**EJERCICIO FINAL - ATAQUES A INFRAESTRUCTURA DE SISTEMAS Y**

**REDES**

**Definición de alcance y requisitos**

**Suponed que tenemos un cliente (vosotros) y queréis conocer el estado de vuestra red.**

**Vais a realizar vuestra primera "incursión" en entorno real, sin usar máquinas virtuales preparadas, y generaros un informe para vosotros mismos sobre lo que**

**habéis hecho.**

**Para realizar este ejercicio hay que tener en cuenta que los ataques y análisis van a realizarse en la propia red personal de cada uno, por lo que es necesario**

**antes de nada, "pedir permiso" e "informar" al resto de usuarios de la red de los objetivos, horario para poder hacerlo, si el router está accesible para reiniciarlo**

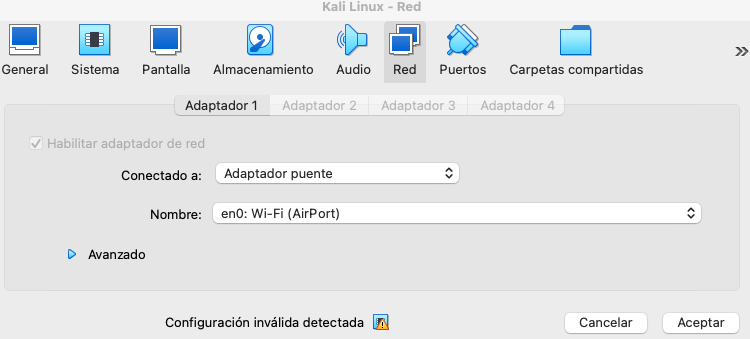
**(se puede quedar tonto en un ARP Spoofing si es de mala calidad), etc...**

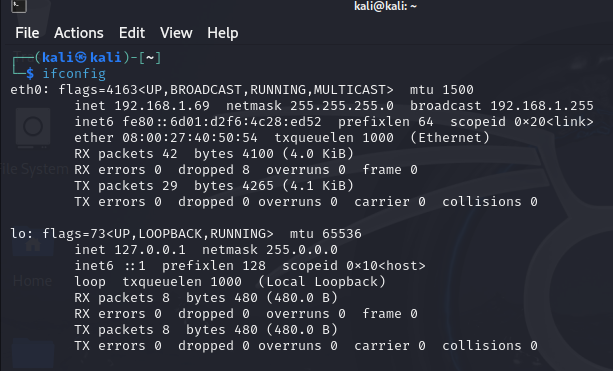
**DISCLAIMER - ¡¡¡Hacedlo con responsabilidad y cabeza!!! :-)**

**1. Configuración**

**Configurar el tipo de red de Kali Linux como Bridge. De esta manera estará configurada como si fuera un equipo de la propia red.**

**Comprobar que la IP asignada está en el rango de red del resto de equipos (móvil y máquina Host).**

****

****

**2. Selección de objetivo**

**Realizar una identificación de equipos de toda la red.**

**Identificar equipos por la MAC Address (recordad que podemos sacar basándonos en la MAC el fabricante y por lo tanto acotar que equipos son).**

**Elegir un equipo como objetivo.**

**Nota: Contad con que al menos en la red hay 4 equipos:**

**Equipo 1 ) Kali Linux en modo Bridge.**

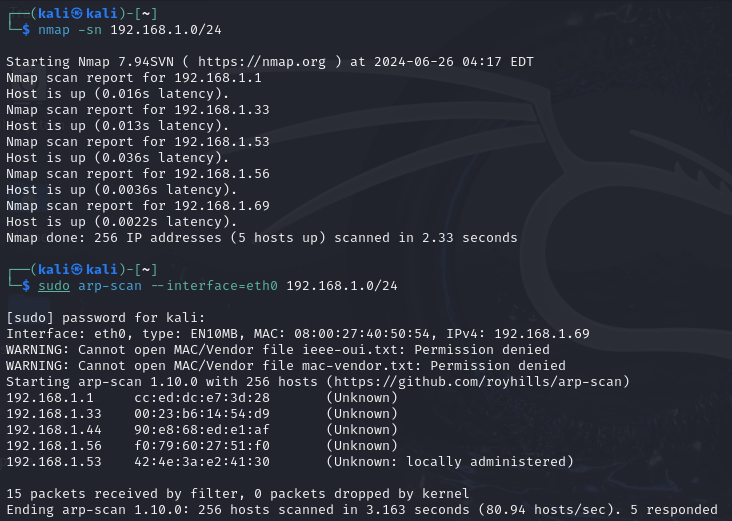
**Equipo 2 ) Vuestra máquina Host.**

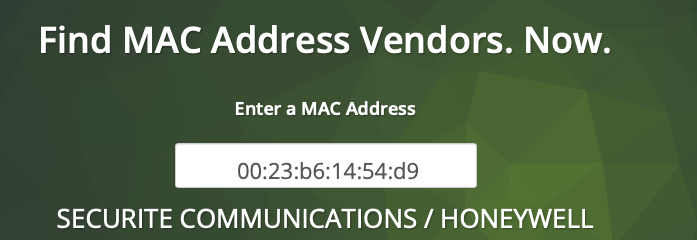
**Equipo 3 ) Un teléfono móvil en la misma red.**

**Equipo 4 ) Router.**

**El resto serán otros equipos conectados (aparte de éstos) que haya en la red.**

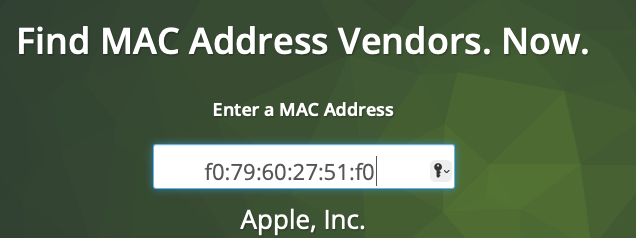
Primero escaneamos con nmap todas las IP y con sudo arp-scan --interface=eth0 192.168.1.0/24 listamos las MAC adresses. Podemos consultar en macvendors.com los tipos de dispositivo según la MAC address.

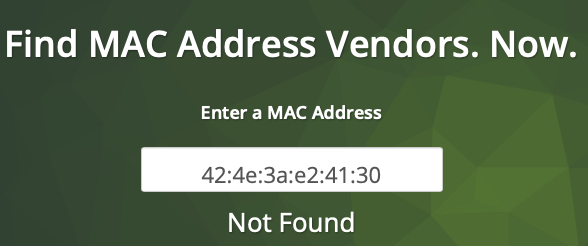
****

****

****

****

****

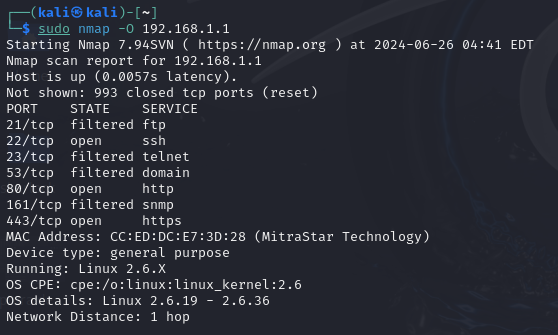
****

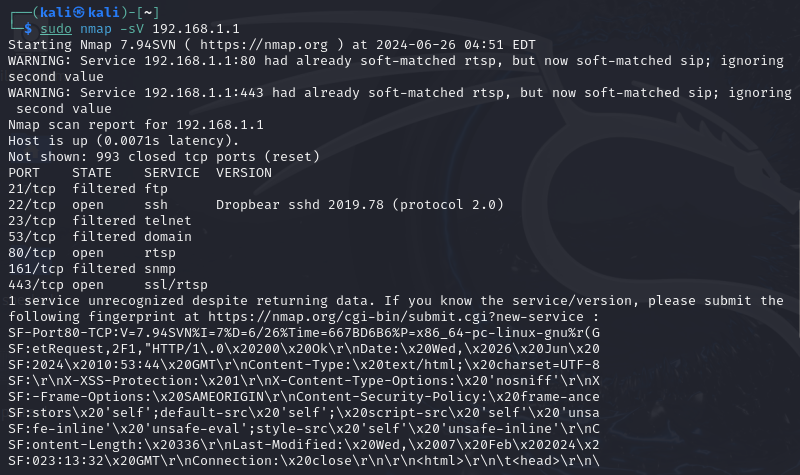
**3. Análisis de vulnerabilidades - Exploración**

**Realizar una identificación de sistema operativo de un equipo objetivo. (También es importante para validar el punto anterior y ver que equipos son).**

**Realizar una identificación de servicios y puertos abiertos del objetivo.**

**Realizar una identificación de versiones de servicios del objetivo.**

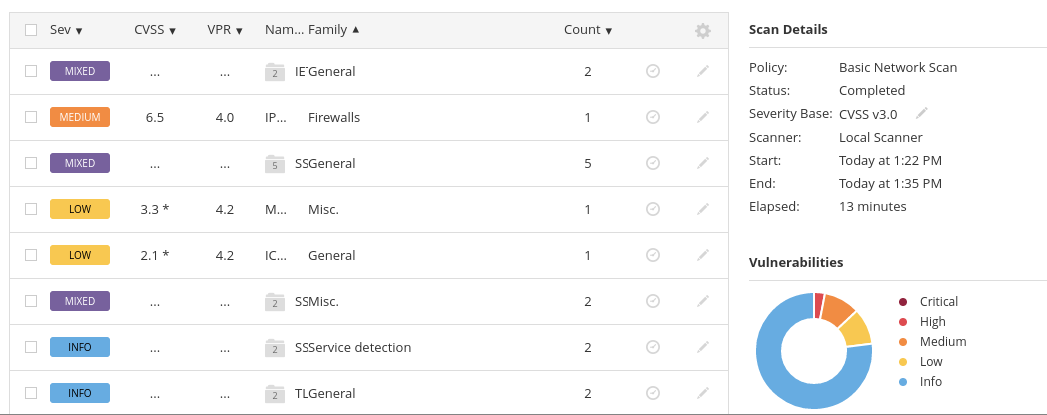




**4. Análisis de vulnerabilidades - Evaluación**

**Realizar un análisis de vulnerabilidades con las herramientas utilizadas sobre el objetivo.**

**Comprobar si hay alguna vulnerabilidad crítica (CVSS alto) sobre el objetivo.**

****

**5. Ataque MITM y captura/sniffing de tráfico**

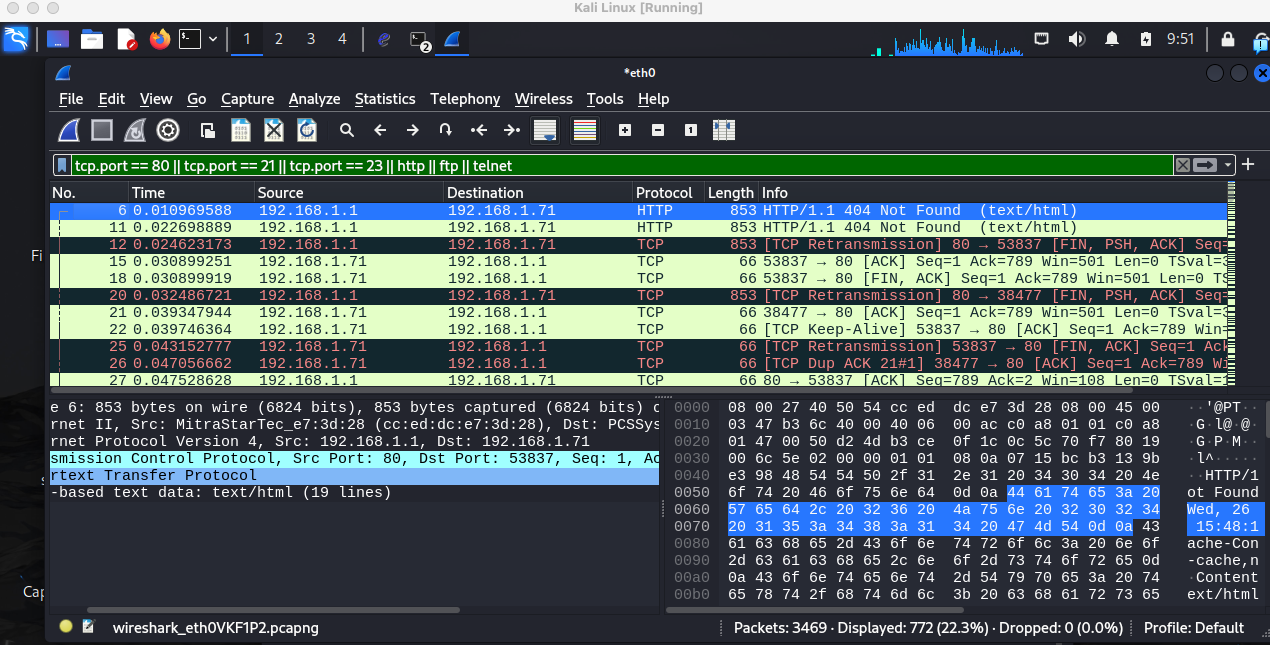
**Realizar un ataque MITM entre un equipo de la red y el router para capturar tráfico entre ellos, e intentar averiguar a qué servicios, IPs y webs se está**

**accediendo.**

**En caso que se utilice algún protocolo inseguro, es posible analizar la información más en detalle utilizando varias reglas en wireshark, de forma "que sea**

**trafico ftp O tráfico telnet o tráfico http" para poder ayudaros en el análisis.**

**Ejemplo: Usuarios y contraseñas que se transmiten en "texto plano", hay en http, ftp y telnet entre otros, como hemos visto en clase.**

****