**WPA2 Attack using Hashcat and Hcxdumptool**

1. **Introduction**

WPA2 is the most used security protocol for securing wireless networks. Even with its robust encryption and security mechanisms, WPA2 is vulnerable to attacks, especially to those involving the handshake process. This report primarily focuses on two key tools used to attack the WPA2 secured network- hashcat and hcxdumptool, by exploiting the vulnerabilities in the handshake procedure. These tools enable threat actors to capture and crack the WPA2 passwords by applying various attack strategies such as dictionary and brute-force attacks.

1. **Understanding WPA2 security**

WPA2 utilizes Advanced Encryption Standard (AES) for encryption and Pre-Shared Key (PSK) for authentication. The WPA2 handshake is essentially a four-way process that builds a secure connection between the client and the access point which are also referred to as supplicant and authenticator respectively. However, the strength of the WPA2 encryption rely deeply on the strength of the pre-shared key.

**WPA2 four-way handshake process**

**Step 1:** The client sends a request to the access point (AP)

**Step 2:** The access point responds with its nonce (number used once)- a random value and message to start the handshake

**Step 3:** The client creates its own nonce along with the AP’s and derives a session key

**Step 4:** Both client and AP share the key information messages that confirms the establishment of a secure connection

At this stage, the handshake is completed and the keys for encryption are exchanged. The attackers try to capture this handshake essential for cracking the WPA2 password with the help of brute-force or dictionary attacks.

1. **Tools for WPA2 attacks**  
   1. **Hashcat**   
      **Hashcat** is a powerful password cracking tool that can be used for a variety of hashing algorithms, including those used in WPA2. Hashcat utilizes the GPU (Graphics Processing Unit) to accelerate the cracking process, allowing for efficient brute-forcing or dictionary-based cracking of passwords.  
        
      **WPA2 Handshake Process**  
      When an attacker captures the WPA2 handshake, it holds the hash of WPA2 Pre-Shared Key (PSK) obtained from the passphrase. This hash can be cracked using hashcat to retrieve the original passphrase.

**Most common attacks in Hashcat:**

**Brute-Force attack**- Hashcat tries all possible combination of characters until it cracks the password.

**Dictionary attack**- The attacker attempts every possible password combination from a wordlist and matches the hash of the word from the wordlists with the captured hash.  
**Rule-based attack-** Hashcat implies pre-defined rules to a dictionary by adding commonly used prefixes and suffixes or replacing alphabets with special characters to create an extensive list of passwords.

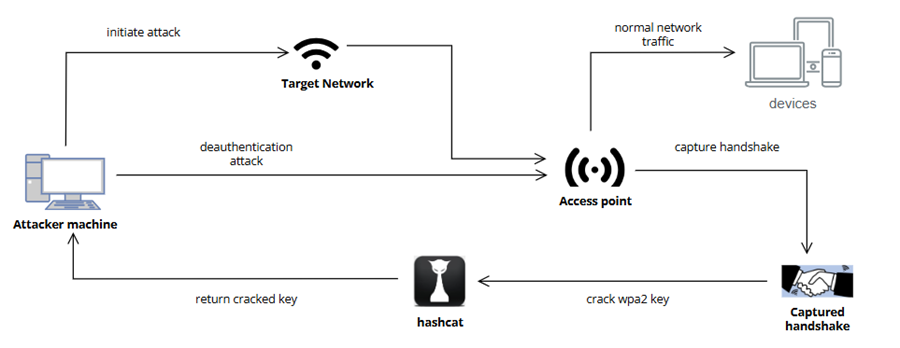
* 1. **Hcxdumptool**  
     **Hcxdumptool** is a tool used for capturing WPA2 handshake from wireless networks. As part of the hcxtools suite, it is designed to attack the WPA2 and WPA3 networks.

**Key features of hcxdumptool:**

**Capture WPA2 handshakes-** hcxdumptool captures the 4-way handshake while the client is attempting to connect with the access point.

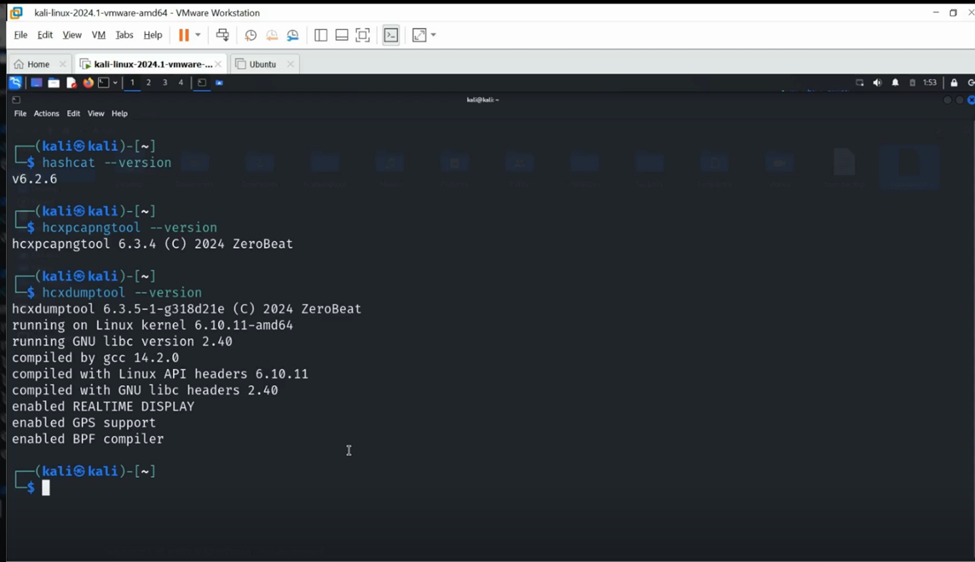
**De-authentication attacks-** hcxdumptool sends de-authentication packets to force clients to reconnect to the access point, initiating a handshake capture.  
   
**Output Formats-** This tool can save the captured handshake in various formats such as .pcapng, which can further be converted for use in hashcat.

1. **Network Diagram**



1. **WPA2 cracking process**

**a) Installation of the required tools**



The tools required for the password cracking are hcxdumptool, hcxpcapngtool and hashcat. The above screenshot shows the installed versions of each of them.

**b) Stopping Network Management Services**

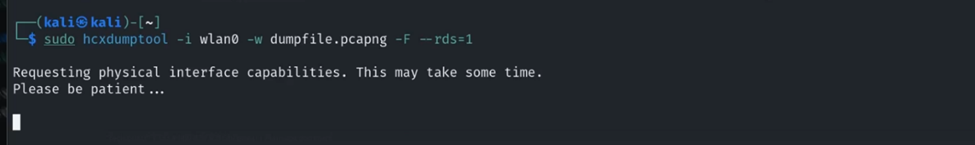
Disable active network connections and management services to prevent interference with Wi-Fi monitoring tools.



NetworkManager.service: Manages network connections on Linux systems.

wpa\_supplicant.service: Handles Wi-Fi authentication for connections using WPA/WPA2.

c) **Capturing Wi-Fi Traffic with hcxdumptool**

  
hcxdumptool will capture Wi-Fi traffic from the wlan0 interface and save it to dumpfile.pcapng for analysis.

Options:

-i wlan0: Specifies the wireless interface for packet capture

-w dumpfile.pcapng: Saves captured packets to a .pcapng file for later analysis

-F: Forces the tool to terminate once a handshake or relevant traffic is captured

--rds=1: Enables Radiotap Signal Detection, providing additional information like signal strength

Output: List of networks scanned and the target network is SM-G950W7648

Output includes a list of scanned networks, with the target network being SM-G950W7648.

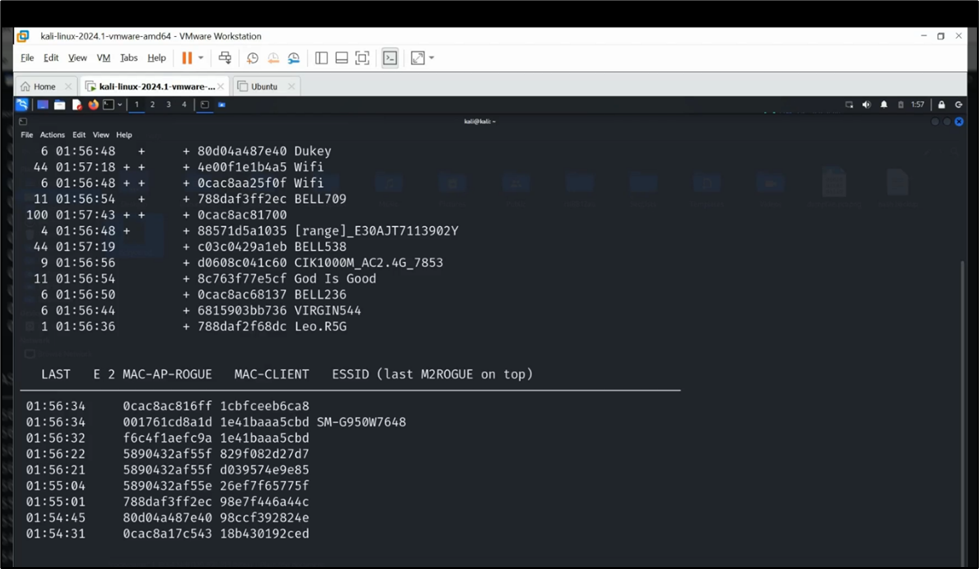
Output displays a list of scanned networks, with the target network, SM-G950W7648, highlighted.

Output lists all scanned networks, with SM-G950W7648 as the target network.

Output provides a list of scanned networks, highlighting SM-G950W7648 as the target.

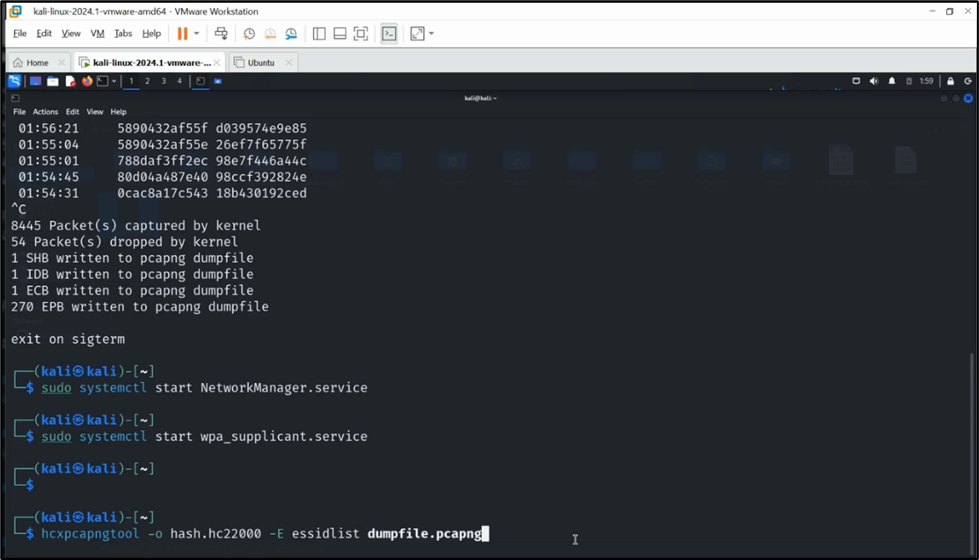
Output shows scanned networks, with SM-G950W7648 marked as the target network.

Output displays scanned networks, emphasizing the target network, SM-G950W7648.



d) **Restart the Network Management Services**

After capturing Wi-Fi traffic with hcxdumptool, we restart wpa\_supplicant.service and NetworkManager.service to restore automatic network management.



e) **Converting Captured Traffic to Hash File**

hcxpcapngtool extracts useful information from the .pcapng file.

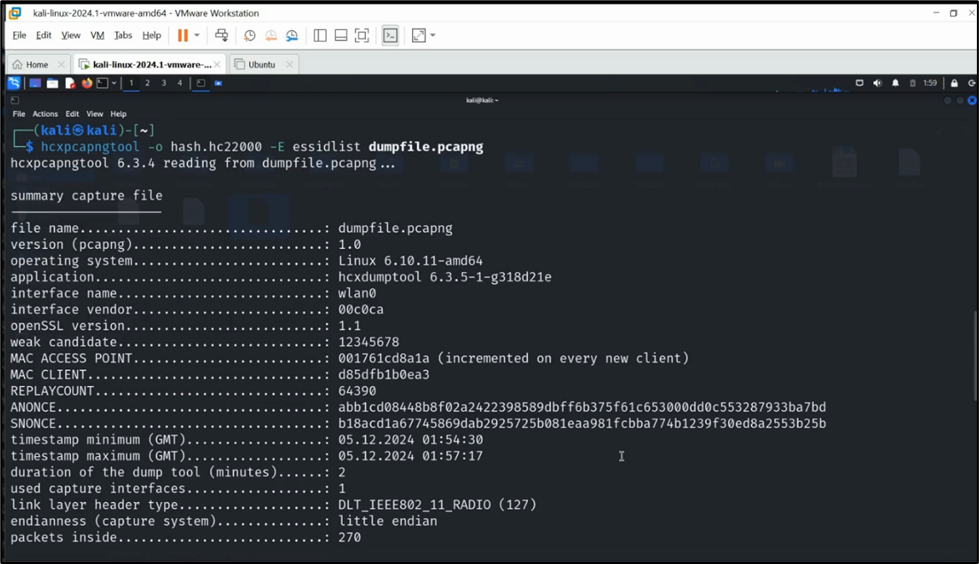
***hcxpcapngtool -o hash.hc22000 -E essidlist dumpfile.pcapng***

Options:

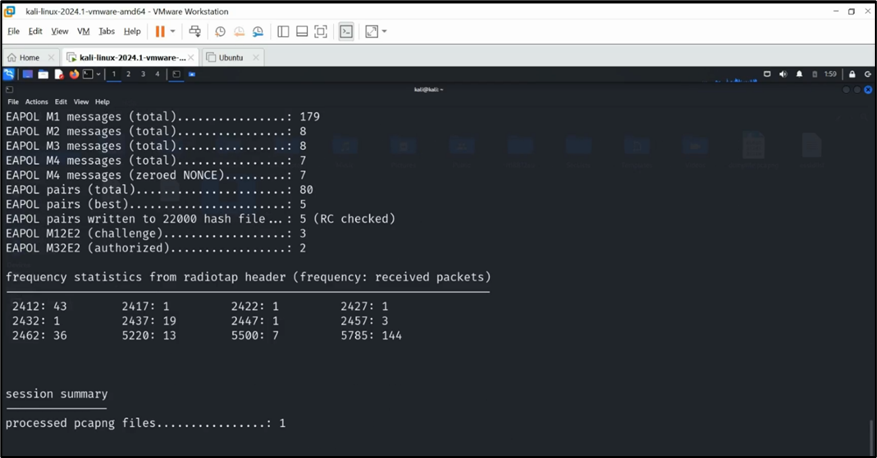
-o hash.hc22000: Saves the extracted hash into a file in the .hc22000 format, compatible with Hashcat.

-E essidlist: Extracts a list of ESSIDs (network names) from the capture.

The following screenshot shows the output of hcxpcapngtool processing the dumpfile.pcapng to generate a hash file (hash.hc22000) for password cracking.

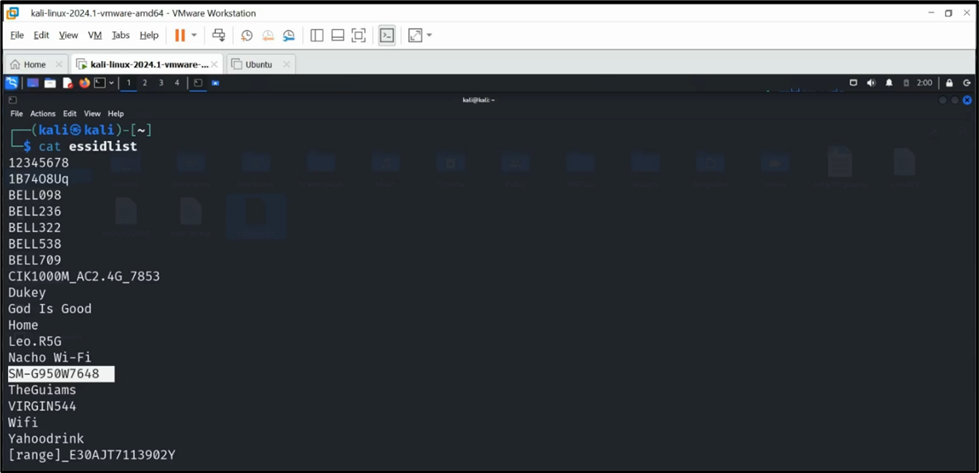


It includes capture details such as timestamps, MAC addresses, EAPOL message counts and packet statistics.

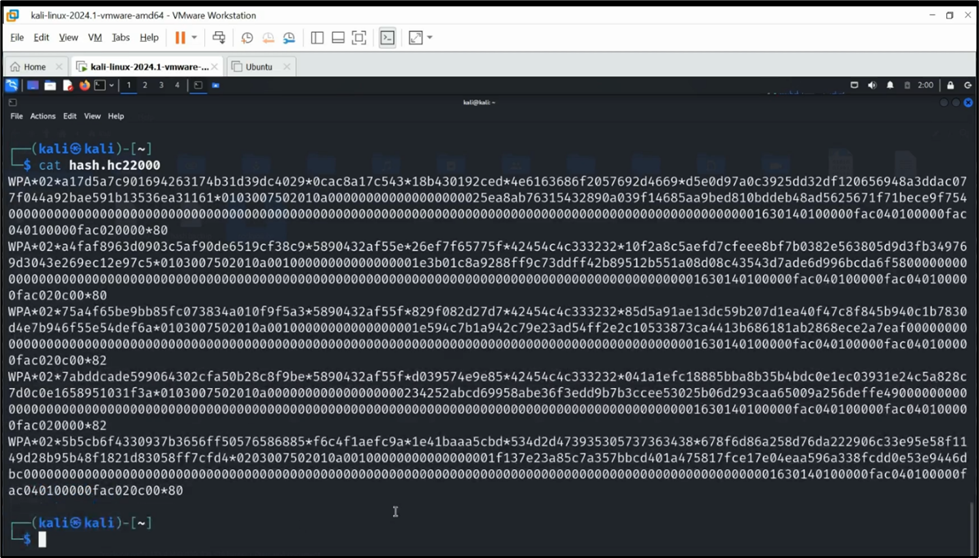


f) **Check if desired ESSID and MAC Address are in Hashcat List**

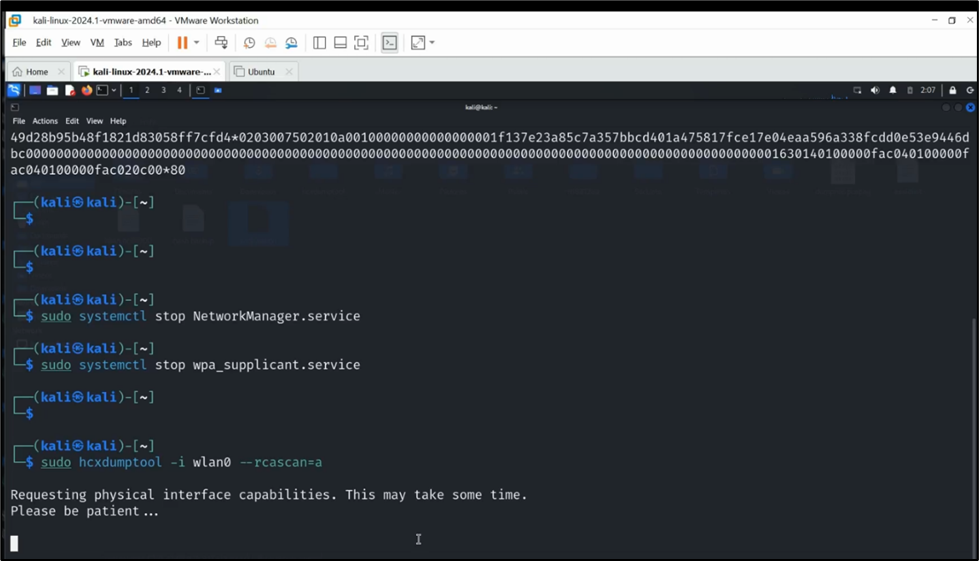
Following shows the output of the ***cat essidlist*** command, which displays the list of Wi-Fi network names (ESSIDs) captured during the previous step using hcxdumptool.



The ***cat hash.hc22000*** command displays the contents of the hash.hc22000 file, which contains the captured hash data from the Wi-Fi networks.



**g) Stopping Network Management Services and Scanning for MAC Addresses with hcxdumptool**

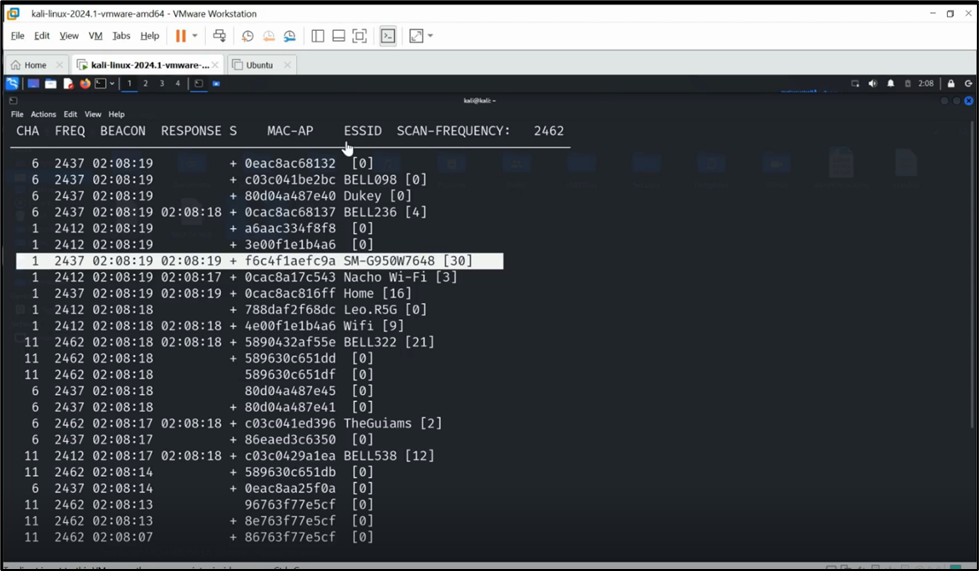
Network Management services is stopped for scanning available Wi-Fi networks and their MAC addresses to retrieve the target’s MAC address.  
  


Then, the following command is used to scan for active Wi-Fi networks and log their MAC addresses, ESSIDs and other details.

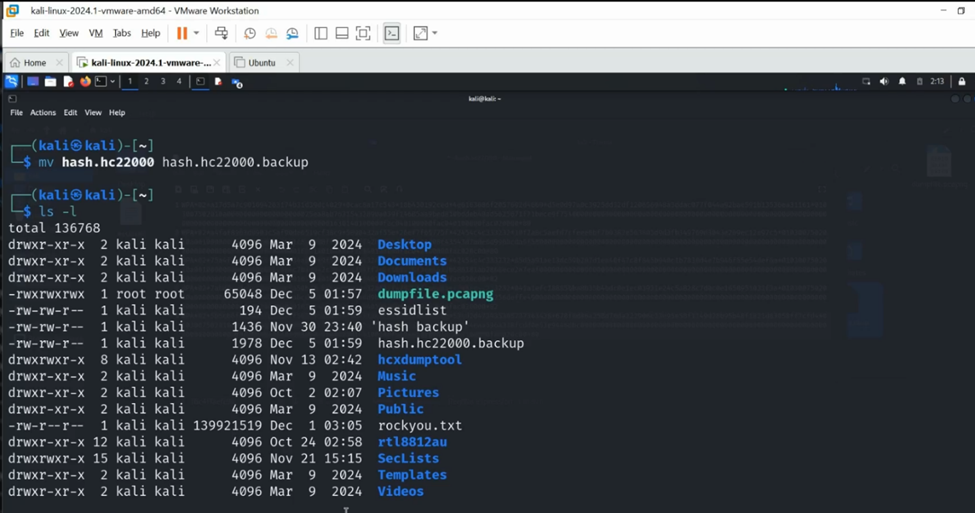
***sudo hcxdumptool -i wlan0 --rcascan=a***

Option:

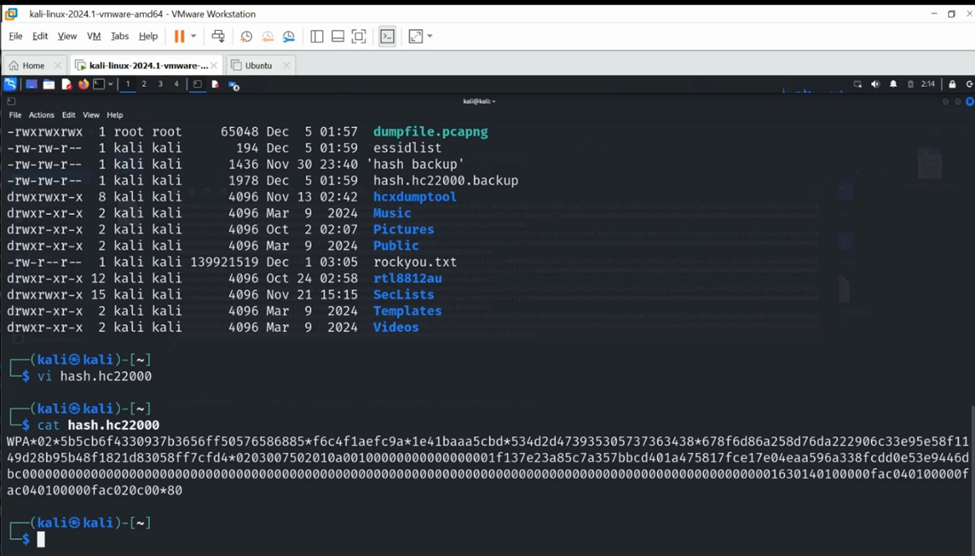
--rcascan=a: Provides detailed information about surrounding networks, including access point MAC addresses and signal strength.

  
h) **Move hash file to backup and edit for specific MAC address cracking**

***mv hash.hc22000 hash.hc22000.backup*** command renames the hash file and creates a backup of the original hashes.



By using ***vi hash.hc22000***, we are editing the file to focus on the specific MAC address for cracking, ensuring only the targeted data (ESSID: SM-G950W7648) is used for cracking the Wi-Fi password.



i) Cracking WiFi hashes

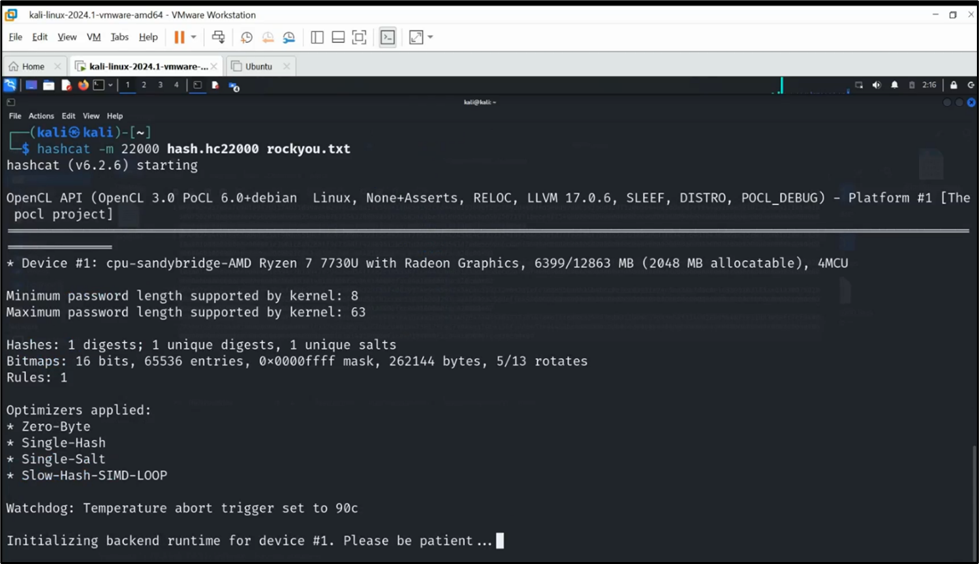
***hashcat -m 22000 hash.hc22000 rockyou.txt*** command uses hashcat to crack WPA/WPA2 Wi-Fi password hashes using dictionary attack.

Options:

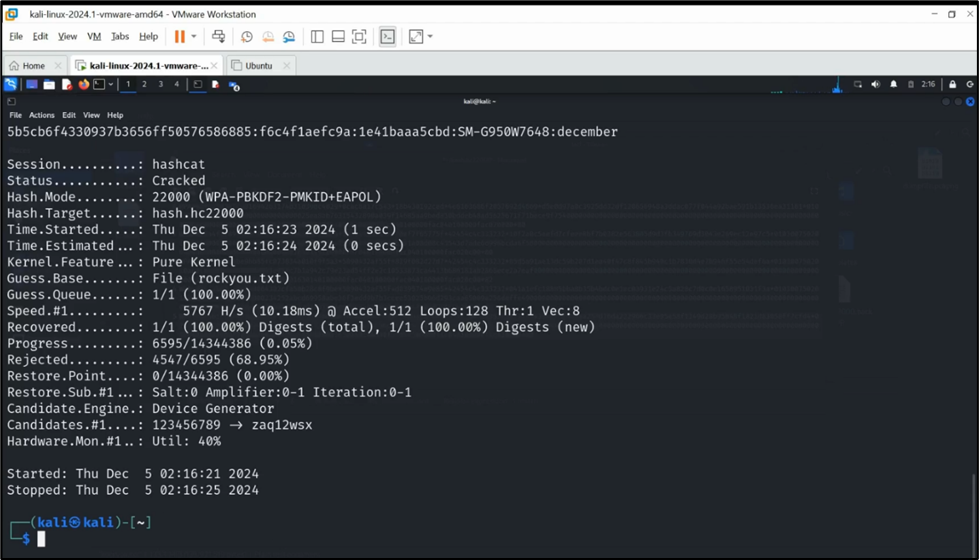
-m 22000: Specifies the hash type for WPA/WPA2 handshakes in .hc22000 format

hash.hc22000: The target hash file containing handshake data

rockyou.txt: A commonly used password dictionary file for cracking



Below screenshot shows that hashcat successfully cracked the WPA2 password hash from hash.hc22000 using the rockyou.txt wordlist. The target Wi-Fi network is **SM-G950W7648**, and the cracked password is **december**.



1. **Mitigation Strategies**

While WPA2 is known to be a strong protocol, it holds certain vulnerabilities. The following measures can assist in mitigating the risk of WPA2 password cracking:

**6.1 Strong Passwords**

The most effective security is a strong and complex password with a length of at least 12- 15 characters. The more complex the password, the harder it gets to crack.  
   
**6.2 Upgrade to WPA3**

WPA3 offers enhanced protection against dictionary-based cracking. It addresses the vulnerabilities found in WPA2, including protecting against offline dictionary attacks.

**6.3 Regular firmware updates**  
Regular firmware updates is essential for maintaining security. Usually, manufacturers release updates periodically which should be checked for and applied to patch any known vulnerabilities.

**6.4 Disable WPS (Wi-Fi Protected Setup)**

WPS is designed for ease of use, allowing quick connections to a Wi-Fi network via a button press or PIN. However, it has known security vulnerabilities, especially the WPS PIN method, which can be exploited through brute-force attacks. Disabling WPS can enhance network security.

**6.5 Avoid open and weak networks**

Connecting to weak networks or the ones without password can be highly vulnerable to attacks such as man-in-the-middle (MITM) and eavesdropping. Therefore, it is recommended to avoid using public Wi-Fi for private purpose such as accessing banking information or entering credentials. Wi-Fi networks such as WPA2 and WPA3 employ strong encryption, fostering a secured connection.

**6.7 Enable Firewall**

A firewall protects the network by monitoring the inbound and outbound traffic and blocking any malicious activities. It is recommended to enable the router’s built-in firewall and consider including firewall software on devices for additional layer of security.

1. **Conclusion**

WPA2 is widely used for securing wireless networks; however, it is susceptible to attacks that target the handshake and PSK. Tools like hashcat and hcxdumptool enable attackers to efficiently capture handshakes and crack passwords. As WPA2 security relies heavily on the strength of the PSK, using long, complex passwords is essential to mitigate the risk of compromise. Additionally, transitioning to WPA3 provides stronger security features that protect against modern attacks.

Understanding these tools and techniques is crucial for both attackers and defenders. While attackers use these methods for penetration testing and security auditing, defenders must implement strong passwords and consider advanced security protocols to protect their networks effectively.