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

GRUPO:\_\_\_\_\_\_\_\_\_\_\_\_\_

1. En nuestro caso, lo vamos a emplear para determinar víctimas potenciales. Abra un terminal y ejecute la orden nmap -F 192.168.0.0/24   
   A partir de la salida de esta orden, indique a continuación las direcciones IP de los equipos conectados en la red:
2. Una vez hayan arrancado, sitúese en el equipo “VÍCTIMA” (diríjase a la consola o ábrala directamente desde *virt-manager*). Ejecute la siguiente orden para consultar su caché arp  
   $sudo arp –na
3. Repita la operación para el equipo atacante. ¿Qué le está mostrando?
4. Copie la salida de *una de las órdenes* anteriores y explique qué hacen ambas:
5. En estos momentos, el envenenamiento estaría teniendo lugar. Vamos a **comprobar si está o no funcionando**. Para ello, consulte de nuevo la caché ARP de los equipos víctima y atacante. Si todo ha ido bien, debería observar cómo el ataque ha surtido efecto y ha cambiado el contenido de la tabla. Copie la salida de la orden sudo arp -na a continuación

**VÍCTIMA:**

**ROUTER:**

1. Justifique los valores de las tablas ARP anteriores:
2. Abra un navegador en el equipo “VÍCTIMA” e intente acceder a la URL http://www.google.es/.Explique el resultado obtenido:
3. Explique por qué es necesario habilitar el reenvío de paquetes en el equipo “ATACANTE”:
4. Indique si el ataque realizado es un ataque activo o pasivo. Explique qué se puede conseguir con este ataque:
5. Indique si desde la máquina atacante puede capturar las credenciales de acceso (usuario y contraseña) que ha introducido para acceder a ‘Aula Virtual’. Si su respuesta es afirmativa, indique en qué mensaje de la captura se encuentran dichos mensajes. Si su respuesta es negativa, justifique detalladamente su respuesta:
6. ¿Ofrece el protocolo http un servicio de confidencialidad de datos? Responda a esta cuestión a partir de los resultados obtenidos en el ejemplo anterior: