Low Cost Network Penetration Device Using Raspberry Pi

Adam Bin Ibrahim
Faculty of Electrical Engineering
University Teknologi MARA (UiTM)
40450 Shah Alam, Selangor, Malaysia
Adamibrahim1987@gmail.com

***Abstract*—Network penetration testing basically known as the proses of actively and systematically testing a deployed network in order to determine the security weakness of the network and what vulnerabilities may be present. Based on the penetration test report, the action can be taken to mitigate or resolve the vulnerabilities of the network. The portable penetration device are quiet costly and penetration tester commonly use a laptop with Kali Linux installed to performed the test in order to save cost without purchasing any portable penetration device. This paper presented how to setup the low cost penetration device by using Raspberry Pi and Kali Linux. By installing Kali Linux at the Raspberry Pi board, a simple penetration test is being conducted with virtual penetration lab that have been created by using GNS3 and verified that Raspberry pi with Kali Linux are suitable acting as penetration device. This experiment also shown the performance between Raspberry Pi and Laptop are quiet similar in term of scanning time of Nmap tool when performing Discovery Scanning, Port Scanning, Fingerprinting and Vulnerability Scanning.**

Keywords*—*Penetration test, Kali Linux, Raspberry Pi, Nmap tool, GNS3, and Virtual Box.

I. INTRODUCTION

Nowadays, attacks against computer systems and the data in the systems are increasingly frequently as internet connectivity increasing which is a millions of new devices attached to the global network [1]. Security-conscious organization always trying to understand what possible weakness of their deployed network rather than just a paper–based analysis of the documented system [1].

By hiring the penetration testers, the vulnerabilities of the network can be determine and with the created report by the tester, the step can be taken in order to mitigate or resolve the vulnerabilities of the deployed network. Penetration test are similar to a hacking which is seeking to breach a network system but with the objective of improve of the network security. Penetration tester only focusing only on a probe of the network without continuing to exploit and cause malicious damage to the network[2][1].

There are a couple of penetration devices available in the market but in term of price these penetration devices are quiet expensive. Thus, many of the penetration tester use Kali Linux with the laptop as a device of the penetration test in order to save cost without buying an expensive penetration device. Kali Linux are free Debian-derived Linux distribution designed for Penetration Testing.

In this research, the Raspberry Pi computer is being setup as a penetration device by installing Kali Linux as it operating system. The main objective of this research are to setup a Raspberry Pi as penetration device and to compare its capabilities with the capabilities of the laptop as penetration device.

In the section 2, there are information about Raspberry Pi and the cost between Raspberry Pi, laptop and the standalone penetration device is being represented. The initial step to setup Raspberry Pi as penetration device is being presented in the section 3 and also the method how to perform penetration testing is being presented in the same section. In the section 4, the discussion of the achieved result is being presented and in the last section are the conclusion and the future work about this research.

II. LITERATURE REVIEW

A. What is Raspberry Pi

Raspberry Pi is a small size, hackable, and cheap computer board that been introduced in 2012. Its performance and cheap price are suitable for interfacing with many devices.

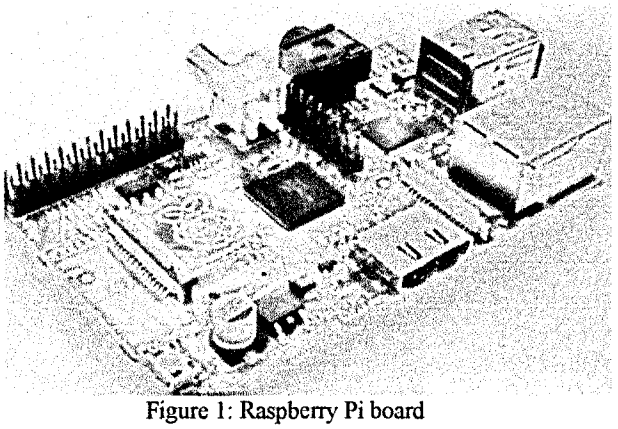

Figure 1: Raspberry Pi board

The Raspberry Pi board contains a processor and graphics chip, program memory (RAM) and various interfaces and connectors for external devices (Fig. 1). Some of these devices are essential, others are optional but all Raspberry Pi models

have the same CPU named BCM2835 which is cheap, powerful, and it does not consume a lot of power [2].

B. Kali Linux

Kali Linux (Kali) is a Linux distribution system that was developed with a focus on the penetration testing task. Previously, Kali Linux was known as **BackTrack**, which itself is a merger between three different live Linux **penetration testing** distributions.

C. Comparison between penetration device

The cost and size of the penetration device is being compared between each other in order to find the lowest cost for penetration device. For Pwn Plug device, although their size are quiet small and portable, the cost for this device are quiet expensive for the penetration tester. Thus, many penetration tester used laptop with kali Linux installed as the penetration device in order to reduce the cost without buying any penetration device. But with the Raspberry Pi, it can be setup as penetration device and the cost are very cheap and it has high portability compare to the existing penetration device. It also has low power consumption and can be power up through USB 5V which is very low power required for this device to be operate compare which the other device.

III. METHODOLOGY

A. Installing Kali Linux as Operating System

Kali Linux is being used as operating system because it's been created for the purpose of penetration test. The Kali Linux Custom Arm image for Raspberry Pi is being downloaded from https://www.offensive-security.com/kali-linux-vmware-arm-image-download/ and have been write to the SD card by using Win32 Disk Imager. Before it can be used through SSH, the Raspberry pi is being connected through HDMI to monitor in order to configure it until can be fully functioning as penetration device. The command Apt-get Update and Apt-get Upgrade is being used in order to upgrade and update the operating system with the new and updated toolset for penetration test.

B. Remotely Access Raspberry Pi through SSH

Secure Shell (SSH) give a full access to the Raspberry Pi operating system from a remote location. It is the common way to manage Linux system using a command line instead of using GUI since GUI are not needed for the most penetration testing. The Raspberry pi is being connected to the LAN port of the Laptop and being statically configure using static address in order to easily been access from Windows 8 through SSH. Putty is being used as a software to access Raspberry Pi through SSH from Window 8 laptop. Some of tool required some GUI order to be used, X Ming software is being install at Window 8 in order to open the GUI from Raspberry Pi in the new window at Window 8.

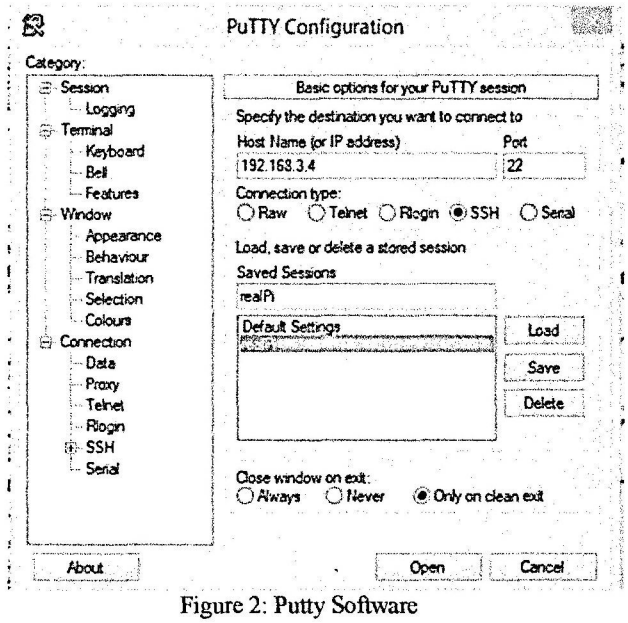

Figure 2: Putty Software

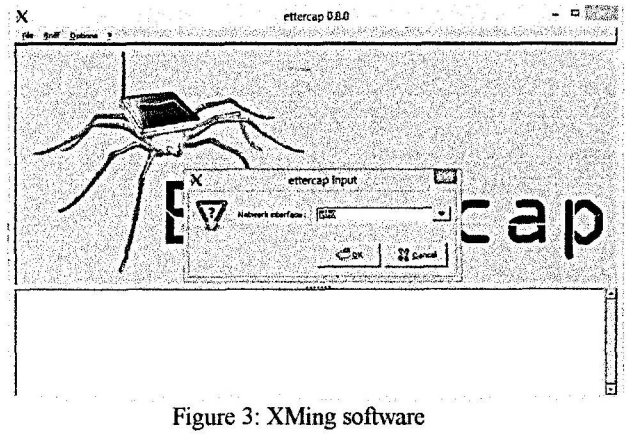

Figure 3: XMing software

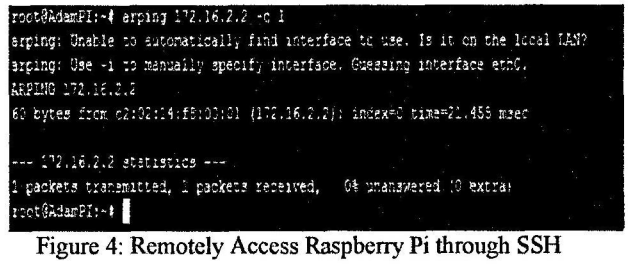

Figure 4: Remotely Access Raspberry Pi through SSH

C. Virtual Lab using GNS3

For penetration test we need to be authorized in order to test it at the real network environment. Since we don't have an authorization to any real network environment, the penetration test is being test on the virtual network lab created by using GNS3 (Graphical Network Simulator). Three of Cisco Router, VirtualBox Window XP, VirtualBox Kali Linux and VirtualBox Metasploitable is being using for this virtual lab. No security configuration is being implemented on this virtual lab. The

capability and performance of the Raspberry Pi as penetration device is being test on this virtual lab.

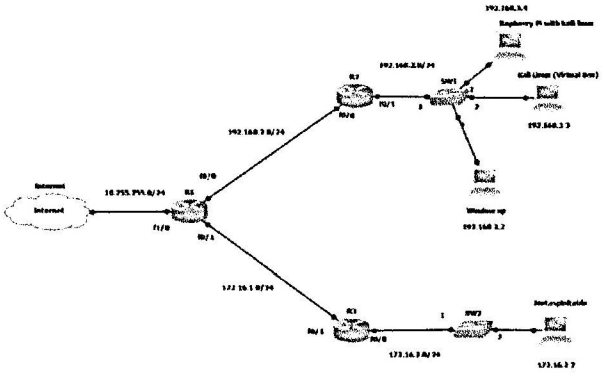

Figure 5: Virtual Lab Topology

For this virtual lab, all the operating system that connected to this network can passing access the internet from the router R1. The EIGRP routing Protocol is being used as in order for the provided connection between host to host even their not in the same LAN group.

- Virtual Box Windows XP

Windows XP is the older operating system and since that, it has many flaws and vulnerabilities that can be exploited in test environment. By enabling of functional service and disabling the security service on this window can increase the risk of compromise.

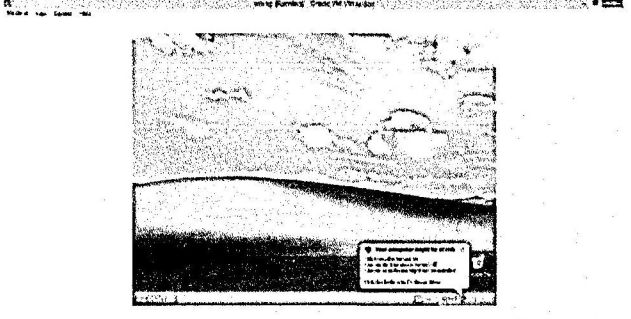

Figure 6: Win XP

- Virtual Box Metasploitable

Metasploitable2 is an intentionally vulnerable Linux distribution and is also a highly effective security training tool. It comes fully loaded with a large number of vulnerable network services and also includes several vulnerable web applications.

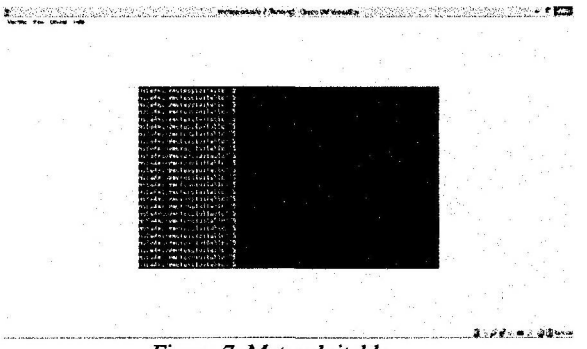

Figure 7: Metasploitable

- Virtual Box Kali Linux

We used virtual Box Kali Linux by installing the image from www.kali.org to the Virtual Box software in order to comparing the performance in term of time taken when performing penetration test. The setting for this Kali Linux is been set to 1GB RAM and 2G RAM with the single processor.

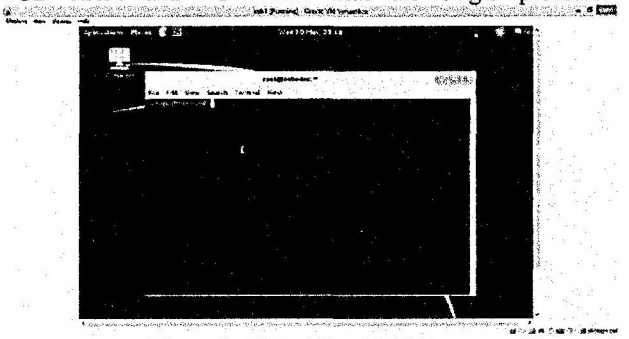

Figure 8: Virtual Box Kali Linux

D. Penetration Test

Penetration testing with the Network Scanning method with is consist of a couple of the step to discover the network. Then the test proceed to Man in the Middle attack.

- Network Scanning

This method are important in penetration test since it can discover the network map and what vulnerabilities can be exploit. In this researched, Nmap tool is being used because it can performance all the step required for network scanning.

1. Discovery Scanning

Discovery scanning are the process of identifying the live on a network. In context of penetration test, this process are performed to identify the potential target to attacks. This process are not exhaust the resources in gathering information about the targets but to finds out were the target are logically located. This method used to find operating protocols at layer 2, layer 3, and layer 4 in the OSI model [3].

1.1. Layer 2 and Layer 3 scanning

Layer 2 and Layer 3 scanning is being performed by using this command:

root@KaliLinux:~# nmap 172.16.2.0-255 –sn

for network 192.168.3.0

root@KaliLinux:~# nmap 192.168.3.0-255 –sn

1.2. Layer 4 scanning
For TCP protocol this command have been used:
root@KaliLinux:~# nmap 192.168.3.0-255 -PA80 -sn
root@KaliLinux:~# nmap 172.16.2.0-255 -PA80 –sn

For UDP protocol this command have been used:
root@KaliLinux:~# nmap 192.168.3.0-255 -PU53 -sn
root@KaliLinux:~# nmap 172.16.2.0-255 –PU53 –sn

2. Port Scanning
Identifying open ports on a target system is the next step to defining the attack surface of a target. Open ports correspond to the networked services that are running on a system. Programming errors or implementation flaws can make these services vulnerable to attack and can sometimes lead to total system compromise. To determine the possible attack vectors, one must first enumerate the open ports on all of the remote systems within the project's scope. These open ports correspond to services that may be addressed with either UDP or TCP traffic. Both TCP and UDP are transport protocols. Transmission Control Protocol (TCP) is the more commonly used of the two and provides connection-oriented communication. User Datagram Protocol (UDP) is a non-connection-oriented protocol that is sometimes used with services for which speed of transmission is more important than data integrity. These techniques should yield enough information to identify whether a service is associated with a given port on the device or server [3].

2.1. UDP scanning Command
root@KaliLinux:~# nmap 172.16.2.2 -sU -p 1-1000
root@KaliLinux:~# nmap 192.168.3.2 -sU -p 1-1000

2.2. TCP Stealth command
root@KaliLinux:~# nmap –sS 172.16.2.2 -p 1-1000
root@KaliLinux:~# nmap –sS 192.168.3.2 -p 1-1000

2.3. TCP connect command
root@KaliLinux:~# nmap –sT 172.16.2.2 -p 1-1000
root@KaliLinux:~# nmap –sT 192.168.3.2 -p 1-1000

3. Fingerprinting
After identifying live systems on the target range and enumerating open ports on those systems, it is important to start gathering information about them and services that are associated with the open ports. These techniques will include banner grabbing, service probe identification, operating system identification, and Firewall identification [3].

3.1. Banner Grabbing
root@KaliLinux:~# nmap -sT 172.16.2.2 -p 1-100 --script=banner
root@KaliLinux:~# nmap -sT 192.168.3.2 -p 1-100 --script=banner

3.2. Service Identification
nmap 172.16.2.2 –sV
nmap 192.168.3.2 –sV

3.3. OS identification
nmap 172.16.2.2 –O
nmap 192.168.3.2 –O

3.4. Firewall Identification
nmap -sA 172.16.2.2
nmap -sA 192.168.3.2

- Man in the Middle Attack

This method is performed as to capture sensitive information from the attacked host or server. It's also means that attacker makes independent connections with the attacked host while actively eavesdropping the communication. This attack also can lead to denial of service. For this attack, Ettercap tool being used in order to become the man in the middle between Virtual box Win Xp to the internet.

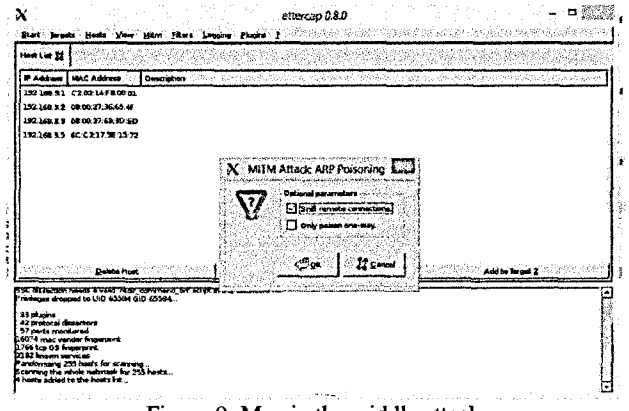

Figure 9: Man in the middle attack

IV. RESULT AND DISCUSSION

The performance of raspberry pi as penetration device is being examine by monitoring the scan time of Nmap tool when performing network scanning. The result are comparing between two devices that running Kali Linux which is Raspberry Pi and VirtualBox with 2GB RAM and 1 GB RAM.

Discovery Scanning

Network 192.168.3.0-255 Nmap tool

Discovering scanning	Scan time (s)		
	Raspberry pi Kali linux	Virtualbox Kali linux (1GB RAM)	Virtualbox Kali linux(2GB RAM)
Layer 2 and Layer3 Scanning	2.76	2.48	2.32
Layer 4 Scanning (TCP)	2.71	2.55	2.49
Layer 4 Scanning (UDP)	2.67	2.58	2.46

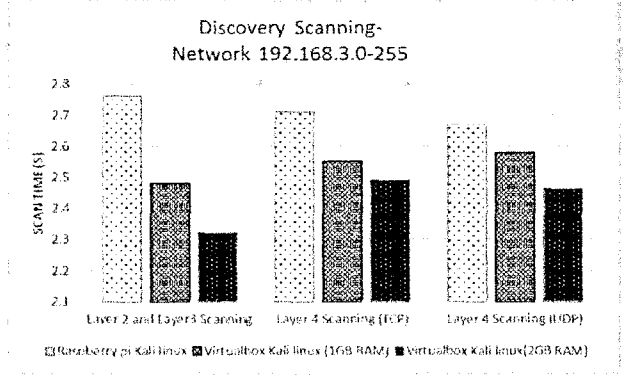

Figure 10: Discovery Scanning Scan time -192.168.3.0-255

Network 172.16.2.0-255 Nmap tool

Discovering scanning	Scan time (s)		
	Raspberry pi Kali linux	Virtualbox Kali linux (1GB RAM)	Virtualbox Kali linux(2GB RAM)
Layer 2 and Layer3 Scanning	23.32	23.27	22.07
Layer 4 Scanning (TCP)	5.15	4.87	4.71
Layer 4 Scanning (UDP)	5.34	5.03	5.01

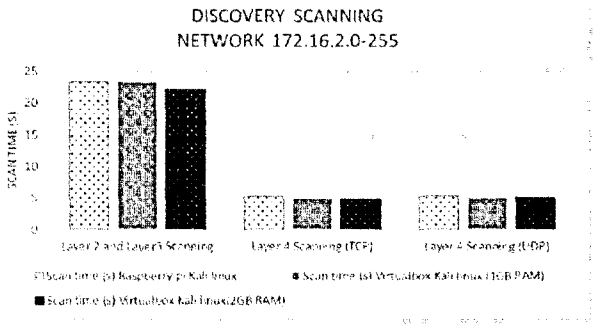

Figure 11: Discovery Scanning Scan time- 172.16.2.0-255

From the figure 10 and figure 11, when performing discover scanning which is consist of layer 2, layer 3, and layer 4 scanning, the time taken for scanning using Raspberry pi quiet similar with time taken for scanning using VirtualBox 1GB RAM and 2GB RAM. For network 192.168.3.0-255, time taken for Raspberry pi to discover live host at this network are 2.76 second while for VirtualBox 1GB RAM are 2.71 second and VirtualBox 2GB RAM are 2.67 second. The different for the time taken using Raspberry Pi are 0.05 and 0.09 second delay only. And when scanning network 172.16.2.0-255, this three device taken more time to scan since the network are not in the same LAN and must go through four hops to reach the network. But, the scanning time of those three device are quiet similar only with the different maximum 1.3 second when perfoming layer 2, layer 3 scan and maximum 0.5 second different when performing layer 4 TCP scan and Layer 4 UDP scan Thus, the capability for Raspberry Pi to perform discovery scanning are quiet similar when using Laptop with 1GB Ram and 2GB RAM.

Port Scanning

Host 192.168.3.2 (Win XP) Nmap tool

Port Scanning	Scan time (s)		
	Raspberry pi Kali linux	Virtualbox Kali linux (1GB RAM)	Virtualbox Kali linux(2GB RAM)
UDP Scanning	3.59	2.14	1.87
Stealth TCP Scanning	2.55	0.96	0.72
Connect TCP scanning	2.53	0.98	0.7

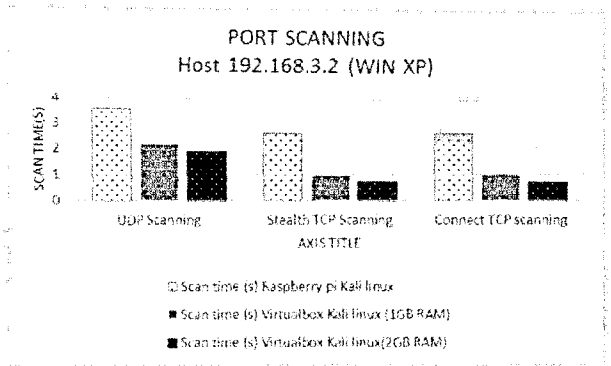

Figure 12: Port Scanning Scan time- 192.168.3.2

host 172.16.2.2 Nmap tool

Port Scanning	Scan time (s)		
	Raspberry pi Kali linux	Virtualbox Kali linux (1GB RAM)	Virtualbox Kali linux(2GB RAM)
UDP Scanning	1081.01	1078.84	1072.47
Stealth TCP Scanning	17.16	15.94	15.63
Connect TCP scanning	20.18	20.11	18.56

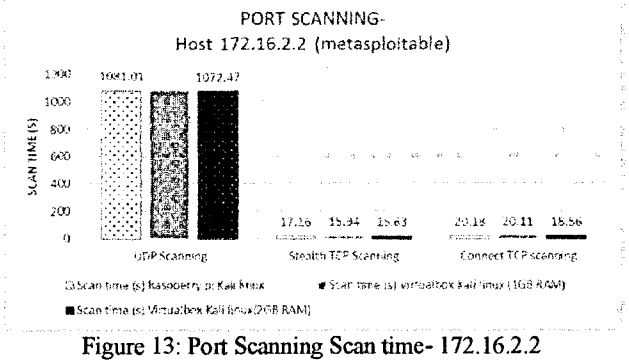

Figure 13: Port Scanning Scan time- 172.16.2.2

Port scanning are process of identifying of open port that correspond to the service that may be addressed with either UDP or TCP traffic. UDP scanning can often be challenging and time consuming but with Nmap tool, this scanning become more easier since Nmap are most effective tool to identify the UDP service on remote systems. Figure 12 and figure 13 shown that the result of UDP scanning perform by Raspberry pi , virtualbox 1GB RAM and virtualbox 2GB RAM on the live hosts that we have discover earlier using discovery scanning which is Windows XP and Linux Metasploitable. When performing UDP scan on Windows XP the time taken was faster compare to the time taken when performing on the Linux Metasploitable which is consume the time up to 1000 seconds using those three device. This is because Win XP are in the same LAN with the penetration device while Linux Metasploitable are 4 hops away from the penetration device. And also, by default the UDP scan will scan 1000 port on the remote system. Since there are a lot of open port at Linux Metasploitable compare with Win XP, the penetration device need a lot of time to identify the service that associates with the open port.

While for TCP scanning, it's consist of two techniques which is Stealth scanning and Connect scanning. The time taken by this three device are quiet similar since the TCP scan are more faster compare to UDP scan. Raspberry Pi are capable to perform port scanning as good as Laptop with 1GB Ram or 2GB RAM since the different of time taken are around 1.8 seconds.

Fingerprinting

host 192.168.3.2 Nmap tool

Fingerprinting	Scan time (s)		
	Raspberry pi Kali linux	Virtualbox Kali linux (1GB RAM)	Virtualbox kali linux(2GB RAM)
Banner Grabbing	12.81	11	10.73
Service Identification	10.8	7.66	7.13
OS identification	18.1	3.39	2.8
Firewall Identification	2.65	0.85	0.67

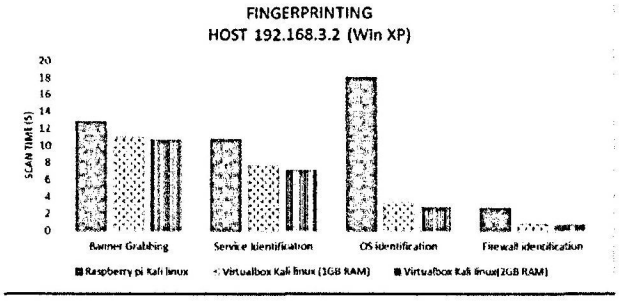

Figure 14: Fingerprinting Scan time- 192.168.3.2

host 172.16.2.2 Nmap tool

Fingerprinting	Scan time (s)		
	Raspberry pi Kali linux	Virtualbox Kali linux (1GB RAM)	Virtualbox Kali linux(2GB RAM)
Banner Grabbing	27.93	26.67	24.27
Service Identification	31.41	28.73	27.51
OS identification	32.97	22.31	16.61
Firewall identification	15.76	15.09	14.1

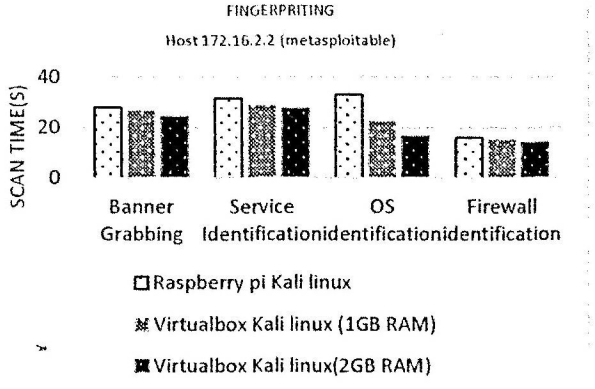

Figure 15: Fingerprinting Scan time- 172.16.2.2

Fingerprinting are the process of gathering information about the services that associates with the open port. For the banner grabbing, only full connect scan can be used since the service banner only can be collected when a full TCP connection is established. The open port that have been collected earlier is being applied with the banner grabbing scripts. The time taken for banner grabbing on Win XP are more faster since its open port are less compare to the Linux metasploitable. The performance for this three device are almost the same performance even the raspberry pi have lowest RAM and processing speed still it can performance well in the fingerprinting process. But, for the OS identification, on the both system, the time taken for Raspberry Pi to complete the OS identification technique are longer than other two device. This is because by using Nmap, it sends a comprehensive series of probing requests and then analyzes the responses to those requests in attempt to identify the underlying Operating system based on OS-specific signatures and expected behavior. To analyze the response faster required more processing speed and RAM. Thus the time taken by the Raspberry Pi to perform OS identification are much longer compare with other two device.

Man in the middle attack

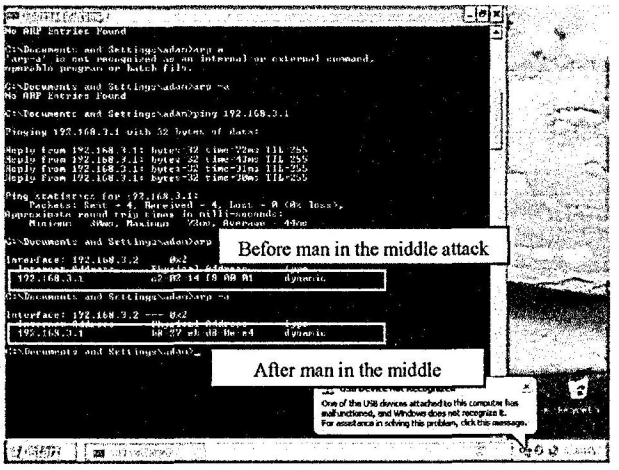

Figure 16: Man in the middle attack using Ettercap

Figure 17: Https attack using sslstrip

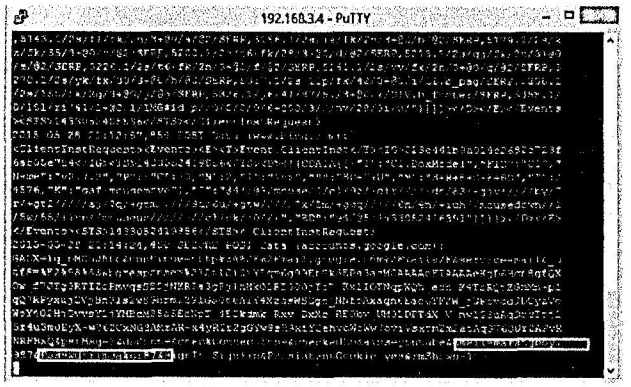

Figure 18: sslstrip log

Man in the middle attack is being perform using Ettercap tool and the attack using Win XP as a primary target and its default gateway as secondary target. By using Ettercap, it can be seen from figure 18 that before the attack the layer 2 address of its default gateway are the address of the router R2 interfaces. After the attack being launch, the physical address of its default gateway are the address of the raspberry pi. All the traffic from Win XP to the internet are going through the Raspberry Pi first. Without forward any ipv4 traffic at Raspberry Pi, this can leading the DOS (Denial of service) at the WIN XP to the internet. By enable ipv4 forward, the raspberry pi acting as the man in the middle and eavesdrop the information from the Win XP to the internet.

After become the man in the middle, the SSlstrip tool is being used to beat HTTPS since web server use SSL encryption and all the information is being encrypted. By using this tool, when a user of WIN XP access their gmail/facebook account, a response from the web server is being change from HTTPS to HTTP traffic. Thus when user enter its username and password, the information are in the plain text and can be seen in the SSLstrip log as in figure 18.

V. CONCLUSION

As the conclusion, Raspberry Pi are capable to become low cost penetration device since the performance of itself are quiet similar with the laptop performance. For the future, by using Kali linux as operating system with the upcoming Raspberry Pi 2, its can be one of the powerful device for the penetration testing and the cost of the device also same with the oldest one.

ACKNOWLEDGMENT

It is a pleasure to acknowledge my supervisor Professor Madya Dr. Mat Ikram Bin Yusof for kindness, guidance and support throughout project preparation and implementations. The cooperation, support and assistance from my colleague are really appreciated to finish this project within the time frame.

REFERENCES

[1] K. Xynos, I. Sutherland, H. Read, E. Everitt, and A. Blyth, "Penetration Testing and Vulnerability Assessments: A Professional Approach," *Proc. 1st Int. Cyber Resil. Conf.*, no. August, 2010.

[2] V. Vujović and M. Maksimović, "Raspberry Pi as a Wireless Sensor Node : Performances and Constraints," *Inf. Commun. Technol. Electron. Microelectron. (MIPRO), 2014 37th Int. Conv.*, no. May, pp. 1247–1252, 2014.

[3] J. Hutchens, *Kali Linux Network Scanning Cookbook*.

[4] F. Kaup, P. Gottschling, and D. Hausheer, "PowerPi: Measuring and modeling the power consumption of the Raspberry Pi," *39th Annu. IEEE Conf. Local Comput. Networks*, pp. 236–243, 2014.

[5] R. Shanmugapriya, "A study of network security using penetration testing," *2013 Int. Conf. Inf. Commun. Embed. Syst.*, pp. 371–374, 2013.

[6] S. Banerjee, D. Sethia, T. Mittal, U. Arora, and A. Chauhan, "Secure sensor node with Raspberry Pi," *IMPACT 2013 - Proc. Int. Conf. Multimed. Signal Process. Commun. Technol.*, pp. 26–30, 2013.

[7] M. Kochláň, M. Hodoň, L. Čechovič, J. Kapitulik, and M. Jurecka, "WSN for Traffic Monitoring using Raspberry Pi Board," vol. 2, pp. 1023–1026, 2014.

[8] M. I. P. Salas and E. Martins, "A Black-Box Approach to Detect Vulnerabilities in Web Services Using Penetration Testing," vol. 13, no. 3, pp. 707–712, 2015.

[9] K. Raguvaran, "Raspberry PI Based Global Industrial Process Monitoring Through Wireless Communication," no. February, 2015.

[10] B. Varghese, N. Carlsson, G. Jourjon, A. Mahanti, and P. Shenoy, "Greening Web Servers : A Case for Ultra Low-power Web Servers," 2014.