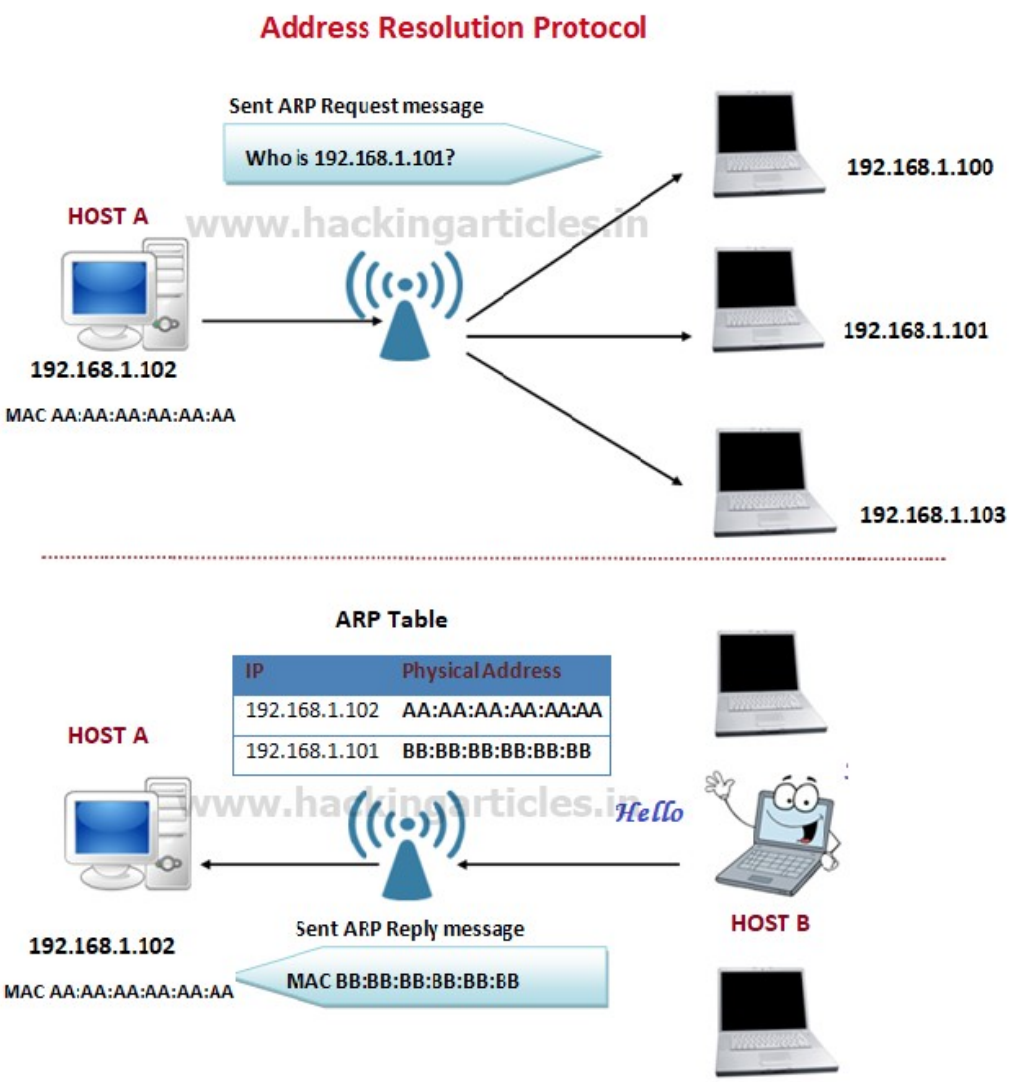
Práctica Ataque MitM

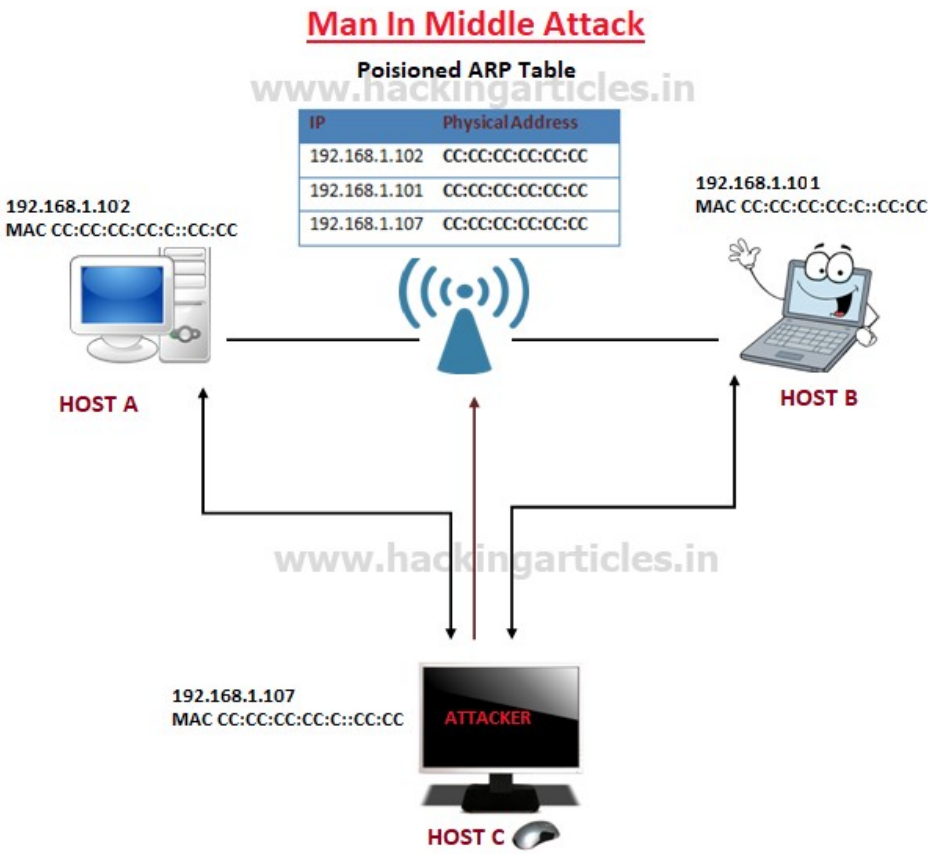
El siguiente ejercicio, consiste en realizar un ataque MitM. Para ello, el atacante previamente ha accedido a nuestra red. En este ataque explotará las vulnerabilidades del protocolo ARP, pero existen otras opciones, como el DHCP Spoofing o el Port Stealing.

Para realizar el siguiente ataque, se necesita un equipo Kali (atacante) con la herramienta Ethercap y Wireshark, un equipo Ubuntu (cliente) v→y/o un servidor web). Todos los equipos deberán estar en la misma red.

Se deberá conocer el funcionamiento del protocolo ARP, ya que se hará un envenenamiento de la tabla ARP.



El escenario, con el atacante, será el siguiente:



A continuación se realizará la demo. Tomad los apuntes necesarios.

Preguntas:

1. ¿Cómo es posible evitar este ataque?
   - Instalando un analizador de tablas arp en los equipos.
2. ¿Una vez realizado el ataque MitM, sería posible robar credenciales HTTP?
   - http si, https no
3. ¿Qué es XARP? ¿Cómo funciona?
   - Era un analizador de tablas arp, que nos avisa en caso de encontrar irregularidades