Tarea: Herramientas de cracking

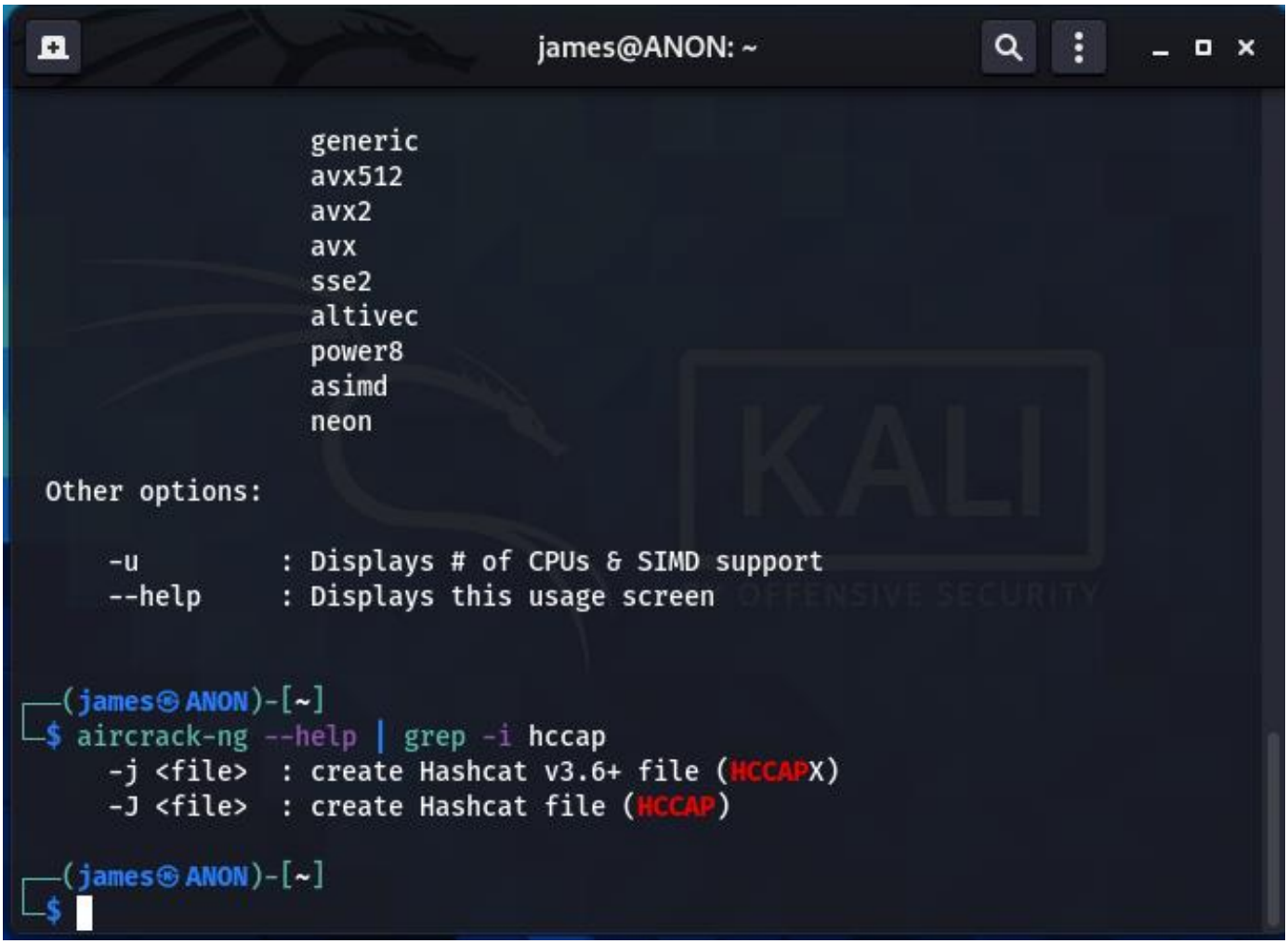
Asignatura: Criptografía

Alumno: Jaime Navarro

He elegido la herramienta Aircrack-ng, la cual está integrada en cualquier distribución de Kali Linux, el cual está basado en Debian.

Está enfocada a romper los cifrados de las contraseñas Wi-Fi, como lo son WEP, WPA y WPA2 (aunque el reciente WPA3 se rumorea que también ya ha sido comprometido, ver : https://www.adslzone.net/2019/04/10/wifi-wpa3-hack-dragonblood/). En este caso, usé un ataque de diccionario contra unos paquetes del handshake que capturé de un equipo cualquiera.

El proceso es el siguiente: primero expulso a un equipo de la red Wi-Fi de la ufv, en concreto "zona_ufv", pues no es fácil romper el cifrado de la red "eduroam" al estar basado en RADIUS. Después, con "airodump-ng" capturo los paquetes que intenta mandar infinitamente el PC en cuestión hasta que se reconecte a dicha red. Esos paquetes son el anterior mencionado handshake, de manera que cuando los tengo cierro el comando y reviso el archivo donde está escrito. Con Aircrack-ng creo un nuevo archivo ".hccapx" a partir del ".cap", con la opción "-j"



En esta captura, se puede ver la ayuda del comando, pero sólo muestro lo que coincida con la expresión “hccap”. Una vez escrito este archivo clave, se puede usar Aircrack-ng para un ataque de diccionario, fuerza bruta, rainbow table, o incluso de expresión regular. Pero en este caso, al ser una prueba, construí con “Crunch”, otra herramienta integrada en esta distribución de Linux, un diccionario, que entre las 5 posibilidades se encuentra la contraseña que es de dominio público “zonawifiufv”.

Se puede apreciar el resultado que arroja esta herramienta cuando encuentra la contraseña adecuada. En la terminal de la derecha, muestro el contenido del diccionario que utilicé a modo de prueba.

A la izquierda, el resultado de lanzar la herramienta, con su comando escrito otra vez a continuación para que se pueda apreciar cómo se usa, por entrada parametrizada especificando tanto el archivo con el handshake, el diccionario, y el archivo donde queremos que nos escriba la contraseña encontrada.