

Aaron Lee Cowdry, BSc. Computer Networks, UWTSD Swansea, School of Applied Computing

Student ID: P134514 | acowdry.134514@student.uwtsd.ac.uk

1. Introduction

The project has configured a virtualised network will in VMware. The network included a sever installed with Windows 2012 and three Windows 10 Client. A forth client was installed with Kali Linux to carry out the penetration testing.

VMware was chosen type 2 hypervisor.

Various wireless attacks were carried out using the virtual network.

The project then evaluated the effectiveness of security features against a wireless network attack.

2. Aims & Objectives

Aim -

The aim of the project was to create a client-server based network using VMare in WLAN environment.

Different ethical hacking techniques will be carried out with no security features active on the network and then repeated with certain security features active.

Objectives -

- Review the current literature in the field.
- Carry out an experiment using the features of Kali Linux.
- Compare the results of the wireless penetration technique's scenarios.

3. Literature Review

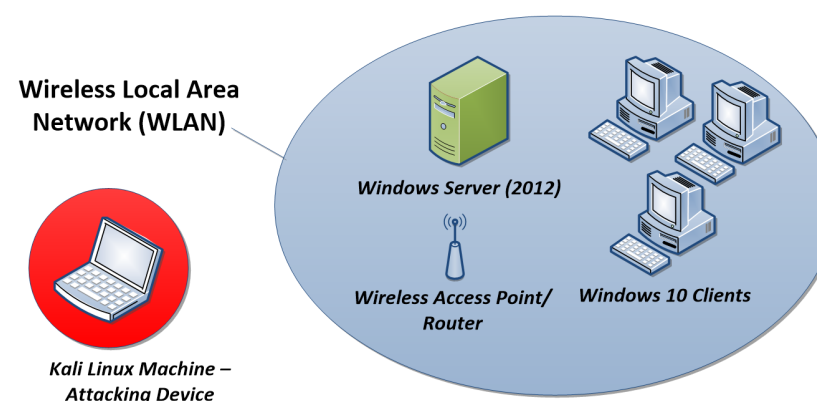
Key Findings of the literature review:

- A Man In The Middle attacks are the most successful in wireless networks.[1]
- Wireless Networks are more vulnerable[2]
- Request to Send (RTS) packets most successful in Wireless Networks Denial of Service attacks [3]
- A Rogue Access Point is a highly effective way to attack a wireless network and its hosts. [4]

vmware®

4. Design

A virtual network was configured in VMware. A physical access point (AP was configured to allow the clients to connect the virtual network. The implementation of a virtual or software based AP was not successful.



5. Findings

Key Findings of the experimental aspect of the project:

- Two of the three attacks were successful.
- Man in the Middle attack was unsuccessful.
- Denial of Service attack failed to cause a dissociation with the wireless access point.
- The number of packets that attacked the router with security features enabled was less than without any implemented.

6. Recommendations for Future Work

- To carry out the same attacks using a type one hypervisor.
- Implement a virtual wireless access point.
- Carry out a further investigation into the success of different types of wireless network attacks.

7. References

- [1] M.Conti, N.Dragoni and V. Lesyk, A Survey of Man In The Middle Attacks. IEEE Communications & Survey Tutorials - Vol. 18. 2016.
- [2] M.Agarwal, S Biswas and S. Nandi, "Advanced Stealth Man-in-the - Middle Attack in WPA2 Wi-Fi Networks. 2015.
- [3] P. Stojanoski, M. Bogdanoski and A Risteski, "Wireless Local Area Network Behaviour under RTS Flood DoS Attack" 20th Telecommunication forum. 2012
- [4] 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-2016].

