retrieved November 14 2013, from http://www.blog.gurukpo.com/software-prototyping

[6] Liao, M. K. (2003). U.S. Patent No. 6,544,075. Washington, DC: U.S. Patent and Trademark Office.

[7] Rowett, K. J., Sikdar, S., & Yukelson, M. (2006). U.S. Patent Application 11/382,327.

[8] Coley, C. D., & Wesinger Jr, R. E. (1998). U.S. Patent No. 5,826,014. Washington, DC: U.S. Patent and Trademark Office.

[9] Aho, A. V., Gitlin, R. D., Ramjee, R., & Woo, T. Y. C. (2001). U.S. Patent No. 6,198,941. Washington, DC: U.S. Patent and Trademark Office.

[10] Xiao, H. (2003). U.S. Patent No. 6,663,420. Washington, DC: U.S. Patent and Trademark Office.