

Informe Laboratorio 3

Sección x

Javier Ahumada

e-mail: javierigna.ahumada@mail.udp.cl

Mayo de 2023

Índice

1. Descripción de actividades	2
2. Desarrollo (PASO 1)	2
2.1. identificar en qué se destaca la red del informante del resto	2
2.2. explica matemáticamente porqué se requieren más de 5000 paquetes para obtener la pass	3
2.3. obtiene la password con ataque por defecto de aircrack-ng	3
2.4. indica el tiempo que demoró en obtener la password	4
2.5. descifra el contenido capturado	4
2.6. describe como obtiene la url de donde descargar el archivo	4
3. Desarrollo (PASO 2)	6
3.1. indica script para modificar diccionario original	6
3.2. cantidad de passwords finales que contiene rockyou_mod.dic	6
4. Desarrollo (Paso 3)	7
4.1. obtiene contraseña con hashcat con potfile	7
4.2. identifica nomenclatura del output	7
4.3. obtiene contraseña con hashcat sin potfile	8
4.4. identifica nomenclatura del output	8
4.5. obtiene contraseña con aircrack-ng	8
4.6. identifica y modifica parámetros solicitados por pycrack	9
4.7. obtiene contraseña con pycrack	11

1. Descripción de actividades

Su informante quiere entregarle la contraseña de acceso a una red, pero desconfía de todo medio para entregársela (aún no llega al capítulo del curso en donde aprende a comunicar una password sin que nadie más la pueda interceptar). Por lo tanto, le entregará un archivo que contiene un desafío de autenticación, que al analizarlo, usted podrá obtener la contraseña que lo permite resolver. Como nadie puede ver a su informante (es informante y debe mantener el anonimato), él se comunicará con usted a través de la redes inalámbricas y de una forma que solo usted, como experto en informática y telecomunicaciones, logrará esclarecer.

1. Identifique cual es la red inalámbrica que está utilizando su informante para enviarle información. Obtenga la contraseña de esa red utilizando el ataque por defecto de aircrack-ng, indicando el tiempo requerido para esto. Descifre el contenido transmitido sobre ella y descargue de Internet el archivo que su informante le ha comunicado a través de los paquetes que usted ha descifrado.
2. Descargue el diccionario de RockyouLinks to an external site. (utilizado ampliamente en el mundo del pentesting). Haga un script que para cada string contenido en el diccionario, reemplace la primera letra por su letra en capital y agregue un cero al final de la password.
3. Todos los strings que comiencen con número toca eliminarlos del diccionario. Indique la cantidad de contraseñas que contiene el diccionario modificado debe llamarse rock-you_mod.dic A continuación un ejemplo de cómo se modifican las 10 primeras líneas del diccionario original.

2. Desarrollo (PASO 1)

2.1. identificar en qué se destaca la red del informante del resto

Se destaca sobre las otras redes por la excesiva data que se capturaba con la tarjeta de wi fi

2.2 explica matemáticamente porqué se requieren más de 5000 paquetes para obtener la $pass$ DESARROLLO (PASO 1)

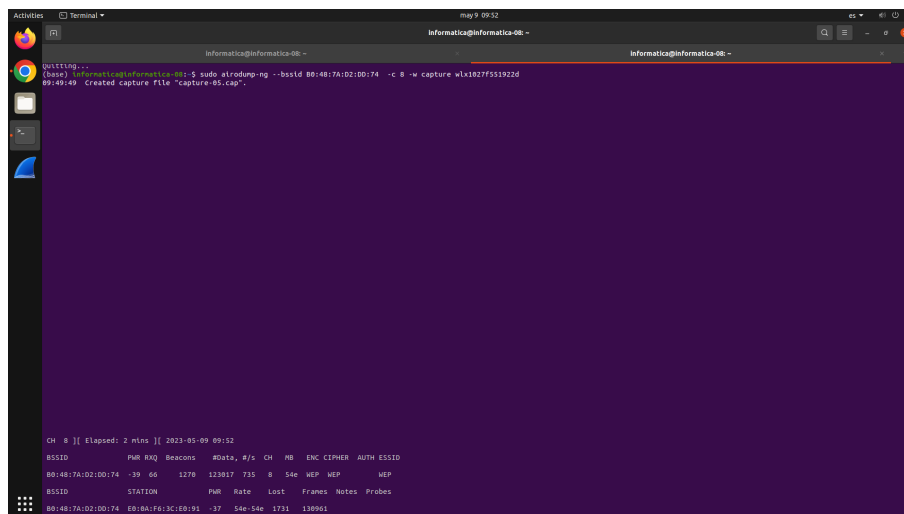


Figura 1: Airodump de la red WEP

2.2. explica matemáticamente porqué se requieren más de 5000 paquetes para obtener la $pass$

Porque en ataques de diccionario se necesitan suficientes paquetes capturados para obtener la clave de cifrado. En el caso de WEP, se requieren alrededor de 5000 IVs para tener una probabilidad razonable de recuperar la clave

2.3. obtiene la password con ataque por defecto de aircrack-ng

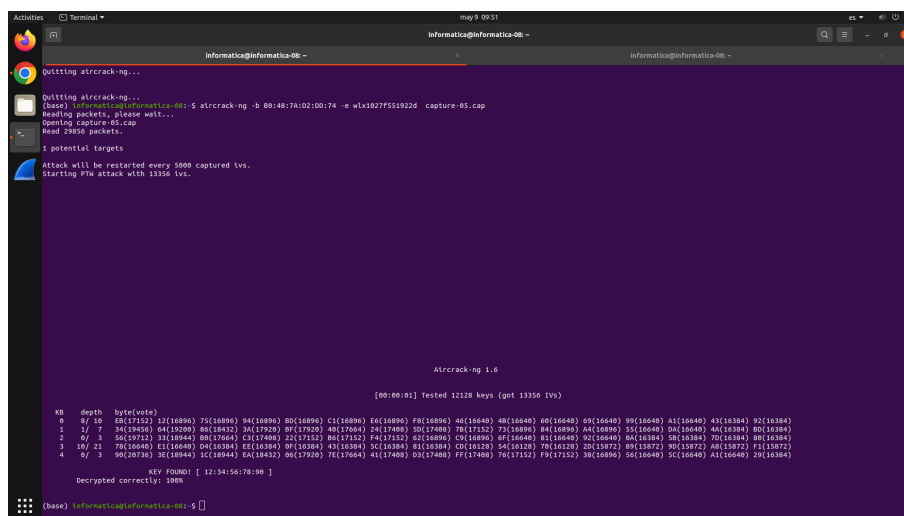


Figura 2: Dado el BSSID de WEP se obtiene la KEY 12:34:56:78:90

2.4. indica el tiempo que demoró en obtener la password

1 hora y 20 minutos

2.5. descifra el contenido capturado

```
javier@javier-Nitro-AN515-53:~/Escritorio/cripto/j/lab3$ airdecap-ng -w 12:34:56:78:90 capture-05.cap
Total number of stations seen      5
Total number of packets read      314811
Total number of WEP data packets  141542
Total number of WPA data packets  0
Number of plaintext data packets  2
Number of decrypted WEP packets  141542
Number of corrupted WEP packets  0
Number of decrypted WPA packets  0
Number of bad TKIP (WPA) packets  0
Number of bad CCMP (WPA) packets  0
```

Figura 3: Dado el airodump capture-05.cap generado anteriormente y la KEY obtenida, se descifra el contenido y genera un nuevo archivo .cap

2.6. describe como obtiene la url de donde descargar el archivo

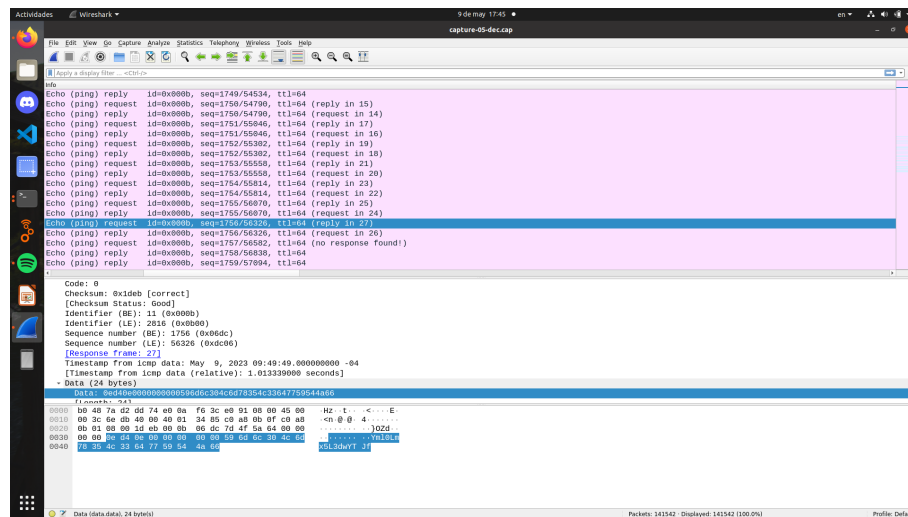


Figura 4: Se puede ver que en cada paquete del nuevo archivo generado se repiten los ultimos bytes.

2.6 describe como obtiene la url de donde descargar el archivo DESARROLLO (PASO 1)

Decode from Base64 format

Simply enter your data then push the decode button.

Yml0Lmx5L3dwYTJf

For encoded binaries (like images, documents, etc.) use the file upload form a litt

UTF-8

Source character set.

☒

Decode each line separately (useful for when you have multiple entries).

☐ Live mode OFF

Decodes in real-time as you type or paste (supports only tt

< DECODE >

Decodes your data into the area below.

bit.ly/wpa2_

Figura 5: Luego se toma esa data y se decodifica en base 64 y se obtiene un link

handshake.pcap 1.1 Kb · 13 packets · more info						
Start typing a Display Filter						
#	No.	Time	Source	Destination	Protocol	Length Info
1	0.000000		ee:de:67:8c:df:8b	Tp-LinkT_d2:dc:18	802.11	125 Association Request, Sm=2292, Pm=0, Flags=....., SSID=WTR-1645213
2	0.000002		ee:de:67:8c:df:8b	ee:de:67:8c:df:8b (RA)	802.11	18 Acknowledgement, Flags=.....
3	0.002401		Tp-LinkT_d2:dc:18	ee:de:67:8c:df:8b	802.11	182 Association Response, Sm=1184, Pm=0, Flags=.....
4	0.002402		Tp-LinkT_d2:dc:18	ee:de:67:8c:df:8b (b0:48:7a:d2:dc:18) (RA)	802.11	18 Acknowledgement, Flags=.....
5	0.007381		ee:de:67:8c:df:8b	ee:de:67:8c:df:8b	EAPOL	133 Key (Message 1 of 4)
6	0.009336		Tp-LinkT_d2:dc:18	ee:de:67:8c:df:8b (b0:48:7a:d2:dc:18) (RA)	802.11	18 Acknowledgement, Flags=.....
7	0.017880		ee:de:67:8c:df:8b	Tp-LinkT_d2:dc:18	EAPOL	155 Key (Message 2 of 4)
8	0.017882		ee:de:67:8c:df:8b	ee:de:67:8c:df:8b (RA)	802.11	18 Acknowledgement, Flags=.....
9	0.017887		ee:de:67:8c:df:8b	ee:de:67:8c:df:8b (RA)	802.11	18 Clear-to-send, Flags=.....
10	0.050774		Tp-LinkT_d2:dc:18	ee:de:67:8c:df:8b	EAPOL	189 Key (Message 3 of 4)
11	0.050776		ee:de:67:8c:df:8b	Tp-LinkT_d2:dc:18 (b0:48:7a:d2:dc:18) (RA)	802.11	18 Acknowledgement, Flags=.....
12	0.054559		ee:de:67:8c:df:8b	Tp-LinkT_d2:dc:18	EAPOL	133 Key (Message 4 of 4)
13	0.054560		ee:de:67:8c:df:8b	ee:de:67:8c:df:8b (RA)	802.11	18 Acknowledgement, Flags=.....

Frame 1: 123 bytes on wire (984 bits), 123 bytes captured (984 bits)

IEEE 802.11 Association Request, Flags:

IEEE 802.11 Wireless Management

0000 00 00 3a 01 b0 48 7a d2 dc 18 ee de 67 8c df 8bR2....9...
0010 3a 48 7a d2 dc 18 48 8f 31 84 01 00 00 00 56 54H...01.....VT
0020 52 2d 31 36 34 35 32 31 33 01 00 02 84 8b 96 8c R-1645213.....
0030 12 18 24 38 14 01 00 00 0f ac 04 01 00 00 0f ac98.....
0040 04 01 00 00 0f ac 02 00 00 32 04 38 48 00 6c 3b2.8H...
0050 10 51 53 54 73 74 75 76 77 78 7c 7d 7e 7f 80005Tstuvwxj...
0060 82 7f 05 04 00 00 00 01 dd 87 00 20 f2 02 00 01P.....
0070 00 dd 08 8c fd fd 01 01 02 01 00

Figura 6: El archivo descargado es handshake.cap

5

3. Desarrollo (PASO 2)

3.1. indica script para modificar diccionario original

```
# Abrir el archivo de texto para leer y crear un nuevo archivo para escribir
with open('rockyou.txt', 'r', encoding='ISO-8859-1') as archivo_origen, open('rockyou_mod.txt', 'w') as archivo_modificado:
    # Contador de cadenas modificadas
    contador = 0
    # Iterar sobre cada línea del archivo de origen
    for linea in archivo_origen:
        # Eliminar el carácter de nueva línea al final de la línea
        linea = linea.strip()
        # Comprobar si la línea está vacía
        if not linea:
            # Saltar esta línea porque está vacía
            continue
        # Comprobar si el primer carácter es un número
        if linea[0].isdigit():
            # Saltar esta línea porque el primer carácter es un número
            continue
        # Convertir el primer carácter en mayúscula y agregar un cero al final de la línea
        linea_modificada = linea[0].upper() + linea[1:] + '0'
        # Escribir la línea modificada en el archivo modificado
        archivo_modificado.write(linea_modificada + '\n')
        # Incrementar el contador de cadenas modificadas
        contador += 1

# Imprimir el número de cadenas modificadas
print(f'Se han modificado {contador} cadenas.')
```

Figura 7: Script genera rockyou_modt.txt donde se realizas el solicitado

3.2. cantidad de passwords finales que contiene rockyou_mod.dic

```
> javier@javier-Nitro-AN515-53:~/Escritorio/cripto/j/lab3$ sudo python3 script.py
Se han modificado 11059725 cadenas.
> javier@javier-Nitro-AN515-53:~/Escritorio/cripto/j/lab3$
```

Figura 8: 11059725 passwords

4. Desarrollo (Paso 3)

4.1. obtiene contraseña con hashcat con potfile

```

jsh@kali:~/Downloads$ cd ~/Downloads/hashcat-6.2.6/; ./hashcat -n 22000 7779_1683685351.hc22000 rockyou_mod.txt --potfile-path potfile.txt --force
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 1.2 pocl 1.4, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: pthread-Intel(R) Core(TM) i5-8300H CPU @ 2.30GHz, 6865/13794 MB (2848 MB allocatable), 8MCU

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Hashes: 1 digests; 1 unique digests; 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x00000fff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash -SMD-LOOP

Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 2 MB

Dictionary cache hit:
* Filename..: rockyou_mod.txt
* Passwords.: 11859707
* Bytes.....: 120186275
* Keyspace...: 11859707

1811acb976741b46d43369fb96dbf90:b0487ad2dc18:eede078cdf8b:VTR-1645213:Security0

Session.....: hashcat
Status.....: Cracked
Hash mode.....: 22000 (NPA-PBKDF2-PBKID+EAPOI)
Hash target....: 7779_1683685351.hc22000
Time started...: Tue May 9 23:37:20 2023, (1 sec)
Time estimated.: Tue May 9 23:37:21 2023, (0 secs)
Kernel feature.: Pure Kernel
Guess base.....: file (rockyou_mod.txt)
Guess queue....: 1/1 (100.00%)
Speed.#1.....: 2276 H/s (11.52ms) @ Accel:64 (loops:1824 Thr:1 Vec:8)
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 2987/11859707 (0.03%)
Rejected.....: 1372/2987 (49.16%)
Restore point...: 1965/11859707 (0.02%)
Restore sub.#1.: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate engine.: Device Generator
Candidates.#1...: Magandaakob -> Dangerous0
Hardware mon.#1.: Temp: 93C Util: 35%

```

Figura 9: El archivo potfile se utiliza para almacenar los hashes que ya han sido descifrados, de modo que Hashcat no tenga que volver a descifrarlos

4.2. identifica nomenclatura del output

```

1 55e1e0f08ed75380f627c6dc48207454b754983771ffc8031d89c5198d6fac76*5654522d31363435323133:Security0

```

Figura 10: El output se divide en tres partes: el hash que ha sido crackeado, informacion adicional del hashcat y la contraseña encontrada Security0

4.3. obtiene contraseña con hashcat sin potfile

```
javier@javier-Mitro-AN515-S3:~/Descargas/hashcat/hashcat-6.2.6/hashcat-6.2.6$ ./hashcat.bin -m 22000 7779_1683685351.hc22000 rockyou_mod.txt --force
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 1.2 pocl 1.4, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: pthread-Intel(R) Core(TM) i5-8300H CPU @ 2.30GHz, 6865/13794 MB (2048 MB allocatable), 0MCU

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Hashes: 1 digests: 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90C

Host memory required for this attack: 2 MB

Dictionary cache built:
* Filename..: rockyou_mod.txt
* Passwords.: 11059725
* Bytes.....: 120106275
* Keyspace...: 11059707
* Runtime...: 0 secs

1013ac9b9741b446d43369fb96dbf90:b0487ad2dc18:eede678cdf8b:VTR-1645213:Security0

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target.....: 7779_1683685351.hc22000
Time.Started.....: Tue May 9 23:31:23 2023, (1 sec)
Time.Estimated.....: Tue May 9 23:31:24 2023, (0 secs)
Kernel.Feature.....: Pure Kernel
Guess.Base.....: File (rockyou_mod.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 2082 H/s (12.40ms) @ Accel:64 Loops:1024 Thr:1 Vecs:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 2907/11059707 (0.03%)
Rejected.....: 1371/2907 (47.16%)
Restore.Point.....: 1965/11059707 (0.02%)
Restore.Sub.#1...: Salt=0 Amplifier=0-1 Iteration=0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Magandaak00 -> Dangerous0
Hardware.Mon.#1..: Temp: 86C Util: 36%
```

Figura 11:

4.4. identifica nomenclatura del output

En base a la imagen anterior, por defecto, hashcat guarda el resultado de la operación en un archivo de texto en la carpeta de trabajo actual. Donde se identifica la contraseña, el modo de hash, el hash crackeado, las contraseñas del diccionario usadas y la cantidad de bytes, el tiempo corrido y otros parametros.

4.5. obtiene contraseña con aircrack-ng

```
javier@javier-Mitro-AN515-S3:~/Escritorio/cripto/j/lab3$ aircrack-ng -w rockyou_mod.txt handshake.pcap
Reading packets, please wait...
Opening handshake.pcap
Read 13 packets.

# BSSID          ESSID          Encryption
1 B0:4B:7A:D2:DC:18 VTR-1645213    WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening handshake.pcap
Read 13 packets.

1 potential targets
```

Figura 12: Ataque por fuerza bruta dado un diccionario y un handshake.pcap

4.6 identifica y modifica parámetros solicitados por pycrack 4 DESARROLLO (PASO 3)

```
Aircrack-ng 1.6

[00:00:00] 3385/9285363 keys tested (7100.67 k/s)

Time left: 21 minutes, 47 seconds                                0.04%

KEY FOUND! [ Security0 ]

Master Key      : 55 E1 E0 F0 8E D7 53 80 F6 27 C6 DC 48 20 74 54
                  B7 54 98 37 71 FF C8 03 1D 89 C5 19 8D 6F AC 76

Transient Key   : 3C 1B 89 A6 31 30 BA 04 B6 59 D9 7E 65 BD D2 07
                  9E C6 8D 2A D6 EF 7F 9E A1 95 1C BC CC 62 A6 5D
                  CC 07 B2 E3 9D 12 99 A7 66 D4 3C D7 61 56 53 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 18 13 AC B9 76 74 1B 44 6D 43 36 9F B9 6D BF 90
```

Figura 13:

4.6. identifica y modifica parámetros solicitados por pycrack

```
#RunTest()
#Read a file of passwords containing
#passwords separated by a newline
with open('rockyou_mod.txt') as f:
    S = []
    for l in f:
        S.append(l.strip())
#ssid name
ssid = "VTR-1645213"
#ANonce
aNonce = a2b_hex('4c2fb7eca28fba45accefd3ac5e433314270e04355b6d95086031b004a31935')
#SNonce
sNonce = a2b_hex('38bde6b043c2aff8ea482dee7d788e95b634e3f8e3d73c038f5869b96bbe9cdc')
#Authenticator MAC (AP)
apMac = a2b_hex('b0:48:7a:d2:dc:18')
#Station address: MAC of client
cliMac = a2b_hex('ee:de:67:8c:df:8b')
#The first MIC
mic1 = "1813acb976741b446d43369fb96dbf90"
#The entire 802.1x frame of the second handshake message with the MIC field set to all zeros
data1 = a2b_hex("30140100000fac040100000fac040100000fac020000")
#The second MIC
mic2 = "a349d01089960aa9f94b5857b0ea10c6"
#The entire 802.1x frame of the third handshake message with the MIC field set to all zeros
data2 = a2b_hex("db0eb43c3faf2c0e8b7e8a471f962c307e707e4718be724459167a88fa281f4d7ce38f012943da788d0a7159c9fac6ad71483d788cecf18b")
#The third MIC
mic3 = "9dc01ca6c4c729648de7f00b436335c8"
#The entire 802.1x frame of the forth handshake message with the MIC field set to all zeros
data3 = a2b_hex("0")
#Run an offline dictionary attack against the access point
TestPwds(S, ssid, aNonce, sNonce, apMac, cliMac, data1, data2, data3, mic1, mic2, mic3)
```

Figura 14: Se modifican los campos solicitados

4.6 identifica y modifica parámetros solicitados por pycrack 4 DESARROLLO (PASO 3)

```
4 0.002402 Tp-LinkT_d2:dc:18 (b0:48:7a:d2:dc:18) (RA) 802.11 10 Acknowledgement, Flags=.....
5 0.002403 Tp-LinkT_d2:dc:18 (b0:48:7a:d2:dc:18) (RA) 802.11 133 Key (Message 4 of 4)
6 0.009336 Tp-LinkT_d2:dc:18 (b0:48:7a:d2:dc:18) (RA) 802.11 10 Acknowledgement, Flags=.....
7 0.017080 ee:de:67:8c:df:8b Tp-LinkT_d2:dc:18 EAPOL 155 Key (Message 2 of 4)
8 0.017082 ee:de:67:8c:df:8b (ee:de:67:8c:df:8b) (RA) 802.11 10 Acknowledgement, Flags=.....
9 0.017087 ee:de:67:8c:df:8b (ee:de:67:8c:df:8b) (RA) 802.11 10 Clear-to-send, Flags=.....
10 0.050774 Tp-LinkT_d2:dc:18 ee:de:67:8c:df:8b EAPOL 189 Key (Message 3 of 4)
11 0.050776 Tp-LinkT_d2:dc:18 (b0:48:7a:d2:dc:18) (RA) 802.11 10 Acknowledgement, Flags=.....
12 0.054559 ee:de:67:8c:df:8b Tp-LinkT_d2:dc:18 EAPOL 133 Key (Message 4 of 4)
13 0.054560 ee:de:67:8c:df:8b (ee:de:67:8c:df:8b) (RA) 802.11 10 Acknowledgement, Flags=.....

IEEE 802.11 QoS Data, Flags: .....F.
Logical-Link Control
802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 95
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 1]
  Key Information: 0x008a
  Key Length: 16
  Replay Counter: 1
WPA Key Nonce: 4c2fb7eca28fba45accefde3ac5e433314270e04355bd95...
Key IV: 00000000000000000000000000000000
WPA Key Der: 0000000000000000
```

Figura 15: aNonce

```
6 0.009336 Tp-LinkT_d2:dc:18 (b0:48:7a:d2:dc:18) (RA) 802.11 10 Acknowledgement, Flags=.....
7 0.017080 ee:de:67:8c:df:8b Tp-LinkT_d2:dc:18 EAPOL 155 Key (Message 2 of 4)
8 0.017082 ee:de:67:8c:df:8b (ee:de:67:8c:df:8b) (RA) 802.11 10 Acknowledgement, Flags=.....
9 0.017087 ee:de:67:8c:df:8b (ee:de:67:8c:df:8b) (RA) 802.11 10 Clear-to-send, Flags=.....
10 0.050774 Tp-LinkT_d2:dc:18 ee:de:67:8c:df:8b EAPOL 189 Key (Message 3 of 4)
11 0.050776 Tp-LinkT_d2:dc:18 (b0:48:7a:d2:dc:18) (RA) 802.11 10 Acknowledgement, Flags=.....
12 0.054559 ee:de:67:8c:df:8b Tp-LinkT_d2:dc:18 EAPOL 133 Key (Message 4 of 4)
13 0.054560 ee:de:67:8c:df:8b (ee:de:67:8c:df:8b) (RA) 802.11 10 Acknowledgement, Flags=.....

IEEE 802.11 QoS Data, Flags: .....T
Logical-Link Control
802.1X Authentication
  Version: 802.1X-2001 (1)
  Type: Key (3)
  Length: 117
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 2]
  Key Information: 0x010a
  Key Length: 0
  Replay Counter: 1
WPA Key Nonce: 30bde6b043c2aff8ea482dee7d788e95b634e3f8e3d73c03...
Key IV: 00000000000000000000000000000000
WPA Key Der: 0000000000000000
```

Figura 16: sNonce

```
6 0.009336 Tp-LinkT_d2:dc:18 (b0:48:7a:d2:dc:18) (RA) 802.11 10 Acknowledgement, Flags=.....
7 0.017080 ee:de:67:8c:df:8b Tp-LinkT_d2:dc:18 EAPOL 155 Key (Message 2 of 4)
8 0.017082 ee:de:67:8c:df:8b (ee:de:67:8c:df:8b) (RA) 802.11 10 Acknowledgement, Flags=.....
9 0.017087 ee:de:67:8c:df:8b (ee:de:67:8c:df:8b) (RA) 802.11 10 Clear-to-send, Flags=.....
10 0.050774 Tp-LinkT_d2:dc:18 ee:de:67:8c:df:8b EAPOL 189 Key (Message 3 of 4)
11 0.050776 Tp-LinkT_d2:dc:18 (b0:48:7a:d2:dc:18) (RA) 802.11 10 Acknowledgement, Flags=.....
12 0.054559 ee:de:67:8c:df:8b Tp-LinkT_d2:dc:18 EAPOL 133 Key (Message 4 of 4)
13 0.054560 ee:de:67:8c:df:8b (ee:de:67:8c:df:8b) (RA) 802.11 10 Acknowledgement, Flags=.....

Logical-Link Control
802.1X Authentication
  Version: 802.1X-2001 (1)
  Type: Key (3)
  Length: 117
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 2]
  Key Information: 0x010a
  Key Length: 0
  Replay Counter: 1
WPA Key Nonce: 30bde6b043c2aff8ea482dee7d788e95b634e3f8e3d73c03...
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 1813acb976741b446d43369fb96dbf90
WPA Key Data Length: 22
WPA Key Data: 3014010000fac040100000fac040100000fac020000
```

Figura 17: Key MIC 1

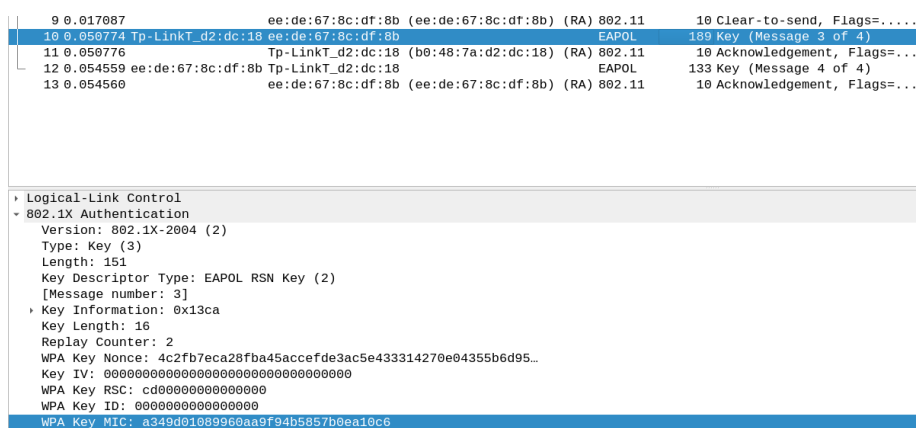


Figura 18: Key MIC 2

4.7. obtiene contraseña con pycrack

No logrado

Conclusiones y comentarios

Para concluir se comenta que hubieron percances al usar hashcat, debido al modo hash utilizado -m 22000 ya que al parecer se utiliza para redes WPA. Tambien respecto a drivers que no se encontraban actualizados en este PC referente a OpenCL se recurre a forzar el crackeo.