**Acceso en redes inalámbricas con cifrado WPA2 / Enterprise y ataques MITM en redes**



Daniel Escaño Hernández CET Ciberseguridad

# 

# **1. Índice:**

[**1. Índice:**](#_4jq84lualx9d) **1**

[**2. Práctica 2-2**](#_ofiic1av8ddq) **2**

[**2.1 Ataques con diccionarios del Handshake**](#_5d38uxjyswtl) **2**

[**2.2 Ataque a redes WPA Enterprise**](#_wspsorply0gj) **4**

[**2.3 Ataque a redes WPA Enterprise**](#_ped8g84d047) **8**

[**2.4 Ataque a portales cautivos**](#_njx1fpq8lvb3) **10**

[**2.5 Suplantación de ARP**](#_3dbaizqdjk3x) **12**

[**2.6 Ataque DNS spoof.**](#_gmq7spq93gyh) **14**

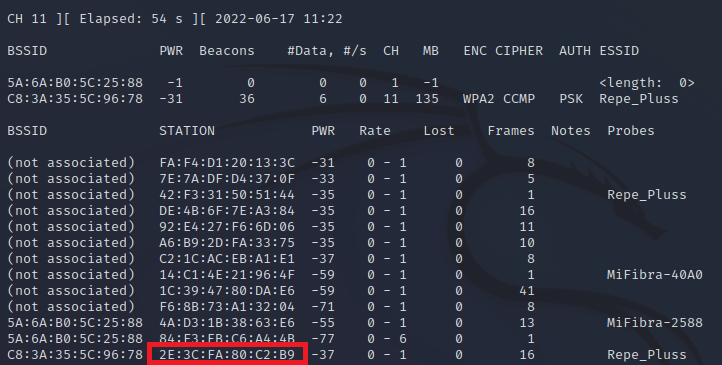
# **2. Práctica 2-2**

### **2.1 Ataques con diccionarios del Handshake**

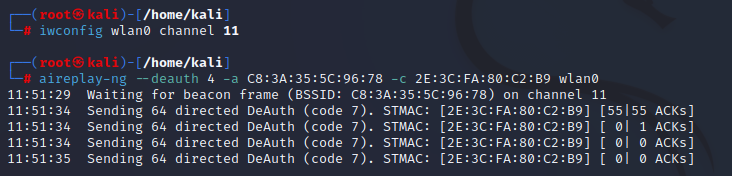
Necesitamos tener la tarjeta de red wifi en modo monitor:



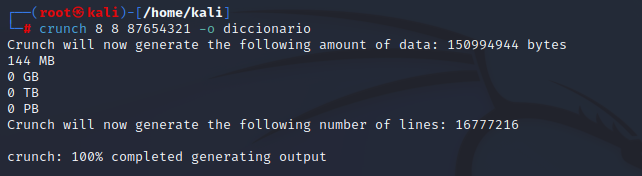
Observamos las redes disponibles y esperamos hasta que se conecte algún dispositivo

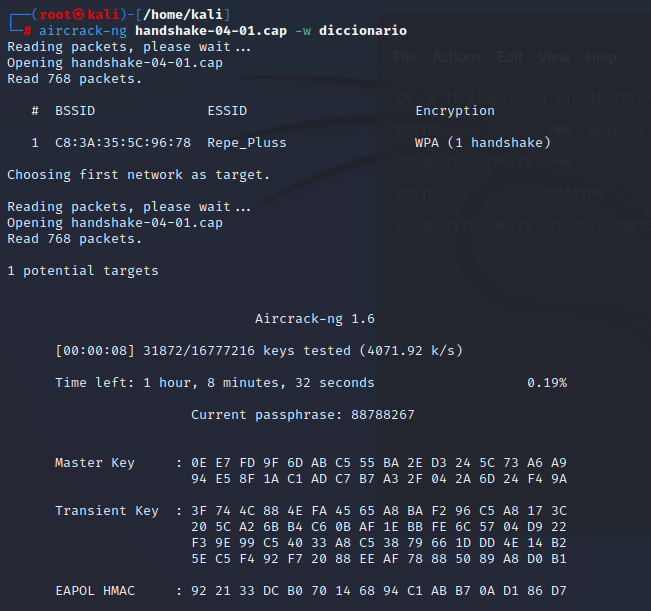


Ejecutando el siguiente comando, se desconecta el dispositivo escogido de la red wifi seleccionada



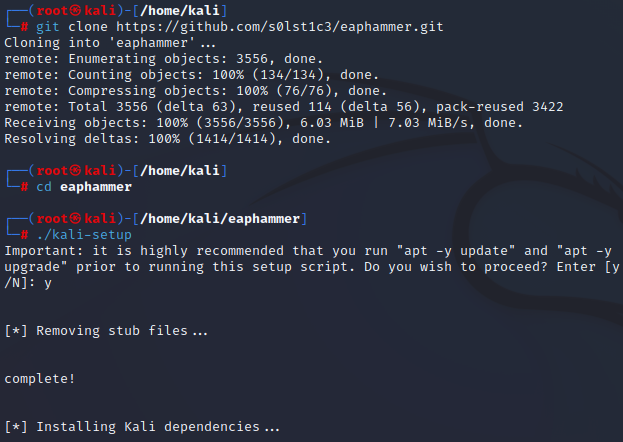
Ahora realizamos un ataque para comenzar a descifrar la contraseña:



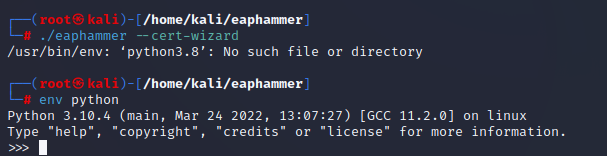


### **2.2 Ataque a redes WPA Enterprise**

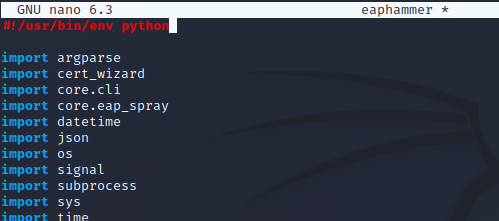
Empezamos clonando un repositorio de github y procedemos a instalarlo.



Realizamos unas comprobaciones previas referentes a python



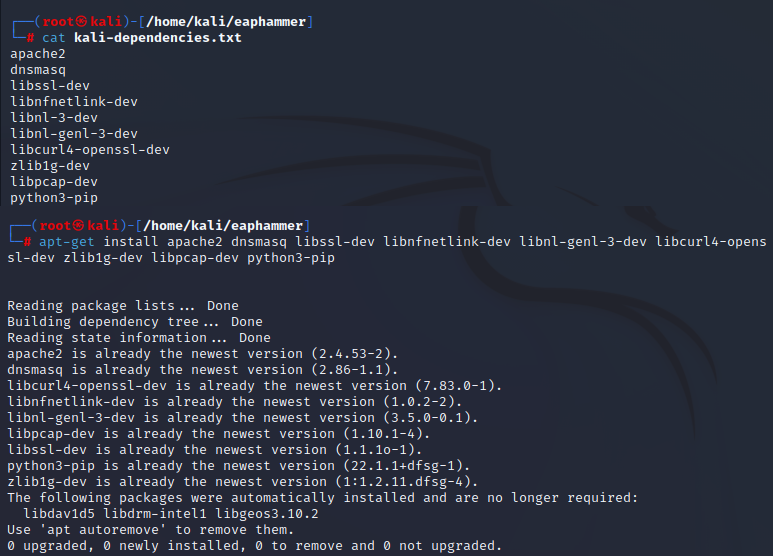
Modificamos el siguiente archivo y ejecutamos para obtener nuestro certifcado



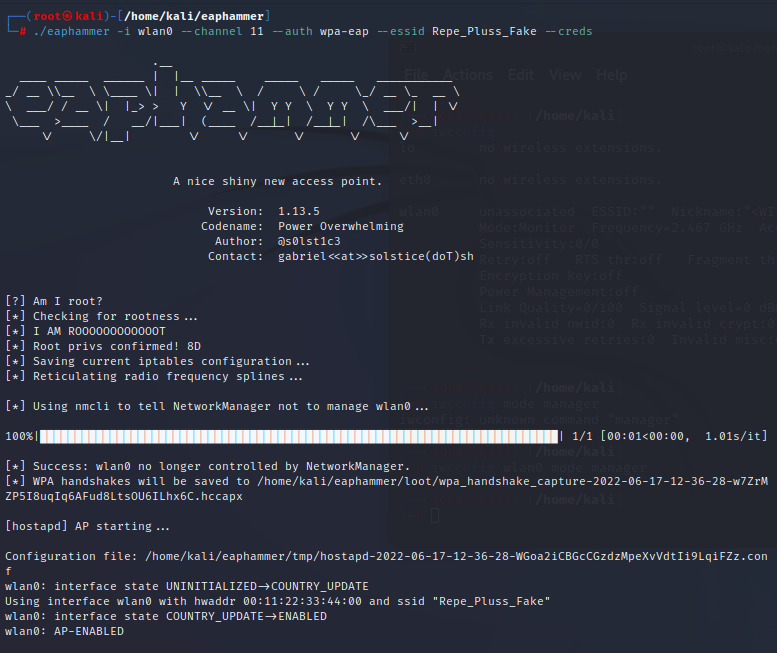




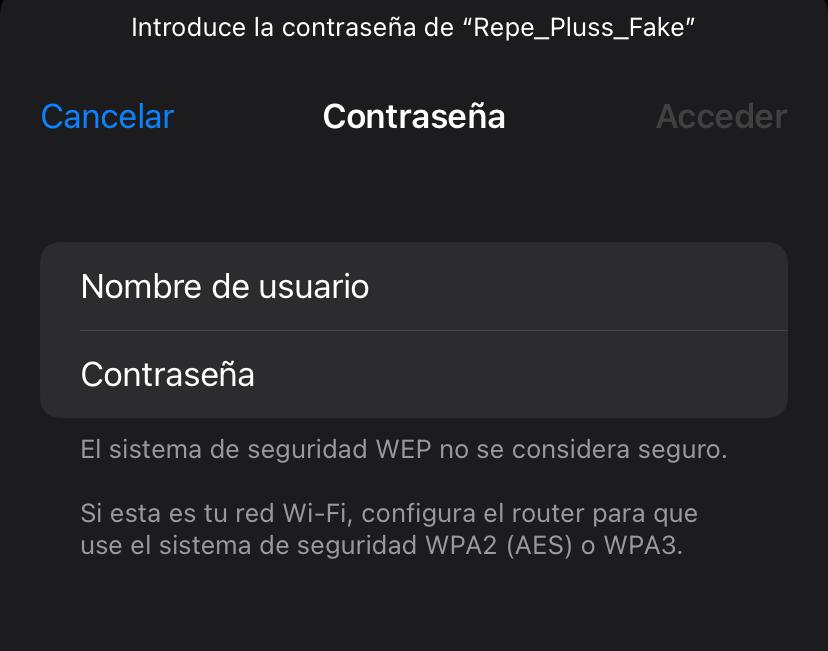
Comprobamos que tenemos todas las dependencias instaladas y actualizadas



Ejecutamos eaphammer para activar nuestro punto de acceso

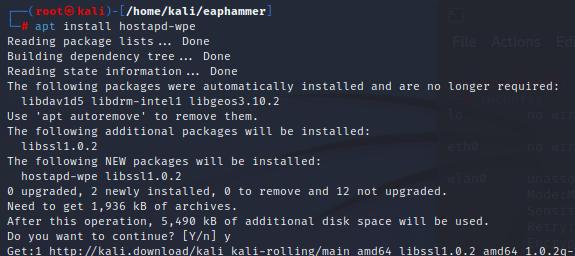


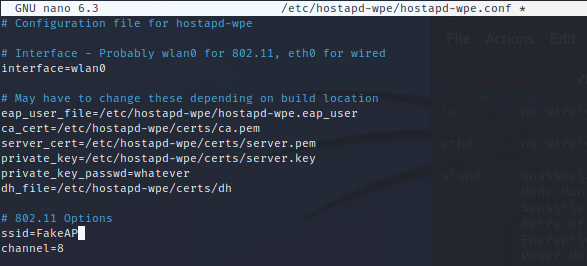
Ahora podremos visualizarlo



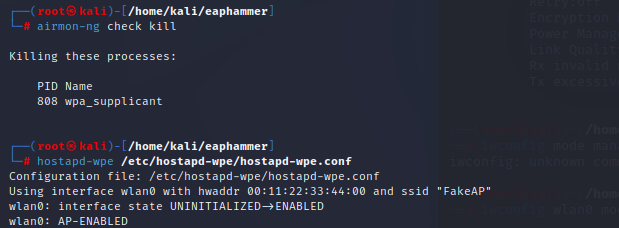
### **2.3 Ataque a redes WPA Enterprise**

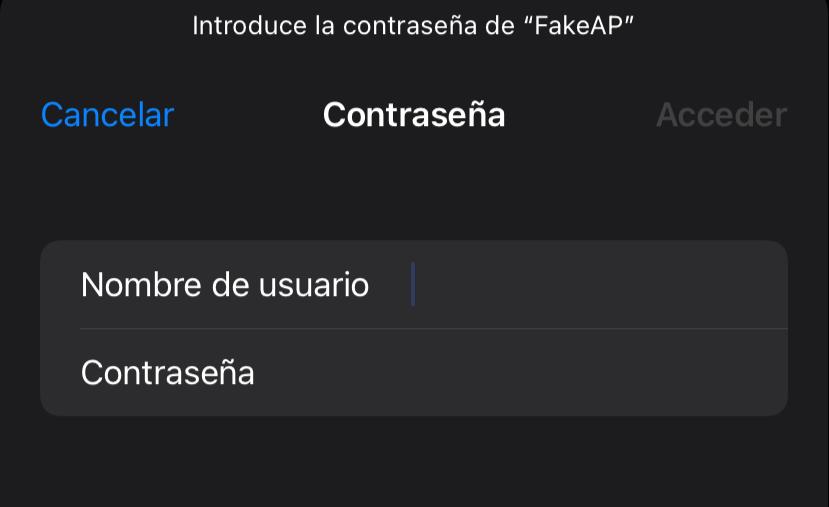
Instalamos y configuramos el fichero de hostapd que hemos instalado con los siguientes parámetros:



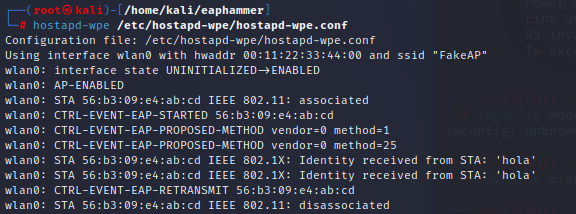


Y activamos nuestro punto de acceso

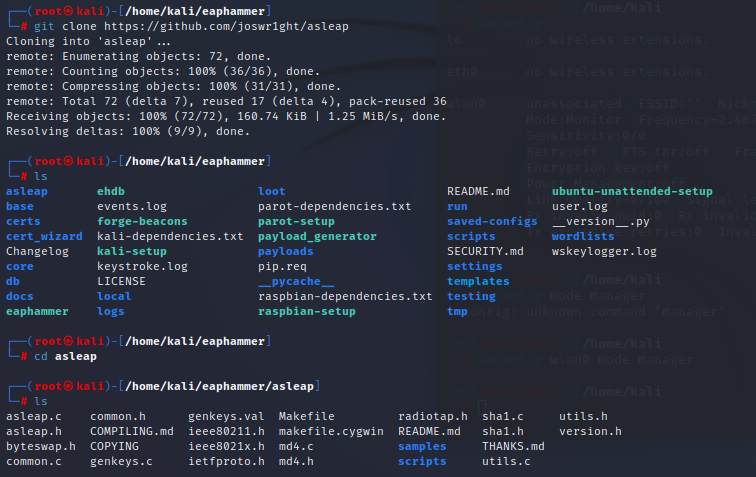


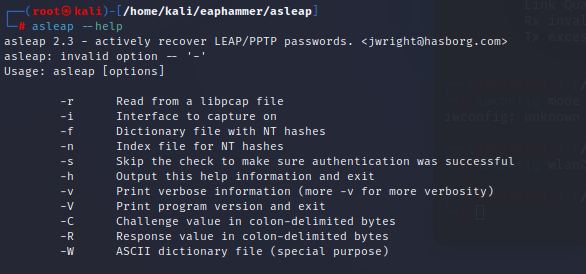


Introducimos los datos requeridos y se desconectará como si fuera un error. Kali estará recibiendo estos datos.



Lo siguiente es instalar asleap



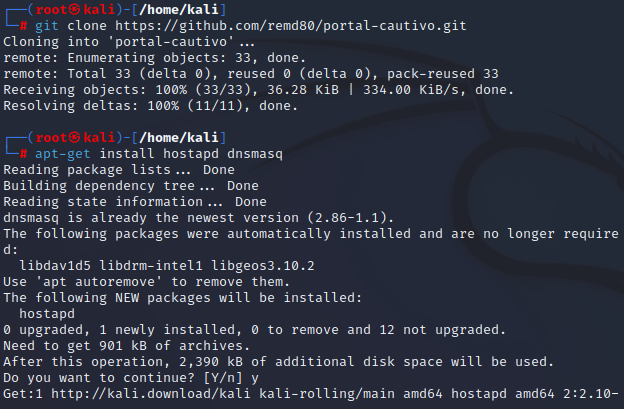


Y ejecutamos

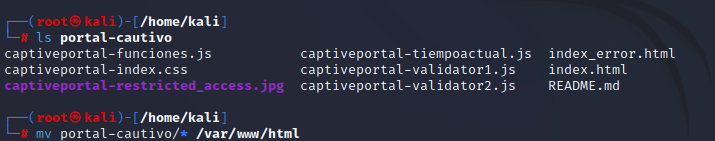


### **2.4 Ataque a portales cautivos**

Necesitamos realizar un clonado de la siguiente página de github e instalamos hostapd y dnsmasq



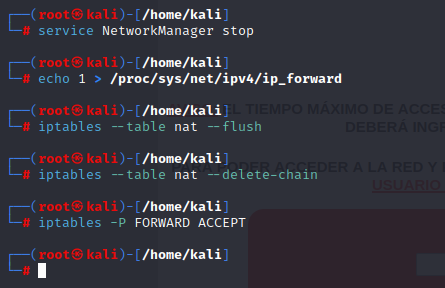
Necesitamos mover todos los archivos que contiene la carpeta a la siguiente ruta: /var/www/html



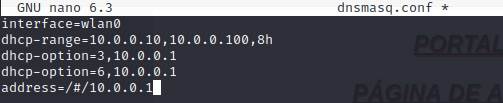
Visitamos localhost

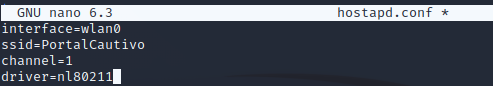


Introducimos los siguientes comandos para que Kali pueda realizar IPForwarding

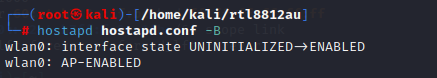


Creamos los siguientes ficheros de configuración y ejecutamos



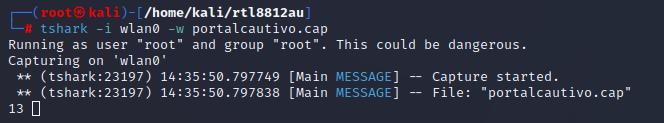


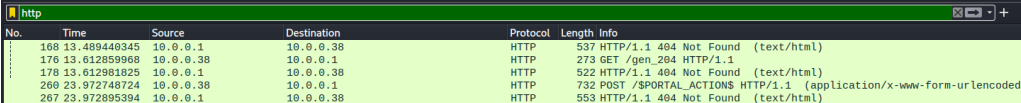
Y ejecutamos para inicializar el punto de acceso





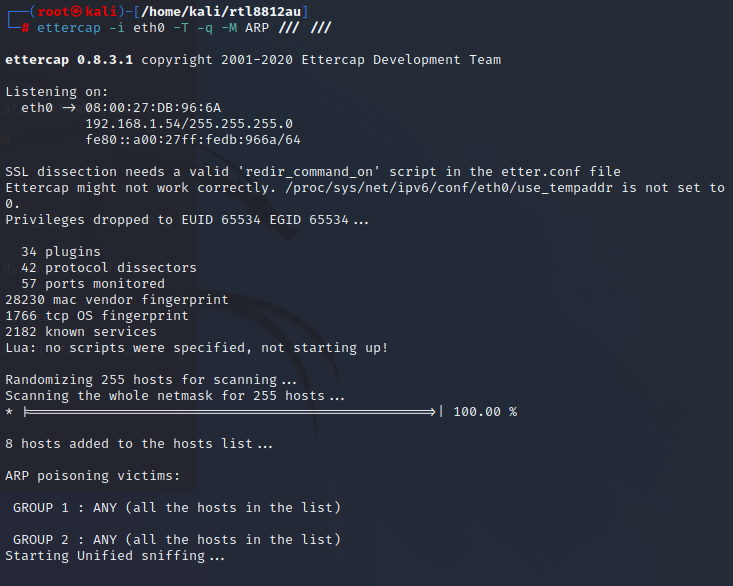
Comenzamos a registrar el tráfico, accederemos al portal y con wireshark, concluimos investigando los paquetes



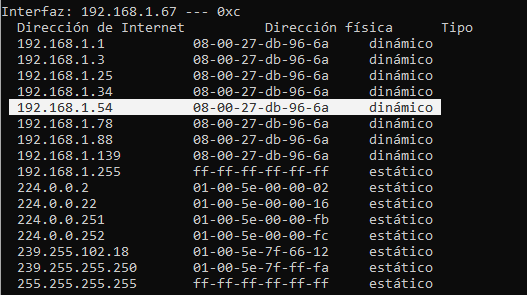


### **2.5 Suplantación de ARP**

Realizamos un ataque ARP hacia una máquina Windows 10



Necesitamos realizar una consulta arp desde la máquina Windows 10

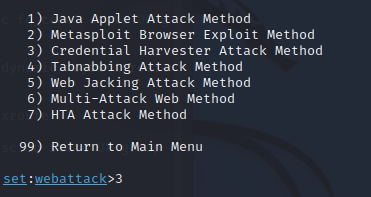


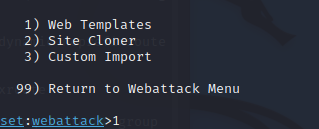
### **2.6 Ataque DNS spoof.**

Para esta sección, trabajaremos con setoolkit, la ejecutamos y navegamos por el menu

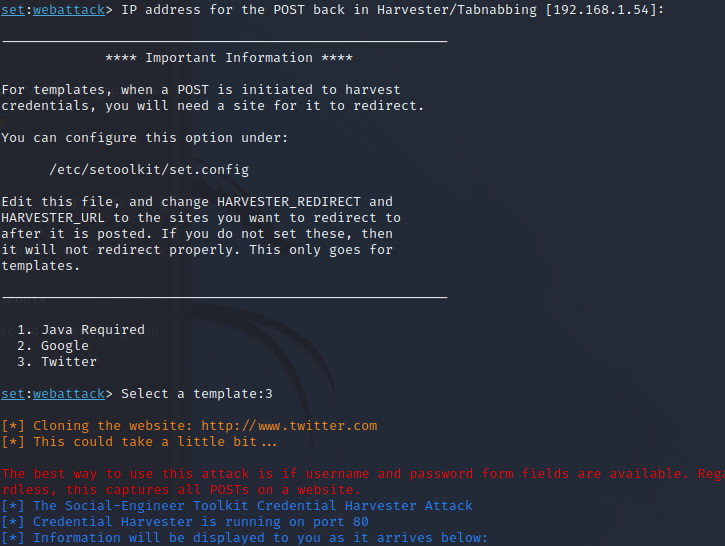


Seleccionamos las siguientes opciones

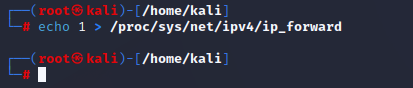




La dirección IP la dejamos por defecto y seleccionamos Twitter



Debemos tener activo el servicio de ip forwarding, lo activamos de la siguiente manera:



Y finalmente lanzamos el ataque desde otra terminal, añadiendo la ip de la maquina Windows 10 y la ip del router

### 