**AUDITORIA REDES INALÁMBRICAS**

|  |  |  |
| --- | --- | --- |
| **NOMBRE** | **APELLIDOS** | **DNI** |
|  |  |  |

PUESTO: GRUPO:

1. Indique cuál es el tamaño teórico de dicho diccionario compuesto por todas las posibles claves de hasta 9 caracteres. Tenga en cuenta que el tamaño mínimo de la clave en PSK es de 8 caracteres
2. Genere el diccionario usando la herramienta *crunch* mediante la siguiente orden:  
   crunch 8 9 –f /usr/share/crunch/charset.lst mixalpha-numeric

Indique el tamaño del diccionario resultado en bytes y número de palabras. Detenga la generación

1. Estime el tiempo medio necesario para determinar la clave teniendo en cuenta el tamaño del diccionario y la velocidad de verificación (que podemos obtener ejecutando *pyrit benchmark*)
2. Genere este nuevo diccionario usando la herramienta ***crunch***. Ten en cuenta que la forma de indicar a ***crunch*** que en una determinada posición hay un número es mediante el carácter ***%***. Escriba la orden utilizada e indique el tamaño del diccionario resultando en bytes y número de palabras.
3. Realice el ataque para obtener la clave. Indique las órdenes que ha usado para preparar pyrit y obtener la clave.
4. ¿Cuál es la clave obtenida?. Indique el tiempo (aproximado) que ha tardado en obtener la captura. ¿Se corresponde con su estimación?
5. Para continuar con la herramienta Crunch, genere los siguientes diccionarios e indique las órdenes que usado para cada uno de ellos:
   1. Diccionario de palabras de 9 caracteres con la primera letra en mayúsculas, resto en minúsculas y que el 9º carácter sea un símbolo.
   2. Diccionario de teléfonos móviles (9 números) que empiecen por 60912(patrón 60912NNNN).
   3. Diccionario de palabras de 8 letras, que contengan **admin** en el medio (patrón XXadminX)

I.

II.

III.

IV.

1. Si observamos los parámetros de dichas redes, vemos que una emplea CCMP (WPA2) y otra TKIP (WPA). ¿Influye el uso de CCMP o TKIP en la resistencia de la red inalámbrica ante un ataque de diccionario? Justifique su respuesta.
2. A partir de la información que tenemos sobre este caso, genere el diccionario usando ***crunch***. Indique la orden utilizada, y el tamaño del diccionario en palabras y bytes.
3. Estime el tiempo medio necesario para obtener la clave para ambas redes usando ***pyrit***:
4. Anote todas las órdenes necesarias para llevar a cabo el ataque: