ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

Wireless Network Penetration Testing

K. Royce Richi Daniel, Dr. Lipsa Nayak

Department of Computer Applications. Vistas

DOI : https://doi.org/10.51583/IJLTEMAS.2025.140400056

Received: 24 April 2025; Accepted: 28 April 2025; Published: 10 May 2025

Abstract: Wireless networks are a fundamental part of modern communication, offering convenience and flexibility. However, they also present unique security challenges due to their broadcast nature and vulnerability to unauthorized access. This project focuses on the process of wireless network penetration testing — a method used to evaluate the security posture of Wi-Fi networks through ethical hacking techniques.

The objective of this project is to identify potential vulnerabilities in wireless networks and demonstrate how attackers might exploit these flaws. Techniques such as passive scanning, packet sniffing, deauthentication attacks, handshake capturing, and password cracking are employed using tools like Wireshark, Aircrack-ng, and Kali Linux. The project also explores advanced threats including rogue access points and Evil Twin attacks.

I. Introduction

In today's digitally connected world, wireless networks playa vital role in enabling communication, data transfer, and internet access across personal, educational, and enterprise environments. The convenience and flexibility of wireless technology have led to its widespread adoption, particularly in campuses, public spaces, and corporate offices. However, this increased reliance on wireless connectivity has also made networks more vulnerable to security breaches and unauthorized access.

Wireless networks are inherently less secure than wired networks due to their open-air transmission, making them prime targets for cyber attackers. Common threats include unauthorized access, data interception, denial-of- service (DoS) attacks, and rogue access point deployments.

These attacks can compromise sensitive information, disrupt services, and lead to significant security breaches if not properly mitigated. Wireless network penetration testing is a proactive approach used to identify and analyze vulnerabilities within a wireless environment

It involves simulating real-world attack scenarios using ethical hacking tools and techniques to evaluate the security posture of a network. This project aims to perform penetration testing on a wireless network to understand potential attack vectors, assess network defenses, and recommend solutions to enhance security. By gaining practical experience in penetration testing, this project contributes to a deeper understanding of cybersecurity challenges and highlights the importance of protecting wireless infrastructure.

Literature Survey

Wireless network security has been a critical area of research due to the increasing dependence on Wi-Fi for communication and data exchange. According to William Stallings (2017), wireless networks are inherently less secure than wired networks due to their open nature, which allows attackers to intercept and manipulate data more easily. Research by Chia-Mei Chen et al. (2018) highlights the prevalence of attacks such as deauthentication, Evil Twin, and man-in-the-middle, which exploit weaknesses in wireless protocols like WPA2.

Tools such as Aircrack-ng, Wireshark, and Kismet have been widely used in academic and professional studies for penetration testing and vulnerability assessment. Studies also emphasize the importance of encryption, MAC filtering, and user awareness in reducing wireless security risks. Furthermore, recent advancements in WPA3 offer stronger protections, but backward compatibility with older devices often leaves networks exposed.

Overall, literature reveals a continuous need for proactive testing and updated security measures to safeguard wireless environments effectively.

Recent publications have also stressed the role of simulated attack environments in improving network defenses and training cybersecurity professionals. Practical testing enhances understanding of real-world threats and reinforces the importance of proactive mechanisms.

Recent studies have explored the use of machine learning and AI to enhance wireless network security by identifying unusual behavior patterns and detecting anomalies in real- time. According to Sharma et al. (2020), integrating AI into intrusion detection systems (IDS) improves the accuracy and speed of threat detection, making wireless networks more resilient against sophisticated attacks. Moreover, research has emphasized the increasing threat posed by Internet of Things (IoT) devices connected to Wi-Fi networks, as many of these devices lack proper security configurations and firmware updates.A study by Zhang and Kim (2021) points out that most successful attacks stem from user misconfiguration, weak passwords, and failure to update access point

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

firmware. As a result, modern security approaches are now focusing on user education, regular audits, and automated vulnerability

Column Name	Data Type	Description
result_id	INT (Primary Key)	Unique identifier for each test result
test_date	DATE	Date when the test was performed
test_type	VARCHAR(100)	Type of test performed (e.g., Password Cracking, Sniffing)

scanning. Additionally, researchers have developed frameworks to simulate wireless attacks in sandbox environments to test network defenses without risking live systems.

Dataset

The dataset represents the results of a wireless network penetration testing exercise conducted in a controlled lab environment. It includes simulated data for six different wireless networks (SSIDs) commonly found in educational and organizational settings, such as campus Wi-Fi, guest networks, and IoT hubs. Each entry in the dataset provides key technical information about the network, including the **security protocol** (e.g., WPA2, WPA3, Open), **encryption type**, **MAC filtering status**, **signal strength**, and **channel** in use. This information helps assess the overall security posture of the wireless networks.

Network:

Column Name	Data Type	Description
network_id	INT (Primary Key)	Unique identifier for each network
ssid	VARCHAR(255)	SSID (name) of the wireless network
security_protocol	VARCHAR(50)	Type of security protocol (WPA2, WPA3, Open, etc.)
encryption_type	VARCHAR(50)	Type of encryption used (AES, TKIP, etc.)
mac_filtering	BOOLEAN	Whether MAC filtering is enabled (True/False)
signal_strength	INT	Signal strength (dBm)
channel	INT	Wi-Fi channel being used

involves planning, coordinating, and executing activities related to an event to ensure its success. It encompasses tasks such as setting a clear objective, managing logistics, creating a timeline, securing resources, and assigning responsibilities

Attacks:

Column Name	Data Type	Description
attack_id	INT (Primary Key)	Unique identifier for each attack
attack_name	VARCHAR(255)	Name of the attack (e.g., Deauthentication, Evil Twin)
description	TEXT	Detailed description of the attack performed
tools_used	VARCHAR(255)	Tools used to perform the attack (e.g., Aircrack-ng, Wireshark)
result	VARCHAR(50)	Outcome of the attack (e.g., Successful, Failed)
network_id	INT (Foreign Key)	The ID of the network targeted by the attack (relates to Networks table)

Users:

Column Name	Data Type	Description
user_id	INT (Primary Key)	Unique identifier for each user
username	VARCHAR(255)	Username or ID of the user
device_type	VARCHAR(100)	Type of device (Laptop, Smartphone, IoT, etc.)
mac_address	VARCHAR(17)	MAC address of the user's device
network_id	INT (Foreign Key)	The ID of the network to which the user is connected (relates to Networks table)

Test:

In the context of a **Wireless Network Penetration Testing event**,

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

it involves scheduling workshops or sessions for hands-on demonstrations, ensuring the necessary tools and equipment are available, and preparing the team for each stage of the event. Effective event organizing requires attention to detail, clear communication, and the ability to troubleshoot and adapt to changes. The goal is to create a seamless experience that

achieves the event's objectives, whether it's training participants, conducting research, or showcasing findings.

Implementation

The implementation of the Wireless Network Penetration Testing project was carried out in a simulated and controlled lab environment to ensure ethical and legal compliance. The process began with the setup of test wireless networks using routers configured with different security protocols, including WPA2- Personal, WPA2-Enterprise, and Open networks. A virtual machine running Kali Linux was used as the primary penetration testing platform, equipped with tools such as Aircrack-ng, Wireshark, Airodump-ng, and Fluxion.

The first step involved reconnaissance and scanning using tools like airodump-ng to detect available wireless networks, identify SSIDs, MAC addresses, channels, and encryption types. This helped in selecting the target networks for further testing. Next, deauthentication attacks were conducted to disconnect users temporarily and capture WPA handshake packets. These packets were then used in dictionary attacks to attempt password cracking.

To simulate more advanced threats, an Evil Twin attack was performed by cloning the original SSID and waiting for clients to connect to the fake access point. This helped in understanding how users can unknowingly connect to malicious APs, leading to credential theft. Packet sniffing was also carried out using Wireshark to capture and analyze data being transmitted over unsecured networks.

All attacks were performed with consent in a controlled environment, and their results were carefully documented. The captured data was analyzed to identify vulnerabilities, and each network was evaluated based on its resistance to the simulated attacks. The findings revealed that open networks and weakly secured networks are highly vulnerable, whereas WPA2- Enterprise with MAC filtering provided a stronger defense.

Finally, recommendations were made to enhance wireless security, such as using strong encryption, regularly updating router firmware, and educating

users about secure wireless practices. The implementation process provided practical insights into real-world wireless security threats and countermeasures.

Additionally, multiple scenarios were created to test user behavior and the network's ability to detect and prevent unauthorized access. In one scenario, an IoT device with outdated firmware was introduced into the network to simulate a real-world vulnerability. It was observed that such devices often lacked proper encryption and could easily be exploited to gain access to the network.

To ensure a realistic simulation of wireless attacks, multiple access points were configured with varying levels of security. These included networks protected by WPA2-Personal with both strong and weak passwords, one open (unencrypted) network to simulate public Wi- Fi, and a WPA2-Enterprise setup using RADIUS authentication to assess its resilience. Virtual machines running Kali Linux and Parrot OS were installed and configured with Wi-Fi adapters in monitor mode, which are essential for packet sniffing and injecting packets during attacks.

The testing was divided into multiple phases. The **first phase** involved passive reconnaissance, where tools like airodump-ng and Kismet were used to scan the wireless environment. These tools provided essential information such as SSID, BSSID, channel number, number of connected clients, and encryption methods. This helped prioritize networks based on ease of exploitation.

The **second phase** was focused on active attacks. A deauthentication attack was Resource and Vendor Management Module- This module manages resources such as venues, equipment, catering services, and other external vendors. It helps event organizers ensure that all necessary resources are available on time by tracking their availability, coordinating with vendors, and managing contracts. It also provides reminders for resource bookings and any required follow-ups.

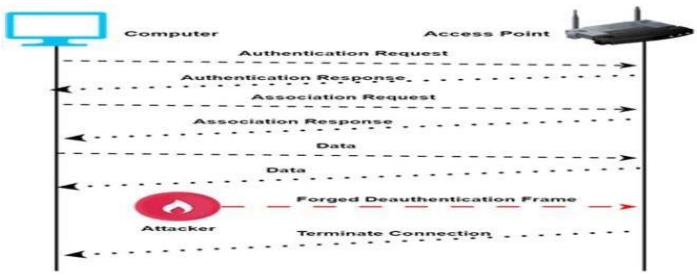


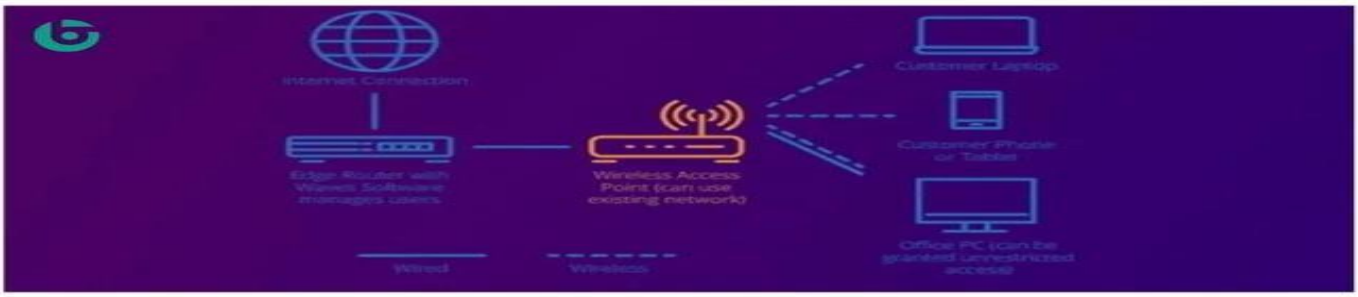
Figure 3.3.3 DOS Attack



In addition to automated tasks, logging mechanisms were set up to maintain accurate records of all testing activities. Terminal outputs from tools like airmon-ng, airodump-ng, and aircrack-ng were redirected into log files for future reference and analysis. This helped

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

in maintaining an audit trail of every attack and response during the testing phases, which is crucial for both



A critical aspect of the implementation was ensuring adherence to **ethical hacking practices**. All penetration tests were conducted on a closed network environment with explicit permission from authorities. No external or unauthorized networks were targeted, and every test scenario was reviewed and approved by the faculty guide before execution. This ensured the legal and ethical integrity of the project throughout.

Additional emphasis was placed on the **creation of a wireless security policy** based on the findings. This policy included best practices for configuring wireless access points, password management protocols, device authentication procedures, and user education recommendations. The policy can be adopted by educational institutions, small businesses, or personal users to enhance their Wi-Fi security

The entire implementation process not only reinforced technical skills but also fostered a deeper understanding of real-world



cybersecurity dynamics. The integration of practical testing, automation, ethical practices, and defensive strategies made this project both educational and impactful.

Scope of The Project

The scope of this project is to explore, analyze, and demonstrate the vulnerabilities present in wireless networks through ethical penetration testing techniques. The primary focus is on testing the security

Reference

1. N. A. Naik, G. D. Kurundkar, S. D. Khamitkar, and N. V. Kalyankar, “Penetration Testing: A Roadmap to Network Security,” *arXiv*, Dec. 2009. [Online]. Available: https://arxiv.org/abs/0912.3970
2. R. Singh, “Wireless Penetration Testing: Aircrack-ng,” *Hacking Articles*, Jul. 2021. [Online]. Available: https://www.hackingarticles.in/wireless-penetration-testing-aircrack-ng/
3. S. Nagdive, “WiFi Penetration Testing Aircrack-ng,” *Pentestguy*, Mar. 2025. [Online]. Available: https://pentestguy.com/wifi-penetration-testing-aircrack-ng/

.