Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Hacking Ético

UD02. Analizando la red Wi-FI.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

Caso práctico

Una vez han adquirido los conocimientos y las técnicas utilizadas para comprobar la seguridad de las redes Wi-Fi, el equipo quiere realizar una primera revisión.

Es la primera vez que se realizan pruebas de este tipo y deciden dividir la auditoría en tres fases.

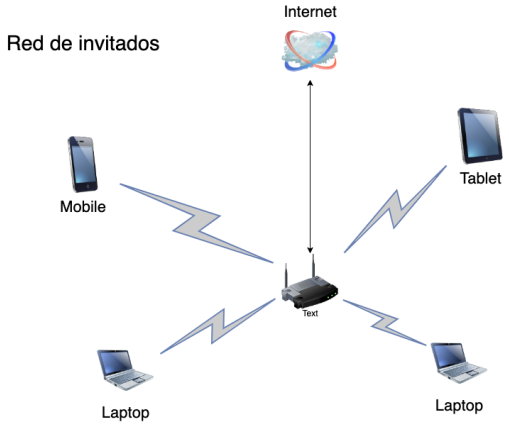
- ✓ **La primera fase se centrará en buscar debilidades de diseño de la red Inalámbrica y contemplará las casuísticas en el que se estén utilizando tipologías de redes Wi-Fi que no resulten adecuadas para la funcionalidad que desempeñan.**
- ✓ **En la segunda fase realizarán una monitorización de las redes de la empresa con la finalidad de disponer de un inventario de Puntos de Acceso, nombre de redes y canales.**
- ✓ **Para finalizar, se emplearán las técnicas descritas en los apartados de "Ataques a redes Wi-Fi" para comprobar si sería posible acceder a las redes Wi-Fi analizadas.**

¿Qué te pedimos que hagas?

- ✓ **Apartado 1: Revisar el diseño de la red Wi-Fi**

  A continuación, se muestran varios diagramas de la red. Teniendo en cuenta los conocimientos adquiridos en esta unidad, comenta para cada una de las redes que se muestran la problemática de diseño existente y cómo sería la infraestructura ideal.

  - ➢ **Red de invitados**: La compañía dispone de una red Wi-Fi de invitados tipo **OPEN** para dotar de conectividad las salas de reuniones cuando tienen visitas de clientes o proveedores. También es común que en ciertas ocasiones se conecten los propios empleados con sus equipos corporativos dado que la cobertura en las salas de reuniones es mejor. Necesitas resolver las siguientes cuestiones:
    - Justificar que problemas de seguridad dispone esta red en base al tipo de red Wi-Fi que es, y el uso que se hace de ella.
    - Justificar los tipos de ataque a los que está expuesta.
    - Mejoras que implementarías en la red
  - ➢ A continuación, se muestra el diagrama de la red de invitados:



Sergio Romero Redondo. Elaboración Propia (CC0)

Los **problemas de seguridad** en este caso parten de usar una red diseñada para invitados que es utilizada por los empleados y sus equipos corporativos, quedando expuestos, al no disponer de ningún tipo de cifrado para este canal.

Es un tipo de red sin validación de acceso y por ello, no confiable.

Los equipos utilizados podrían servir como punto de ataque hacia el exterior.

Los **tipos de ataque** en una red OPEN, podrán ser de Acceso no autorizado (con conectarnos, podemos tener acceso a otros dispositivos conectados de esta misma red). Además, también podrán ser por ausencia de cifrado, con nuestra tarjeta en modo monitor para monitorizar las tramas de red intentando conseguir la información expuesta no cifrada.

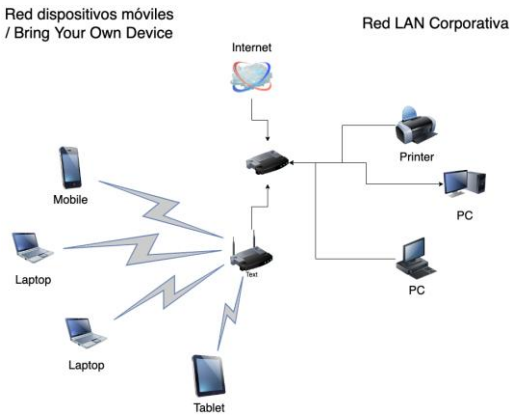
Las **mejoras que implementar** -siempre que sea necesaria esta red- serían:

- ✓ Mejora de la cobertura de la red corporativa.
- ✓ Revisar las políticas de seguridad para que los equipos corporativos solo se conecten a la red corporativa recién mejorada.
- ✓ Implementación de seguridad WPA2-PSK y gestión de contraseñas.
- ✓ Plan de formación y concienciación.
- ✓ Reducción de la señal en las salas de reuniones.
- ✓ Bloqueo de direcciones MAC de los equipos corporativos para evitar accesos a la red de invitados.
- ✓ Monitorización de la red.

➢ **Red de dispositivos móviles**: La compañía adoptó hace varios años la filosofía "Bring Your Own Device" mediante la cual dispone de una red específica para que los empleados puedan utilizar sus equipos personales (smartphone, tablet o portátil) para acceder a ciertos servicios en la red de empleados, como acceso al correo electrónico, al servidor de ficheros y a imprimir con las impresoras. La red se encuentra protegida mediante **WPA2-PSK**. Además, en los últimos meses se han ido varios empleados a trabajar a la fábrica de al lado, aunque el administrador de la red no ha notado que la red tenga menos usuarios conectados.

- Justificar que problemas de seguridad dispone esta red en base al tipo de red Wi-Fi que es, y el uso que se hace de ella.
- Justificar los tipos de ataque a los que está expuesta.
- Mejoras que implementarías en la red

➢ A continuación, se muestra el diagrama de la red de dispositivos móviles:



Sergio Romero Redondo (CC0)

Algunos de los **problemas de seguridad** de este diseño vienen por permitir que antiguos trabajadores puedan seguir utilizando su contraseña establecida y pueden seguir accediendo a servicios.

Un protocolo así solo da una contraseña (que no tiene por qué ser además robusta) como medida de filtrado, pero no es un sistema de autenticación.

De hecho, acaba siendo una forma de conexión inalámbrica para toda la red corporativa, con los riesgos que supone.

Los **ataques** pueden venir desde los propios antiguos empleados con un ataque desde dentro, al seguir teniendo acceso, o averiguando la contraseña desde el exterior, crackeando el Handshake de autenticación en caso de usuarios conectados, o el PMKID, mediante monitoreo de escucha de la red.

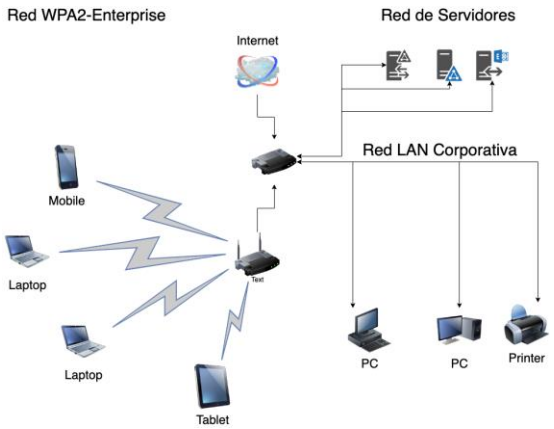
Las **mejoras** que implementar:

- ✓ Monitoreo de red.
- ✓ Política de generación de contraseñas que evite el acceso futuro de exempleados.
- ✓ Implementar un firewall para evitar que una dirección MAC no registrada pueda acceder.

➢ **Red corporativa**: Para finalizar, la compañía dispone de una red Wi-Fi en la que sólo está permitido el acceso a los usuarios legítimos de la empresa. La particularidad de esta red es que proporciona el mismo nivel de acceso a la red que cualquier equipo conectado por cable. Para proporcionar este nivel de acceso, la red es de tipo **WPA2-Enterprise** a la cual los empleados acceden **autenticándose con su usuario y contraseña**. En este sentido su proveedor habitual de servicios le ha indicado que necesita desplegar un MDM para garantizar una mayor protección en la red, este **MDM está presupuestado, pero aún no se ha desplegado**.

- Justificar que problemas de seguridad dispone esta red en base al tipo de red Wi-Fi que es, y el uso que se hace de ella.
- Justificar los tipos de ataque a los que está expuesta.
- Mejoras que implementarías en la red

➢ A continuación, se muestra el diagrama de la red corporativa para su acceso mediante Wi-Fi:



Sergio Romero Redondo (CC0)

Problemas de seguridad:

No hay CA, y solo tienen presupuestado el MDM, sin desplegar y por tanto, podrían atacar la red fácilmente.

El acceso a esta Wi-Fi proporciona acceso a la red corporativa.

El **ataque** puede ser a través de un "Punto de Acceso Falso", donde capturar los intentos de autenticación de los empleados y obtener las credenciales.

Mejoras que implementar:

- ✓ Monitoreo de red.
- ✓ Política de generación de contraseñas.
- ✓ Implementación del MDM presupuestado.

✓ Apartado 2: Monitorización de datos

Dada la siguiente captura de airodump responde a las siguientes cuestiones:

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

18:D6:C7:E8:CF:C0  -33       18        5    0  36 1170   WPA2 CCMP   PSK  Skynet_plus
18:D6:C7:E8:CF:C1  -43       17        2    0  11  195   WPA2 CCMP   PSK  Skynet
98:00:6A:A0:9B:C4  -73       11        4    0   5  130   WPA2 CCMP   PSK  DIGIFIBRA gima
DC:53:7C:14:71:E4  -76        9        0    0   7  130   WPA2 CCMP   PSK  Delfin
A4:97:33:4A:82:1E  -77       15        0    0  52 1733   OPN              MOVISTAR_PLUS_8210
DC:53:7C:59:55:3F  -78       16        0    0 108 1170   WPA2 CCMP   PSK  ONO6C63-5G
DC:53:7C:59:55:3E  -79       10        0    0  11  195   WPA2 CCMP   PSK  ONO6C63
16:66:78:72:A8:EF  -82       11        0    0   6  130   WPA2 CCMP   PSK  iPhone de Melisa
DC:F8:B9:A1:50:83  -82       12        0    0   7  130   WPA2 CCMP   PSK  DIGIFIBRA-tdTS
DC:F8:B9:A1:50:84  -84       15        0    0  44  780   WPA2 CCMP   PSK  DIGIFIBRA-PLUS-tdTS
10:5D:DC:72:F2:10  -84        7        0    0   1  360   WPA2 CCMP   PSK  PATRALEX
98:97:D1:35:E4:36  -84        9        3    0   1  130   WPA2 CCMP   PSK  MOVISTAR_E435
98:00:6A:A0:9B:C5  -85       15        0    0  44  780   WPA2 CCMP   PSK  DIGIFIBRA-PLUS-gima
CC:D4:A1:E1:7B:B4  -85        4        0    0   6  130   WPA2 CCMP   PSK  MOVISTAR_7BB3
10:5D:DC:72:F2:15  -85        7        0    0   1  360   WPA2 CCMP   PSK  <length:  0>
86:97:D1:35:E4:3E  -86       15       12    0  52 1733   WPA2 CCMP   PSK  MOVISTAR_E435
98:97:D1:35:E4:3E  -86       15       32    0  52 1733   WPA2 CCMP   PSK  MOVISTAR_PLUS_E435
CC:ED:DC:C9:03:58  -86        3        0    0   1  130   WPA2 CCMP   PSK  MOVISTAR_0358
26:57:60:92:DB:F8  -87       13        0    0  56 1733   WPA2 CCMP   PSK  Skynet
34:57:60:92:DB:F8  -87       13        7    0  56 1733   WPA2 CCMP   PSK  Skynet_plus
DC:53:7C:14:71:E5  -87       12        0    0  44  270   WPA2 CCMP   PSK  ONOAABA-5G
6A:CE:DA:7D:FA:47  -89        3        0    0 100 1733   WPA2 CCMP   PSK  MiFibra-FA43
A4:CE:DA:7D:FA:46  -89        5        0    0 100 1733   WPA2 CCMP   PSK  <length:  0>
44:48:B9:29:3D:C0   -1        0        0    0  11   -1                   <length:  0>
A4:CE:DA:7D:FA:45  -84        1        0    0   6  130   WPA2 CCMP   PSK  MiFibra-FA43
A4:2B:B0:A8:70:5E  -85        3        0    0   1  270   WPA2 CCMP   PSK  TP-LINK_A8705E
C6:D4:A1:E1:7B:BC   -1        0        0    0  36   -1                   <length:  0>
62:1E:A3:67:32:47  -86        1        0    0   6  130   WPA2 CCMP   PSK  vodafone1BE0
34:57:60:92:DB:F0  -88        3        0    0  11  130   WPA2 CCMP   PSK  Skynet
62:1E:A3:67:32:44  -88        3        0    0   6  130   WPA2 CCMP   PSK  <length: 10>

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   1A:57:5D:CC:D0:20  -81    0 - 1      0         4
(not associated)   5C:CF:7F:B4:F4:2C  -86    0 - 1      0         2         ONOD79D
(not associated)   FE:67:59:20:66:3A  -87    0 - 6      0         2
(not associated)   C6:AA:99:2F:47:00  -87    0 - 1      0         2         MiFibra-0B4B
(not associated)   62:A8:65:A0:8D:D5  -88    0 - 6      0         2
16:66:78:72:A8:EF  48:D2:24:BA:04:43  -84    0 - 6      0         1
DC:F8:B9:A1:50:83  CE:EA:84:22:53:46  -87    0 -11      0         1
86:97:D1:35:E4:3E  6E:52:AC:9D:B4:87   -1    6e- 0      0         2
86:97:D1:35:E4:3E  D0:B1:28:14:A7:AD   -1    6e- 0      0         5
98:97:D1:35:E4:3E  04:54:53:EB:26:F6   -1    6e- 0      0        26
```

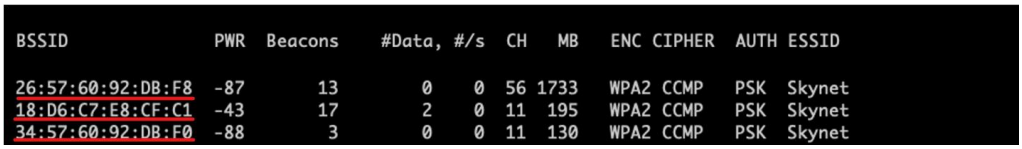
Sergio Romero Redondo (CC0)

- Indica los BSSID de los Puntos de Acceso de las Redes **Skynet** y **Skynet_Plus**.

Skynet:

18:D6:C7:E8:CF:C1

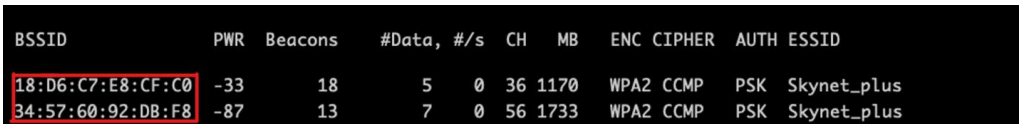
26:57:60:92:DB:F8
34:57:60:92:DB:F0



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
26:57:60:92:DB:F8	-87	13	0	0	56	1733	WPA2	CCMP	PSK	Skynet
18:D6:C7:E8:CF:C1	-43	17	2	0	11	195	WPA2	CCMP	PSK	Skynet
34:57:60:92:DB:F0	-88	3	0	0	11	130	WPA2	CCMP	PSK	Skynet

Skynet_Plus:

18:D6:C7:E8:CF:C0
34:57:60:92:DB:F8

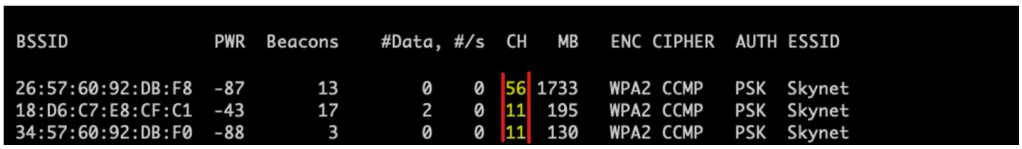


BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
18:D6:C7:E8:CF:C0	-33	18	5	0	36	1170	WPA2	CCMP	PSK	Skynet_plus
34:57:60:92:DB:F8	-87	13	7	0	56	1733	WPA2	CCMP	PSK	Skynet_plus

- Indica en que bandas de frecuencia y en que canales operan las redes **Skynet** y **Skynet_Plus**.

Skynet:

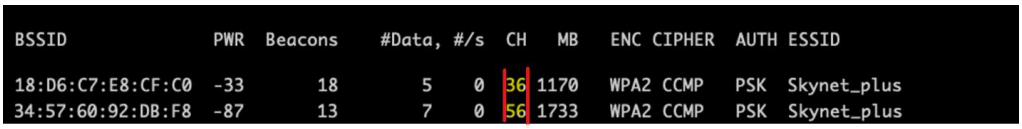
56 (5GHz), 11 (2,4GHz) y 11 (2,4GHz)



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
26:57:60:92:DB:F8	-87	13	0	0	56	1733	WPA2	CCMP	PSK	Skynet
18:D6:C7:E8:CF:C1	-43	17	2	0	11	195	WPA2	CCMP	PSK	Skynet
34:57:60:92:DB:F0	-88	3	0	0	11	130	WPA2	CCMP	PSK	Skynet

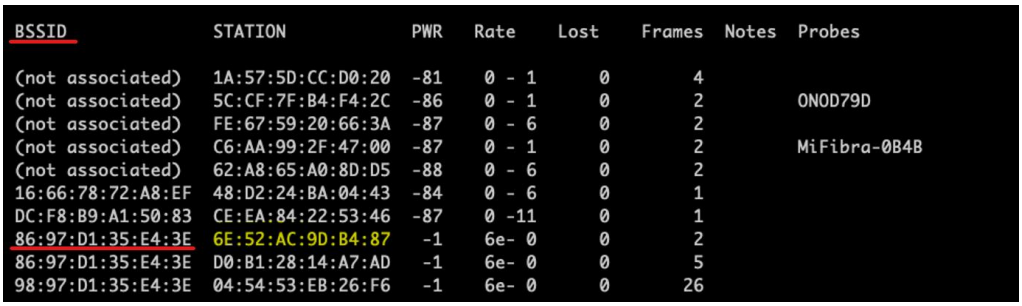
Skynet_Plus:

36 (5GHz) y 56 (5GHz)



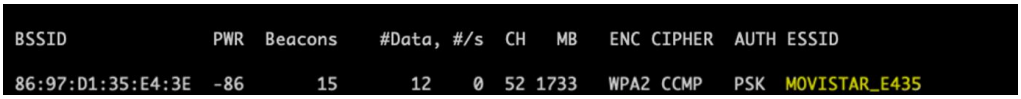
BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
18:D6:C7:E8:CF:C0	-33	18	5	0	36	1170	WPA2	CCMP	PSK	Skynet_plus
34:57:60:92:DB:F8	-87	13	7	0	56	1733	WPA2	CCMP	PSK	Skynet_plus

- Indica a qué red está conectado el dispositivo con MAC **6E:52:AC:9D:B4:87**.



BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
(not associated)	1A:57:5D:CC:D0:20	-81	0 - 1	0	4		
(not associated)	5C:CF:7F:B4:F4:2C	-86	0 - 1	0	2		ONOD79D
(not associated)	FE:67:59:20:66:3A	-87	0 - 6	0	2		
(not associated)	C6:AA:99:2F:47:00	-87	0 - 1	0	2		MiFibra-0B4B
(not associated)	62:A8:65:A0:8D:D5	-88	0 - 6	0	2		
16:66:78:72:A8:EF	48:D2:24:BA:04:43	-84	0 - 6	0	1		
DC:F8:B9:A1:50:83	CE:EA:84:22:53:46	-87	0 -11	0	1		
86:97:D1:35:E4:3E	6E:52:AC:9D:B4:87	-1	6e- 0	0	2		
86:97:D1:35:E4:3E	D0:B1:28:14:A7:AD	-1	6e- 0	0	5		
98:97:D1:35:E4:3E	04:54:53:EB:26:F6	-1	6e- 0	0	26		

La red a la que se conecta es: **MOVISTAR_E435**



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
86:97:D1:35:E4:3E	-86	15	12	0	52	1733	WPA2	CCMP	PSK	MOVISTAR_E435

➢ Indica en que red intenta conectarse el dispositivo **5C:CF:7F:B4:F4:2C**.

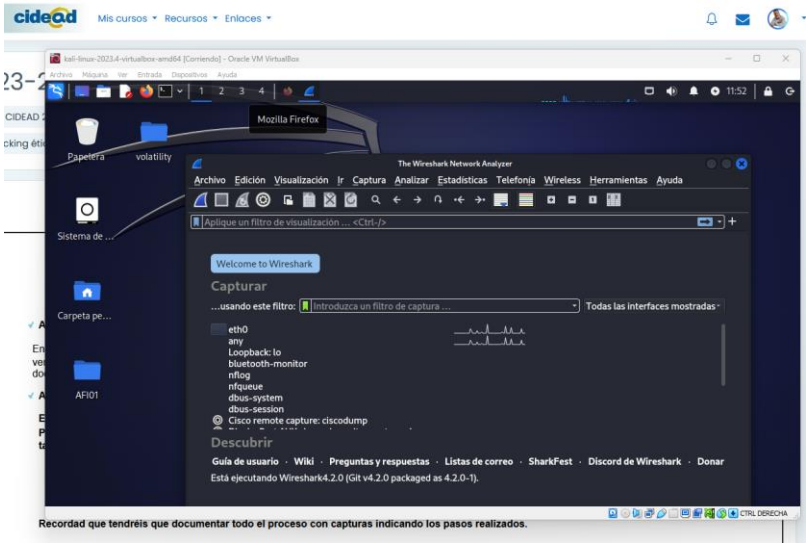
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
(not associated)	1A:57:5D:CC:D0:20	-81	0 - 1	0	4		
(not associated)	5C:CF:7F:B4:F4:2C	-86	0 - 1	0	2		ONOD79D
(not associated)	FE:67:59:20:66:3A	-87	0 - 6	0	2		
(not associated)	C6:AA:99:2F:47:00	-87	0 - 1	0	2		MiFibra-0B4B
(not associated)	62:A8:65:A0:8D:D5	-88	0 - 6	0	2		
16:66:78:72:A8:EF	48:D2:24:BA:04:43	-84	0 - 6	0	1		
DC:F8:B9:A1:50:83	CE:EA:84:22:53:46	-87	0 -11	0	1		
86:97:D1:35:E4:3E	6E:52:AC:9D:B4:87	-1	6e- 0	0	2		
86:97:D1:35:E4:3E	D0:B1:28:14:A7:AD	-1	6e- 0	0	5		
98:97:D1:35:E4:3E	04:54:53:EB:26:F6	-1	6e- 0	0	26		

La red a la que se conecta es: **ONO79D**

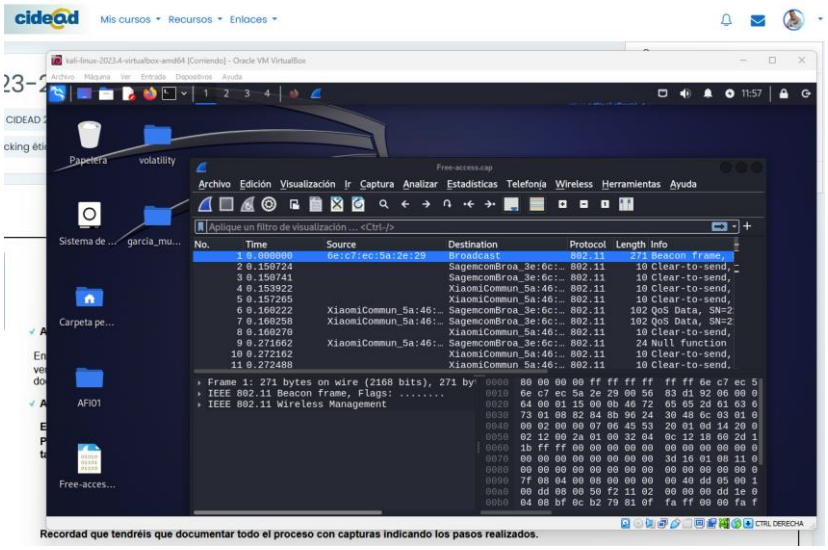
✓ Apartado 3: Exposición en redes OPEN

En este apartado se proporciona una Captura de red de la monitorización de una red OPEN (cap - 383,21 KB) . Entre las tramas de gestión capturadas podréis ver cómo se exponen ciertos protocolos en claro, localizarlos con wireshark y mostrar la comunicación que se establece en el protocolo HTTP. Recordad documentar todo el proceso mediante capturas y detallar los pasos que se realizan durante el proceso.

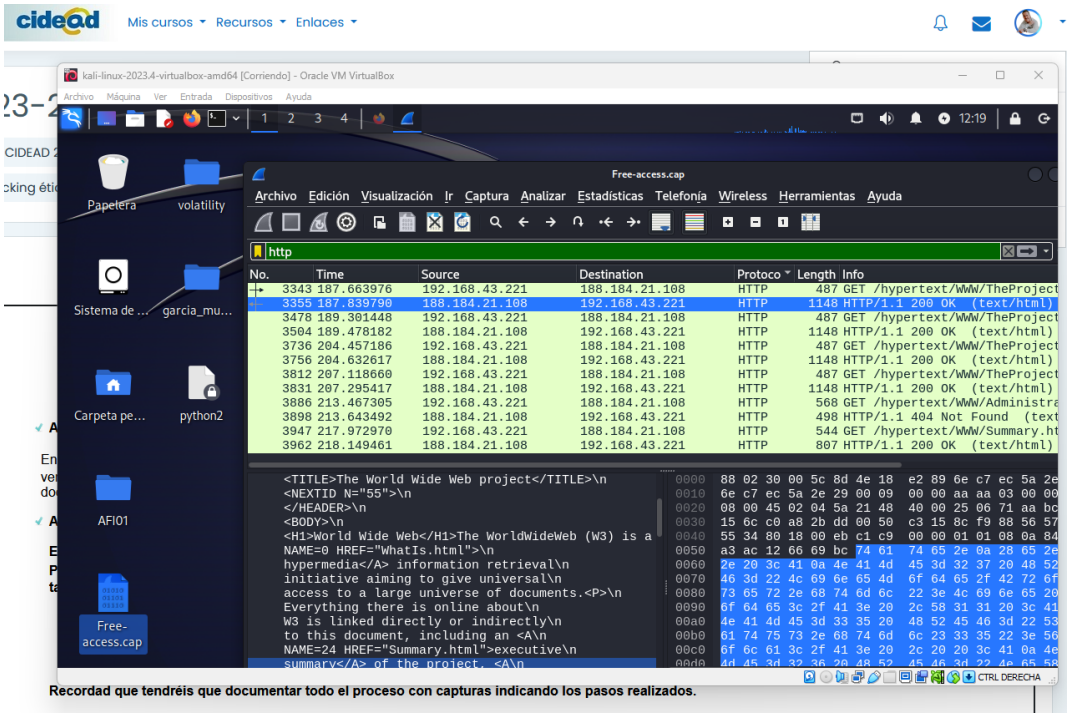
Utilizo para estos ejercicios una VM de Kali Linux, con la que puedo iniciar Wireshark.



Abro el archivo de la captura para observar los datos.

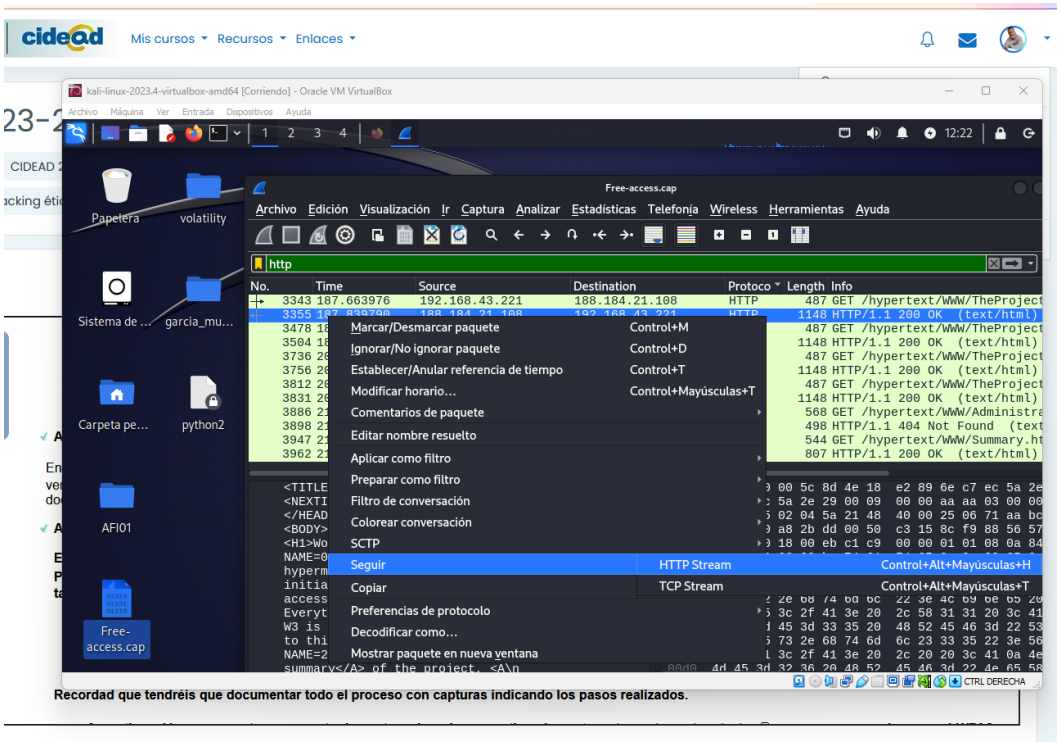


Añado como filtro el protocolo **`http`** y pulso **`enter`** para que muestre las tramas en HTTP, y seleccionando cualquiera, podemos ver la información en texto plano

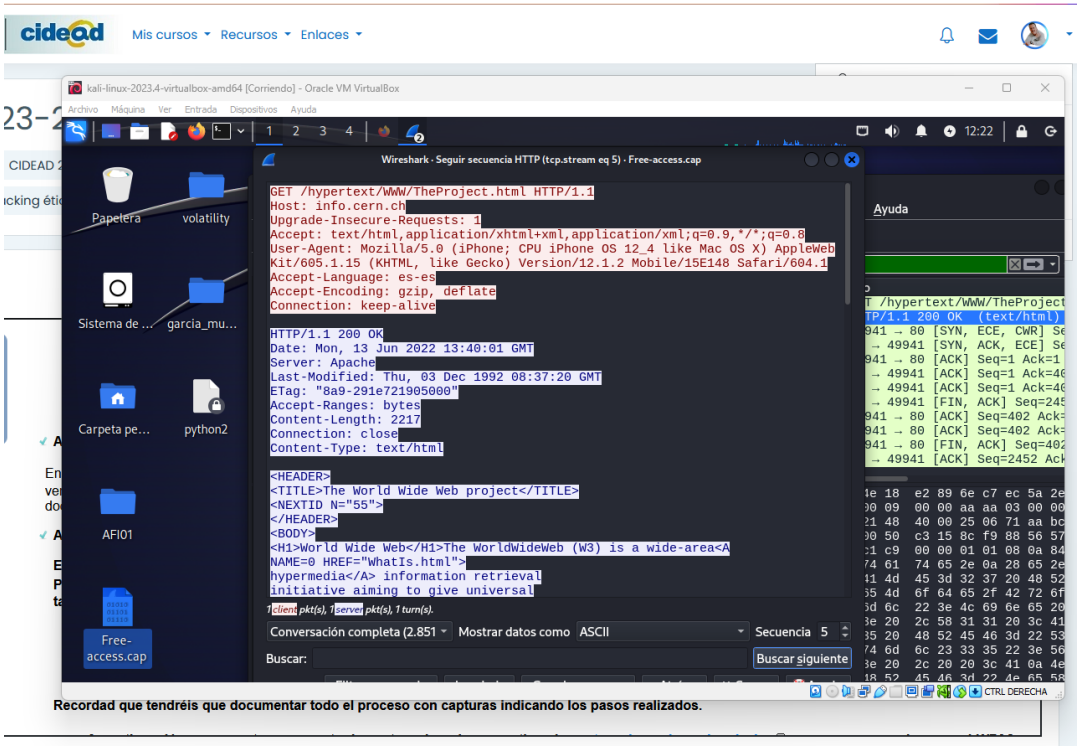


Si queremos observarlo con mayor claridad, nos ofrece la opción desde el menú secundario

`Seguir-> HTTP Stream`



Esto nos facilita ver toda la información de la web de manera más clara en una ventana aparte.



✓ **Apartado 4: Debilidades en las redes inalámbricas.**

En este apartado se entregan varios ficheros de captura para que podáis realizar sobre ellos las técnicas de cracking descritas durante el módulo. Para no extendernos mucho en la realización de la tarea se ha configurado un diccionario (txt - 16,25 KB) que podéis utilizar para la resolución de la tarea. Cabe destacar que si queréis ver el proceso de la captura podéis cargar el fichero de captura en airodump-ng con el operador -r

```
$ airodump-ng -r fichero_de_captura
```

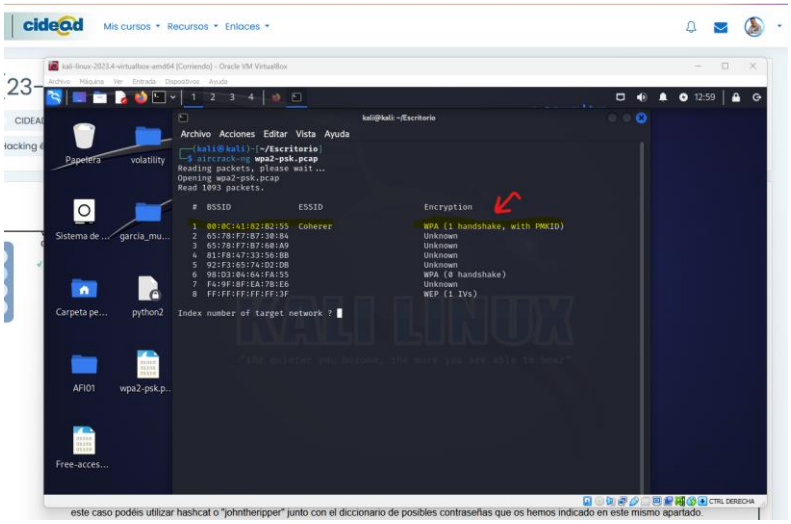
Recordad que tendréis que documentar todo el proceso con capturas indicando los pasos realizados.

➢ **A continuación se presenta un paquete de captura de red que contiene la captura de un 4-way-handsake (pcap - 175,76 KB) de una red WPA2-PSK para aplicarle una técnica de cracking offline. Podéis utilizar el propio aircrack-ng junto con el diccionario de posibles contraseñas que os hemos indicado en este mismo apartado.**

Abro una consola en la que ejecutar aircrack-ng con la captura descargada.

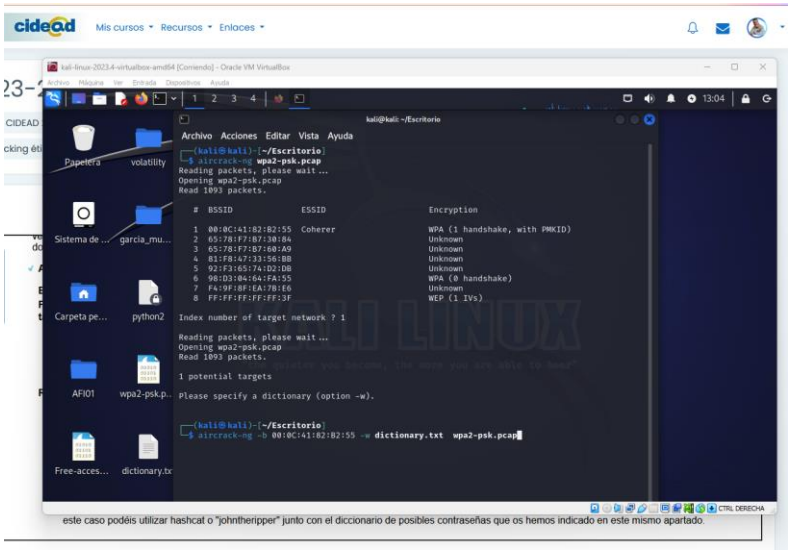
`aircrack-ng wpa2-psk.pcap`

Nos interesa la red 1, que contiene el handsake.

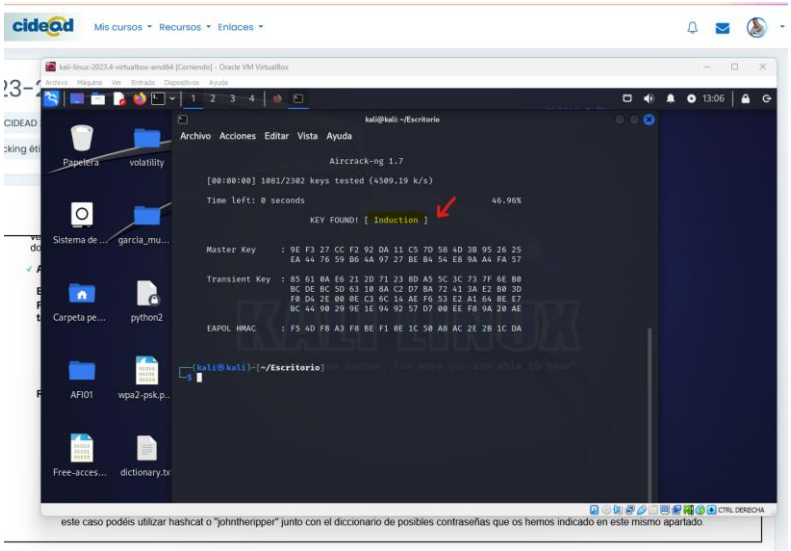


Volvemos entonces a ejecutar aircrack, seleccionando la red a través de su MAC y añadiendo el diccionario facilitado.

`aircrack-ng -b 00:0C:41:82:B2:55 -w dictionary.txt wpa2-psk.pcap`



Obtenemos la clave: **`Induction`**

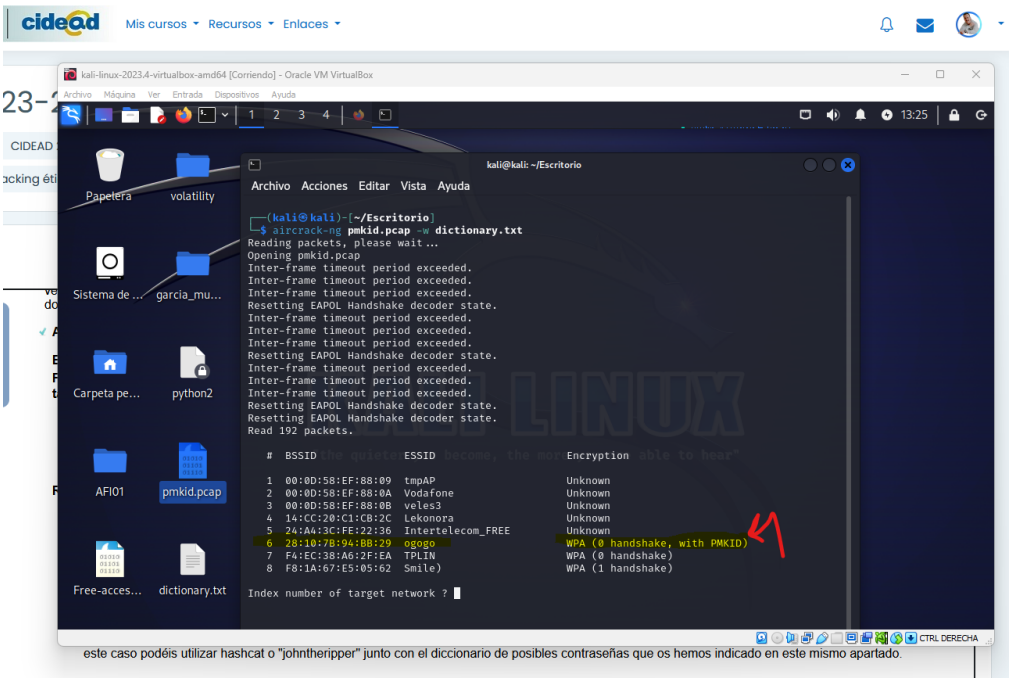


- A continuación se presenta un paquete de captura de red que contiene la captura de un PMKID (pcap - 27,71 KB) de una red WPA2-PSK (Tenéis que realizar esta técnica sobre la red que contiene el PMKID) para aplicarle una técnica de cracking offline. En este caso podéis utilizar el propio aircrack-ng junto con el diccionario de posibles contraseñas que os hemos indicado en este mismo apartado.

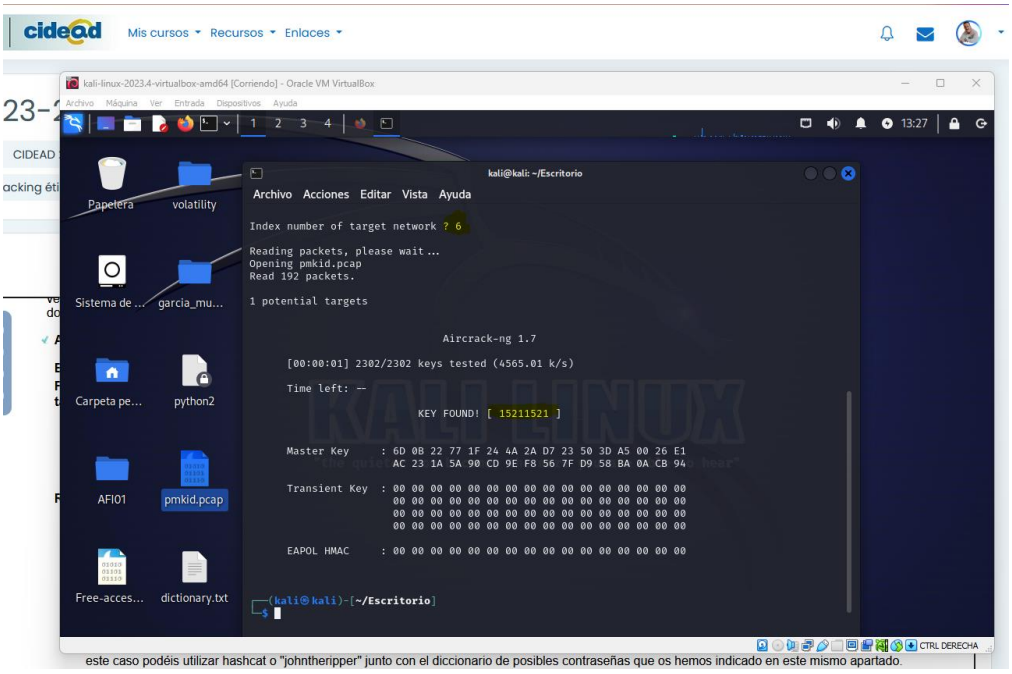
Procedo de forma similar al apartado anterior, pero con la nueva captura suministrada.

`aircrack-ng pmkid.pcap -w dictionary.txt`

Podremos ver como nos interesa seleccionar la red 6, que tiene el PMKID.



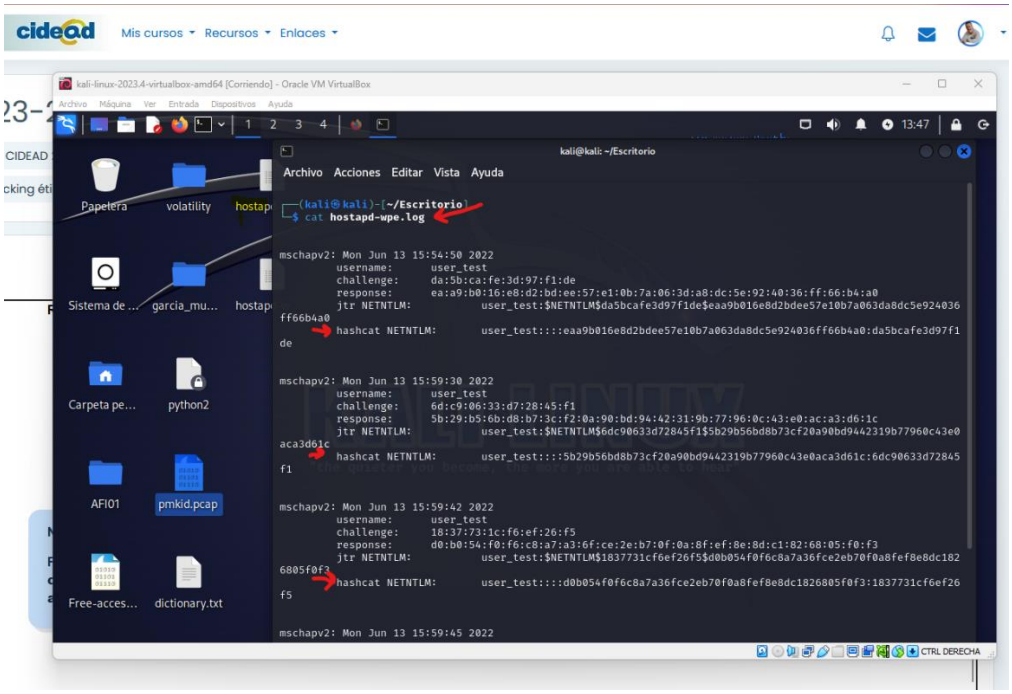
Tras esto, nos muestra la clave: **15211521**



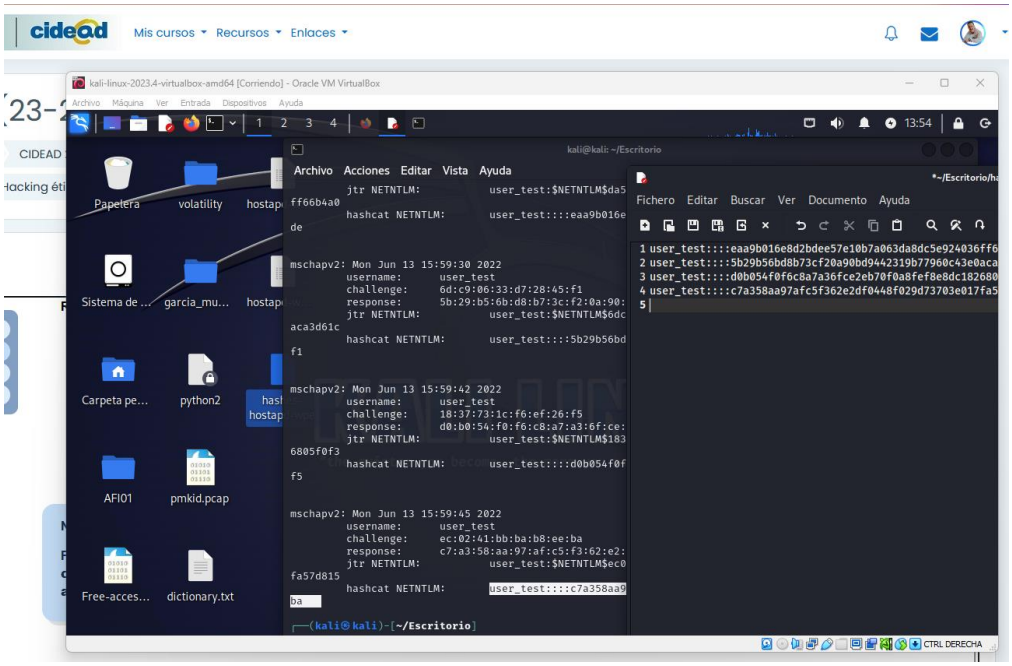
- A continuación se presentan los ficheros de log resultantes de la captura de autenticación WPA2-Enterprise (Log ejecución hostapd-wpe (log - 4,92 KB) - Log autenticación capturada (log - 1,52 KB)) mediante un punto de acceso falso, en este caso también podréis aplicar una técnica de cracking offline. En este caso podéis utilizar hashcat o "johntheripper" junto con el diccionario de posibles contraseñas que os hemos indicado en este mismo apartado.

Descargamos los archivos y los abrimos para comprobar el contenido de los logs.

```
cat hostapd-wpe.log
```

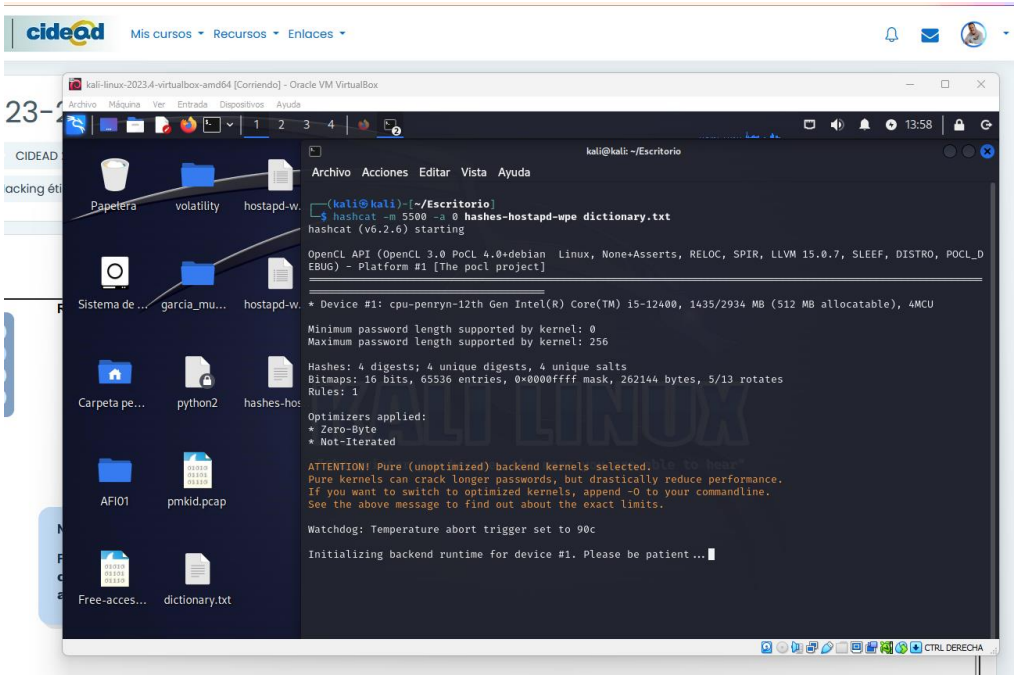


Tras comprobar que contiene hashes tanto de hashcat como de johntheripper, copiamos los de hashcat a un archivo de texto para poder pasarlos a través de hashcat.

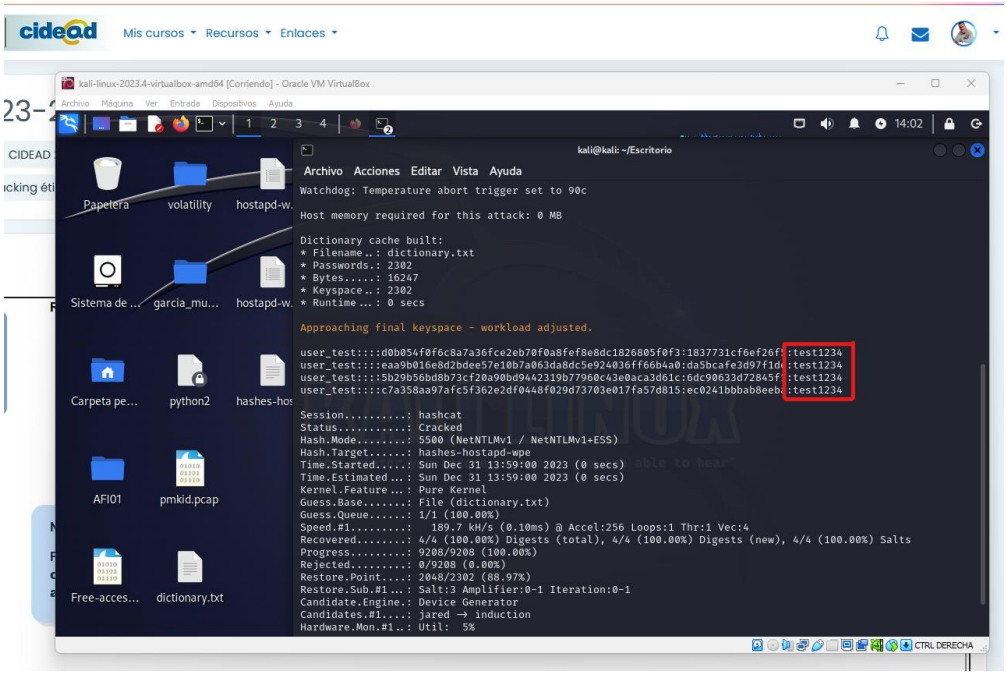


Proceso al craking con hashcat, indicando con **`-m 5500`** que es NETNTLVM y con **`-0`** que se ataca desde el diccionario.

```
hashcat -m 5500 -a 0 hashes-hostapd-wpe dictionary.txt
```



Obtenemos para ellos la contraseña: **`test1234`**



Webgrafía.

Temario plataforma CIDEAD UT02.- Hacking ético en entornos inalámbricos

Documentación Wireshark: https://www.exploit-db.com/docs/50549