INFORME ETHICAL HACKING WIRELESS

ASUNTO: Ethical Hacking a red inalámbrica corporativa.

EMPRESA: Alumnos Hacker Mentor

FECHA EMISION: 30-10-2021

1. OBJETIVO

Verificar seguridad de redes inalámbricas de la empresa Alumnos Hacker Mentor.

2. ALCANCE

Nuestra empresa ha detectado 1 SSID correspondiente a la empresa:

Ítem	SSID	BSSID a evaluar	Modelo AP	Características	Modo Seguridad
1	ALUMNO_MENTOR	18:D6:C7:BB:03:19	TPLINK	VISIBLE	WPA2 PERSONAL

3. PROCEDIMIENTOS

Las acciones realizadas en el ejercicio son las siguientes:

- Escaneo y enumeración de señales.
- Visualización de equipos conectados a la red objetivo.
- Deautenticacion de clientes para obtención de handshake.
- Ataque a través de reglas hashcat para descifrado de contraseña con ayuda de diccionario a medida.
- Análisis de buenas prácticas para robustecer red corporativa.
- Informe de resultados.

4. RESUMEN DE ETHICAL HACKING WIRELESS

Se realizan pruebas de seguridad en red inalámbrica visible ALUMNOS_MENTOR bajo AP TPLink con el siguiente resultado:

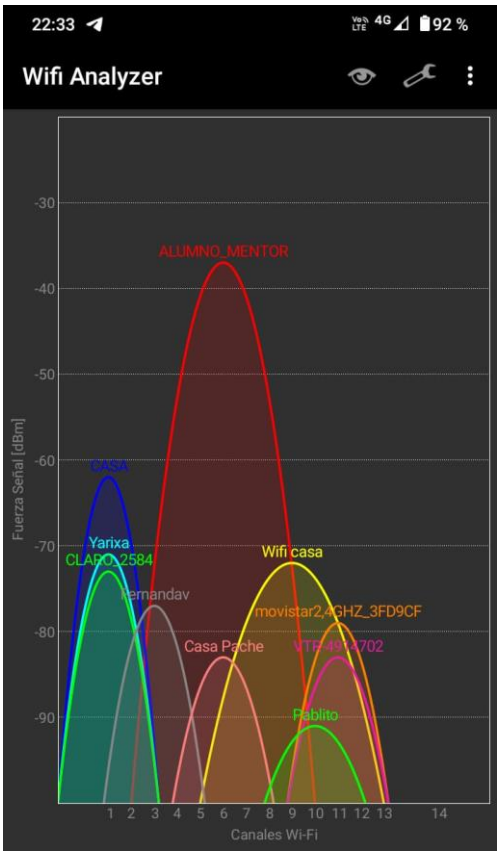
Red wifi ALUMNOS_MENTOR con vulnerabilidad identificada en base a contraseña poco robusta, obteniendo como resultado la clave de la red.

5. EVIDENCIA

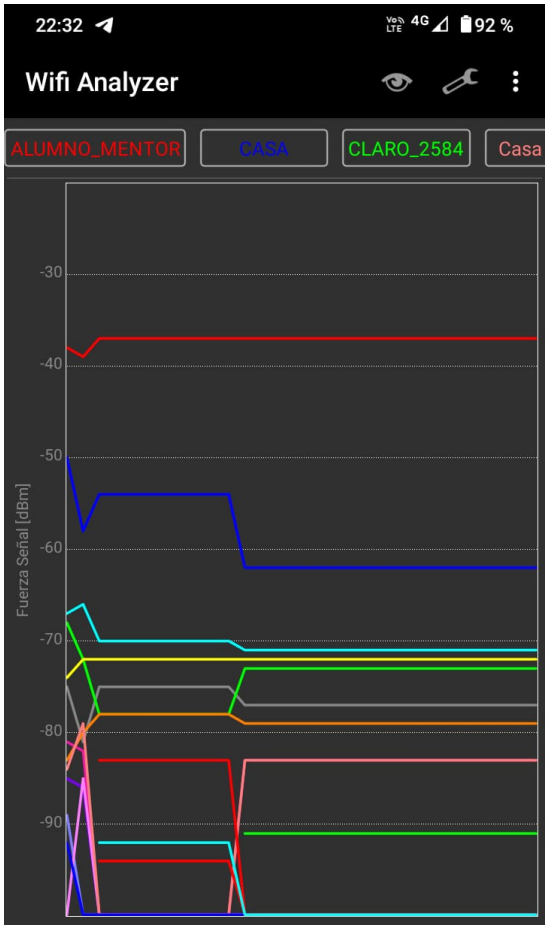
Se indica red evaluada con el siguiente detalle:

5.1 RED: ALUMNOS_MENTOR

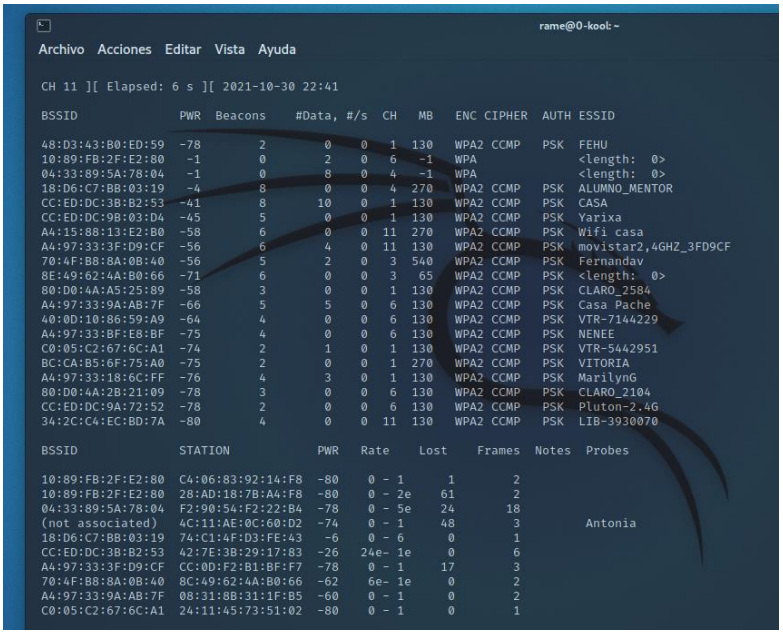
La red inalámbrica aludida, se muestra con detalle de intensidad:



Evaluación de red 2.4GHZ:

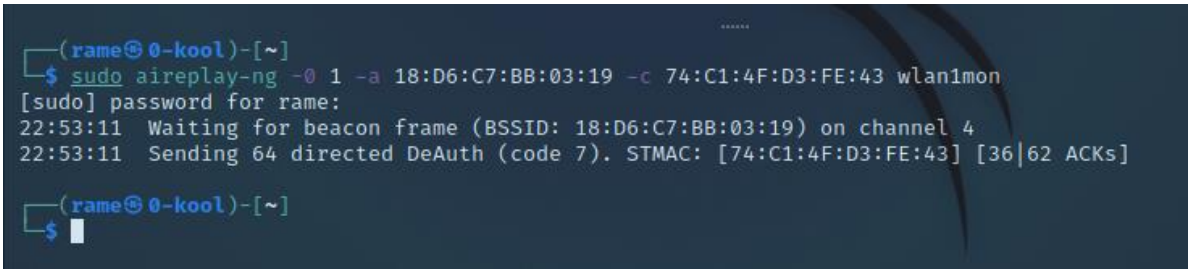


Se realiza escaneo y enumeración de redes:

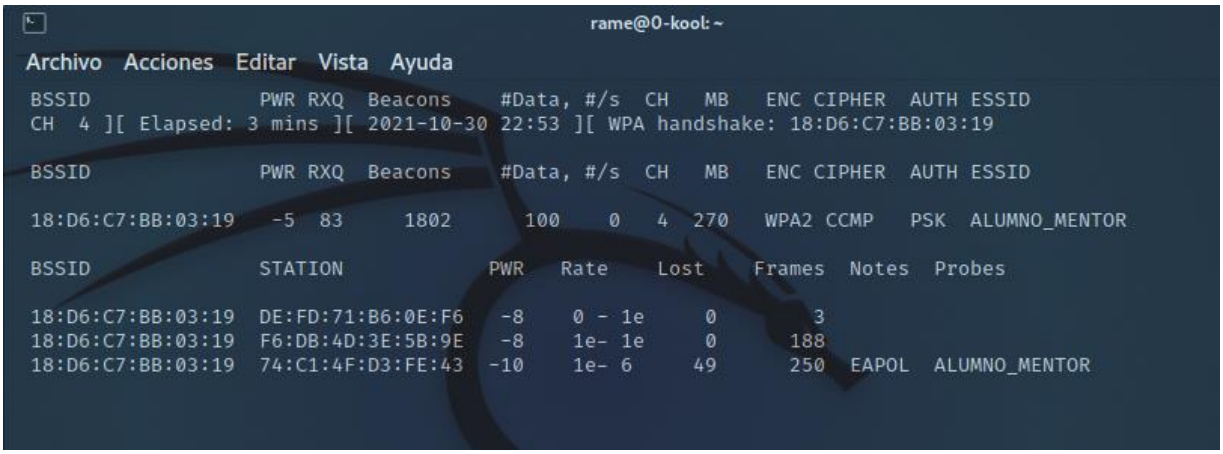


Se buscan equipos conectados a la red ALUMNOS_MENTOR:

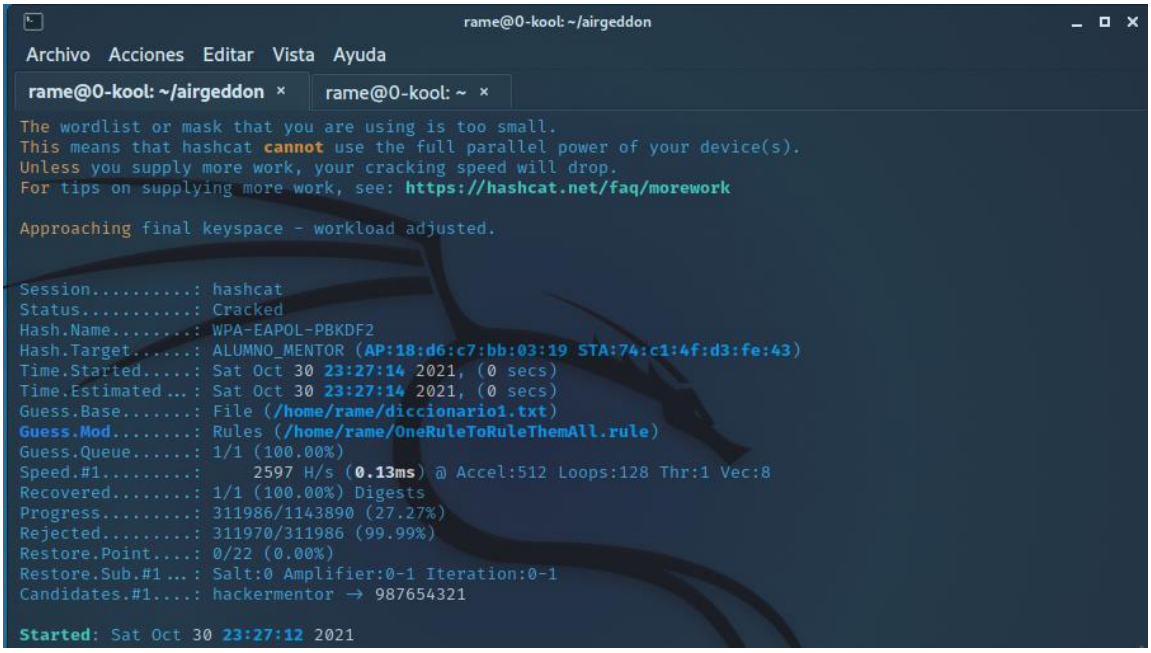
Se realiza ataque de deautenticacion:



Con esto, se recupera handshake de conexión víctima:



Se utiliza airgeddon para realizar ataque en base de reglas y diccionario creado a la medida de la red a evaluar:



Se logra descifrar contraseña y guarda evidencia de lo realizado:

RECOMENDACIONES

De acuerdo a lo informado por el sitio hivesystems una contraseña segura debería tener al menos 10 caracteres que incluyan números, mayúsculas, minúsculas y símbolos para asegurar un ataque por fuerza bruta. Aun así, se recomienda considerar contraseñas de al menos 12 caracteres, que no sean palabras y con las mismas reglas mencionadas para no ser víctimas de ataques de diccionario.

6. RECOMENDACIONES GENERALES

Es necesario plantearse como empresa cambiar la seguridad de la red de una seguridad tipo WPA2 personal, a redes WPA2 Enterprise, que incluya generación de certificado, usuario y contraseña además de configuraciones en servidor Radius que no permitan más de una conexión simultanea por usuario.

7. ARQUITECTURA RECOMENDADA