ARL-SR-0507 ● JUNE 2025

Hands-on Cybersecurity Studies: Session Hijacking and Safe Wi-Fi Practices

by Ana Rodriguez and Jaime C. Acosta

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

ARL-SR-0507 ● JUNE 2025

Hands-on Cybersecurity Studies: Session Hijacking and Safe Wi-Fi Practices

Ana Rodriguez
University of Texas at El Paso

Jaime C. Acosta
DEVCOM Army Research Laboratory

REPORT DOCUMENTATION PAGE

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
		START DATE	END DATE
June 2025	Special Report	October 2024	March 2025

4. TITLE AND SUBTITLE
Hands-on Cybersecurity Studies: Session Hijacking and Safe Wi-Fi Practices

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**

6. AUTHOR(S)
Ana Rodriguez and Jaime C. Acosta

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
DEVCOM Army Research Laboratory ATTN: FCDD-RLA-ND Adelphi, MD 20783-1138	ARL-SR-0507

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
ORCID: Jaime C. Acosta, 0000-0003-2555-9989

14. ABSTRACT
This report provides participants with insights into cybersecurity, specifically focusing on Wi-Fi and network traffic analysis. Through hands-on engagement, attendees develop proficiency in understanding wireless networks, highlighting the risks posed by weak encryption and open networks. Well-known and publicly available tools from the Aircrack-ng suite (including airmon-ng, airodump-ng, aireplay-ng, airdecap-ng, and aircrack-ng) are used for packet capture, deauthentication, and password analysis. Additionally, Wireshark is used for traffic analysis, showcasing how session cookies and user sessions work. By simulating a real-world scenario, participants enhance their ability to recognize and mitigate Wi-Fi security issues, reinforcing best practices for secure network configurations and user protection.

15. SUBJECT TERMS
cybersecurity; wireless network security; Wi-Fi traffic analysis; packet sniffing; Aircrack-ng suite; airmon-ng; airodump-ng; aireplay-ng; airdecap-ng; aircrack-ng; Wireshark; Cyber Rapid Innovation Group; CyberRIG; Network, Cyber, and Computational Sciences

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	C. THIS PAGE		
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UU	25

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER *(Include area code)*
Jaime C. Acosta	(520) 691-5956

STANDARD FORM 298 (REV. 5/2020)
Prescribed by ANSI Std. Z39.18

Contents

1. Introduction

Wireless network security is a critical aspect of cybersecurity, particularly as attackers exploit vulnerabilities in Wi-Fi protocols to intercept and manipulate network traffic. According to public resources, attackers can leverage techniques such as deauthentication attacks and session hijacking to gain unauthorized access to network resources.[1] By analyzing network traffic and understanding these attacks, the general user and security professionals can develop countermeasures to mitigate risk and strengthen wireless security defenses.

1.1 Exercise Overview

In this exercise, participants will simulate a real-world cybersecurity attack and defense scenario by analyzing Wi-Fi network traffic, capturing encrypted packets, and demonstrating session hijacking techniques. This exercise is largely based on online laboratory exercises.[2] Using tools from the Aircrack-ng suite, participants will conduct a deauthentication attack to force a target device to reconnect to a wireless network, allowing them to capture Wi-Fi Protected Access 2 (WPA2) handshake packets. Additionally, they will use Wireshark to inspect captured traffic, extract session cookies, and analyze network vulnerabilities. This exercise highlights the risks of unencrypted communications on public Wi-Fi and emphasizes the importance of secure authentication and encryption methods. Through hands-on experience, participants will develop a deeper understanding of strategies, detection techniques, and best practices for mitigating wireless security threats.

1.2 Session Hijacking and Wi-Fi Attacks Overview

Session hijacking occurs when an attacker captures a victim's session token and reuses it to impersonate the user. This is particularly effective over insecure Wi-Fi networks where traffic is unencrypted. Attackers can achieve this by capturing HTTP session cookies from network traffic. Deauthentication attacks, another common attack vector, force a user to disconnect from a Wi-Fi network, allowing attackers to intercept the ensuing WPA2 handshake for potential password cracking.

1.3 Wireless Network Monitoring and Security Tools: Aircrack-ng Suite

The Aircrack-ng suite is a powerful open-source set of tools for assessing Wi-Fi security, enabling users to monitor, test, and analyze wireless networks.[3] **Airmon-ng** allows wireless adapters to enter monitor mode, capturing network traffic without needing to connect. **Airodump-ng** is a packet sniffer that gathers information on access points and clients, capturing WPA2 handshakes for password cracking. **Aireplay-ng** enables packet injection, such as deauthentication attacks, to force reconnections and capture authentication handshakes. **Airdecap-ng** decrypts Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) encrypted traffic once the correct passphrase is obtained. **Aircrack-ng** performs password cracking using dictionary or brute-force attacks on captured handshakes.

1.4 Wireshark for Network Analysis

Wireshark is a packet analysis tool that allows users to inspect captured network packets in detail. It is used for deep packet inspection, enabling the analysis of session cookies, unencrypted HTTP traffic, and other network vulnerabilities. Tools like Wireshark demonstrate how attackers can exploit weak Wi-Fi security and highlight the importance of strong encryption, secure authentication methods, and protective countermeasures.

2. Setup and Configuration

The setup of the exercise includes one virtual machine (VM) with the software listed below.

- Kali Linux 2024.4 64-bit VM[4]
- VMware Workstation 17 Pro[5]
- Docker (preinstalled for simulation purposes)[6]
- Wireshark
- Aircrack-ng suite[3]

The U.S. Army Combat Capabilities Development Command Army Research Laboratory's South Cyber Rapid Innovation Group Collaborative Innovation Testbed serves as the hosting environment for the Kali Linux VMs. This setup creates a secure and controlled environment, ideal for demonstrating common Wi-Fi vulnerabilities such as session hijacking and unauthorized access. With the comprehensive suite of software tools (including VMware, Kali Linux VMs,

Docker, Aircrack-ng suite, and Wireshark), participants can effectively explore potential security threats while gaining hands-on experience in cybersecurity.

3. Learning Objectives

The exercise aims to provide participants with practical skills and knowledge in cybersecurity, emphasizing Wi-Fi security vulnerabilities and network traffic monitoring tools. Specific learning objectives include the following:

- Understand Wi-Fi network security basics: learn about the different Wi-Fi security protocols (e.g., WEP, WPA, and WPA2) and their vulnerabilities, explore how WPA2 handshakes work, and understand their importance in cracking Wi-Fi passwords.
- Comprehend the Aircrack-ng suite and related tools: gain hands-on experience with the tools, learning how to capture and analyze Wi-Fi traffic using airodump-ng, airmon-ng, aireplay-ng, and airdecap-ng. Learn to use Wireshark to inspect captured packets and identify security flaws such as unencrypted session cookies.
- Learn techniques for capturing and cracking Wi-Fi credentials: practice enabling monitor mode on wireless interfaces, capturing WPA2 handshakes, and executing deauthentication attacks to force clients to reconnect. Learn to use dictionary and brute-force attacks with aircrack-ng to crack Wi-Fi passwords from the captured handshakes.
- Demonstrate the application of session hijacking: explore session hijacking by manipulating captured cookies to gain unauthorized access to a website. Learn to use tools like wpa_supplicant to connect to a compromised Wi-Fi network, retrieve session information, and analyze decrypted traffic with Wireshark to hijack user sessions.
- Explore countermeasures for Wi-Fi and session hijacking attacks: understand the importance of strong Wi-Fi encryption, HTTP Secure (HTTPS), and virtual private networks (VPNs) to protect against session hijacking and deauthentication attacks. Learn about best practices for securing Wi-Fi networks and safeguarding user data from common vulnerabilities.

By achieving these learning objectives, participants will enhance their comprehension of cybersecurity principles and acquire practical experience in defending against sophisticated cyber threats.

4. Exercise

Objective:

This exercise aims to demonstrate the importance of secure Wi-Fi practices by showing how attackers can capture cookies from network traffic and gain unauthorized access. Students will learn about Aircrack-ng, wireless adapters, monitor mode, authentication handshakes, and tools like airmon-ng, aireplay-ng, airodump-ng, airdecap-ng, and Wireshark.

Part 1. Preliminaries: Become Familiar with Key Concepts and Tools

1. Wireless Adapters and Monitor Mode

- Wireless adapters can operate in different modes: managed (normal use) and monitor (can be used for capturing traffic).
- Enabling monitor mode allows the adapter to capture all wireless traffic within range.

2. Wireless Interfaces, Channels, and Authentication

- Wireless networks operate on different channels (frequencies) and require authentication (WPA2-PSK in this case).
- Handshakes occur when a client connects to a network and they contain enough data to attempt password cracking.

3. Wi-Fi Security Protocols

- **WEP—the first Wi-Fi security protocol:** WEP stands for Wired Equivalent Privacy. It was the first Wi-Fi security protocol (approved in September 1999) and is not as secure as desired. WEP is used at the two lowest layers of the OSI model, the data link and physical layers; therefore, it does not offer end-to-end security. It is outdated and insecure. Avoid using WEP in any modern network
- **WPA—temporary enhancement for WEP:** WPA stands for Wi-Fi Protected Access. It was adopted by the Wi-Fi Alliance as an alternative to WEP. 256-bit encryption technology was introduced to WPA, an increase compared with the 64- and 128-bit encryption in WEP. WPA is older, and less secure compared with WPA2, but better than WEP.
- **WPA2—improvement based on WPA:** WPA2 stands for Wi-Fi Protected Access 2. WPA2 was ratified as the new Wi-Fi security standard in 2004. The improvement in the WPA2 security standard is the implementation of

the Advanced Encryption Standard, which provides higher security and performance. There is still a vulnerability that brings security problems because a hacker can get access to a secure WPA2 network and obtain certain keys to attack other devices on the same network. This is a security issue that matters for enterprise networks, instead of home network users.

- **PSK:** PSK stands for Pre-Shared Key. It is a method of authentication used in wireless networks, particularly in WPA and WPA2 protocols, where a shared secret key (password or passphrase) is used by both the client (device) and the wireless access point (router) to establish a secure connection.

4. Tools

Aircrack-ng suite: a complete suite of tools to assess Wi-Fi network security, focusing on different areas:

Monitoring: packet capture and export of data to text files for further processing by third-party tools.

Attacking: replay attacks, deauthentication, fake access points, and more via packet injection.

Testing: checking Wi-Fi cards and driver capabilities (capture and injection).

Cracking: WEP and WPA-PSK (WPA 1 and 2).

- Airmon-ng: enables monitor mode on wireless network interfaces. Monitor mode allows capturing all wireless traffic in the area, even from networks to which you are not connected.
- Airodump-ng: packet sniffer that captures wireless packets, including WPA handshakes, which can later be used for cracking passwords. It also provides information about available access points and associated clients.
- Aireplay-ng: a tool used for injecting packets into a network. This can be used to deauthenticate clients from an access point, forcing them to reconnect so the attacker can potentially capture the WPA handshake.
- Airdecap-ng: a tool for decrypting WEP and WPA-PSK encrypted capture files (such as those collected by airodump-ng) using the correct passphrase.
- Aircrack-ng: the primary tool for cracking WEP and WPA-PSK (WPA2, WPA3) encryption keys. It works by using captured packets and a dictionary or brute-force attack to crack the password.
- Wireshark: analyzes network packets, including cookies and log-in sessions.

****

Part 2: Data Breach Investigation at a Local Café

You are hired to investigate a data breach reported by a local café after several customers complained about suspicious activity in their bank accounts and personal information being stolen. The café's public Wi-Fi network, "wifi-coffeeShop," is suspected to have been compromised, but management is unaware of how the breach occurred.

Your job is to determine whether the café's Wi-Fi network was exploited and, if so, how the attackers accessed sensitive data.

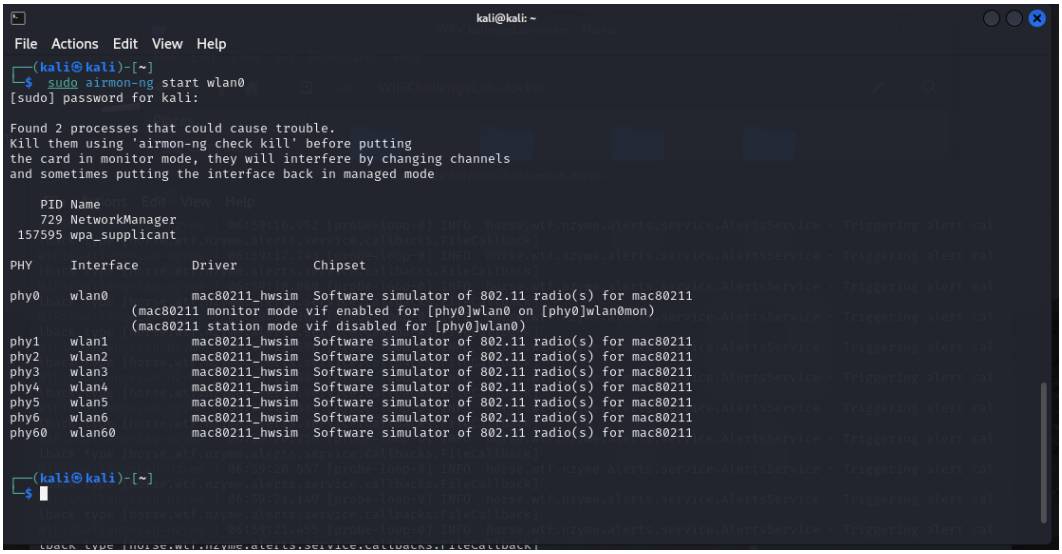
Step 1: Enable Monitor Mode

Before you can monitor the Wi-Fi traffic, you need to put your wireless adapter into monitor mode by running the command to enable monitor mode on your `wlan0` wireless interface. Look at the aircrack-ng tools below and their descriptions to fill in the parameter. Open your terminal and enter the following command:

`sudo <aircrack-ng suite tool> start <interface>`

Solution: `sudo airmon-ng start wlan0`

This command prepares your network interface (wlan0) for packet capture, allowing you to monitor traffic on nearby wireless networks.



Step 2: Traffic Monitoring

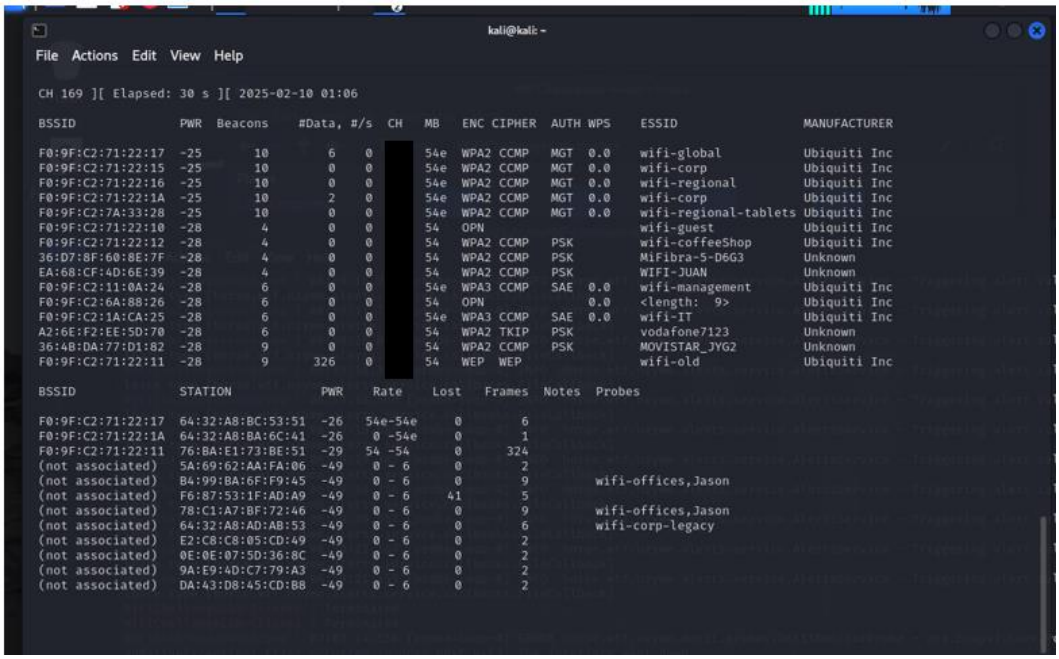
Before you begin monitoring the traffic, it is good practice to create a directory to store all the captured files. This will keep your files organized and make it easier to locate them.

1. **Create a directory for captured files:** first, create a directory to store the captured data. This keeps things organized and ensures that all files from your monitoring session are saved in one place.

   ```
   mkdir ~/wifi
   ```

2. **Find the channel:** run the following command:
   ```
   sudo airodump-ng wlan0mon -w ~/wifi/scan --manufacturer --wps --band abg
   ```

   What channel does wifi-coffeeShop use?



sudo – Runs the command with superuser privileges, which is required for monitoring network traffic.
airodump-ng – A tool that captures packets from wireless networks in monitor mode.
wlan0mon – This is the wireless interface in monitor mode (e.g., wlan0mon is the monitor mode version of wlan0).
-w ~/wifi/scan – Saves the captured data (packet dump) to a file in the ~/wifi/ directory with the filename prefix scan.
--manufacturer – Displays the manufacturer (vendor) of detected access points and clients using their Media Access Control (MAC) address.
--wps – Shows information about Wi-Fi Protected Setup (WPS), such as whether WPS is enabled and the version.
--band abg – Scans all Wi-Fi frequency bands:

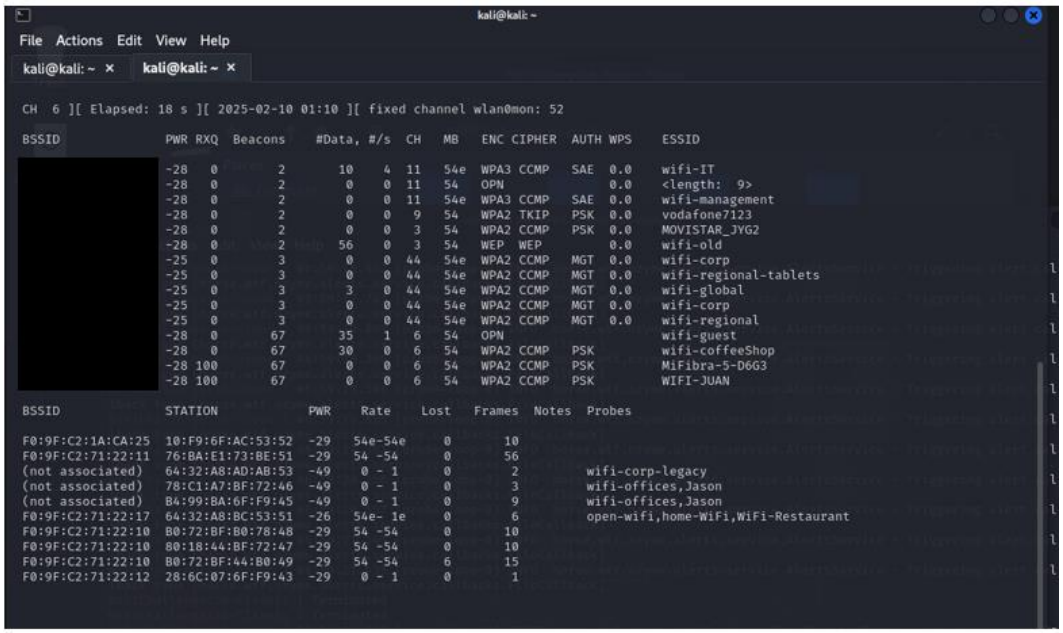
- a → 5 GHz (802.11a)
- b → 2.4 GHz (802.11b)
- g → 2.4 GHz (802.11g)

Note: `wlan0mon`: This is your wireless interface in monitor mode.

3. **Monitoring network traffic:** with your interface in monitor mode, you can start monitoring the network traffic. You begin by scanning for available Wi-Fi networks. Using one of the aircrack-ng suite tools, you can monitor the traffic of the "wifi-coffeeShop" network. The tool will allow you to scan nearby Wi-Fi networks, display information about each network, and allow you to capture packets.

```
sudo <aircrack-ng suite tool> wlan0mon -w ~/wifi/scanc -c
<channel number> --wps
```

wlan0mon – The wireless interface in monitor mode (wlan0mon is the monitor-mode version of wlan0).
-w ~/wifi/scanc – Saves the captured data (packet dump) in the ~/wifi/ directory with the filename prefix scanc.
-c 6 – Captures only Wi-Fi traffic on channel 6.
--wps – Displays Wi-Fi Protected Setup (WPS) information for detected access points (whether WPS is enabled, the version, etc.).



Do not close or end this.

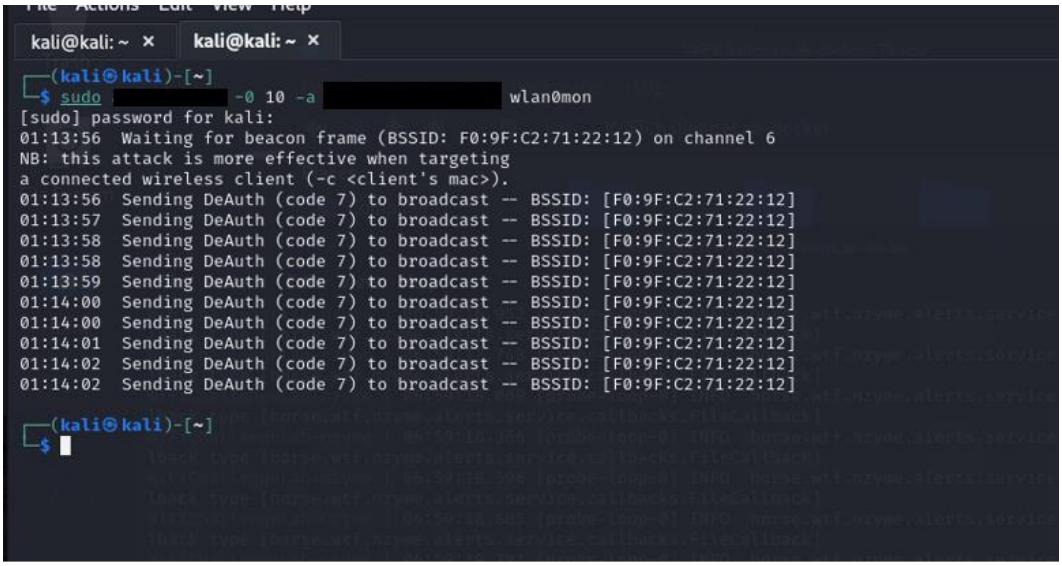
This command captures data from the “wifi-coffeeShop” network, including its MAC address and any connected devices. During this process, you gather information about the network’s MAC address and the clients connected to it.

What is the MAC address associated with wifi-coffeeShop? _____

4. **Deauthentication attack:** once you notice a client connected to the network, you decide to expedite the capture of the WPA2 handshake. You launch a deauthentication attack using one of the Aircrack-ng suite tools to force the client to disconnect and reconnect, which generates a handshake.

   Open another tab in terminal and run the following command:

   `sudo <aircrack-ng suite tool> -0 10 -a <wifi-coffeeShop mac address> wlan0mon`



After this completes, wait 2–3 min, then proceed to next step.

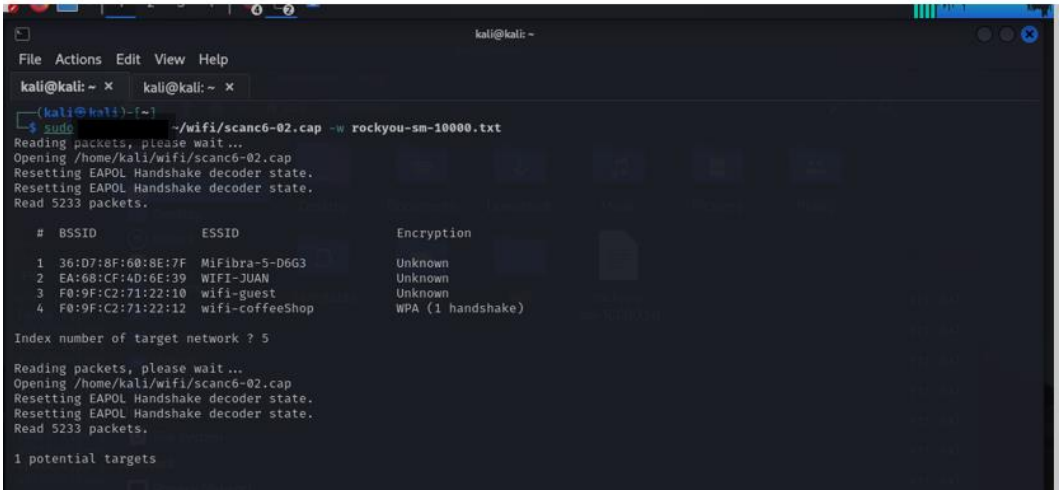
This command sends 10 deauthentication packets to the specified MAC address of the client, forcing them to disconnect from the network and prompting them to reconnect, thus generating the WPA2 handshake needed for password cracking.

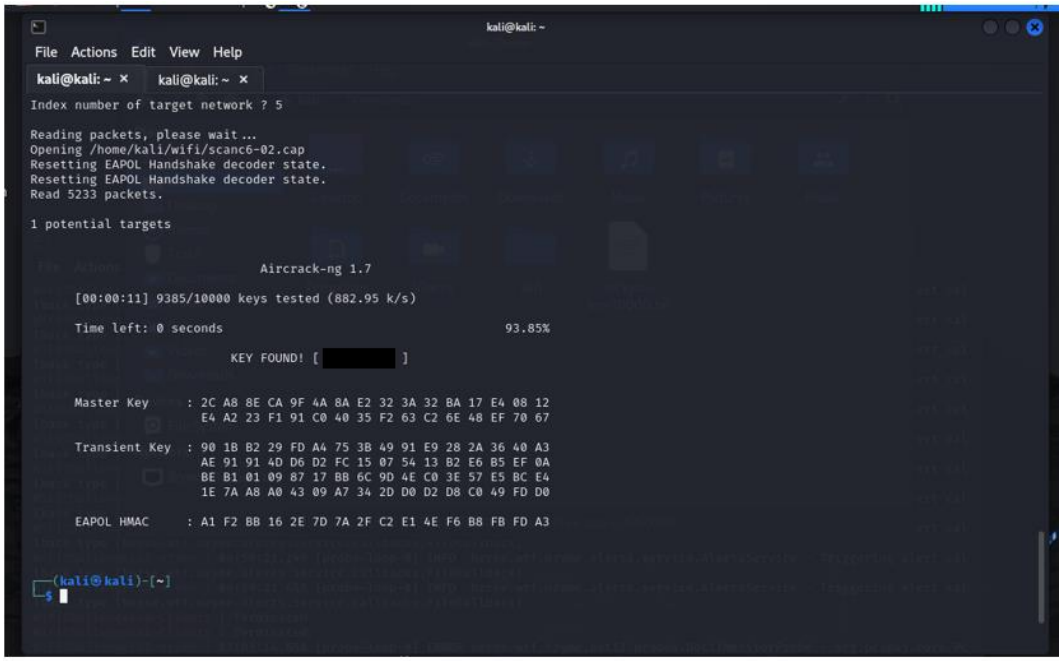
After 2–3 min have passed, you may close or Ctrl+C the tab we left running that captured data from the “wifi-coffeeShop” network.

5. **Cracking the WPA2 password**: with the WPA2 handshake captured, you now attempt to crack the Wi-Fi password. You use one of the Aircrack-ng suite tools with a wordlist like rockyou.txt to attempt to find the correct password.

```
sudo <aircrack-ng suite tool> ~/wifi/scanc.cap -w ~/rockyou-sm-10000.txt
```

~/wifi/scanc.cap – The capture file (.cap) that contains the WPA/WPA2 handshake (collected using airodump-ng).
-w ~/rockyou-sm-10000.txt – Specifies a wordlist file (rockyou-sm-10000.txt) to use for a dictionary attack.





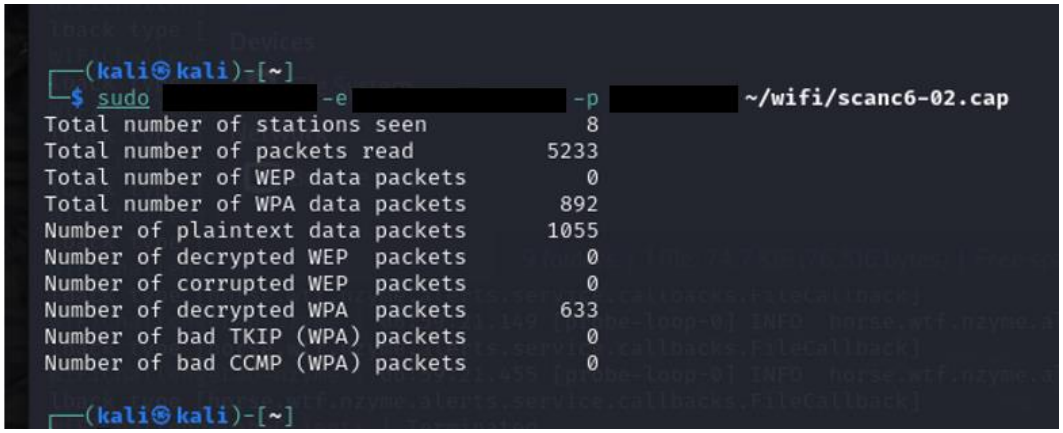
After running the cracking process, the tool successfully decodes the Wi-Fi password, revealing that it was weak and easily guessable.

What was the password? _____

6. **Decrypting network traffic:** now that you have the Wi-Fi password, you can decrypt the previously captured traffic. Using one of the Aircrack-ng suite tools, you decrypt the packets captured earlier.

   ```
   sudo <aircrack-ng suite tool> -e <wifi name> -p <password> ~/wifi/scanc.cap
   ```

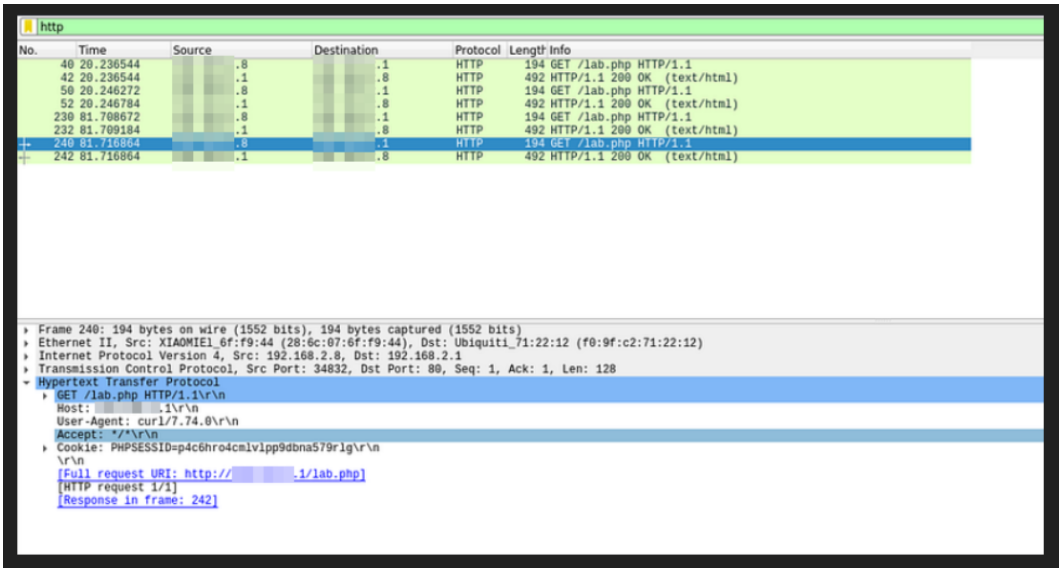
   This command decrypts captured WPA/WPA2-encrypted traffic using the provided Wi-Fi service set identifier (SSID) and password. Once decrypted, the capture file will contain readable network traffic, including unencrypted data like HTTP requests.



   After decryption, use the following command to open the resulting file in Wireshark to analyze the traffic. Upon inspection, you discover that one of the IPs in the decrypted traffic is associated with the HTTP server.

   ```
   wireshark ~/wifi/scanc.cap
   ```

   What is the IP? _____



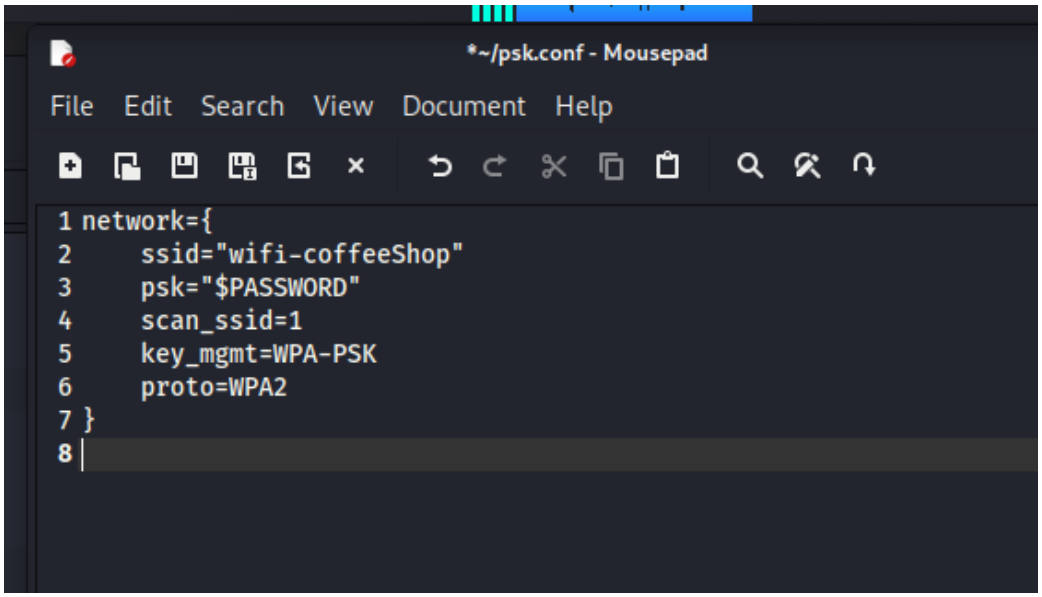
Save the cookies for future use.

7. **Session hijack:** The first thing we must do is to connect to the network. To do that, we can use “wpa_supplicant.”

   First, create a file called psk.conf with the following:
   `psk.conf`

```
network={
    ssid="wifi-coffeeShop"
    psk="$PASSWORD"
    scan_ssid=1
    key_mgmt=WPA-PSK
    proto=WPA2
}
```

   Note: change $password to contain the network’s password.



Run:

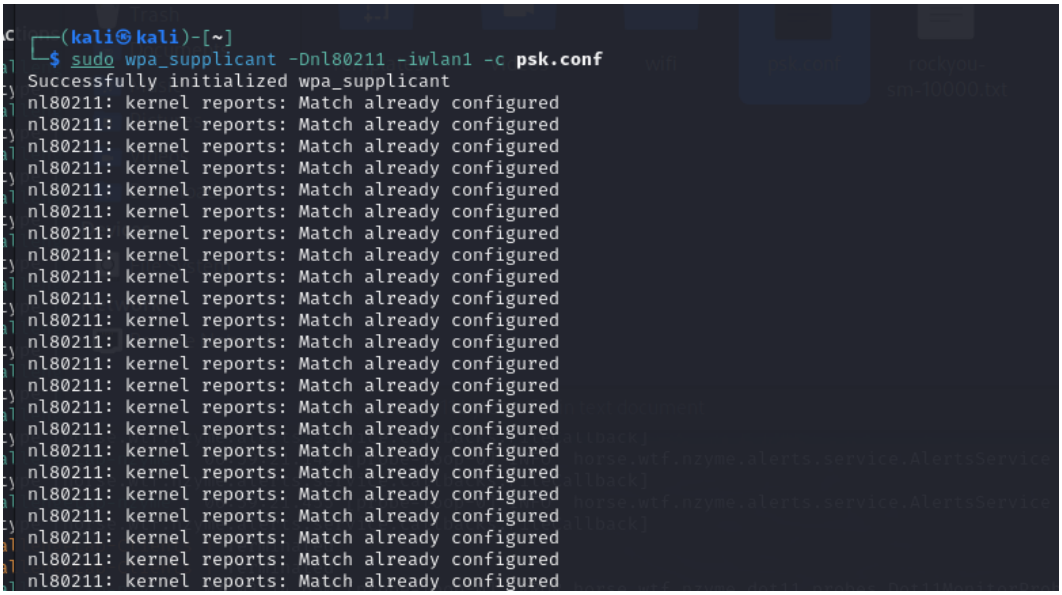
```
sudo wpa_supplicant -Dnl80211 -iwlan1 -c psk.conf
```

This command connects to a WPA/WPA2 Wi-Fi network using the settings stored in psk.conf. It does the following:

a. Loads the Wi-Fi credentials from psk.conf.

b. Uses the nl80211 driver to communicate with the network card.

c. Attempts to establish a connection on the wlan1 interface.



In another tab, type the following:

```
sudo dhclient wlan1 -v
```

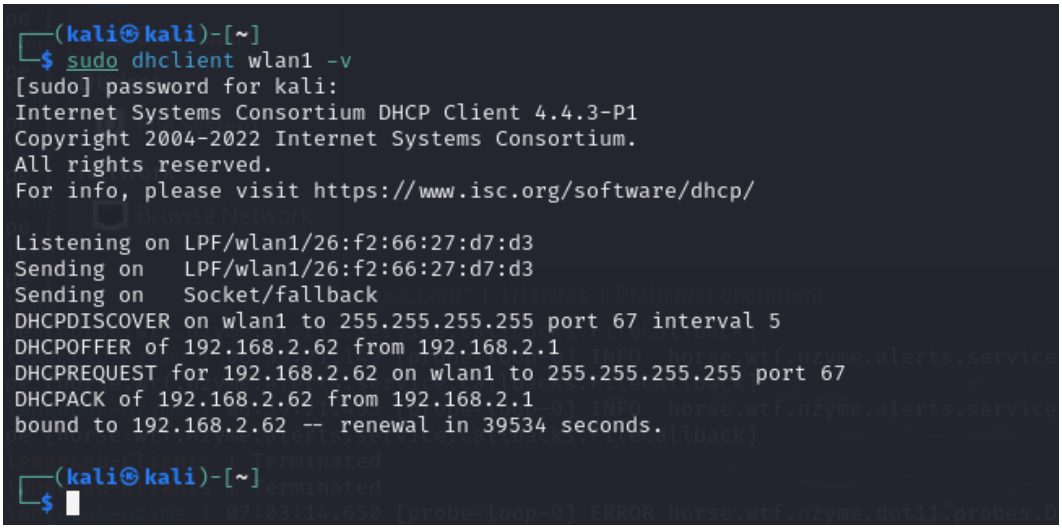
This command requests an IP address for the wlan1 interface from a Dynamic Host Configuration Protocol (DHCP) server (typically your router). It does the following:

a. Sends a DHCP discover request on wlan1 to find an available DHCP server.

b. Requests an IP lease from the DHCP server.

c. Assigns the received IP address to wlan1, allowing internet access.

d. Displays detailed logs of the process.

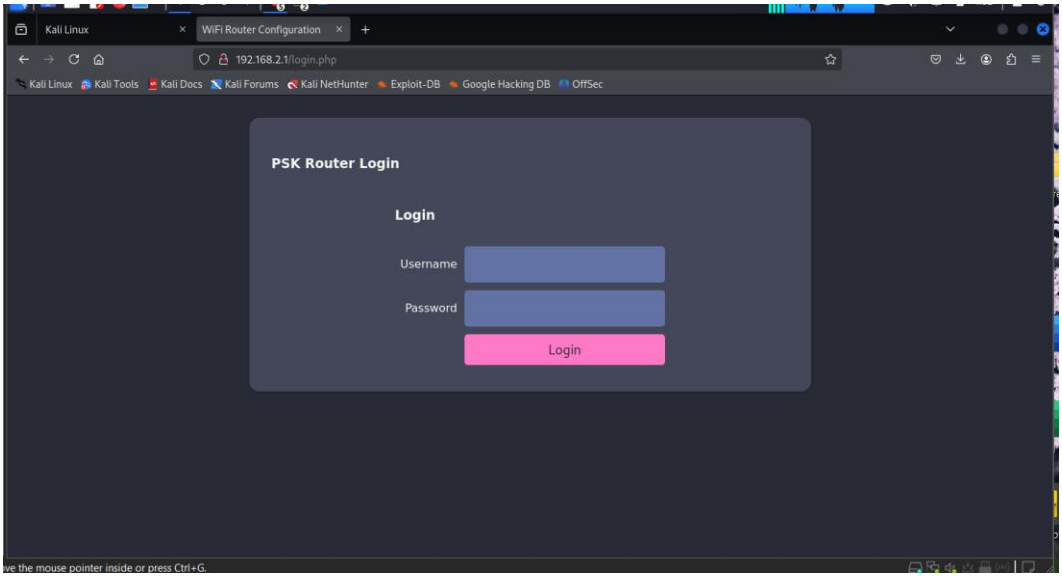


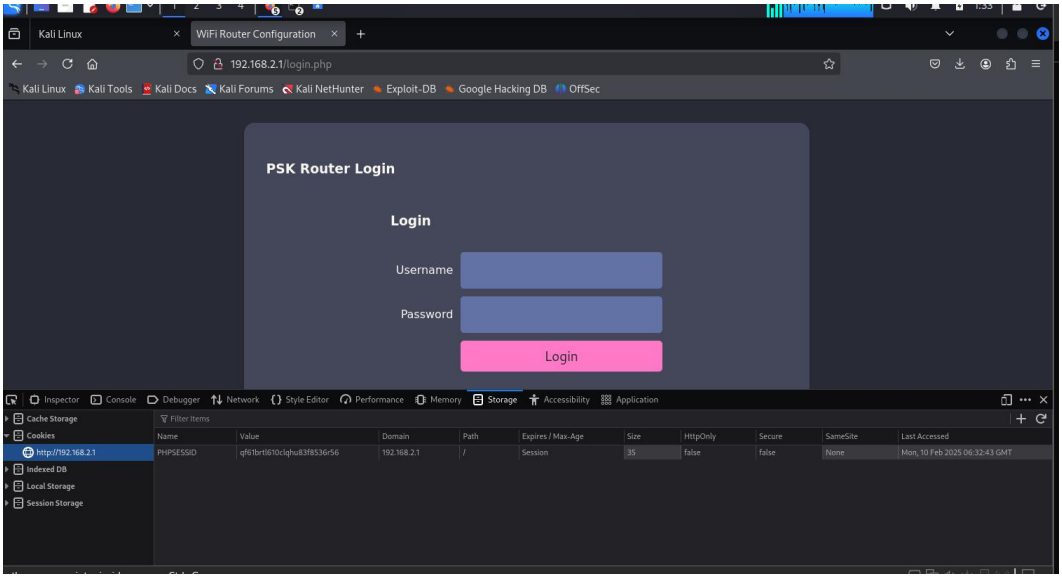
We can use the session cookie to gain access and obtain the flag.

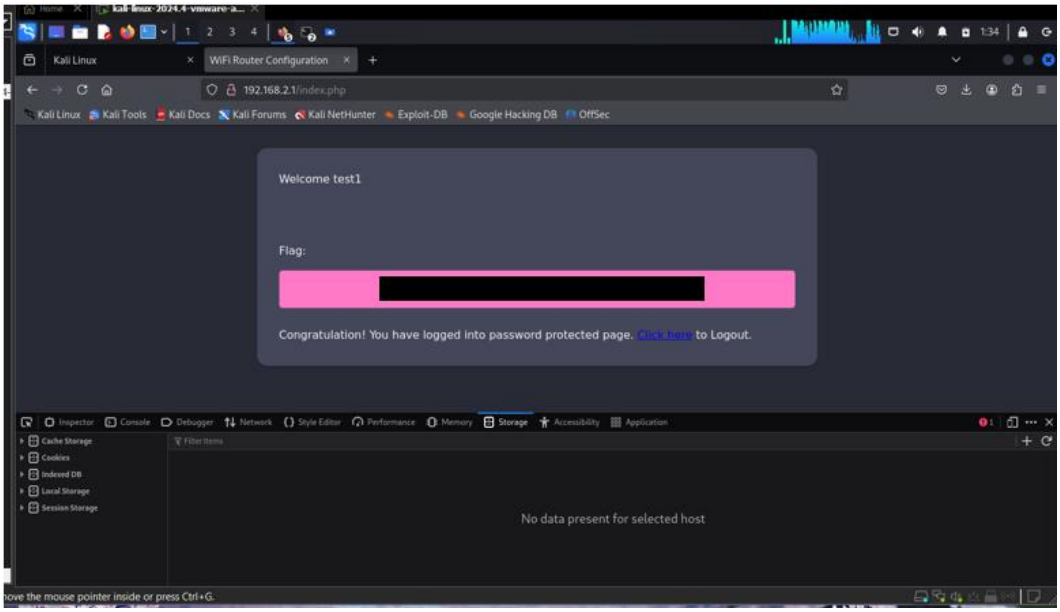
Open your browser and go to the server's IP.

Go to developer tools > storage and change the value of the cookie.

Now try accessing index.php. Can you see the flag?


Kali Linux
WiFi Router Configuration
192.168.2.1/login.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
PSK Router Login
Login
Username
Password
Login
ve the mouse pointer inside or press Ctrl+G.


Kali Linux
WiFi Router Configuration
192.168.2.1/login.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
PSK Router Login
Login
Username
Password
Login
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Cache Storage
Cookies
http://192.168.2.1
Indexed DB
Local Storage
Session Storage
Filter Items
Name Value Domain Path Expires / Max-Age Size HttpOnly Secure SameSite Last Accessed
PHPSESSID qf61brtl610clqhu83f8536r56 192.168.2.1 / Session 35 false false None Mon, 10 Feb 2025 06:32:43 GMT



Flag: _____

You realize this is how customers' data has been accessed.

Why is this attack possible? Open or weakly protected networks allow interception.

How can users protect themselves? Use HTTPS, VPNs, and strong Wi-Fi encryption.

Use strong, unique passwords: avoid dictionary words and use long, random passwords to make brute-force attacks infeasible.

Enforce HTTPS on websites: ensuring all web traffic is encrypted with HTTPS prevents attackers from stealing session cookies via packet sniffing.

What are countermeasures against deauthentication attacks? Implement WPA3, 802.11w, and monitoring tools.

5. Conclusion

This exercise provides participants with valuable hands-on experience in Wi-Fi security by simulating real-world attack scenarios such as capturing network traffic, cracking Wi-Fi passwords, and performing session hijacking. Using tools like the Aircrack-ng suite, Wireshark, and wpa_supplicant, participants develop a deep understanding of Wi-Fi security protocols and the vulnerabilities that can be exploited by attackers. By learning how to monitor, decrypt, and manipulate network traffic, participants gain practical skills to identify and mitigate common

Wi-Fi security risks. The exercise also emphasizes the importance of using strong encryption, secure passwords, and HTTPS to protect against unauthorized access and data theft in both personal and public network environments.

6. References

1. Walkthrough WiFiChallenge Lab v2.0. Raúl Calvo Laorden; c2025 [accessed 2025 Apr]. https://r4ulcl.com/posts/walkthrough-wifichallenge-lab-2.0/
2. WiFiChallengeLab-docker. GitHub, Inc; c2025 [accessed 2025 Apr]. https://github.com/r4ulcl/WiFiChallengeLab-docker
3. Aircrack-ng. Aircrack-ng; c2023 [accessed 2025 May]. https://www.aircrack-ng.org/
4. Kali Linux operating system. OffSec Services Limited; c2025 [accessed 2025 May]. https://www.kali.org/
5. VMware. Broadcom; c2025 [accessed 2025 May]. https://www.vmware.com/
6. Docker desktop. Docker Inc; c2025 [accessed 2025 May]. https://www.docker.com

List of Symbols, Abbreviations, and Acronyms

DHCP	Dynamic Host Configuration Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
MAC	Media Access Control
SSID	service set identifier
VM	virtual machine
VPN	virtual private network
WEP	Wired Equivalent Privacy
WPA-PSK	Wi-Fi Protected Access Pre-Shared Key
WPA2	Wi-Fi Protected Access 2
WPS	Wi-Fi Protected Setup

1 (PDF)	DEFENSE TECHNICAL INFORMATION CTR DTIC OCA
1 (PDF)	DEVCOM ARL FCDD RLB CI TECH LIB