# Lab 5 Report

By Julian Flum and Miftahul Huq

**Q1.** Why does the NIC need to be on monitor mode?

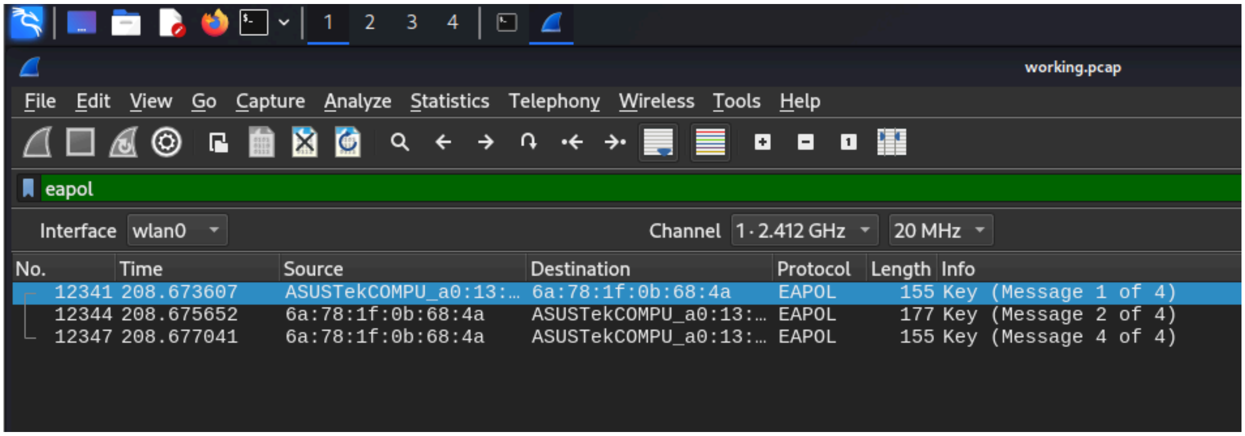
Regardless of the destination address, the Network Interface Card (NIC) can record all wireless communication within its range when in monitor mode. This mode offers an extensive view of the wireless network's activity, making it essential for network analysis and security testing. In contrast to managed mode, which involves the NIC filtering out packets that are not addressed to it, monitor mode guarantees that no data is lost, allowing for a thorough examination of network performance, security flaws, and troubleshooting problems.

**Q7.** Are you able to read the content of the data frames in WPA-PSK? How about the headers?

No, data frame content in WPA-PSK (Wi-Fi Protected Access Pre-Shared Key) networks is encrypted, rendering it unintelligible without the right decryption key. The purpose of this encryption is to shield user communications and data from illegal access and eavesdropping. To maintain appropriate wireless communication management and routing, the headers of these data frames are not encrypted. The headers do not contain the sensitive content of the message itself, but they do contain information that is required for the network to function, such as source and destination addresses, frame control fields, and duration.

**Q8.** What are the most important packets you will need to capture inorder to crack WPA2-PSK? Briefly describe what elements are in these packets and how they are used to generate a key. Include screenshots to explain.

Capturing EAPOL (Extensible Authentication Protocol over LAN) packets is essential to cracking WPA2-PSK. The four-way handshake used in WPA2 for key management and authentication includes EAPOL packets. They hold important data, including the encrypted PTK (Pairwise Transient Key), MIC (Message Integrity Code), ANonce (Authenticator Nonce), and SNonce (Suppliant Nonce). It is possible to determine the session keys used to encrypt communication by examining these components, particularly when paired with other known details like the password hash and SSID. This compromises the security of the network.



working.pcap

eapol

Interface wlan0

Channel 1 · 2.412 GHz 20 MHz

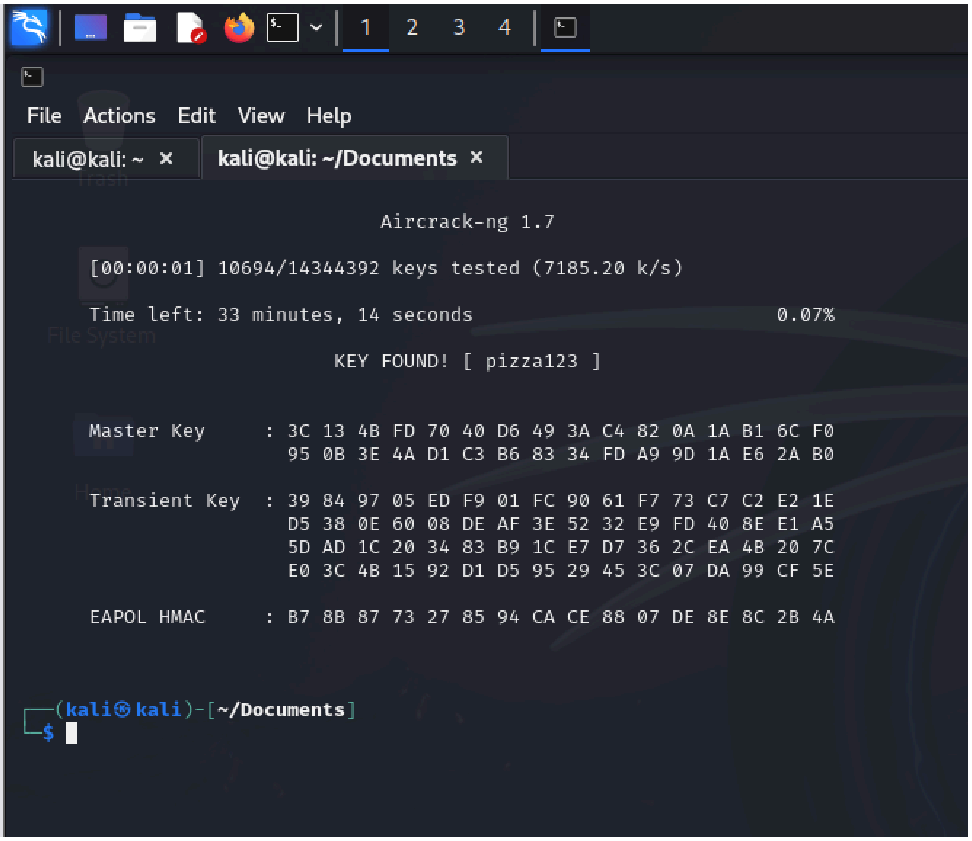
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 12341 | 208.673607 | ASUSTekCOMPU_a0:13:… | 6a:78:1f:0b:68:4a | EAPOL | 155 | Key (Message 1 of 4) |
| 12344 | 208.675652 | 6a:78:1f:0b:68:4a | ASUSTekCOMPU_a0:13:… | EAPOL | 177 | Key (Message 2 of 4) |
| 12347 | 208.677041 | 6a:78:1f:0b:68:4a | ASUSTekCOMPU_a0:13:… | EAPOL | 155 | Key (Message 4 of 4) |

**Q9.** What is the WPA2 Pre-Shared Key you discovered? Is it the same as your passphrase?

The WPA2 Pre-Shared key that was discovered was pizza123. It is the same as the passphrase. Discovering the WPA2 Pre-Shared Key, such as "pizza123," demonstrates the vulnerability of using weak, easily guessable passwords.

**Q10.** How long did it take to crack the WPA2-PSK? Include a screenshot in your report.

It takes 1 second.



```
                               Aircrack-ng 1.7

      [00:00:01] 10694/14344392 keys tested (7185.20 k/s)

      Time left: 33 minutes, 14 seconds                          0.07%

                           KEY FOUND! [ pizza123 ]


      Master Key     : 3C 13 4B FD 70 40 D6 49 3A C4 82 0A 1A B1 6C F0
                       95 0B 3E 4A D1 C3 B6 83 34 FD A9 9D 1A E6 2A B0

      Transient Key  : 39 84 97 05 ED F9 01 FC 90 61 F7 73 C7 C2 E2 1E
                       D5 38 0E 60 08 DE AF 3E 52 32 E9 FD 40 8E E1 A5
                       5D AD 1C 20 34 83 B9 1C E7 D7 36 2C EA 4B 20 7C
                       E0 3C 4B 15 92 D1 D5 95 29 45 3C 07 DA 99 CF 5E

      EAPOL HMAC     : B7 8B 87 73 27 85 94 CA CE 88 07 DE 8E 8C 2B 4A


┌──(kali㉿kali)-[~/Documents]
└─$ 
```

**Q11.** What other information do you need to enter to get the pre-shared key?

The SSID plays a crucial role in this process, serving as a nonce to add complexity to the encryption. However, with tools like aircrack-ng, capturing the four-way handshake packets and using them along with the SSID can allow attackers to perform dictionary or brute-force attacks to discover the network's PSK.

**Q12.** Looking at steps 4 and 5, how do you think one can mitigate this attack (other than using a complex passphrase)?

In addition to employing a complicated passphrase, the following techniques help lessen WPA2-PSK attacks:

changing the PSK and SSID of the network on a regular basis to keep attackers from having a permanent target.

putting in place extra security measures, including network segmentation, to restrict access even in the event that the PSK is hacked.

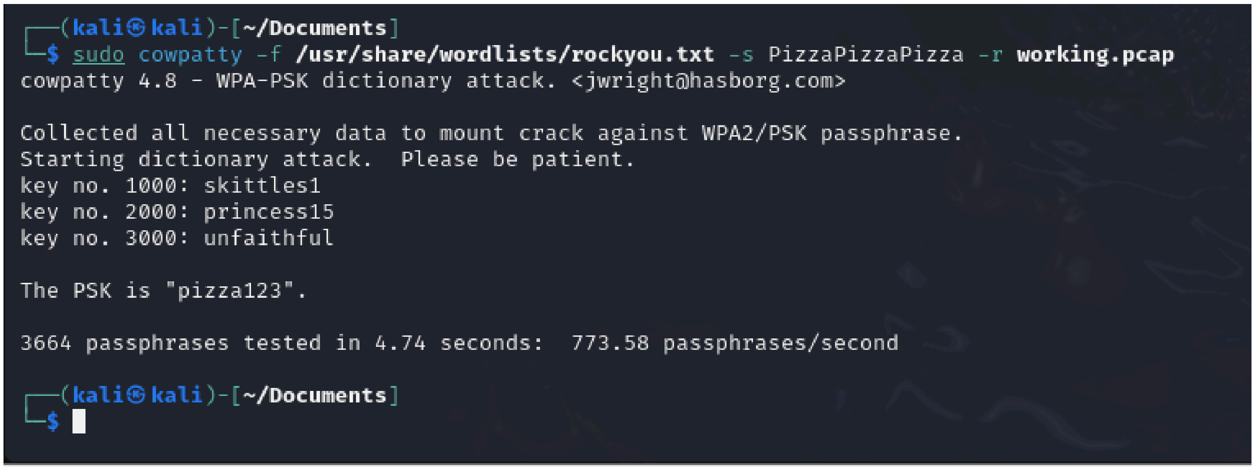
employing cutting-edge encryption techniques, such as WPA3, which provides stronger defense against brute-force attacks.

utilizing anomaly detection and network monitoring tools to quickly spot and address questionable activity.

By including these thorough explanations in your paper, readers will gain a better understanding of wireless network security, WPA2-PSK vulnerabilities, and the steps required to safeguard wireless networks.

**Q13.** How long did it take to crack the same WPA2-PSK of Activity 4?

It takes 4.74 seconds.



```
┌──(kali㉿kali)-[~/Documents]
└─$ sudo cowpatty -f /usr/share/wordlists/rockyou.txt -s PizzaPizzaPizza -r working.pcap
cowpatty 4.8 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA2/PSK passphrase.
Starting dictionary attack.  Please be patient.
key no. 1000: skittles1
key no. 2000: princess15
key no. 3000: unfaithful

The PSK is "pizza123".

3664 passphrases tested in 4.74 seconds:  773.58 passphrases/second

┌──(kali㉿kali)-[~/Documents]
└─$ 
```