



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Dissertation

Penetration Testing Of A Wireless Network

MSc Computer Networks And Cyber Security

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk

By
Fatema Namazi

Introduction

Penetration testing (pen testing) of a wireless network is the process of evaluating the security of a system or network by simulating an attack. In this presentation, we will focus on using an external adapter and Aircrack-ng to carry out a wireless network penetration test.

Why use an External Adapter?

An external adapter is used to enable any device to connect to the wireless network. Aircrack-ng requires an external adapter to send and receive signals and can be used for more comprehensive testing.

What is Aircrack-ng?

Aircrack-ng is a powerful tool designed for test wireless networks. It has various features, including packet capturing and decryption, WEP, WPA, and WPA2 cracking, and identifying vulnerabilities. Aircrack-ng can aid in testing of security measures.

Steps to perform Penetration testing of wireless network

1. Start the wireless interface in monitor mode using airmmon-ng
2. Scan for wireless networks using airodump-ng
3. Capture packets from the wireless network using airodump-ng
4. Crack WEP key with aircrack-ng
5. Perform WPA/WPA2 cracking
6. Analyze captured data with Wireshark.

Step 1: Start the Wireless Interface in Monitor Mode

To start the wireless interface on monitor mode, use the `airmon-ng` command. It will show all wireless interface names available.

Step 2: Scan for Wireless Networks

The next step is to scan for wireless networks.

Use the airodump-ng command to scan and get information like BSSID, channel, and ESSID.

Step 3: Capture Packets from Wireless Network

In this step, the airodump-ng command is used to capture packets from the wireless network.

Airodump-ng will capture all packets sent to or from the access point.

Step 4: Crack WEP Key with Aircrack-ng

Aircrack-ng can be used to crack the WEP key. The command used for this is `aircrack-ng -n 64 <filename>.cap`

Step 5: Perform WPA/WPA2 cracking

The next step is to perform WPA/WPA2 cracking using Aircrack-ng. This can be done by using the aircrack-ng command and the capture file. This process may take time based on the length of the passphrase.

Step 6: Analyse Captured Data with Wireshark

In this step, the captured data can be analysed using Wireshark, a powerful network protocol analyser. The capture file can be opened to view individual packets and analyse network traffic.

Key Takeaways

- External adapters are used to connect a device to a wireless network for comprehensive testing.
- Aircrack-ng is a powerful tool to test wireless networks, proving capabilities such as packet capturing and decryption, WEP, WPA, and WPA2 cracking, and identifying vulnerabilities.
- To perform a wireless network penetration test using external adapter and Aircrack-ng, the process involves starting the wireless interface on monitor mode, scanning for wireless networks, capturing packets, cracking WEP key with aircrack-ng, perform WPA/WPA2 cracking and analyzing captured data with Wireshark.

References

1. Aircrack-ng official documentation – <https://www.aircrack-ng.org/>
2. Offensive Security Wireless Attacks – <https://www.offensive-security.com/metasploit-unleashed/wireless-attacks/>
3. Wi-Fi Security – https://www.researchgate.net/publication/328750706_Wi-Fi_Security_Vulnerabilities_and_Countermeasures_A_Literature_Review
4. Wireshark – <https://www.wireshark.org/docs/>



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Thank-you

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

www.uwtsd.ac.uk