

Project Report

by Aaron Lee Cowdry

FILE	17216_AARON_LEE_COWDRY_PROJECT_REPORT_78196_1727258992 .DOCX (481.41K)		
TIME SUBMITTED	05-MAY-2016 02:32PM	WORD COUNT	3835
SUBMISSION ID	57263023	CHARACTER COUNT	23886

**SECURITY PENETRATION TESTING WITH
ORACLE VM VIRTUALBOX AND KALI LINUX,
WIRELESS SOLUTIONS**

by

Aaron Lee Cowdry

Supervisor: Dr Carlene E-A Campbell

Second Marker: Dr Kapilan Radhakrishnan

Project submitted as part of the requirements
for the award of BSc (Hons) Computer Networks

May 2016

Declaration of Originality

I, Aaron Lee Cowdry declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

This work has not previously been accepted as part of any other degree submission.

Signed :

Date :

FORM OF CONSENT

I Aaron Lee Cowdry hereby consent that my Project, submitted in candidature for the B.Sc.(Hons) Computer Networks degree, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

Signed :

Date :

Copyright Acknowledgement

I acknowledge that the copyright of this project report, and any product developed as part of the project, belong to University of Wales Trinity Saint David, Swansea.

TABLE OF CONTENT

Table of Content

List of Figures

List of Tables

Acknowledgements

Copyright Acknowledgement.....	ii
CHAPTER 1 - INTRODUCTION	1
1.1 Introduction.....	1
1.2 AimS.....	2
1.3 Objectives.....	2
CHAPTER 2 - RESEARCH & REVIEW OF LITERATURE.....	3
Introduction	3
Wireless Network Attacks	3
Man In The Middle Attack	3
Denial OF SERVICE (DOS) ATTACK.....	3
MAC ADDRESS SPOOFING.....	4
PENERTRATION TESTING METHODS	4
WIRELESS SECURITY	6
CHAPTER 3 - RESEARCH METHODOLOGY	8
Introduction	8
Research Overview	8
3.1.1 Research Philosophy & Approach.....	8
3.1.2 Research Strategies.....	9
3.1.3 Data Collection	9
3.1.4 Reliability and validity	10
3.1.5 Triangulation.....	10
CHAPTER 4 - DESIGN & IMPLEMENTATION	11
4.1 Introduction.....	11
4.2 problem formulation	11
4.3 Design	12

4.3.1 Virtual Machine Configuration.....	12
4.3.2 Windows Server 2012 Configuration	13
4.3.3 Windows 7 Client Configuration.....	14
4.3.4 KALI LINUX Client Configuration.....	15
4.4 Implementation.....	15
4.5 Conclusion.....	15
CHAPTER 5 – REFERENCES.....	17

LIST OF FIGURES

Figure 1 - Initial Network Design.....	11
Figure 2- Virtual Machines Configuration	12
Figure 3- Windows Server Configuration	13
Figure 4- Windows 7 Client.....	14
Figure 5- Kali Linux Client	15

ACKNOWLEDGEMENTS

Include any acknowledgements you may have in this section.

CHAPTER 1 - INTRODUCTION

1.1 INTRODUCTION

According to Cisco [1], Network Security is the protection of services and data that exist on the network. Network attacks come in many variations and the most common include; Viruses, Hacker attacks, Denial of Service (DOS) attacks and Data interception attacks.

These types of security breaches can cause major disruption to organisation operations and in some cases their reputations may be damaged. The Internet service provider, TalkTalk Telecom Group PLC is an example of this: the company suffered from a suspected Distributed Denial of Service attack; millions of customers' payment details were also stolen by the hackers and posted online [2]. The company has recently placed a £35 million figure on the security breach and is predicting a major loss in the revenue [3].

A virtualised network has been created, where penetration testing can test the security features of the network. Wi-Fi has been used as the local area network solution. The virtualisation software chosen is Oracle VM VirtualBox. Virtual Box is a type two hypervisor and runs in conjunction with a current host operating system. The virtualised network consists of a Windows Server (2008 R2) with three Windows clients connected wirelessly. In addition, to the Windows clients a Kali Linux client will be introduced into the network. Kali Linux is a security penetration testing software that offers a range of security tools that will allow the testing of the virtualised wireless network. The same test will be repeated to the evaluation effectiveness of security features added to the network. Security features such as firewalls, intrusion detection and logging events on the network could be added to prevent unauthorised access.

1.2 AIMS

The main aim of the project is to investigate penetration testing, by carrying out an experiment to evaluate the effectiveness of security in a wireless networks. The experimental aspect will use a number of attacks to carry out the evaluation of the virtualised network.

1.3 OBJECTIVES

- Review the current literature with in the field of security and penetration testing to ensure that the research is valid and appropriate.
- Carry out an investigation into the use of Kali Linux in the penetration testing of a wireless local area network.
- Compare the results of the wireless penetration techniques; with and without the configuration of security features.
- Analyse information captured from wireless networks in the local geographical area to in order evaluate the security of these networks. This will determine if the network is vulnerable to a security attack.

CHAPTER 2 - RESEARCH & REVIEW OF LITERATURE

INTRODUCTION

WIRELESS NETWORK ATTACKS

MAN IN THE MIDDLE ATTACK

Yuan et al [4], defines a Man in the Middle (MITM) attack as an interception of traffic between two computers. Usually in a wireless environment the attacker uses a Rogue Access Point that is not part of the usual network. A Rogue AP captures packets and potentially modifies them or analyse the packet depending upon the type of encryption. The paper states that a critical part of a MITM attack is the relying on the host to associate with the Rouge AP. Once the association between the host and the AP is complete the host believe the AP is a legitimate AP and part of the network.

DENIAL OF SERVICE (DOS) ATTACK

According to SANS Institute [6], a DOS attack can be targeted against both a wireless and wired network. DOS attacks are normally achieved by sending amount of packets to request a service, application or device being utilised on the network. The aim of such attack would be to exhaust a server, router or access point capability of handling such traffic. The paper further describes the types of DOS attacks that are targeted at particular network layers. Application layer attacks are the most common DOS attack used; attacks at the application layer involve the targeting of networking applications such as HTTP. An example attack would be HTTP flood attack using the SYN and SYN ACK packet types. DOS application layer attacks can be highly effective when targeted at wireless networks, resulting in complete network loss or degraded performance. In addition, the paper further describes attacks at the network layer: it identifies that wireless access points with no security access configured are more likely to be exposed to this type of attack. ICMP flooding is an example of an attack at this layer. Compton [6] describes this attack as "The ICMP flood attack works by an attacker sending so many ICMP ECHO REQUEST packets to the target wireless system that it cannot respond fast enough to ease the amount of traffic." Furthermore, Compton [6] states that attackers may spoof the source IP address;

this would allow the attacker to use all the network's services. The network will be forced to use all of its resources to process packets that are being sent from the attacker's IP address. This would potentially cause quality of service to be degraded and potentially stop the wireless network from operating completely. This is caused by the attacker consuming the available network bandwidth. The paper [6] further describes the DOS attacks at the MAC layer; this type of attack used a spoof MAC address of a wireless access point. The client receiving the spoofed packets cannot differentiate from the legitimate and illegitimate packets and requests being made.

MAC ADDRESS SPOOFING

Huang et al [7], identifies that the MAC layer of IEEE 802.11-based WLAN is a high risk of attacks. The paper identifies that MAC address spoofing would allow an attack to initialise many types of attacks including denial of service attack and a man in the middle attack. Furthermore, the paper points out that wireless security protocol such as WEP, WPA and WPA 2 only offer protection upon data transmission of the data from the source. Huang et al [7], go on to discuss the protection protocols such as the Microsoft PANS protocol and Lancaster protocol and the current ineffectiveness of these protocol to prevent attacks targeted at the MAC address layer and in particular the protection against MAC address spoofing attacks.

PENERTRATION TESTING METHODS

Johns [8] describes that techniques and tools required to carry penetration testing in a wireless environment. These techniques and application are directly related to penetration testing that were carried out in the experimental part of this project. Johns [8]explains and evaluated the use of wireless penetration testing tools such as: NetStumbler, WEP Crack, aircrack and Metasploit. The publication does not directly discusses the use of Kali Linux or of these techniques in a virtualised environment but the publication does offer an in-depth investigation on wireless penetration testing techniques that are used in industry and could be applied in the implementation stage of the project.

Mehta et al [9] investigates the use of mobile devices using an android operating system installed with Kali Linux and an application called Connector that analysis information related to username and passwords. The paper goes on to describe the how they used Kali Linux to set up a rouge Wi-Fi access point also known as an Evil twin and the use Wire shark, a tool that Kali Linux to capture wireless packets. This research is similar to the proposed project but the project apply some of the similar tool and attack types available used in this example.

Buchanan [10] in addition to Mehta investigation describes the use of similar penetration techniques in a Microsoft/Linux network environment. The publication describes in-depth the process of creating a venerable machine in the windows environment. It states to create vulnerabilities on a network creating service on a network must be made venerable such as a DNS server being placed in position that could be compromised on a wireless network.

Buchanan [8] describes the methodology for cracking WEP using a penetration tool available in Kali Linux application called Airbase in addition Python and iptables are used to create the environment to effectively crack WEP. The publication [8] describes in detail the process of cracking WEP and setting up the network infrastructure on the Kali Linux side of the wireless network. In addition, Buchanan [8] investigates the process of cracking WPA-2. This is done by capturing the WPA-2 handshakes using again Airbase that could potentially reveal sensitive information about that network and its configurations. Furthermore the procedure of creating a man in the middle attack is described this type of attack is created using the Airbase -ng application with in Kali Linux. This also included using a MAC filter tool, this allows for specific devices to targeted by an attack rather than attacking every device with the access points range. The publication [8] describes how to DNS spoof a wireless device using a specific command within airplay called airplay-ng. These types of techniques and methodologies are similar to what the project aimed to achieve with in the virtualised network, the techniques are not specific to the Windows wireless network environment but are related to

tools with in Kali Linux. Buchanan [8] research does not provide any examples for implementing these types of attacks in Oracle VM VirtualBox.

Allen et al [11], states that wireless penetration testing techniques can be carried out in a virtual machine environment. It recommends the use of Oracle VM VirtualBox and Kali Linux to evaluate the security on of a Network. The publication does not discuss the use of Kali Linux in a wireless penetration testing situation.

WIRELESS SECURITY

Lashkari et al, [12] investigate the effectiveness of the most common wireless security protocols that are actively used in wireless networks today, such as WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA2/802.11i (Wi-Fi Protection Access, Version 2). In addition, the paper identifies the main security weakness with the various security protocols. The paper identifies WEP as being the most redundant and lease secure protocol. The paper identifies the protocol as having a faulty RC-4 algorithm, allowing brute-force attacks to be possible due to a poor and weak encryption key. It highlights the simple procedure imitate and replay encrypted packets to gain access to the protected data and the simple to process to modify encrypted data and forge authentication packets.

Lashkari et al [4], further identifies characteristic and faults of WPA and WPA2.

Vanhoef and Piessens [13], paper investigates the vulnerabilities that are common with WPA2 (WPA-TKIP). The paper looks at the use of TKIP in networks and highlights the problems with TKIP as a wireless security protocol. It describes TKIP as an improved version of WEP but uses the faulty the MIC algorithm. In addition, TKIP uses the same faulty RC-4 algorithm that is present in WEP.

Vanhoef and Piessens [13], research finds TKIP is still used in high number of networks despite the well documented faults. The paper included an investigation of commercial areas in Belgian and states that 71% of networks surveyed use or supported TKIP, with 19% of the networks solely using TKIP in their wireless network. It is also noted that 14% of the wireless networks use WEP as their choice security protocol. Vanhoef and Piessens concludes that TKIP is still in operation today could be down to the reason that routers and access points

configured by default to use a mixed security mode, this would allow the use of both TKIP and the more secure CCMP.

Dobrilovic et al [14], paper investigates the wireless security options available, such as WEP, 802.1x Extensible Authentication Protocol (EAP), WPA, WPA2 and WPS. The paper involves carrying out a survey of wireless networks in a number of geographical locations. The purpose of this was to evaluate and survey the type of security that wireless networks were using. Dobrilovic et al [6], used Wardriving techniques and software to gather the information and document the types of wireless security such WEP, WPA and WPA2. They also investigated the number of wireless networks using WPS.

Dobrilovic et al. [14] study evaluated the security of nearly 3000 networks in Serbia in a period of almost a year. The investigation concluded that the majority of networks were using a mixed mode of WPA and WPA2. Also it identified that 4.88% of networks with in this geographical location were using WEP; which is obsolete and is no longer recommended for use. In addition, Dobrilovic et al.[6], identify that only 24% of networks were using CCMP and identify these as highly protected networks; the majority of the other remaining networks being protected by the much less secure TKIP. Dobrilovic et al. [6], identify that 35% of the APs assessed has WPS enabled; they state this is percentage is too high and unacceptable because of the well know security faults with the protocol.

Both papers [13] and [14]research have similar conclusions and identify that the proportion of networks still using legacy protocols such as WEP and WPA and using the authentication method T-KIP is too high and offer potential security risk to Wireless networks.

CHAPTER 3 - RESEARCH METHODOLOGY

INTRODUCTION

RESEARCH OVERVIEW

3.1.1 Research Philosophy & Approach

The project will use the following research strategies:

- Positivism (Philosophy)
- Deductive (Approach)

Positivism

For this project a positivism research philosophy will be used. A positivism approach will be used because the project relies on observations to determine a result. The project is based on an experiment of comparing to scenarios applied to a wireless network; this would indicate that a research philosophy using a positive approach would be best suited.

Deductive

The approach best suited to the proposed project would be deductive. A deductive approach is best suited with a positivism research philosophy. A deductive approach would involve developing a research hypothesis and then developing strategies to test the hypothesis stated.

The hypothesis for this for the project has agreed as:

The network prevented more intrusion and data manipulation with the security facilities turned and firewalls were configured when the network was the network was attacked/penetrated using a Kali Linux virtual machine.

3.1.2 Research Strategies

The project will use the following research strategies:

- Experimental
- Document Review
- Survey

Experimental Strategy

The project will use an experimental strategy to evaluate the relationship between using security facilities on a wireless local area network (WLAN) and unsecure WLAN. The both secure and unsecure LANs will test to evaluate the secureness of the network using Kali Linux.

The attacks to be carried out are:

- Denial of service attack
- Man in the Middle
- *Rogue access point implementation and attack*

Literature Review

A document review will identify the key concepts and theories of penetration test and wireless security. The document reviews will identify relevant research in the whole field of wireless penetration testing and security. The review will also justify the projects practicality, along with identifying the facts involved and give a guide to compare the results of the proposed research.

Survey

The project will carry out a survey into the number of attackable networks in a small geographical area such as city centre. The survey will be to access the amount of vulnerable networks in the area. The survey will highlight the need for penetration testing and wireless security.

3.1.3 Data Collection

Data will be collected in the by carrying out a survey based on how well the network performs during each attack against a common criteria so that each type of attack could be compared with each other.

An example of this type of scale is the Likert Scale which could be used to evaluate the network's security within scenarios, where the security facilities are currently not in place and then they are introduced. The Likert Scale has been used to help evaluate the effectiveness of security of facilities in a wireless environment.

The Likert Scale allows the user to choice from five to seven differing degrees of response with a scale of agree to disagree [15]. This scale offers the user of the survey to be more precise in the response therefore proving a higher accuracy of data collection. An example use of the response criteria from a Likert Scale based survey would be "strongly agree / agree / don't know / disagree / strongly disagree [15]. This type of scale has been used in the project to assess the degree of network security features.

3.1.4 Reliability and validity

The project has repeated all the test carried out a number of times to ensure that the results produced are accurate. Steps would be taken to ensure that no outside factors could affect the results produced.

3.1.5 Triangulation

Triangulation of the research strategies have been used to ensure that the research produced is of quality and is reliable. According to Denzine and Patton triangulation is the comparing the consistent findings generated by using different data collection techniques [16].

CHAPTER 4 - DESIGN & IMPLEMENTATION

4.1 INTRODUCTION

In this chapter a

4.2 PROBLEM FORMULATION

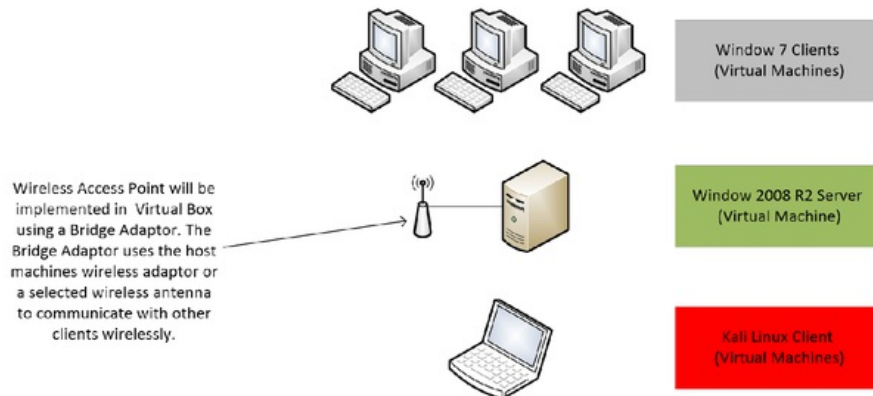


Figure 1 - Initial Network Design

The original solution as described in figure one was to use the host machines wireless card to emulate a Wireless LAN connection to communicate with other host on the network. This solution was unable to implement in Virtual Box using the Bridge Adaptor. Upon further research it was found that this option could only be used for bridging to a physical access point for an Internet connection for use on the virtual machine.

The option of using a Virtual AP was explored using a solution such as Open WRT image and installing it in to a Linux based machine was explored within Virtual Box. Open WRT provides frame ware for APs and could have been potentially used to act as a Virtual AP in the virtualised network. Upon testing this solution the Access Point frame ware were not combatable with the versions of Linux offered in Virtual Box.

A solution of using a Software based access installed on a PC within the network was also investigated and tested this option. Although the AP appeared to be broadcasting it SSID, it would not allow the virtual machines or other test devices

such as the host PC to connect to the AP. This solution was discarded because of the connection issues.

The chose connection solution was to use a NETGEAR EX2700 configured in AP mode to allow the virtual machines to communicate over a wireless network. This solution was the most viable option to ensure that a reliable and flexible communication method.

4.3 DESIGN

4.3.1 VIRTUAL MACHINE CONFIGURATION

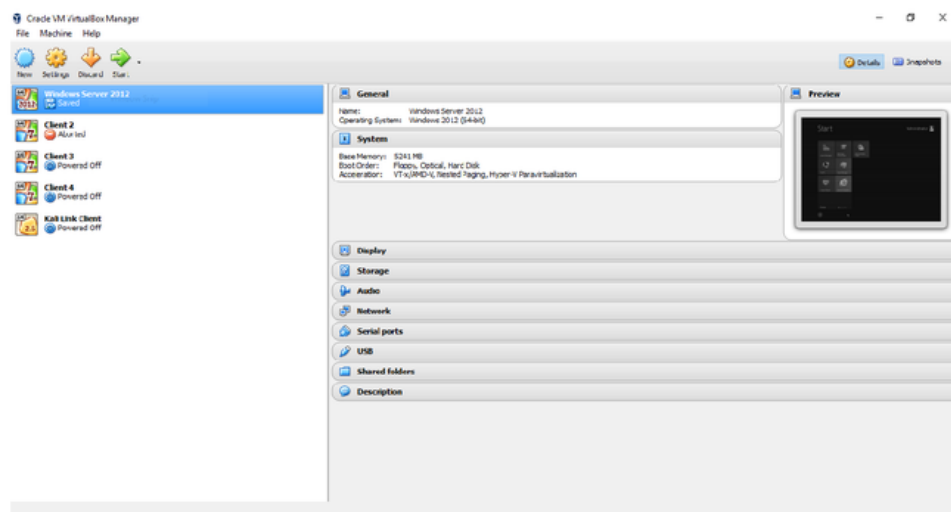


Figure 2- Virtual Machines Configuration

4.3.2 WINDOWS SERVER 2012 CONFIGURATION

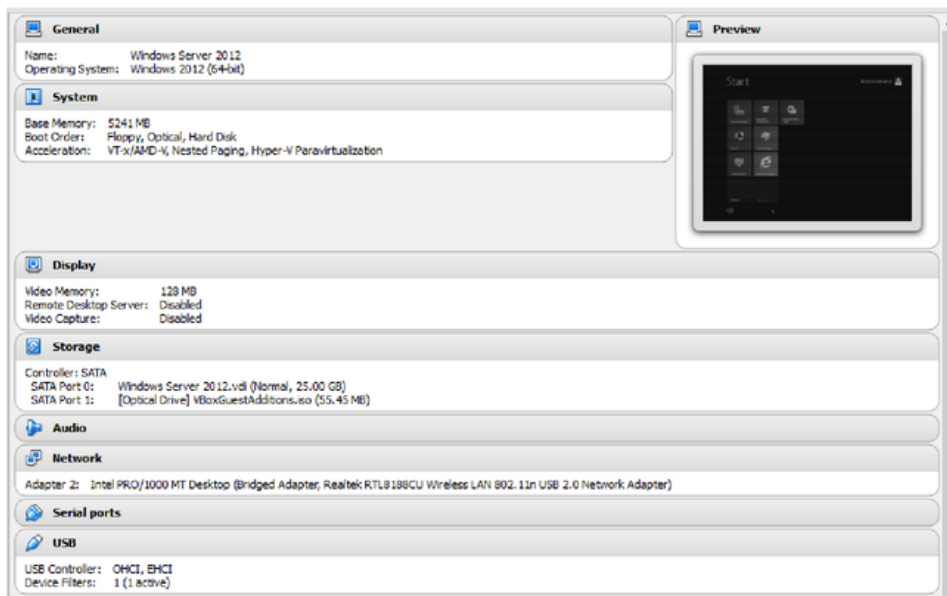


Figure 3- Windows Server Configuration

4.3.3 WINDOWS 7 CLIENT CONFIGURATION

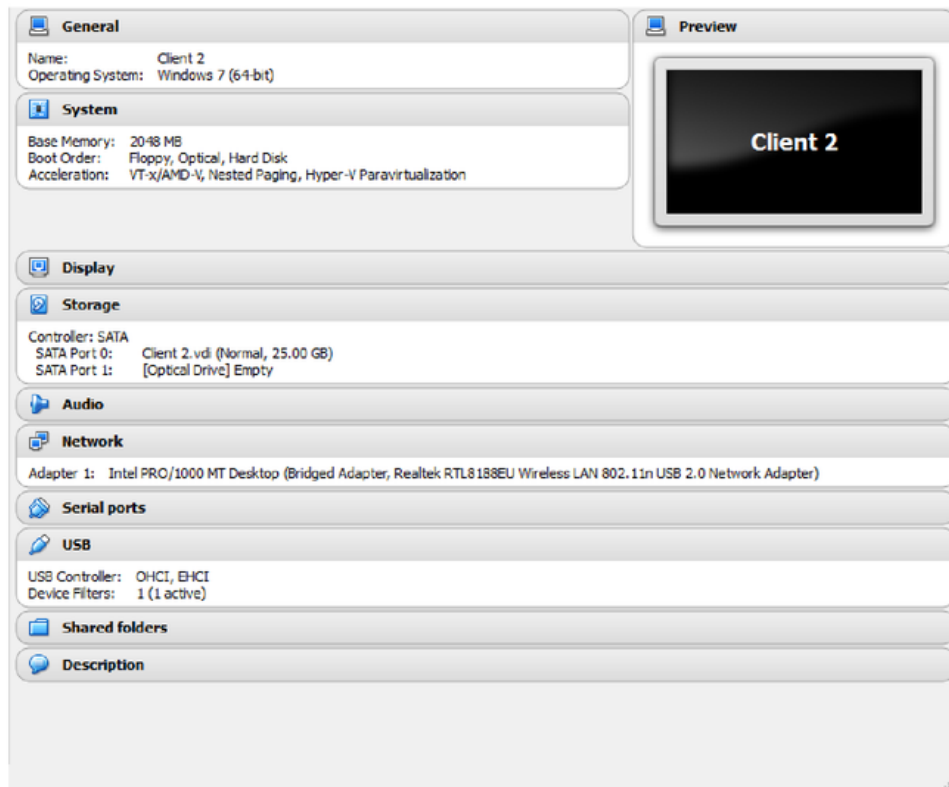


Figure 4- Windows 7 Client

4.3.4 KALI LINUX CLIENT CONFIGURATION

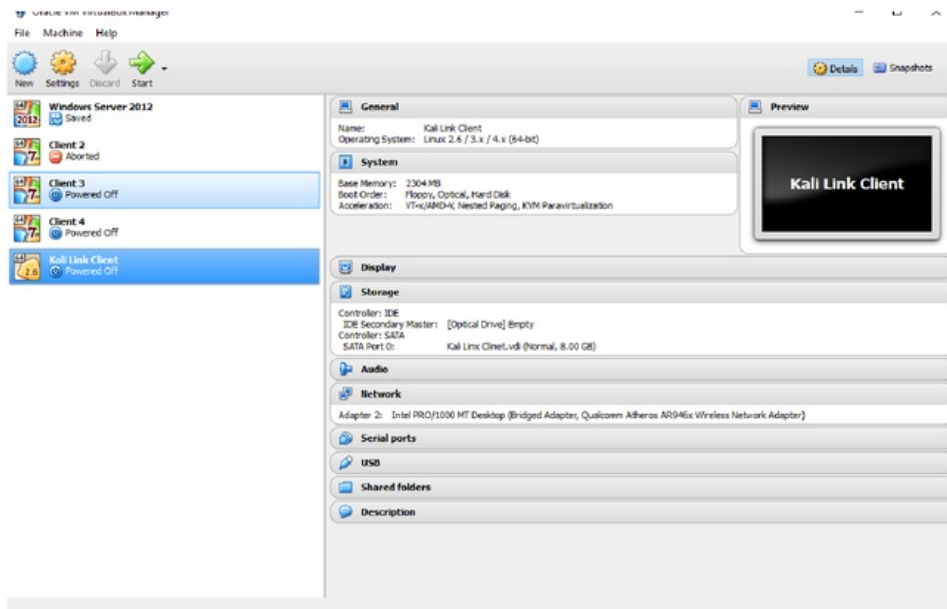


Figure 5- Kali Linux Client

4.4 IMPLEMENTATION

4.5 CONCLUSION

CHAPTER 5 – REFERENCES

- [1] Cisco, "What Is Network Security?," *Cisco*. [Online]. Available: http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html. [Accessed: 16-Nov-2015].
- [2] S. Armstrong, "What are the costs associated with the TalkTalk breach? - SC Magazine UK," *SC Magazine UK*, 2015. [Online]. Available: <http://www.scmagazineuk.com/what-are-the-costs-associated-with-the-talktalk-breach/article/452744/>. [Accessed: 16-Nov-2015].
- [3] BBC, "TalkTalk hack to cost up to £35m - BBC News," *BBC News*, 2015. [Online]. Available: <http://www.bbc.co.uk/news/uk-34784980>. [Accessed: 16-Nov-2015].
- [4] X. Yuan, R. L. Archer, J. Xu, and H. Yu, "A visualization tool for wireless network attacks," *2nd International Multi-Conference on Society, Cybernetics and Informatics, IMSCI 2008*, 2008. [Online]. Available: <http://www.scopus.com/inward/record.url?eid=2-s2.0-79953275343&partnerID=40&md5=8e157b21b050885309eeb428a9a47e2d>. [Accessed: 16-Oct-2015].
- [5] Y. Zou, J. Zhu, and B. Zheng, "Defending Against Eavesdropping Attack Leveraging Multiple Antennas in Wireless Networks," *2013 8th Int. Conf. Commun. Netw. China*, pp. 699–703, 2013.
- [6] S. Compton, "802.11 Denial of Service Attacks and Mitigation," *SANS Institute InfoSec Reading Room*, 2007. [Online]. Available: <https://www.sans.org/reading-room/whitepapers/wireless/80211-denial-service-attacks-mitigation-2108>. [Accessed: 23-Nov-2015].
- [7] I.-H. Huang, K.-C. Chang, Y.-C. Lu, and C.-Z. Yang, "Countermeasures against MAC address spoofing in public wireless networks using lightweight agents," 2010.
- [8] A. Johns, *Mastering Wireless Penetration Testing for Highly Secured Environments*. Packt Publishing Ltd, 2015.
- [9] Mehta, Gourav, Faruki, and Parvez, "WiFi AP Info. Exploitation and Packet Capturing on Android Devices using CONNECTOR & KALI LINUX.," *Res. Gate*, 2014.

-
- [10] C. Buchanan, *Blueprints, Kali Linux CTF Title*. Packt Publishing Ltd, 2014.
- [11] T. Heriyanto, L. Allen, and A. Shakeel, *Kali Linux - Assuring Security by Penetration Testing*. Packt Publishing Ltd, 2014.
- [12] A. H. Lashkari, M. I. R. Mohammad, S. Danesh, and B. Samadi, "A Survey on Wireless Security protocols (WEP , WPA and WPA2 / 802 . 11i)," *Comput. Sci. Inf. Technol. 2009. ICCSIT 2009. 2nd IEEE Int. Conf.*, no. Iv, pp. 48–52, 2009.
- [13] M. Vanhoef and F. Piessens, "Practical verification of WPA-TKIP vulnerabilities," *Proc. 8th ACM SIGSAC ...*, pp. 427–435, 2013.
- [14] D. Dobrilovic, B. Odadzic, Z. Stojanov, and Z. Covic, "Approach in IEEE 802 . 11 security analytics and its integration in university curricula," pp. 2011–2014, 2014.
- [15] Psychology Simply, "Likert Scale," *simplypsychology.org*. [Online]. Available: <http://www.simplypsychology.org/likert-scale.html>. [Accessed: 04-May-2016].
- [16] R. Wood, "RWJF - Qualitative Research Guidelines Project | Triangulation | Triangulation." [Online]. Available: <http://www.qualres.org/HomeTria-3692.html>. [Accessed: 03-Feb-2016].