HACKING ÉTICO

Tarea 2

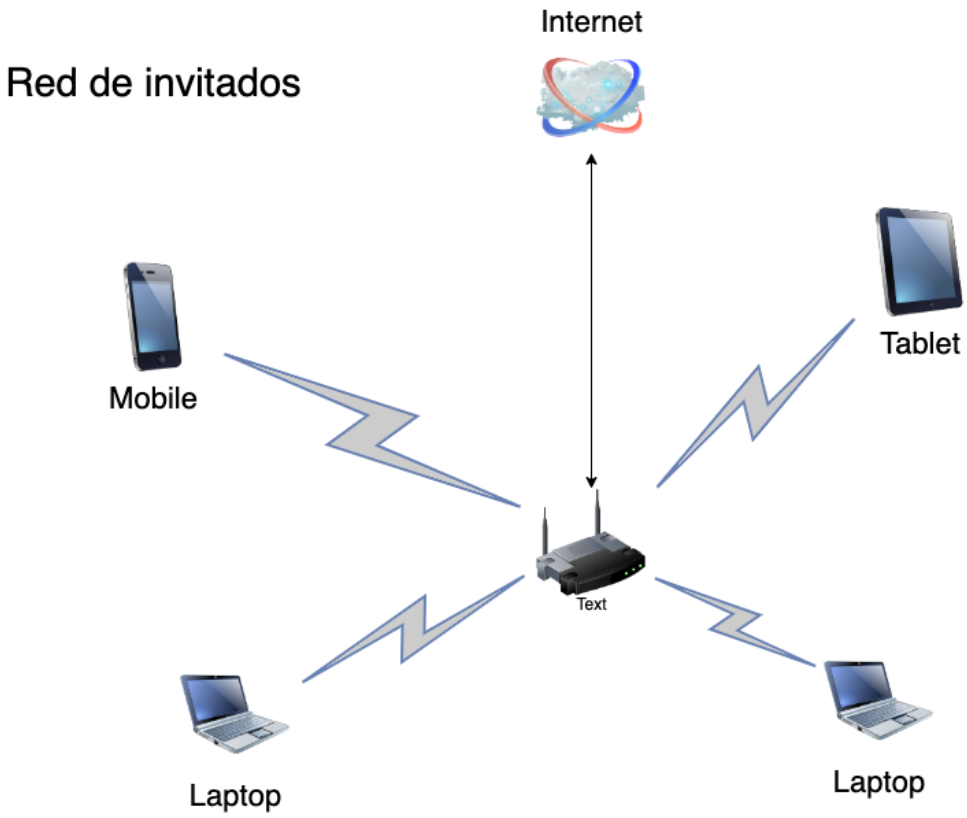
ESTHER CARRILLO GÁLVEZ

Índice

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:



Problemas de seguridad

Los problemas seguridad que implican esta red de invitados tipo OPEN es que no solo las visitas, sino que a veces, personas de la plantilla también se conectan para realizar tareas. Esto conlleva a un nivel de exposición y riesgo muy alto porque es una red sin cifrado y, además, tampoco requiere contraseña para acceder. De modo que se expone el tráfico de datos de todos los usuarios y se comprometen los servidores internos, datos sensibles corporativos y personales.

Si un atacante consiguiera acceder a esta red, sería fatal ya que podría infectar de malware poniendo en peligro a todos los usuarios de esa red, así como al resto de dispositivos de la empresa.

Otro problema es que el atacante puede crear una red wifi con las mismas características que la Red Invitados para espiar o tomar el control del dispositivo.

Tipos de ataque a los que está expuesta

Entre uno de los ataques más comunes para las redes OPEN, se incluye *Man-in-the-Middle*. El ciberdelincuente se sitúa entre el emisor y el receptor con el fin de interceptar los mensajes que se intercambian durante una conversación.

El acceso no autorizado es un ataque que puede realizar el ciberdelincuente en todo momento porque no necesita credenciales o autorización para conectarse a la red.

Mejoras a implementar en la red

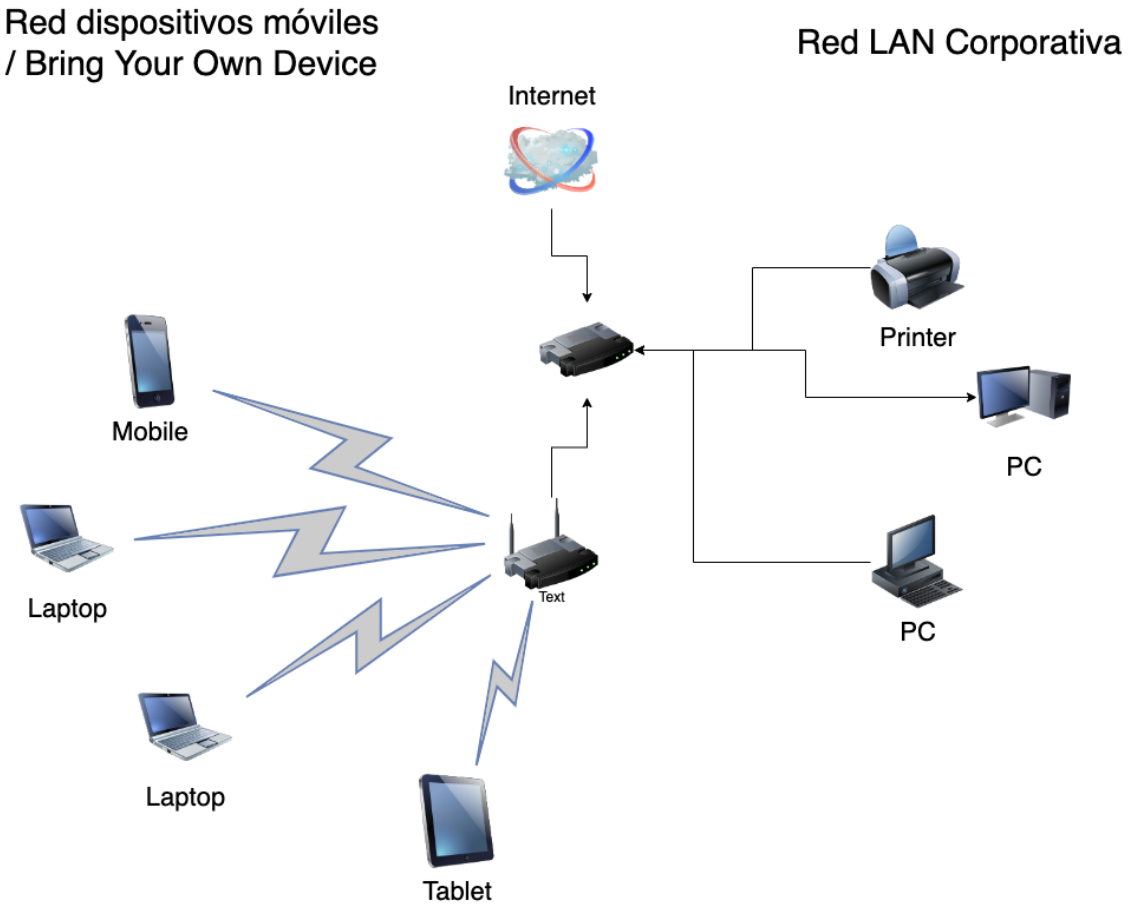
Dentro de las mejoras esenciales para proteger esta red es la segmentación de la red, aislando la red de invitados con la red interna de la compañía.

Otra práctica necesaria es la implementación de un protocolo más robusto y seguro que OPEN, como podría ser WPA2 o WPA3. De este modo, se asegura la integridad de los datos sensibles mediante una clave actualizada temporalmente.

Establecer un control de monitoreo de red con herramientas de escaneo como nmap o OpenVAS para detectar qué puertos tienen abiertos los usuarios de la red.

La concienciación es un pilar fundamental en la ciberseguridad, por lo tanto, lo recomendable es invertir en formación y concienciación para la plantilla.

- **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 qué 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:



Problemas de seguridad

Uno de los mayores problemas de seguridad de una red WPA2-PSK es el uso de una única contraseña para toda la plantilla, permitiendo el acceso a recursos y datos sensibles. Esta clave PSK es un método de autenticación que, mediante una clave compartida, los dispositivos deben utilizar para conectarse a la red. Sin embargo, este es uno de los mayores problemas de seguridad de este tipo de redes porque toda la plantilla usa la misma contraseña, aun incluso si esa persona ha dejado la empresa, permitiendo el acceso a recursos y datos críticos.

Tipos de ataque a los que está expuesta

Según el Instituto Nacional de Ciberseguridad, "en octubre de 2017, se descubrió una vulnerabilidad denominada *ataque KRACK* que permitía a un atacante interceptar, descifrar y manipular el tráfico de una red inalámbrica", convirtiéndose en un protocolo inseguro.

El atacante podría poner en peligro la empresa mediante un ataque de fuerza bruta donde prueba todas las combinaciones posibles hasta desencriptar la contraseña.

Un ataque interno también es posible, ya que una persona que trabajó en la empresa y, que conserva la contraseña, puede aprovechar este factor para acceder al sistema y poner en riesgo los datos corporativos y personales.

Mejoras a implementar en la red

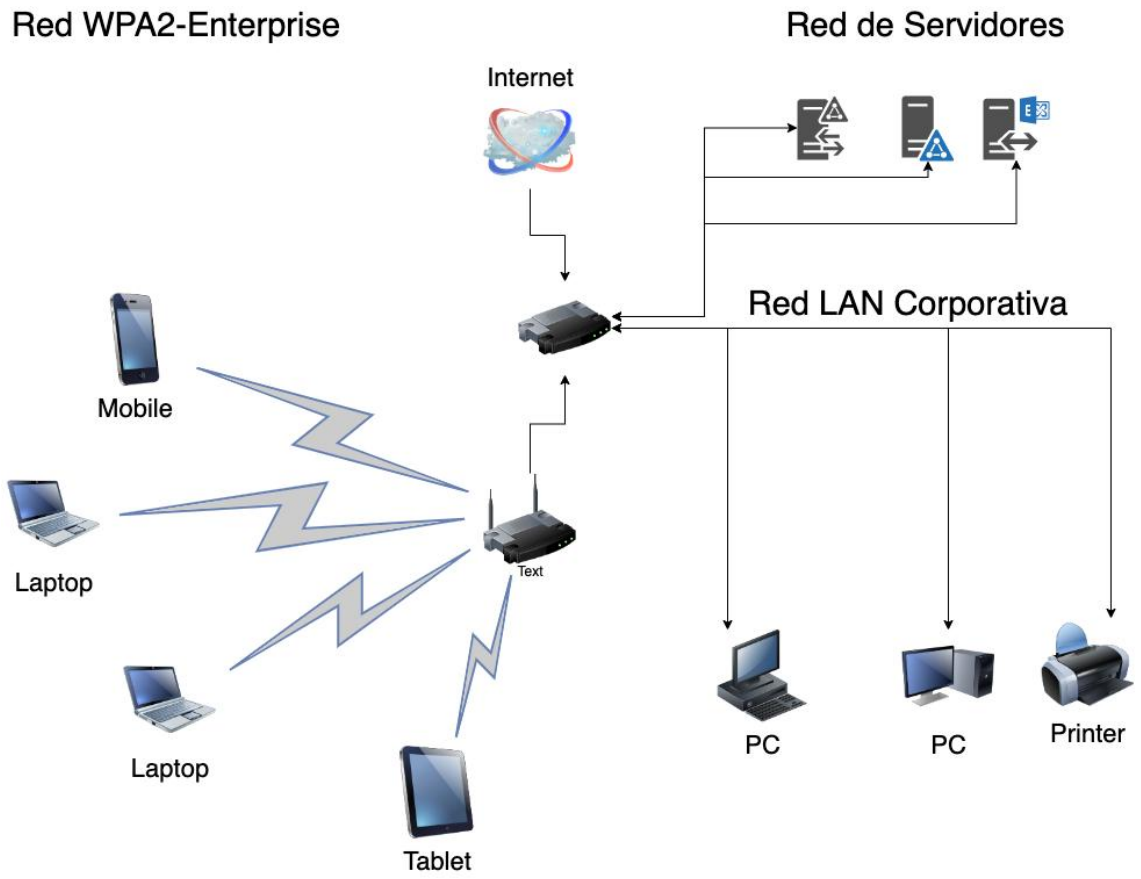
La mejor práctica para evitar este tipo de ataques es abandonar WPA2-PSK para implementar WPA2 Enterprise, de modo que cada empleada acceda con sus propias credenciales.

Al ser una red compuesta por dispositivos personales, lo adecuado sería implementar una gestión de dispositivos móviles (MDM). Esto permite controlar que cuando un usuario se va, automáticamente se eliminan las credenciales de su teléfono.

Una buena combinación de mejoras es la implementación de MFA y un servidor RADIUS. El uso de MFA mediante certificados digitales es la opción más segura, ya que solo existe un certificado digital único para cada persona de la plantilla. Para que el MFA funcione, se instala el servidor RADIUS para decidir si permite el acceso.

Invertir en formación y concienciar a la plantilla de los riesgos reales a los que se exponen cada día si no hay un buen uso de la red.

- **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:



Problemas de seguridad

En este caso, la red corporativa es la más segura hasta el momento. Su implementación combina el uso del servidor RADIUS para la autenticación, proporcionando credenciales únicas para cada usuario. Por lo que, ofrece más robustez que WPA2 (PSK), ya que una contraseña comprometida no afecta a toda la red. No obstante, ello requiere una óptima configuración de RADIUS, de lo contrario, podría suponer un factor de riesgo para la red.

Es un requisito indispensable el despliegue de MDM para consolidar el uso de RADIUS. Aunque el acceso está restringido a la plantilla que dispone de unas credenciales únicas, la empresa no sabe si el teléfono está infectado o vulnerado, aquí es donde MDM cumple su función y valida el estado del dispositivo.

La conexión cable a la LAN corporativa significa que la red es plana y no hay barreras internas entre la conexión wifi y por cable. Al no haber segmentación, si un atacante infecta un móvil, puede saltar desde ese dispositivo hasta los datos más sensibles de la empresa.

Tipos de ataque a los que está expuesta

La seguridad de la red se ve comprometida por la ausencia de certificados, lo que facilita el robo de credenciales mediante ataques de punto de acceso falso. El atacante intenta engañar a los usuarios para que se conecten a un punto de acceso falso que imita a la red corporativa. De este modo, la víctima se conecta a la red falsa, compartiendo los datos con el servidor controlado por el atacante.

Otro riesgo de ataque es la infiltración por un dispositivo comprometido por la falta de un MDM. Esto permite que un empleado involuntariamente introduzca malware al sistema.

Mejoras a implementar en la red

En primer lugar, es clave desplegar un MDM que solo permita el acceso si el dispositivo cumple los requisitos establecidos.

La segmentación de red mediante VLAN para separar el tráfico wifi del tráfico de la LAN cableada. Así como implementar un firewall entre ambas redes.

Implementación de una DMZ para aislar los servicios compartido como los servidores.

Realizar una monitorización y auditoría constante mediante un SIEM y la configuración de RADIUS para detectar alertas en tiempo real.

La concienciación es clave a la hora de prevenir, por lo que se debe impartir en formación de manera periódica.

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
```

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

Skynet	Skynet_Plus
18:D6:C7:E8:CF:C1	18:D6:C7:E8:CF:C0
26:57:60:92:DB:F8	34:57:60:92:DB:F8

34:57:60:92:DB:F0	

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

Skynet		**Skynet_Plus**	
Canal	Frecuencia	Canal	Frecuencia
11	2,4 GHz	36	5 GHz
56	5 GHz	56	5 GHz
11	2,4 GHz		

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

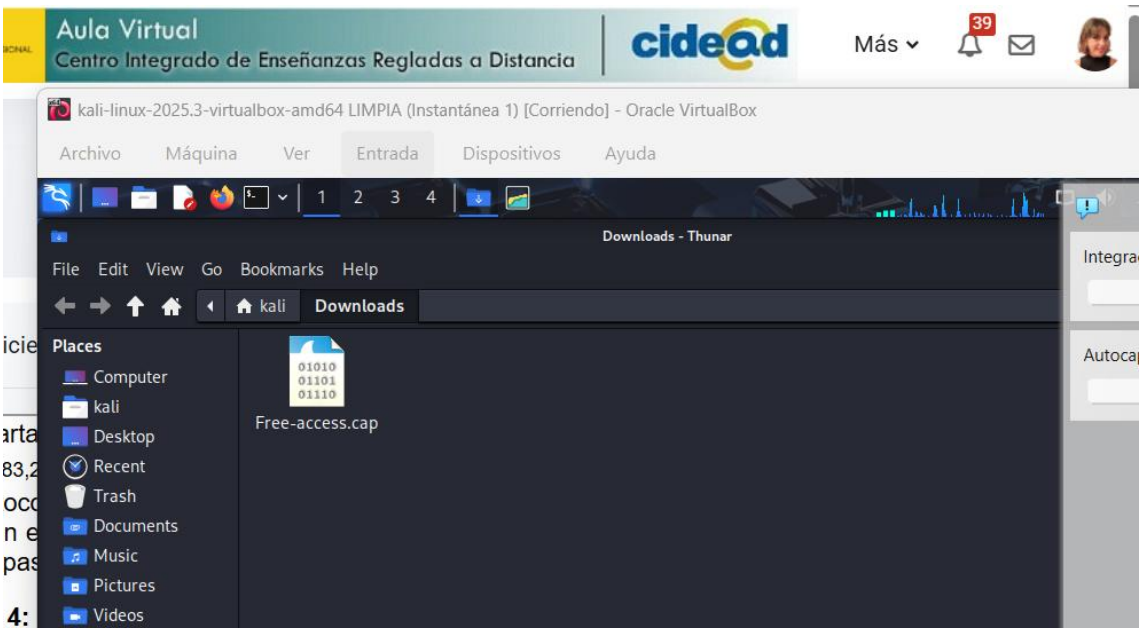
  Está conectado a la red Movistar_E435.

- Indica en qué red intenta conectarse el dispositivo 5C:CF:7F:B4:F4:2C. Intenta conectarse a la red **ONOD79D**

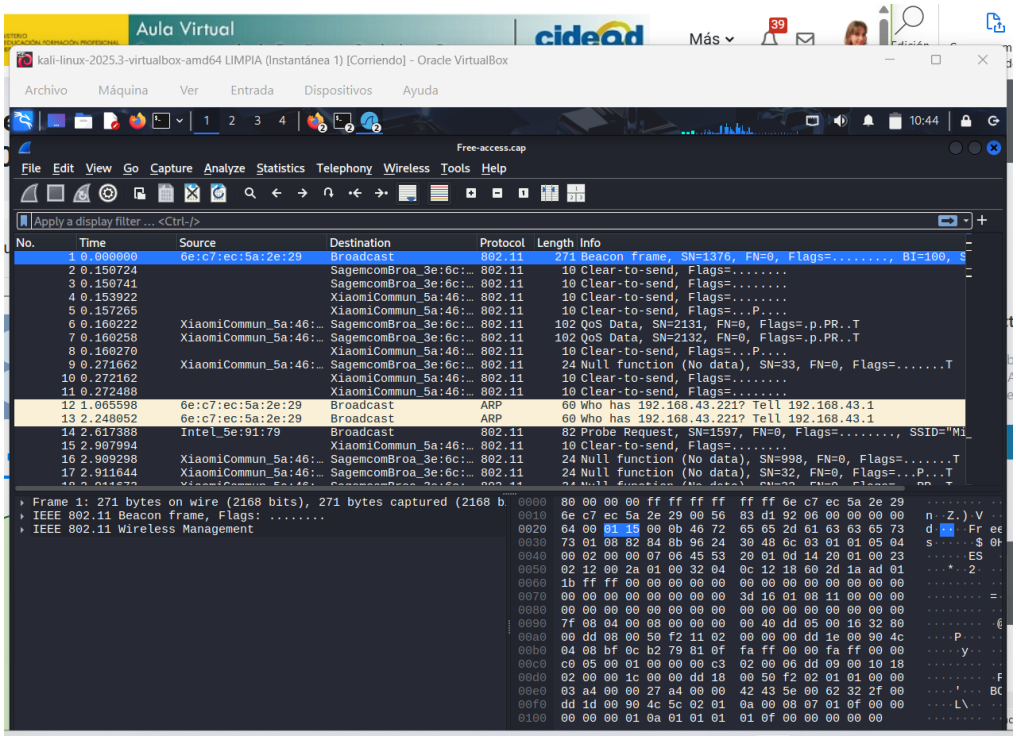
3. Exposición en redes OPEN

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.

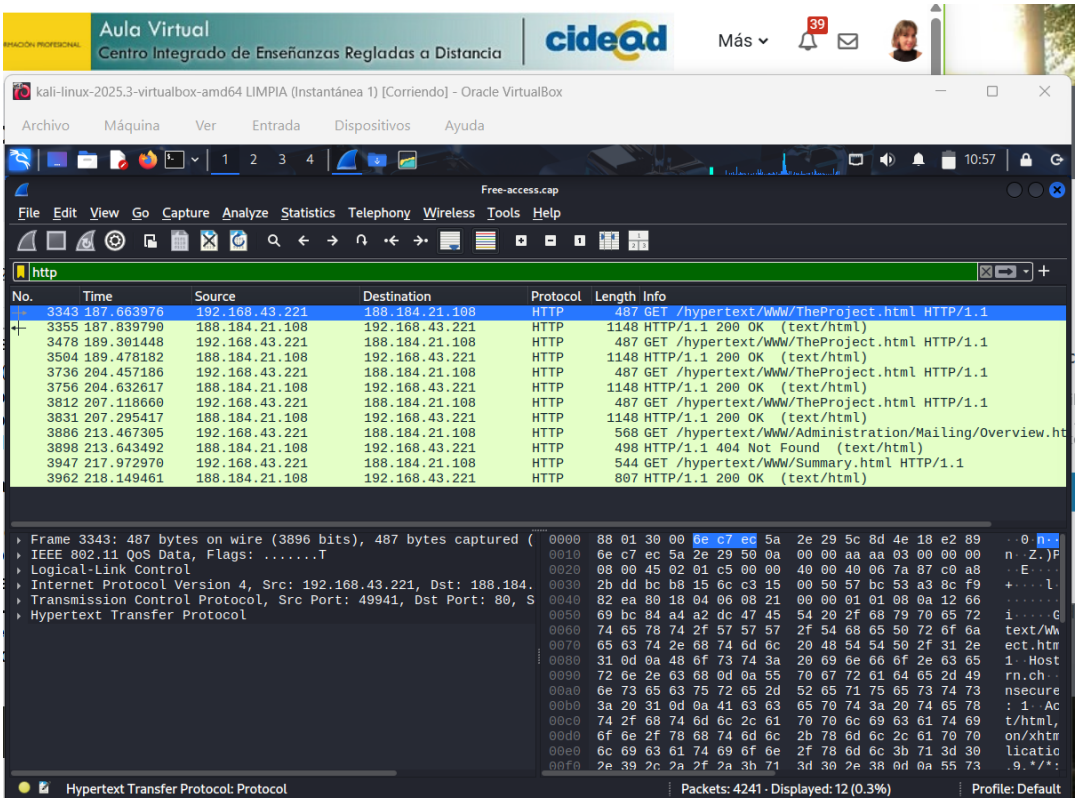
Para la descarga de la captura, se realizará desde Kali Linux instalado en Virtual Box. Tras acceder al aula virtual de CIDEAD, se procede a la descarga del archivo con la captura desde la carpeta de *Donwloads*.



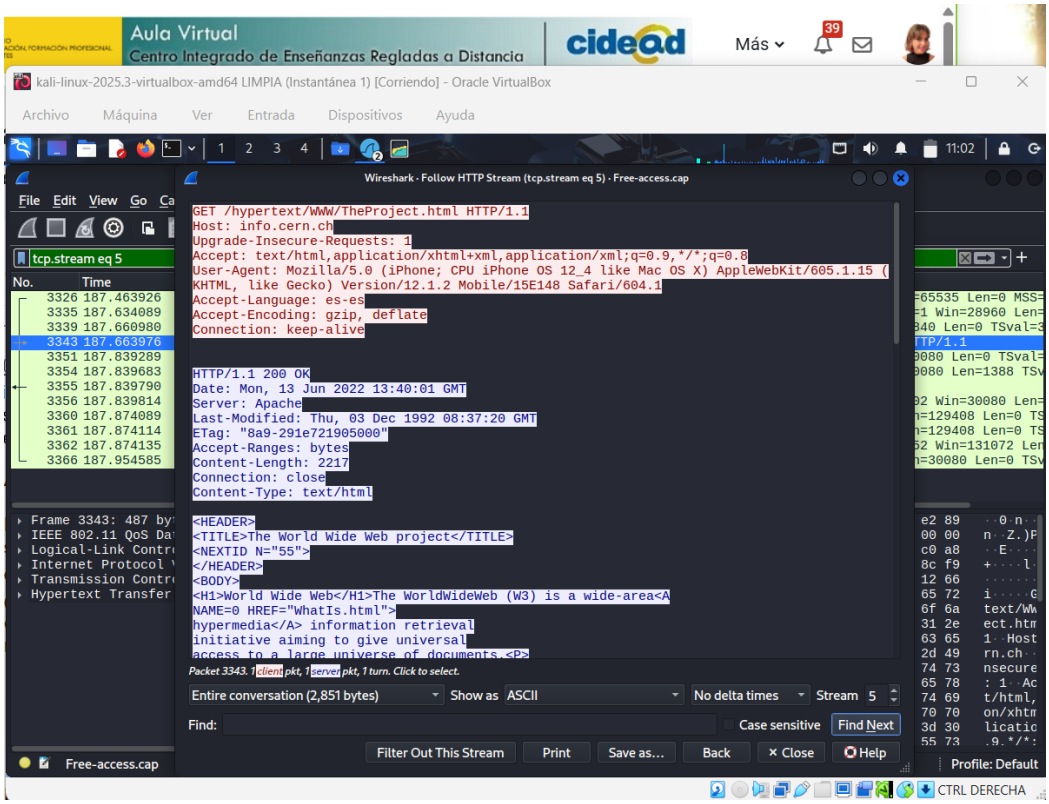
Se abre desde *Wireshark* la descarga de la captura de red de la monitorización de una red OPEN.



Con el filtro *http* se observa un análisis de tráfico HTTP



Para mostrar más detalles del análisis de flujo de datos, con el botón derecho se selecciona *Follow* y *HTTP Stream*, de modo que se obtiene más información sobre la comunicación entre un cliente y un servidor.



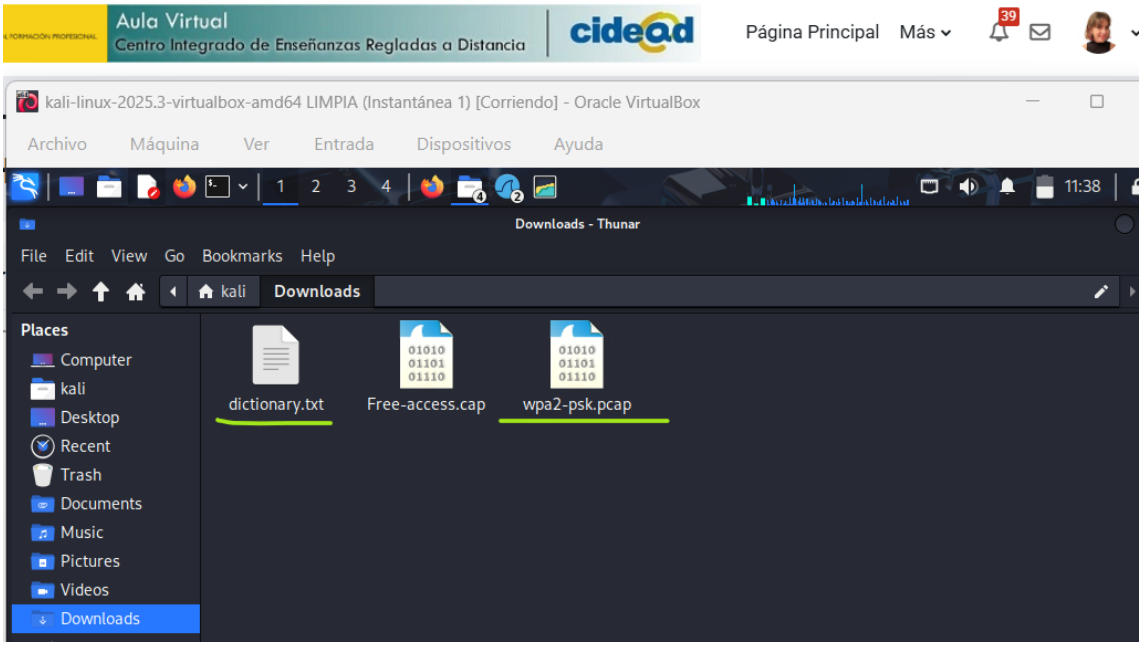
4. Debilidades en las redes inalámbricas

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**

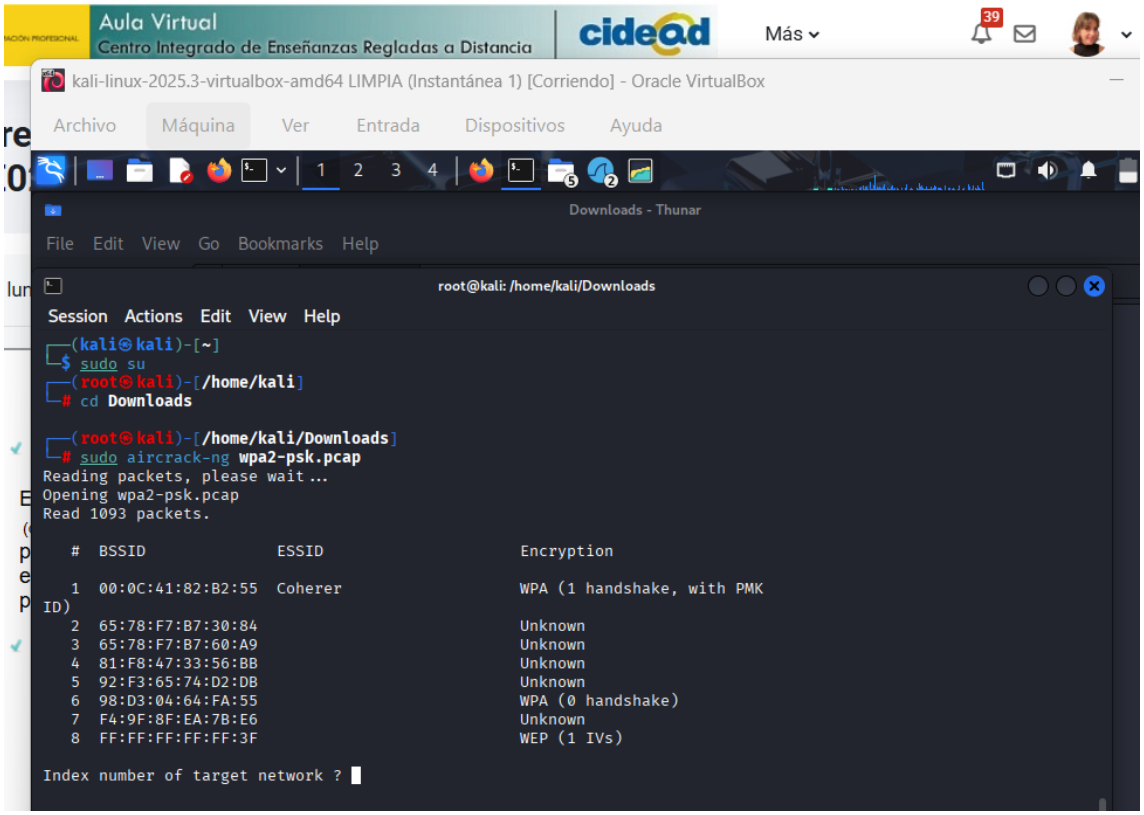
```
$ airodump-ng -r fichero_de_captura
```

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.

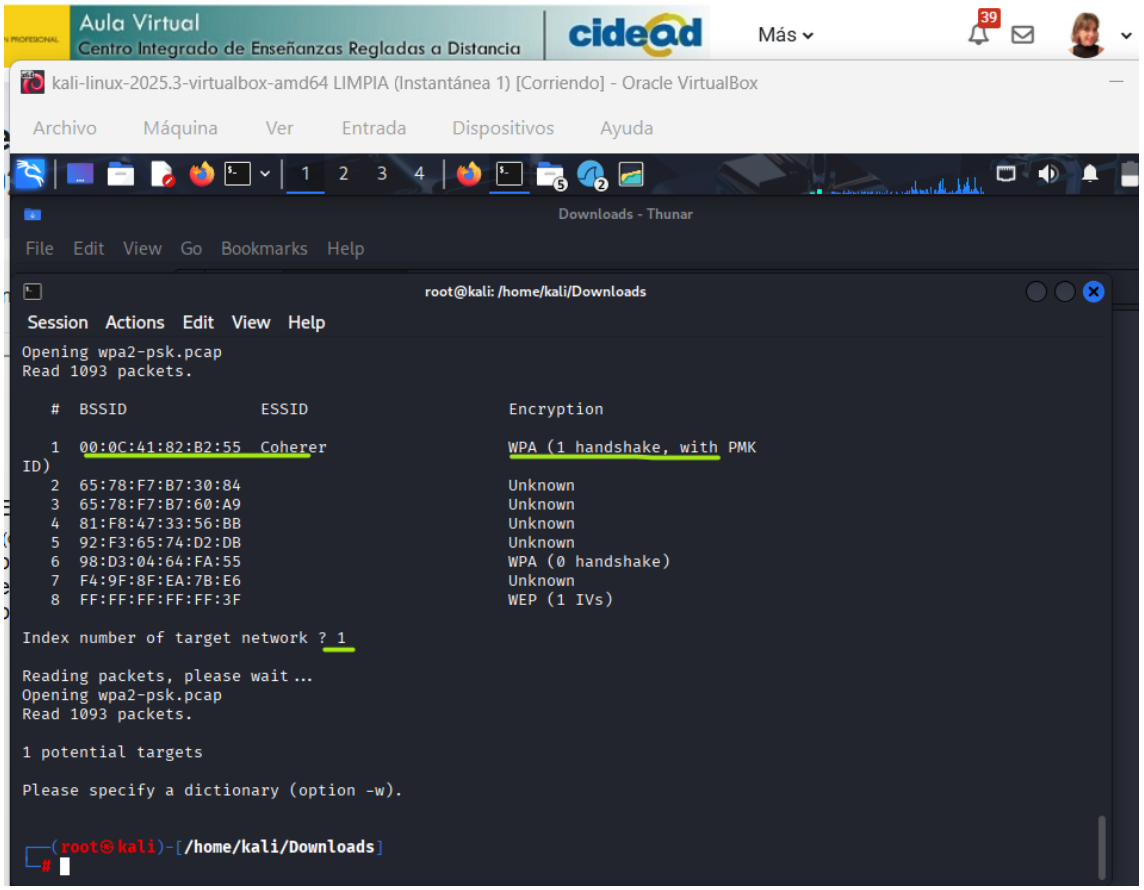
Para este apartado, en primer lugar, se descarga el fichero de captura *wpa2-psk.pcap* y el diccionario de contraseñas *dictionary.txt* en la máquina virtual de Kali Linux que se ha usado en el apartado anterior.



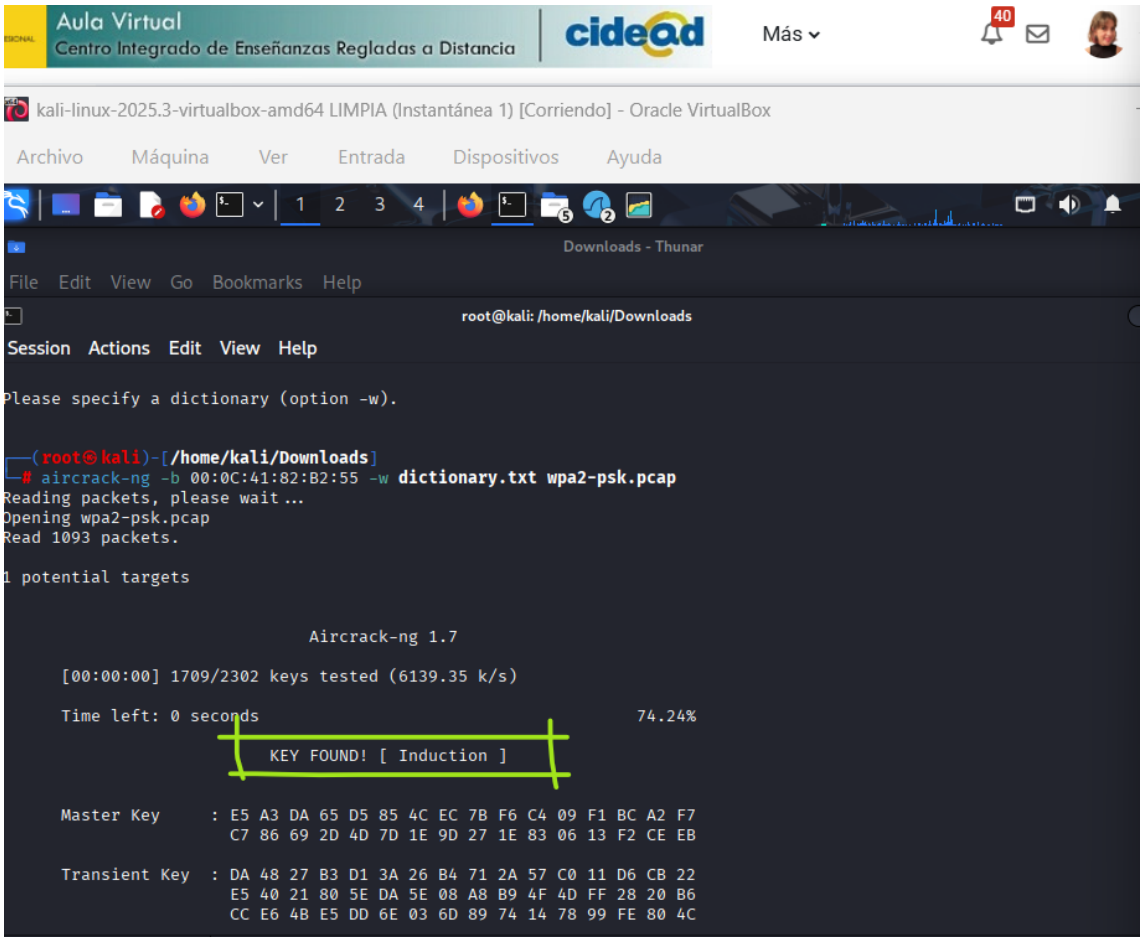
Se ejecuta el comando `sudo aircrack-ng wpa2-psk.pcap` para cargar el fichero. Se analiza el archivo de captura y se observa que tiene un *handshake*.



Una vez abierto el fichero, se selecciona la opción 1 para indicar que se va a trabajar sobre la red *Coherer 00:0C:41:82:B2:55*.

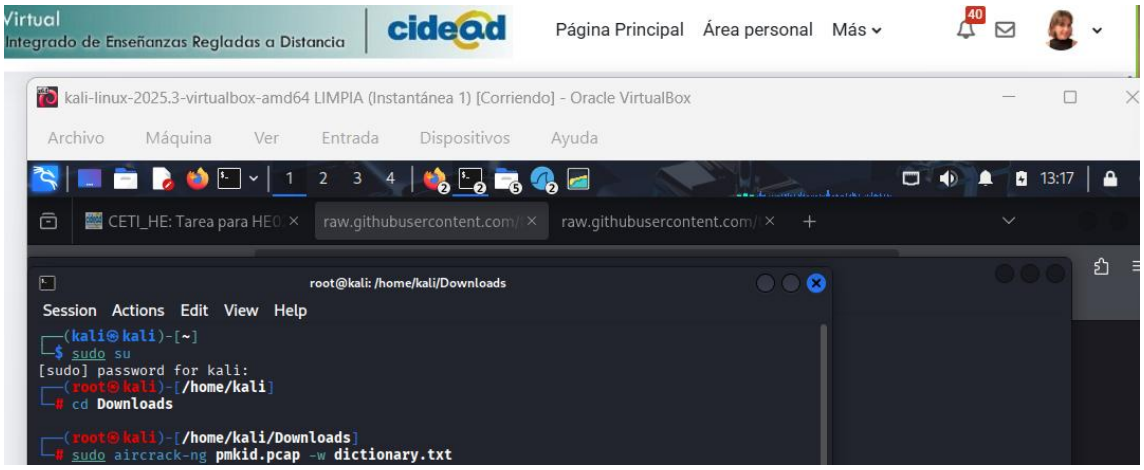


Como solicita el software, se debe incluir el diccionario con la lista de palabras para probar contraseñas contra el handshake capturado. Se ejecuta el parámetro aircrack-ng -b 00:0C:41:82:B2:55 -w dictionary.txt wpa2-psk.pcap. Finalmente, el programa probó las claves y encontró la contraseña de la red wifi: Induction.

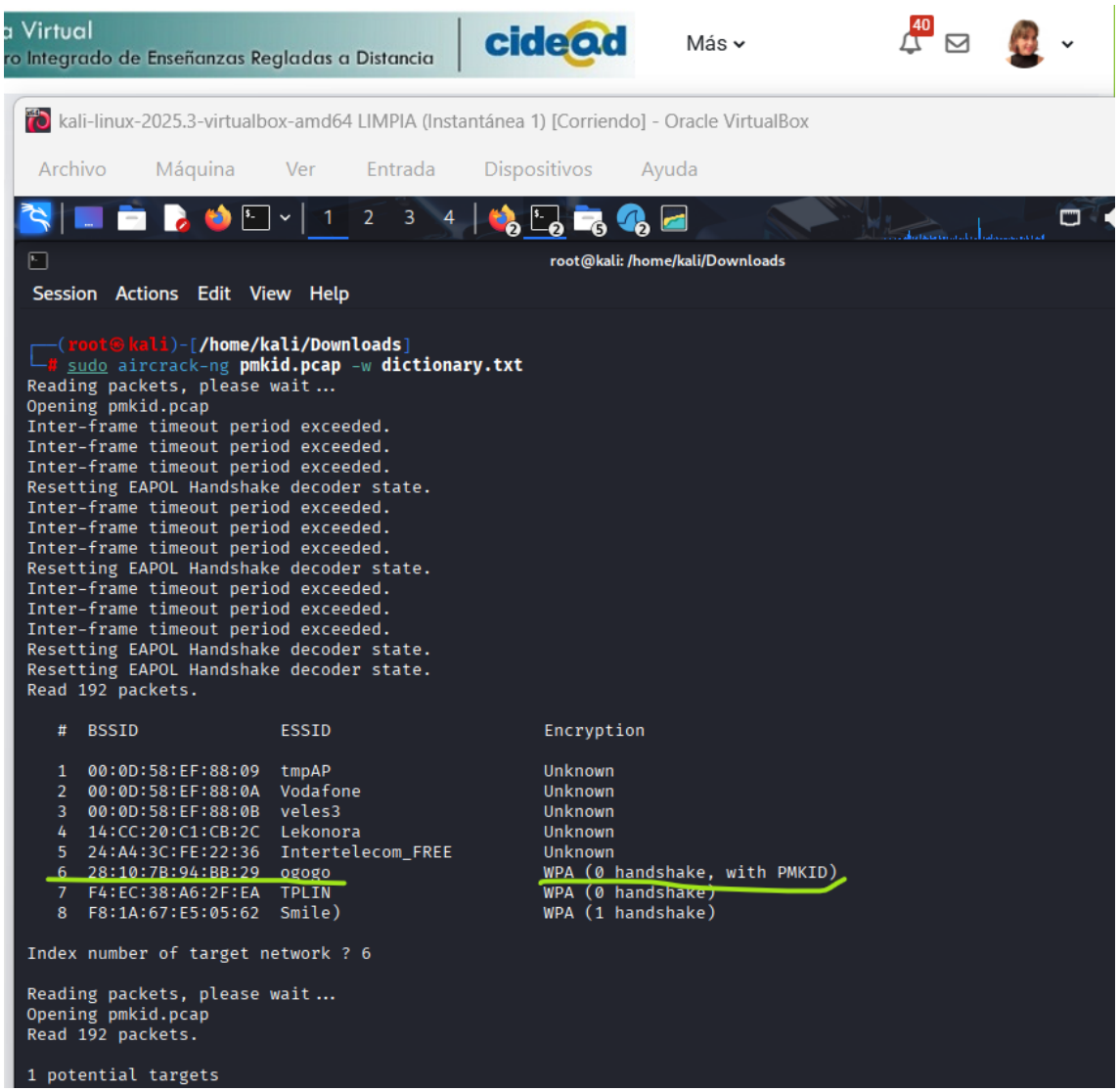


- A continuación se presenta un paquete de captura de red que contiene la captura de un PMKID (pcap - 27,71 KB) de una red WPA2-PSK (Tenéis que realizar esta técnica sobre la red que contiene el PMKID) para aplicarle una técnica de cracking offline. En este caso podéis utilizar el propio aircrack-ng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

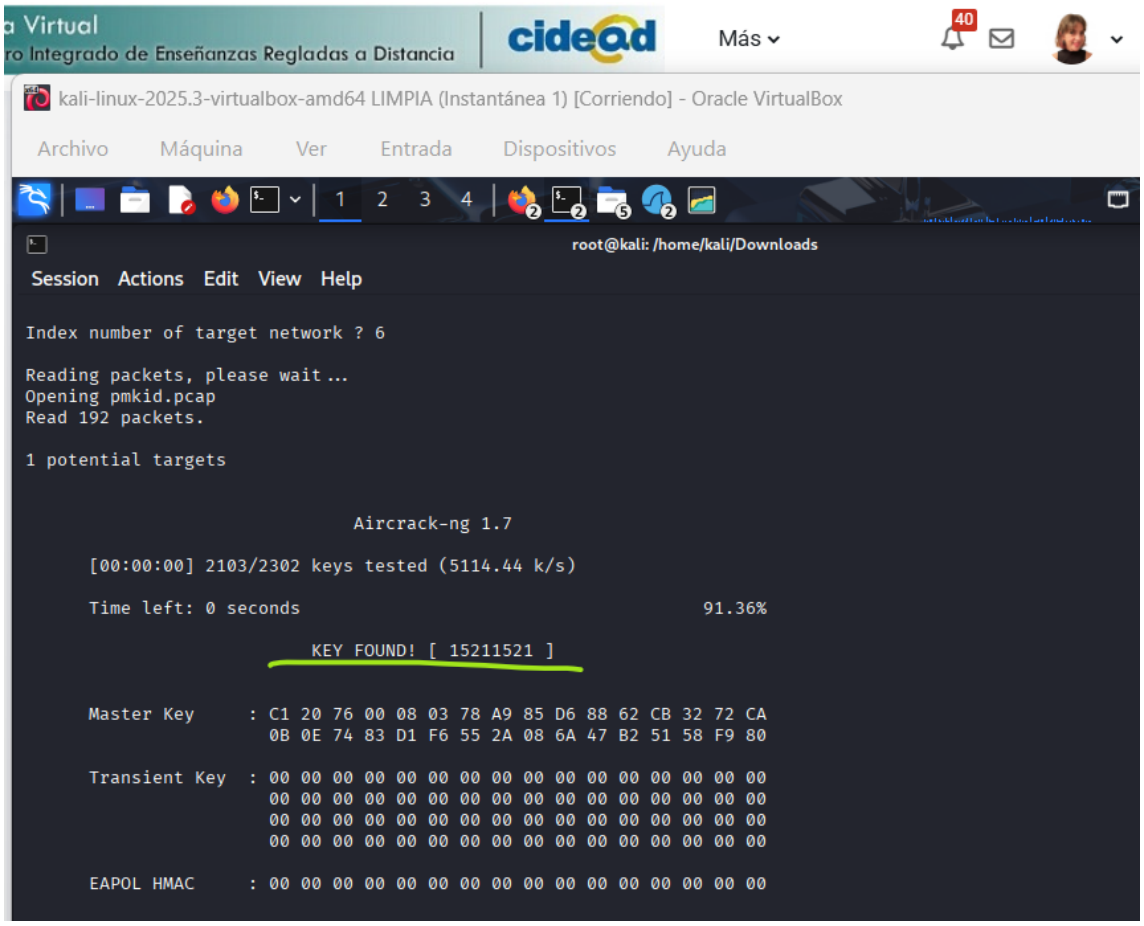
En esta parte, el objetivo es realizar un cracking offline sobre una captura de autenticación WPA2-Enterprise por lo que se utilizarán las herramientas *hashcat* o *johntheripper*. Del mismo modo, se opera desde la máquina virtual Kali Linux y se descarga el archivo de la captura de tráfico de red *pmkid.pcap*. Se ejecuta con el comando sudo aircrack-ng pmkid.pcap -w dictionary.txt para intentar descifrar la clave.



La red número 6 es la que interesa porque contiene el PMKID, material necesario para realizar el ataque sin que, a diferencia de *handshake*, haya que esperar a que el usuario se conecte.



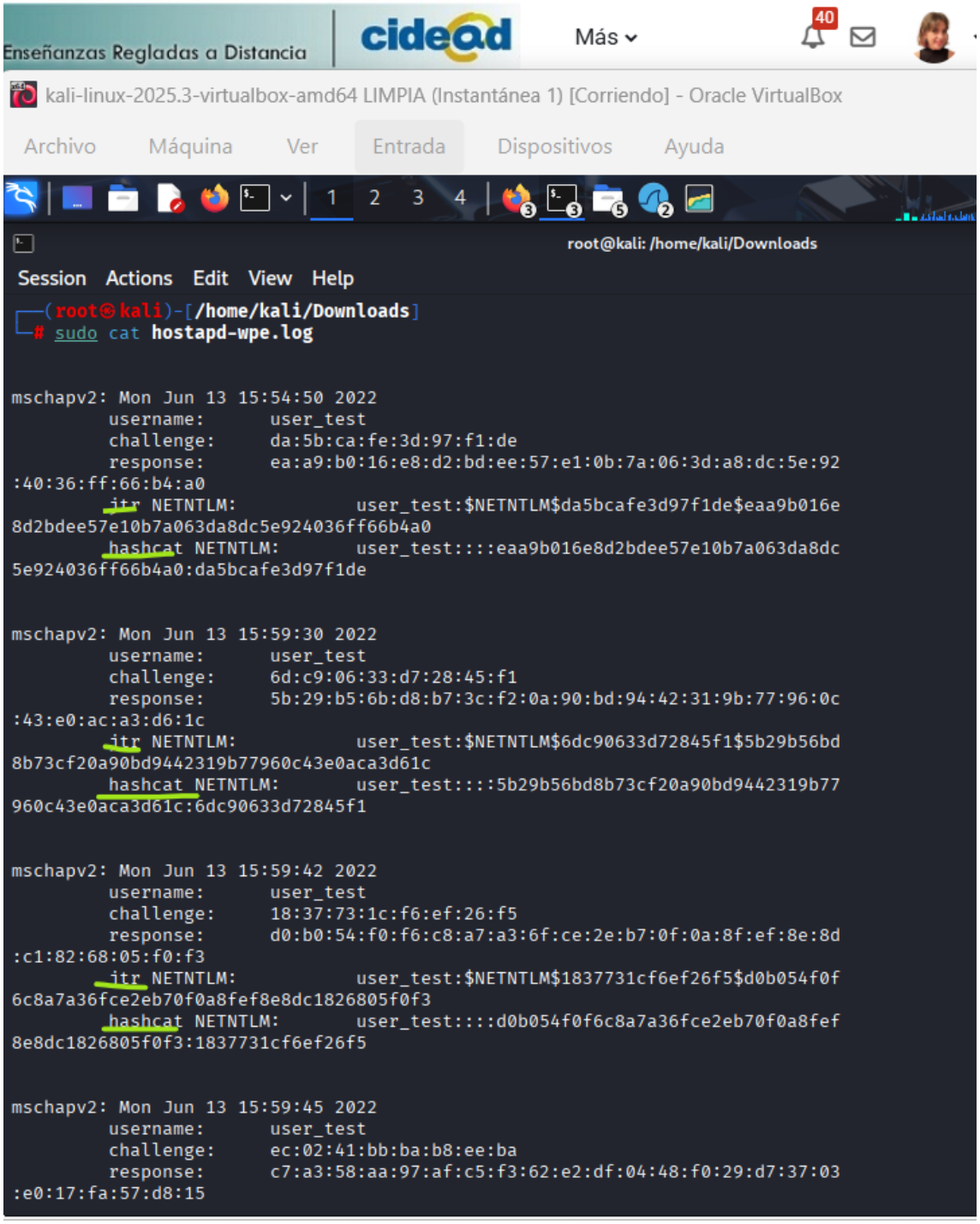
Tras comparar las contraseñas del archivo dictionary.txt con el hash capturado, se consigue la contraseña: 15211521 para la red Ogogo con MAC 28:10:7B:94:BB:29.



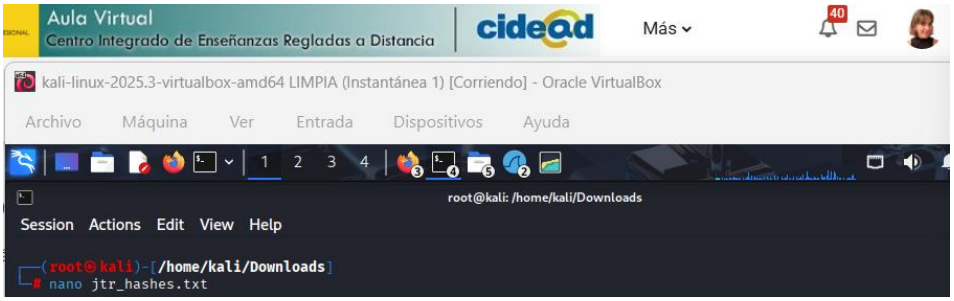
- A continuación se presentan los ficheros de log resultantes de la captura de autenticación WPA2-Enterprise (Log ejecución hostapd-wpe (log - 4,92 KB) - Log autenticación capturada (log - 1,52 KB)) mediante un punto de acceso falso, en este caso también podréis aplicar una técnica de cracking offline.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

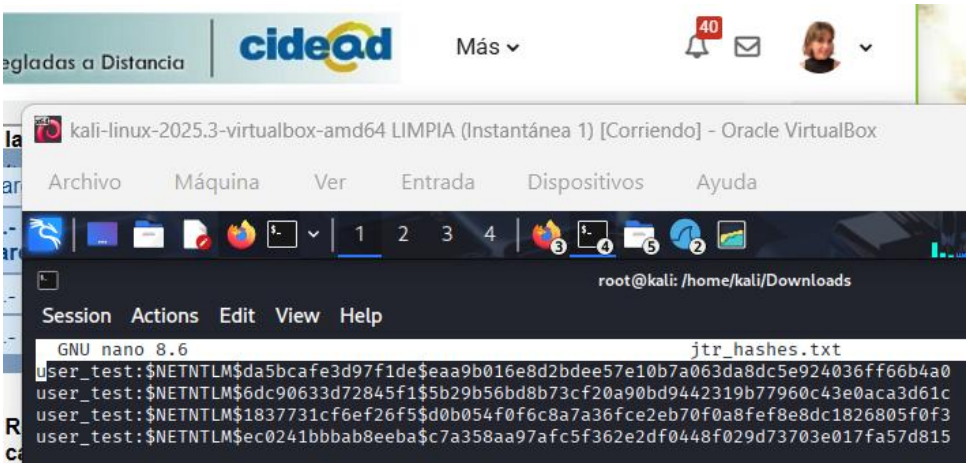
Para este apartado se seguirá la misma metodología que anteriormente. En la misma máquina de Linux se descargan los archivos *hostapd-wpe.log* y *hostapd-wpe-run.log* que son necesarios para hacernos pasar por un punto de acceso falso. En la terminal se ejecuta con el comando: sudo cat hostapd-wpe.log.

Se visualizan las credenciales capturadas que contienen tanto hashes de *hashcat* como *johntheripper*. Una vez conseguido el log con la información, lo siguiente es la preparación de los datos para el ataque, entonces se debe generar el archivo nano *jtr_hashes.txt* que solo contenga los hashes para *johntheripper*.


Enseñanzas Regladas a Distancia
cidead
Más
kali-linux-2025.3-virtualbox-amd64 LIMPIA (Instantánea 1) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali: /home/kali/Downloads
Session Actions Edit View Help
(root㉿kali)-[/home/kali/Downloads]
sudo cat hostapd-wpe.log
mschapv2: Mon Jun 13 15:54:50 2022
username: user_test
challenge: da:5b:ca:fe:3d:97:f1:de
response: ea:a9:b0:16:e8:d2:bd:ee:57:e1:0b:7a:06:3d:a8:dc:5e:92
:40:36:ff:66:b4:a0
jtr NETNTLM: user_test:$NETNTLM$da5bcafe3d97f1de$eaa9b016e
8d2bdee57e10b7a063da8dc5e924036ff66b4a0
hashcat NETNTLM: user_test::::eaa9b016e8d2bdee57e10b7a063da8dc
5e924036ff66b4a0:da5bcafe3d97f1de
mschapv2: Mon Jun 13 15:59:30 2022
username: user_test
challenge: 6d:c9:06:33:d7:28:45:f1
response: 5b:29:b5:6b:d8:b7:3c:f2:0a:90:bd:94:42:31:9b:77:96:0c
:43:e0:ac:a3:d6:1c
jtr NETNTLM: user_test:$NETNTLM$6dc90633d72845f1$5b29b56bd
8b73cf20a90bd9442319b77960c43e0aca3d61c
hashcat NETNTLM: user_test::::5b29b56bd8b73cf20a90bd9442319b77
960c43e0aca3d61c:6dc90633d72845f1
mschapv2: Mon Jun 13 15:59:42 2022
username: user_test
challenge: 18:37:73:1c:f6:ef:26:f5
response: d0:b0:54:f0:f6:c8:a7:a3:6f:ce:2e:b7:0f:0a:8f:ef:8e:8d
:c1:82:68:05:f0:f3
jtr NETNTLM: user_test:$NETNTLM$1837731cf6ef26f5$d0b054f0f
6c8a7a36fce2eb70f0a8fef8e8dc1826805f0f3
hashcat NETNTLM: user_test::::d0b054f0f6c8a7a36fce2eb70f0a8fef
8e8dc1826805f0f3:1837731cf6ef26f5
mschapv2: Mon Jun 13 15:59:45 2022
username: user_test
challenge: ec:02:41:bb:ba:b8:ee:ba
response: c7:a3:58:aa:97:af:c5:f3:62:e2:df:04:48:f0:29:d7:37:03
:e0:17:fa:57:d8:15

Guardamos el archivo *jtr_hashes.txt* con ctrl O y enter y ctrl X para salir.

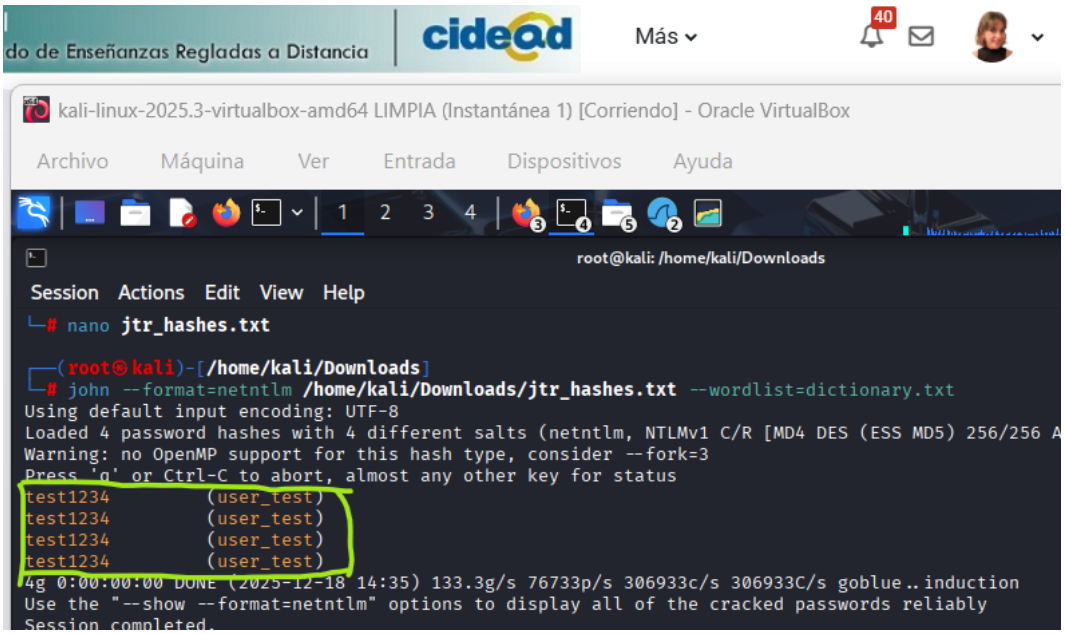




Una vez guardados los hashes en el archivo *nano*, el siguiente paso para descubrir la contraseña de *user_test*, es realizar el cracking offline pasándoselo a *johntheripper* con el siguiente comando:

```
john --format=netntlm /home/kali/Descargas/jtr_hashes.txt --wordlist=dictionary.txt
```

Finalmente, se descubre la contraseña **test1234**.



5. Webgrafía

https://www.incibe.es/ciudadania/formacion/infografias/wifi-publicas-principales-riesgos

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-en-redes-wifi.pdf

https://www.avast.com/es-es/c-evil-twin-attack