



TAREA 02

HACKING ÉTICO EN ENTORNOS INALÁMBRICOS

HACKING ÉTICO

ALBA MOREJÓN GARCÍA

2024/2025

CETI - Ciberseguridad en Entornos de las Tecnologías de la Información

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.

- 1) La primera fase se centrará en buscar debilidades de diseño de la red inalámbrica y contemplar las casuísticas en el que se estén utilizando tipologías de redes Wi-Fi que no resulten adecuadas para la funcionalidad que desempeñan.
- 2) En la segunda fase se realizará 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.
- 3) 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.

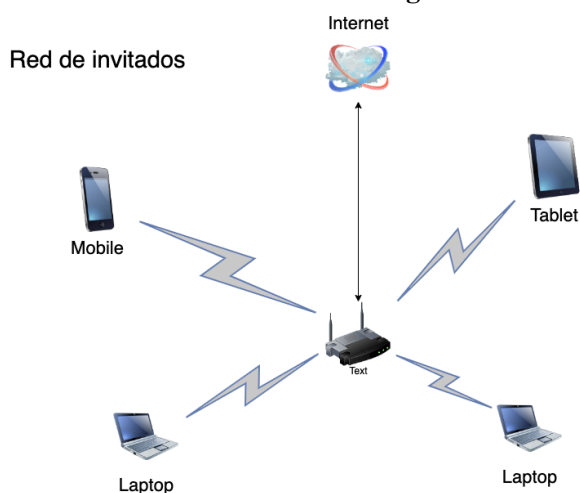
Apartado 1: Revisar el diseño de la red Wi-Fi

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.

A continuación se muestra el diagrama de la red de invitados:



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

El problema de seguridad en cuanto al tipo de red Wi-fi, es que es de tipo OPEN, una red abierta sin requerimiento de autenticación, ni cifrado de conexión. Por tanto, cualquier persona dentro del alcance puede conectarse. El riesgo que existe es que no hay forma de identificar los usuarios conectados y los datos transmitidos entre dispositivos y el punto de acceso no se cifran, lo que facilita la interceptación por parte de atacantes. El segundo problema es el uso compartido de la red, permitir que empleados utilicen la misma red que los visitantes, puede exponer los dispositivos corporativos a una red con baja seguridad, facilitando la propagación de malware. Un atacante conectado a la red de invitados podría realizar ataques como spoofing o inyección de código, afectando a todos los equipos conectados.

Tipos de ataques a los que se ve expuesta una red:

- Acceso no autorizado:

Una red tipo OPEN, permite que cualquier dispositivo dentro del alcance, se conecte sin restricciones lo que facilita el acceso no autorizado. Un atacante puede escanear la red con herramientas como nmap para identificar dispositivos conectados y servicios vulnerables. Además, puede realizar ataques como ARP Poisoning para redirigir el tráfico de otro usuario a su dispositivo, logrando un ataque Man in the Middle y capturar información confidencial como credenciales o datos privados.

- Ausencia de cifrado:

Al no cifrar los datos transmitidos, una red de este tipo permite que cualquier atacante con una tarjeta de red en modo monitor intercepte las tramas de red. Herramientas como Wireshark pueden capturar datos enviados (como contraseñas o correo electrónico). Esto puede escalar mediante ataques como Rogue Access Point, donde el atacante crea un punto de acceso falso que se presenta como la red legítima para capturar más datos.

Implementación mejoras:

- Implementar un cifrado para la red invitados

Al implementar esta seguridad los datos estarán protegidos mediante cifrado y se evitarán ataques como el sniffing y MITM. Se puede utilizar WPA3 en el router, asignando una contraseña para invitados y también está la posibilidad de permitir conexiones sin contraseña pero cifrando los datos automáticamente.

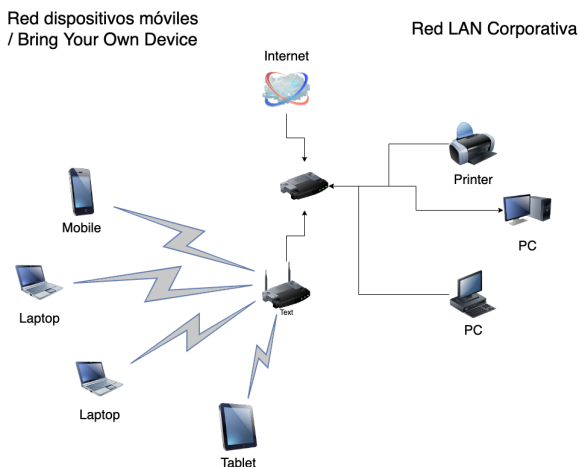
- Segmentar la red de invitados del resto de la red empresarial

Actualmente si un atacante compromete un dispositivo en la red de invitados, podría acceder a la red interna de la empresa. Se podría implementar el uso de VLANs para aislar el tráfico de la red de invitados, asegurar que los dispositivos conectados a esta red no puedan comunicarse con dispositivos internos y limitar la funcionalidad dando únicamente acceso a Internet y bloquear acceso a recursos locales.

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.

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



La red de dispositivos móviles bajo la filosofía “Bring Your Own Device” presenta varios problemas de seguridad debido a su diseño y uso. Al usar WPA2-PSK todos los dispositivos comparten la misma clave, lo que significa que si uno se ve comprometido, toda la red está en riesgo. Además, los dispositivos personales no siempre cumplen con las políticas de seguridad corporativas facilitando la entrada de malware, también existe un alto riesgo de fuga de datos ya que los empleados acceden a información sensible desde dispositivos no asegurados. Por último, el acceso desde la fábrica cercana sugiere la falta de control sobre la geolocalización de los dispositivos autorizados, aumentando la vulnerabilidad de la red.

Tipos de ataque a los que está expuesta:

- Captura del 4-way-handshake, el ataque más común basado en redes con este tipo de seguridad, consiste en que un atacante captura un intento de autenticación de un cliente para obtener la clave, permitiendo un acceso no autorizado.
- Ataques de fuerza bruta y diccionario (ataque de contraseña) si la contraseña no es suficientemente robusta este tipo de redes pueden ser vulnerables.
- Intercepción del tráfico, (ataque basado en red) la variedad de dispositivos que pueden conectarse a la red, puede significar que alguno no implemente bien el cifrado, facilitando a el ataque MitM.
- Phishing, los dispositivos personales son más susceptibles a ataques de ingeniería social. Los atacantes buscan ganarse la confianza del usuario para conseguir credenciales y otros datos sensibles.

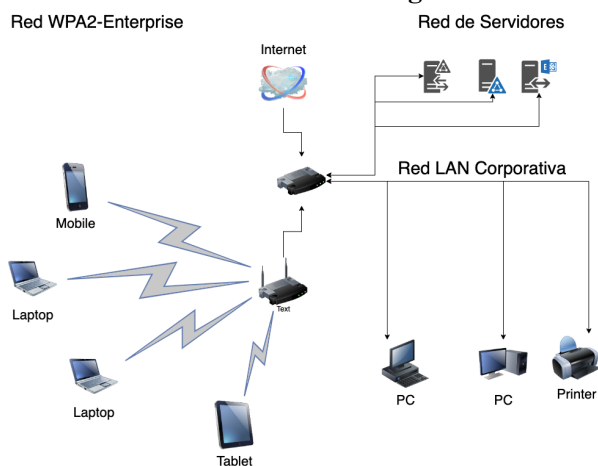
Implementación mejoras:

- Autenticación WPA3-Enterprise, migrar a este tipo de seguridad ofrecería una autenticación individual para cada dispositivo aumentando así la seguridad.
- Software de gestión de dispositivos móviles (MDM) implementar esta solución para asegurar que todos los dispositivos de la red BYOD cumplan con las políticas de seguridad de la empresa incluyendo cifrado, bloqueo remoto y capacidad de limpieza.
- Monitoreo y control de acceso geográfico, utilizar tecnologías que permitan restringir el acceso a la red sólo a dispositivos dentro de una ubicación aprobada.

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.

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



La red corporativa aunque utiliza WPA2-Enterprise para proporcionar una autenticación individual a través de un servidor RADIUS, presenta problemas de seguridad significativos. Si las credenciales de un empleado están comprometidas un atacante podría acceder a la red con privilegios completos. Además, sin una solución de gestión de dispositivos móviles (MDM) implementada, no hay garantía de que todos los dispositivos cumplan con las políticas de seguridad. Al proporcionar el mismo nivel de acceso que la red cableada, un atacante que obtenga acceso a la red Wi-fi puede moverse lateralmente y acceder a recursos internos sensibles.

Tipos de ataque a los que está expuesta:

- Punto de acceso falso, un atacante puede establecer un punto de acceso falso que imite a la red legítima, cuando el empleado intente conectarse, los intentos de autenticación son capturados, para así obtener sus credenciales.
- Ataque de phishing y robo de credenciales, los empleados pueden ser víctimas de un ataque mediante ingeniería social donde se les engañan para que revelen sus credenciales.
- Ataque Man in the Middle, si un atacante logra posicionarse entre el usuario y el punto de acceso, puede intentar interceptar o manipular las comunicaciones, especialmente si hay debilidades en el cifrado o en la autenticación.

Implementación mejoras:

- Despliegue de mobile device management (MDM) para asegurar que todos los dispositivos cumplen con las políticas de seguridad, incluyendo actualizaciones de software y protección contra malware.
- Autenticación multifactor (MFA) utilizar una segunda capa de verificación tras la introducción de credenciales, para reducir el riesgo de accesos no autorizados incluso si se comprometen las credenciales.

Apartado 2: Monitorización de datos

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

- Indica los BSSID de los Puntos de Acceso de las Redes Skynet y Skynet_Plus.
- Indica en qué bandas de frecuencia y en qué canales operan las redes Skynet y Skynet_Plus.
- Indica a qué red está conectado el dispositivo con MAC 6E:52:AC:9D:B4:87.
- Indica en qué red intenta conectarse el dispositivo 5C:CF:7F:B4:F4:2C.

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
18:06:C2:F8:CF:C0	-33	18	5	0	36	1170	WPA2	CCMP	PSK	Skynet-plus
18:06:C2:F8: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	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	ONOG63-5G
DC:53:7C:59:55:3F	-79	10	0	0	11	195	WPA2	CCMP	PSK	ONOG63
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
10:50:DC:72:F2:10	-84	7	0	0	1	360	WPA2	CCMP	PSK	PATRALEX
98:97:D1:35:E4:3E	-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:84	-85	4	0	0	6	130	WPA2	CCMP	PSK	MOVISTAR-78B3
10:50: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	ONOGAA-5G
6A:CE:DA:70:FA:47	-89	3	0	0	100	1733	WPA2	CCMP	PSK	MiFibra-FA43
A4:CE:DA:70: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			PSK	<length: 0>
A4:CE:DA:70: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:8C	-1	0	0	0	36	-1			PSK	<length: 0>
62:1E:A3:67:32:47	-86	1	0	0	6	130	WPA2	CCMP	PSK	vodafone18E0
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
(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
(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	0		2
86:97:D1:35:E4:3E	D0:81:28:14:A7:AD	-1	6e-0	0	0		5
98:97:D1:35:E4:3E	04:54:53:EB:26:F6	-1	6e-0	0	0		26

airodump: herramienta en línea para capturar tramas 802.11 de redes Wi-fi

BSSID: dirección MAC del punto de acceso/router.

Punto de acceso: dispositivos que permiten al Wi-fi conectarse a una red local (LAN)

Bandas de frecuencia: las redes wi-fi operan en bandas de 2.4 GHz y 5GHz cada banda se divide en canales.

Los canales: son los rangos de frecuencia específicos dentro de la banda que se utilizan para evitar interferencias y mejorar el rendimiento.

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 y 26:57:60:92:DB:F0

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

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

Skynet:

18:D6:C7:E8:CF:C1 Canal: 11 Banda: 195MB (2.4GHz)

26:57:60:92:DB:F8 Canal: 56 Banda: 1733MB (5GHz)

26:57:60:92:DB:F0 Canal: 11 Banda: 130MB (2.4GHz)

Skynet_Plus:

18:D6:C7:E8:CF:C0 Canal: 11 Banda: 195MB (2.4GHz)

34:57:60:92:DB:F8 Canal: 36 Banda: 1170MB (5GHz)

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

MOVISTAR_PLUSS_E435

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

MAC:5C:CF:7F:B4:F4:2C - ONOD79D

Apartado 3: Exposición en redes OPEN

En este apartado se proporciona una [Captura de red de la monitorización de una red OPEN](#). 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.

Aula Virtual
Centro Integrado de Enseñanzas Regladas a Distancia

cidead

Mis cursos Recursos Enlaces

ALBA MOREJON GARCIA

Free-access.cap

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1723	165.076724	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request - Transaction ID 0x46
1724	165.077465	fe80::cdf:61d1:560:c...	ff02::16	ICMPv6	128	Multicast Listener Report Message v
1725	165.079534	fe80::cdf:61d1:560:c...	ff02::fb	MDNS	150	Standard query 0x0000 PTR _sleep-pr
1726	165.080480	Apple_18:e2:89	6e:c7:ec:5a:2e:29	802.11	24	Null function (No data), SN=1787, F
1727	165.080498	Apple_18:e2:89	Apple_18:e2:89	802.11	10	Acknowledgement, Flags=.....
1728	165.209868	Apple_18:e2:89	6e:c7:ec:5a:2e:29	802.11	24	Null function (No data), SN=1788, F
1729	165.209885	Apple_18:e2:89	Apple_18:e2:89	802.11	10	Acknowledgement, Flags=.....
1730	165.210185	6e:c7:ec:5a:2e:29	Apple_18:e2:89	802.11	16	Request-to-send, Flags=.....
1731	165.210199	6e:c7:ec:5a:2e:29	6e:c7:ec:5a:2e:29	802.11	10	Clear-to-send, Flags=.....
1732	165.210376	192.168.43.1	192.168.43.221	DHCP	371	DHCP ACK - Transaction ID 0x46
1733	165.210393	Apple_18:e2:89	6e:c7:ec:5a:2e:29	802.11	28	802.11 Block Ack, Flags=.....

Una vez abierta la captura de red, vemos que los protocolos más utilizados son; 802.11, TCP, TLSv1.2, HTTP, ARP, DHCP, ICMPv6, MDNS, DNS...

Análisis protocolos:

Free-access.cap						
No.	Time	Source	Destination	Protocol	Length	Info
3644	194.925049	HuaweiDevice_72:f2:13	SagemcomBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3645	194.955241	HuaweiDevice_72:f2:13	SagemcomBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3646	195.928214	Espressif_c0:2f:a8	SagemcomBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3647	196.454026	Intel_5e:91:79	Broadcast	802.11	82	Probe Request, SN=1709, FN=0, Flags=.....
3648	196.557220	HuaweiDevice_72:f2:13	SagemcomBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3649	196.566922	HuaweiDevice_72:f2:13	SagemcomBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3650	196.574902	HuaweiDevice_72:f2:13	SagemcomBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3651	196.578702	HuaweiDevice_72:f2:13	SagemcomBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3652	196.592285	HuaweiDevice_72:f2:13	SagemcomBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3653	196.630151	HuaweiDevice_72:f2:13	SagemcomBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3654	196.842273	6e:c7:ec:5a:2e:29	42:9f:3b:d6:53:f8	802.11	265	Probe Response, SN=3515, FN=0, Flag=.....
3655	196.845297	6e:c7:ec:5a:2e:29	42:9f:3b:d6:53:f8	802.11	265	Probe Response, SN=3515, FN=0, Flag=.....

Protocolo 802.11 (wlan)

Sources: XiaomiCommun_5a:46:e9, HuaweiDevice_72:f2:13, Espressif_c0:2f:a8, Apple_18:e2:89...

Destination: Broadcast, 6e:c7:ec:5a:2e:29, 192.168.43.221

Observamos una gran variedad de dispositivos (móviles) conectados y comunicándose con la red. Las respuestas que da el servidor broadcast sugieren una difusión generalizada de información y la comunicación directa con una ip, en específico.

Free-access.cap						
No.	Time	Source	Destination	Protocol	Length	Info
2003	168.540638	192.168.43.221	74.125.133.109	TCP	86	49195 → 993 [ACK] Seq=189 Ack=4259
2007	168.541109	192.168.43.221	74.125.133.109	TCP	86	[TCP Window Update] 49195 → 993 [ACK]
2011	168.549061	192.168.43.221	74.125.133.109	TLSv1.2	161	Client Key Exchange
2015	168.557793	74.125.133.109	192.168.43.221	TCP	86	993 → 49196 [ACK] Seq=1 Ack=189 Win=...
2019	168.559202	74.125.133.109	192.168.43.221	TLSv1.2	1474	Server Hello
2020	168.559233	74.125.133.109	192.168.43.221	TCP	1474	993 → 49196 [PSH, ACK] Seq=1389 Ack=...
2024	168.559975	74.125.133.109	192.168.43.221	TLSv1.2	1474	Certificate
2025	168.560027	74.125.133.109	192.168.43.221	TLSv1.2	181	Server Key Exchange, Server Hello D...
2029	168.560103	192.168.43.221	74.125.133.109	TCP	86	49196 → 993 [ACK] Seq=189 Ack=2777
2033	168.561142	192.168.43.221	74.125.133.109	TCP	86	49196 → 993 [ACK] Seq=189 Ack=4260
2037	168.572355	17.57.146.43	192.168.43.221	TCP	86	5223 → 49194 [ACK] Seq=1 Ack=223 Wi...

Protocolo TCP y TLSv1.2 (tpc)

predomina la comunicaciones entre 17.57.146.43, 17.248.180.68, 74.125.133.109 y sobre todo 192.168.43.221

La ip parece ser un punto central de comunicación, un dispositivo o servidor clave en la red, las otras ips podrían ser servidores o servicios externos.

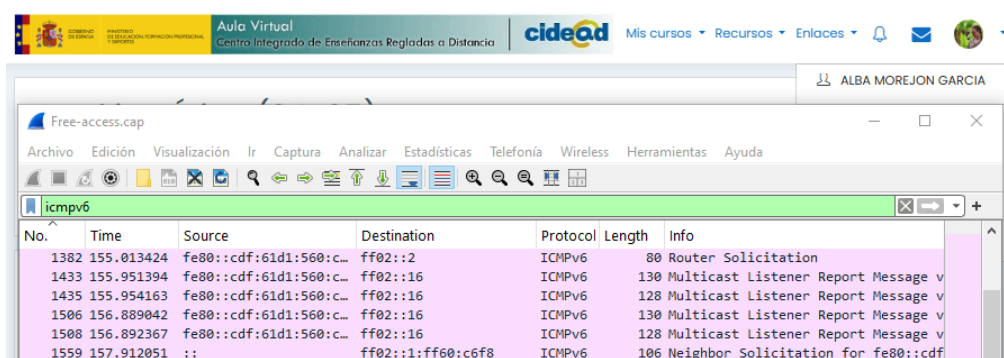
Free-access.cap						
No.	Time	Source	Destination	Protocol	Length	Info
1487	156.567099	Apple_18:e2:89	Broadcast	ARP	62	Who has 192.168.43.221? (ARP Probe)
1489	156.567834	Apple_18:e2:89	Broadcast	ARP	60	Who has 192.168.43.221? (ARP Probe)
1501	156.858338	Apple_18:e2:89	Broadcast	ARP	62	Who has 192.168.43.221? (ARP Probe)
1503	156.862820	Apple_18:e2:89	Broadcast	ARP	60	Who has 192.168.43.221? (ARP Probe)
1519	157.210119	Apple_18:e2:89	Broadcast	ARP	62	ARP Announcement for 192.168.43.221
1521	157.212071	Apple_18:e2:89	Broadcast	ARP	60	ARP Announcement for 192.168.43.221
1532	157.561023	Apple_18:e2:89	Broadcast	ARP	62	ARP Announcement for 192.168.43.221
1534	157.565193	Apple_18:e2:89	Broadcast	ARP	60	ARP Announcement for 192.168.43.221
1541	157.777558	Apple_18:e2:89	Broadcast	ARP	62	ARP Announcement for 192.168.43.221

Protocolo ARP (arp)

Todo son comunicaciones con origen en 6e:c7:ec:5a:2e:29 y destino en el broadcast debido a que el dispositivo está solicitando la dirección MAC de otros dispositivos de la red mediante arp.

Protocolo DHCP:

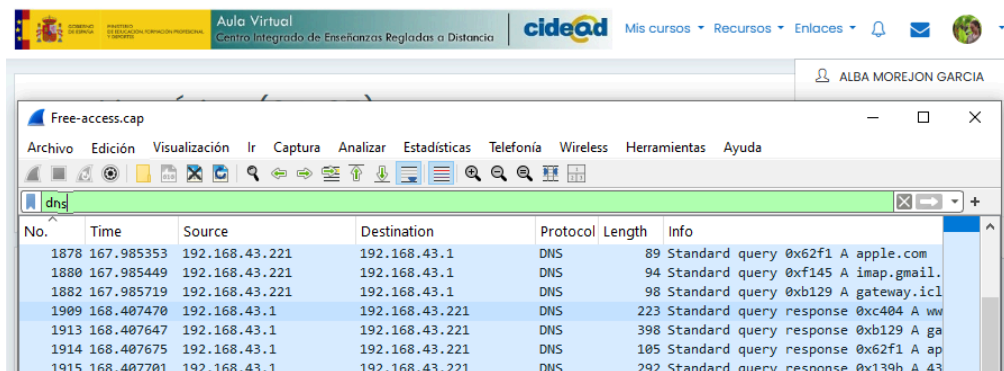
El origen es siempre 0.0.0.0 y el destino 255.255.255.255, esto se debe a que los dispositivos están solicitando una dirección IP y envía la solicitud al servidor DHCP.



No.	Time	Source	Destination	Protocol	Length	Info
1382	155.013424	fe80::cdf:61d1:560:c...	ff02::2	ICMPv6	80	Router Solicitation
1433	155.951394	fe80::cdf:61d1:560:c...	ff02::16	ICMPv6	130	Multicast Listener Report Message v
1435	155.954163	fe80::cdf:61d1:560:c...	ff02::16	ICMPv6	128	Multicast Listener Report Message v
1506	156.889042	fe80::cdf:61d1:560:c...	ff02::16	ICMPv6	130	Multicast Listener Report Message v
1508	156.892367	fe80::cdf:61d1:560:c...	ff02::16	ICMPv6	128	Multicast Listener Report Message v
1559	157.912051	::	ff02::1:ff60:c6f8	ICMPv6	106	Neighbor Solicitation for fe80::cdf

Protocolo ICMPv6

Destination Address: ff02::2 o ff02::16, este tráfico indica que se están descubriendo vecinos, estas direcciones de destino son direcciones multicast utilizadas para la comunicación en la red local



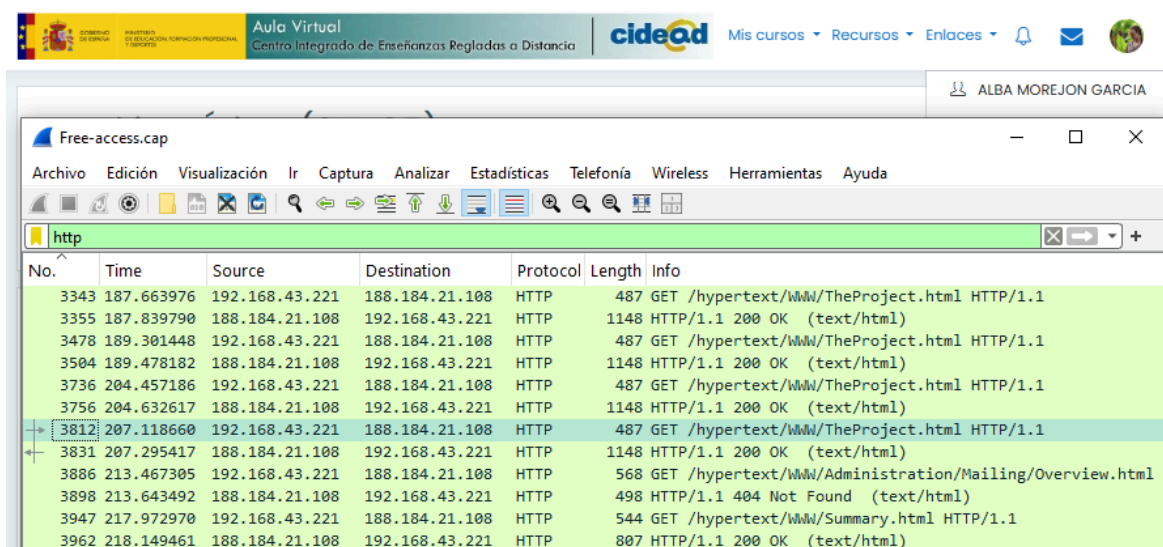
No.	Time	Source	Destination	Protocol	Length	Info
1878	167.985353	192.168.43.221	192.168.43.1	DNS	89	Standard query 0x62f1 A apple.com
1880	167.985449	192.168.43.221	192.168.43.1	DNS	94	Standard query 0xf145 A imap.gmail.
1882	167.985719	192.168.43.221	192.168.43.1	DNS	98	Standard query 0xb129 A gateway.icl
1909	168.407470	192.168.43.1	192.168.43.221	DNS	223	Standard query response 0xc404 A ww
1913	168.407647	192.168.43.1	192.168.43.221	DNS	398	Standard query response 0xb129 A ga
1914	168.407675	192.168.43.1	192.168.43.221	DNS	105	Standard query response 0x62f1 A ap
1915	168.407701	192.168.43.1	192.168.43.221	DNS	292	Standard query response 0x139b A 43

Protocolo DNS

Comunicación entre 192.168.43.221 y 192.168.43.1, una de ellas será el servidor DNS local estarán resolviendo nombres de dominio a través de él y la otra dirección estará haciéndole consultas.

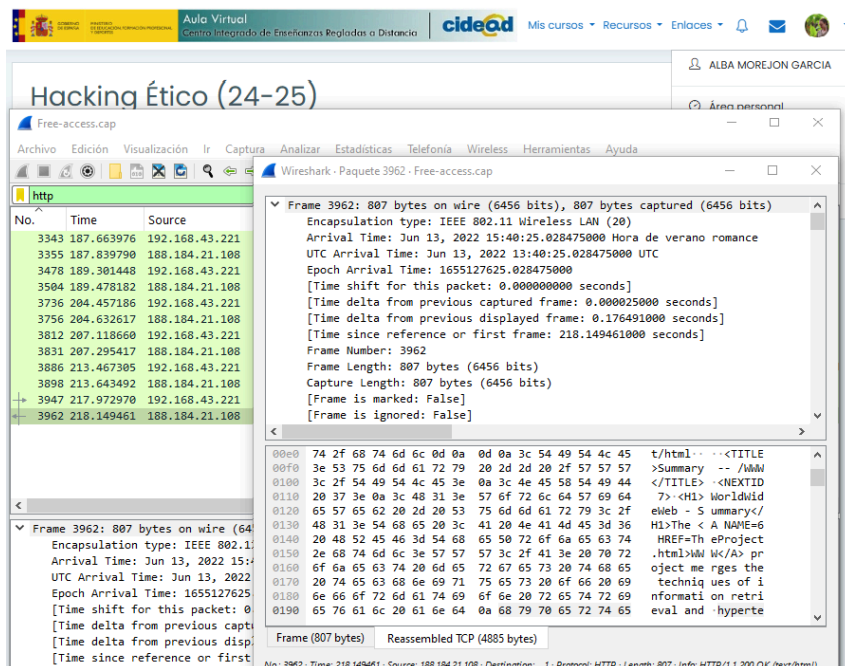
El análisis básico de la red muestra una variedad de dispositivos móviles y otros equipos conectados e intercambiando información. Se observa comunicación entre dispositivos internos y servidores externos, destacando la dirección ip 192.168.43.221 como nodo central de la red. La asignación de ips se hace mediante DHCP y la resolución de nombres a través de un servidor DNS.

La comunicación que se establece en el protocolo HTTP



No.	Time	Source	Destination	Protocol	Length	Info
3343	187.663976	192.168.43.221	188.184.21.108	HTTP	487	GET /hypertext/www/TheProject.html HTTP/1.1
3355	187.839790	188.184.21.108	192.168.43.221	HTTP	1148	HTTP/1.1 200 OK (text/html)
3478	189.301448	192.168.43.221	188.184.21.108	HTTP	487	GET /hypertext/www/TheProject.html HTTP/1.1
3504	189.478182	188.184.21.108	192.168.43.221	HTTP	1148	HTTP/1.1 200 OK (text/html)
3736	204.457186	192.168.43.221	188.184.21.108	HTTP	487	GET /hypertext/www/TheProject.html HTTP/1.1
3756	204.632617	188.184.21.108	192.168.43.221	HTTP	1148	HTTP/1.1 200 OK (text/html)
3812	207.118660	192.168.43.221	188.184.21.108	HTTP	487	GET /hypertext/www/TheProject.html HTTP/1.1
3831	207.295417	188.184.21.108	192.168.43.221	HTTP	1148	HTTP/1.1 200 OK (text/html)
3886	213.467305	192.168.43.221	188.184.21.108	HTTP	568	GET /hypertext/www/Administration/Mailing/Overview.html
3898	213.643492	188.184.21.108	192.168.43.221	HTTP	498	HTTP/1.1 404 Not Found (text/html)
3947	217.972970	192.168.43.221	188.184.21.108	HTTP	544	GET /hypertext/www/Summary.html HTTP/1.1
3962	218.149461	188.184.21.108	192.168.43.221	HTTP	807	HTTP/1.1 200 OK (text/html)

La comunicación se establece entre un dispositivo dentro de la red local, 192.168.43.221 y un servidor externo en internet, 188.184.21.108. El cliente está enviando solicitudes GET y el servidor esta respondiendo exitosamente.



Por lo que hemos analizado el contenido de los paquetes hemos visto que se hacen peticiones desde un móvil Iphone utilizando el navegador safari hacia el servidor info.cern.ch solicitando el recurso /hypertext/WWW/TheProject.html, esta solicitud es exitosa y el servidor apache proporciona la página (en código html).

Luego se hace una solicitud desde el mismo móvil hacia el mismo servidor solicitando el recurso /hypertext/WWW/Administration/Mailing/Overview.htm y en respuesta no se encontró ese servidor, dando el error 404. Por último se vuelve a hacer una petición para acceder al recurso /hypertext/WWW/Summary.html, el servidor Apache de forma exitosa proporciona la página con el contenido html.

Apartado 4: Debilidades en las redes inalámbricas.

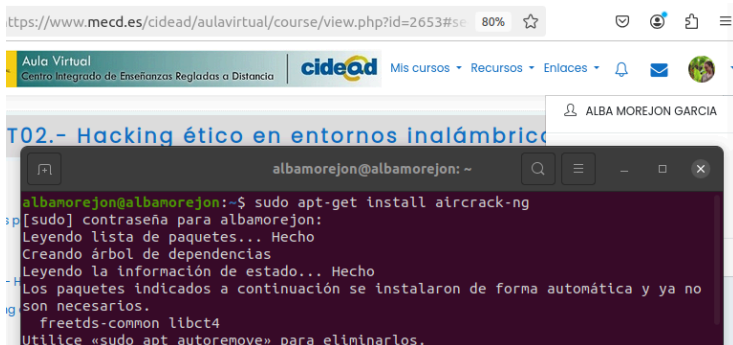
En este apartado se entregan varios ficheros de captura para que podáis realizar sobre ellos las técnicas de cracking descritas durante el módulo. Para no extendernos mucho en la realización de la tarea se ha configurado un diccionario que podéis utilizar para la resolución de la tarea. Cabe destacar 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.

Utilizamos una máquina UbuntuDsktop20 para continuar con la practica

Instalamos la herramienta aircrack con el comando “sudo apt-get install aircrack-ng”



- A continuación se presenta un paquete de captura de red que contiene la captura de un 4-way-handshake 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.

Con el comando “airdump-ng -r /home/albamorejon/Descargas/wpa2-psk.pcap” obtenemos información sobre las redes capturadas

```

CH 0 ][ Elapsed: 18 s ][ 2025-01-08 03:52 ][ Finished reading input file /home/albamorejon/Descargas/wpa2-psk.

BSSID          PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
00:0C:41:82:B2:55 41      398        284    0   1   54   WPA    CCMP   PSK   Coherer
65:78:F7:B7:60:A9 -1         0           0    0  -1  -1      WPA    CCMP   PSK   <length: 0>
FF:FF:FF:FF:FF:3F -1         0           1    0   1  -1      OPN     PSK     <length: 0>

BSSID          STATION            PWR   Rate    Lost    Frames  Notes  Probes
00:0C:41:82:B2:55 00:0D:1D:06:E0:F2 58     0 - 54     0         1
00:0C:41:82:B2:55 00:0D:93:82:36:3A 57    48 - 1     0        218  PMKID  Coherer
65:78:F7:B7:60:A9 11:5A:08:13:2C:86 42     0 - 2     0         4
(not associated) 80:86:49:41:41:3A 54     0 - 1     0         1
(not associated) 00:0F:66:16:94:73 10     0 - 1     0         5      linksys
FF:FF:FF:FF:FF:3F 40:C4:E8:00:41:C1 57     0 - 2     0         1
FF:FF:FF:FF:FF:3F 40:04:94:70:85:FD 42     0 - 2     0         1
FF:FF:FF:FF:FF:3F 40:64:A2:70:85:FD 42     0 - 2     0         1

```

Utilizando aircrack-ng con un diccionario encontramos que la clave para la BSSID 00:0C:41:82:B2:55 es “Induction”

aircrack-ng -w /home/albamorejon/Escritorio/diccionario -b [BSSID]
/home/albamorejon/Descargas/wpa2-psk.pcap

```

Aircrack-ng 1.6

[00:00:00] 1398/2302 keys tested (6274.17 k/s)

Time left: 0 seconds                                60.73%

KEY FOUND! [ Induction ]

Master Key      : 47 5F 3D A4 8F 88 0B D5 F3 85 84 0D 4B 68 94 D9
                  D7 05 C4 9B 1F 4D 35 85 0C A9 4A 45 EE 92 A5 A0

Transient Key   : 39 FF 1A 19 E1 43 18 CE BF D1 3C 84 63 10 12 4F
                  39 E2 E7 A4 C4 35 1F DB A1 FF 1F 45 E3 9F ED 79
                  BC 9D 71 AD E7 CB 87 85 DB 46 A2 95 49 CF 9E 3C
                  E7 4C 6E 38 1B FC 2C 1E B3 84 43 59 C7 8B EC D5

EAPOL HMAC     : 49 AF 57 C5 74 3D BC DA 1A 4A 1C 45 B7 72 AF BE

```

- A continuación se presenta un paquete de captura de red que contiene la captura de un **PMKID** 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.

Desciframos la contraseña utilizando el comando “aircrack-ng -w diccionario pmkid.pcap” situándonos en la ruta donde se encuentra el fichero de la captura de red y el diccionario.

Elegimos la red que deseamos atacar, la número 6 llamada “ogogo” y la clave es “15211521”

```

root@kali: /home/kali/Documents
# aircrack-ng -w diccionario pmkid.pcap
Reading packets, please wait ...
Opening pmkid.pcap
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Resetting EAPOL Handshake decoder state.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Resetting EAPOL Handshake decoder state.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 192 packets.

# BSSID      ESSID      Encryption
1 00:0D:58:EF:88:09 tmpAP      Unknown
2 00:0D:58:EF:88:0A Vodafone   Unknown
3 00:0D:58:EF:88:0B veles3     Unknown
4 14:CC:20:C1:CB:2C Lekonora   Unknown
5 24:A4:3C:FE:22:36 Intertelecom_FREE Unknown
6 28:10:7B:94:BB:29 ogogo      WPA (0 handshake, with PMK
ID)
7 F4:EC:38:A6:2F:EA TPLIN      WPA (0 handshake)
8 F8:1A:67:E5:05:62 Smile)     WPA (1 handshake)

Index number of target network ? 6
  
```

```

Aircrack-ng 1.7

[00:00:00] 2302/2302 keys tested (5364.25 k/s)

Time left: --

KEY FOUND! [ 15211521 ]

Master Key      : 6D 0B 22 77 1F 24 4A 2A D7 23 50 3D A5 00 26 E1
                  AC 23 1A 5A 90 CD 9E F8 56 7F D9 58 BA 0A CB 94

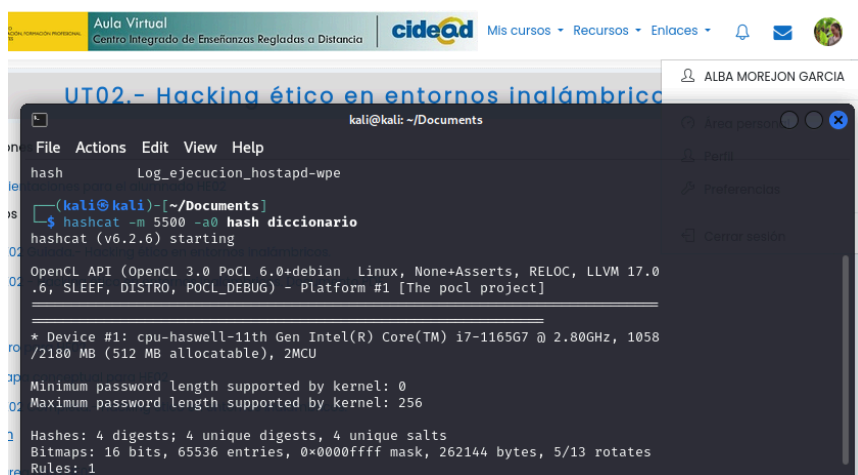
Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  
```

- A continuación se presentan los ficheros de log resultantes de la captura de autenticación WPA2-Enterprise [Log ejecución hostapd-wpe](#) - [Log autenticación capturada](#) 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.

Debido a problemas encontrados en los ficheros, hemos creado un documento conteniendo los usuarios y sus contraseñas cifradas en un documento llamado hash.txt

Utilizando el comando “hashcat -m 5500 -a0 hash diccionario” hemos podido descifrar que la contraseña es: “test1234”.



```

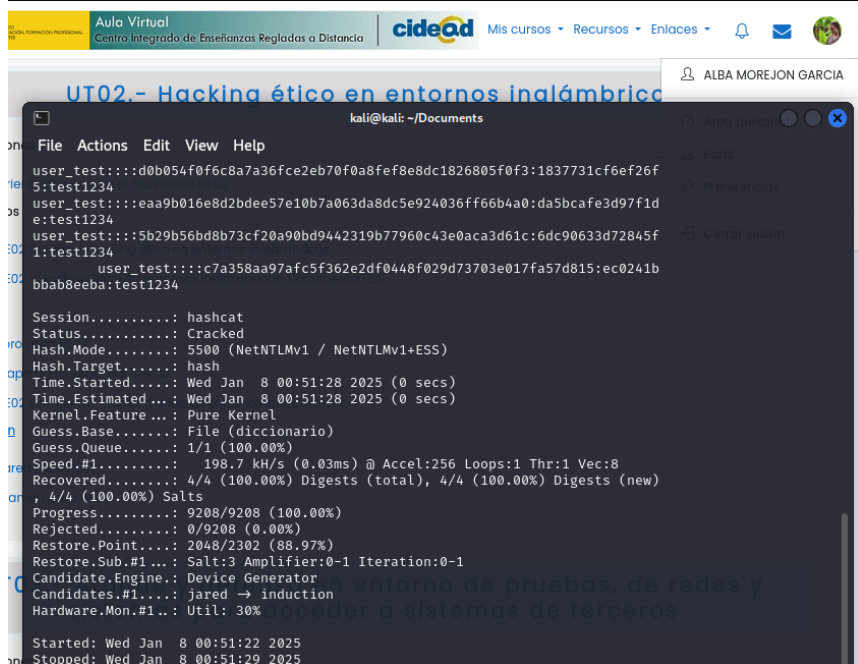
kali@kali: ~/Documents
File Actions Edit View Help
hash Log_ejecucion_hostapd-wpe
(kali@kali) - [~/Documents]
$ hashcat -m 5500 -a0 hash diccionario
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0
.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-haswell-11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz, 1058
/2180 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 4 digests, 4 unique digests, 4 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
  
```



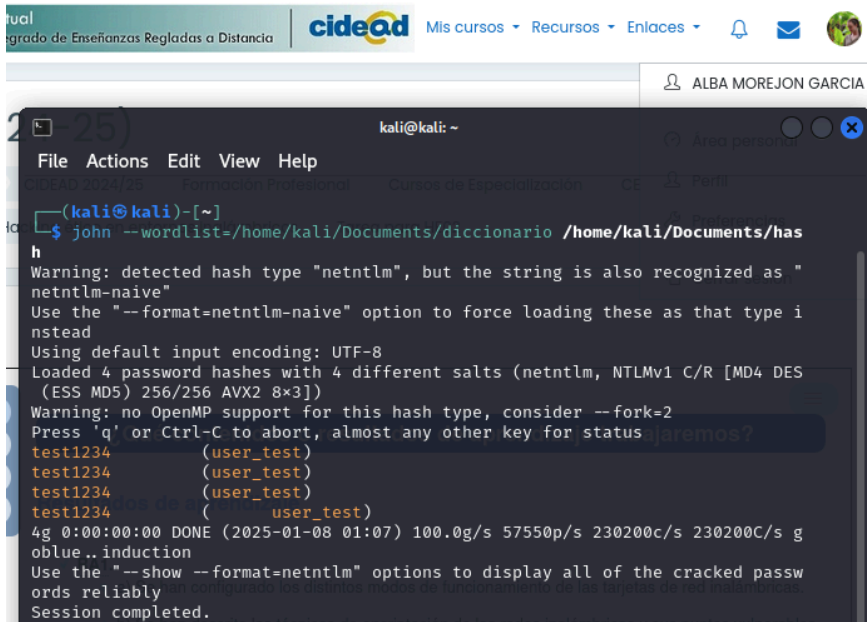
```

kali@kali: ~/Documents
File Actions Edit View Help
user_test:::d0b054f0f6c8a7a36fce2eb70f0a8fef8e8dc1826805f0f3:1837731cf6ef26f
5:test1234
user_test:::eaa9b016e8d2bdee57e10b7a063da8dc5e924036ff66b4a0:da5bcafe3d97f1d
e:test1234
user_test:::5b29b56bd8b73cf20a90bd9442319b77960c43e0aca3d61c:6dc90633d72845f
1:test1234
user_test:::c7a358aa97afc5f362e2df0448f029d73703e017fa57d815:ec0241b
bbab8eeba:test1234

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 5500 (NetNTLMv1 / NetNTLMv1+ESS)
Hash.Target.....: hash
Time.Started.....: Wed Jan  8 00:51:28 2025 (0 secs)
Time.Estimated...: Wed Jan  8 00:51:28 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (diccionario)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 198.7 kH/s (0.03ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 4/4 (100.00%) Digests (total), 4/4 (100.00%) Digests (new)
, 4/4 (100.00%) Salts
Progress.....: 9208/9208 (100.00%)
Rejected.....: 0/9208 (0.00%)
Restore.Point...: 2048/2302 (88.97%)
Restore.Sub.#1...: Salt:3 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: jared -> induction
Hardware.Mon.#1..: Util: 30%

Started: Wed Jan  8 00:51:22 2025
Stopped: Wed Jan  8 00:51:29 2025
  
```

Se ve más claro con el uso del comando “john --wordlist=/home/kali/Documents/diccionario /home/kali/Documents/hash”



```
kali@kali: ~  
File Actions Edit View Help  
CIDEAD 12/04/25 Formación Profesional Cursos de Especialización CE Perfil  
$ john --wordlist=/home/kali/Documents/diccionario /home/kali/Documents/hash  
Warning: detected hash type "netntlm", but the string is also recognized as "netntlm-naive"  
Use the "--format=netntlm-naive" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 4 password hashes with 4 different salts (netntlm, NTLMv1 C/R [MD4 DES (ESS MD5) 256/256 AVX2 8x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Press 'q' or Ctrl-C to abort, almost any other key for status  
test1234 (user_test)  
test1234 (user_test)  
test1234 (user_test)  
test1234 (user_test)  
4g 0:00:00:00 DONE (2025-01-08 01:07) 100.0g/s 57550p/s 230200c/s 230200C/s goblue..induction  
Use the "--show --format=netntlm" options to display all of the cracked passwords reliably  
Session completed.
```