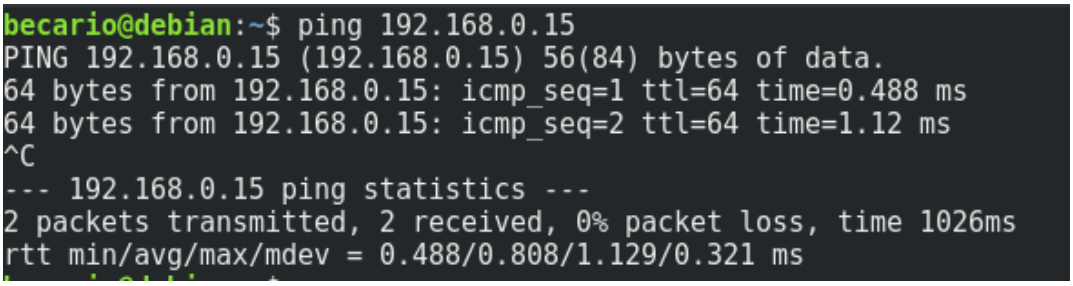
Oscar Espinosa Curiel

Práctica SEToolkit

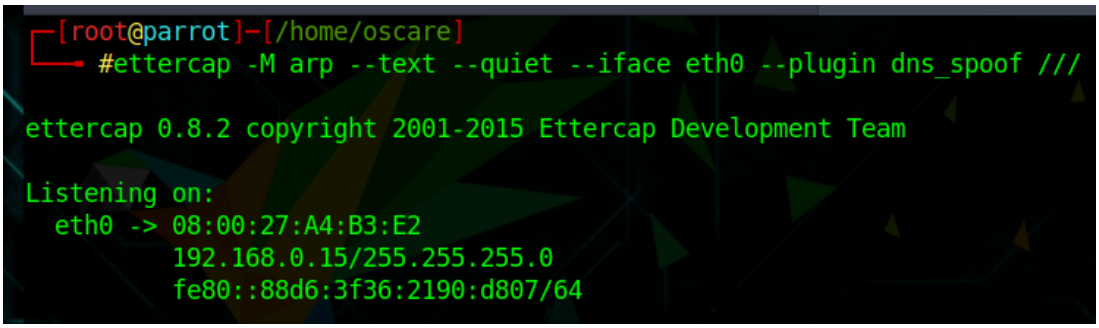
Primero probé la conexión con la máquina atacante desde la víctima:



Posteriormente inicié la herramienta SEtoolkit tal como viene expliacada, definiendo la IP del atacante para el destino de los métodos POST del HTML, como aplicación víctima se usó facebook.com.

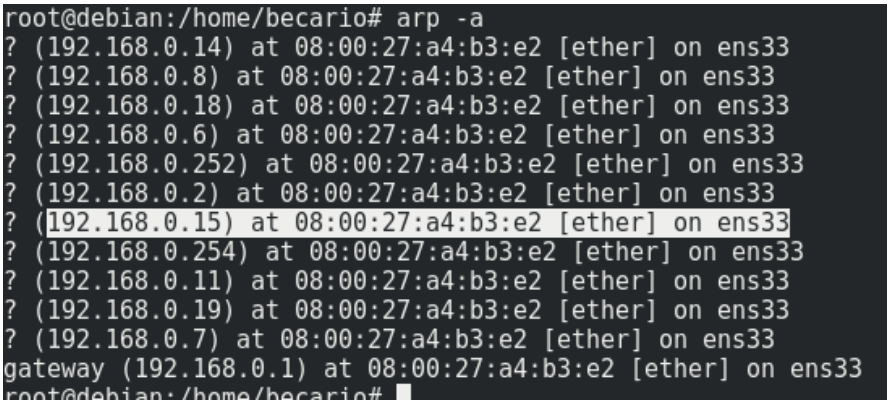
Para poder hacer spoofing en la tabla ARP, se necesita modificar un archivo para el servicio de DNS, en el que agregué la última línea siguiente

Para realizar el ataque ARP poisoning y DNS spoofing, usé la herramienta ettercap, tal como se ve en la imagen

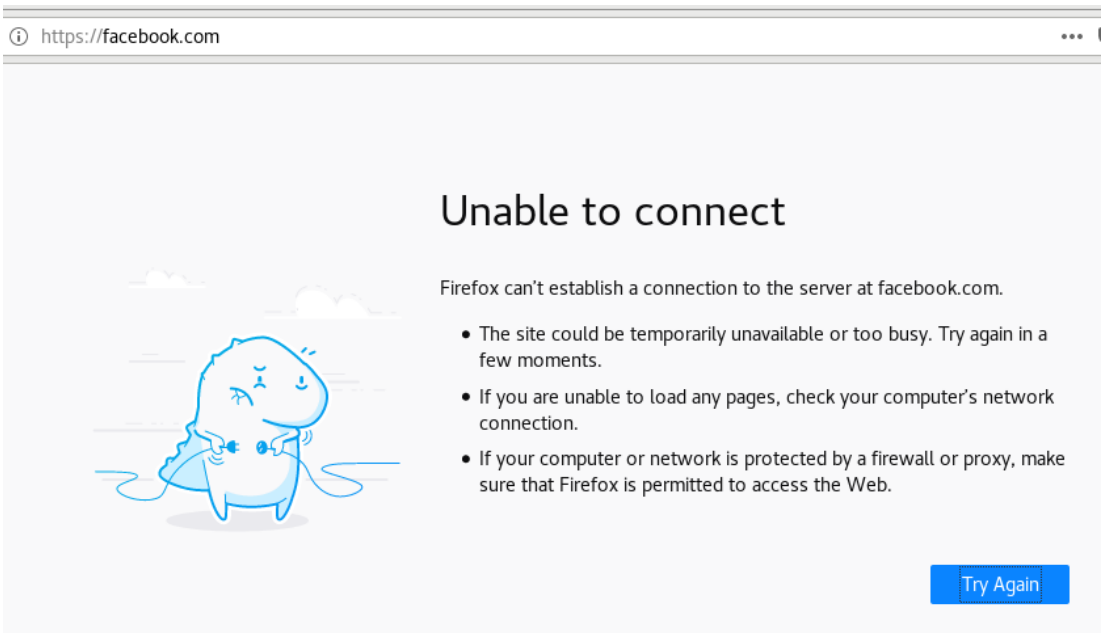


Las banderas indican el método de ataque de MITM (-M), que es sobre la tabla arp, otra es solo para mostrar salida de texto (--text), para no imprimir el contenido de los paquetes (--quiet), la interfaz de red donde se hará el ataque (--iface) y el plugin utilizado en el ataque (--plugin).

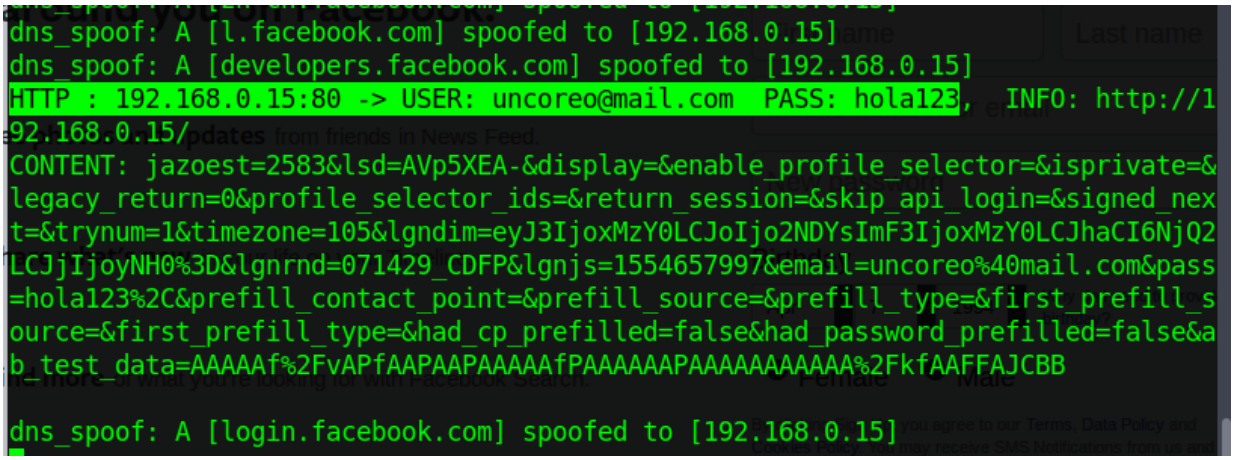
En la máquina víctima revisamos la tabla ARP, en la que ahora aparece la IP del atacante:



Intenté acceder a facebook.com desde la víctima, pero nunca se resolvía nombre de dominio, intente reiniciar el ataque ettercap después de haber configurado el archivo .dns pero seguía sin funcionar. Sin embargo, si ingresaba la IP del atacante, podía acceder a la suplantación del sitio de Facebook



Y tal como se esperaba, en el ettercap apareció los datos que ingresé en el login de la página falsificada



Nunca había tenido algún acercamiento práctico con este tipo de ataques, y este me gustó porque es emocionante ver lo fácil que es suplantar servicios incluso tan grandes como Facebook, obtener credenciales de esta red social se ve ahora tan trivial. No creía cuando al principio varias personas decían que se han vuelto obsesivas con la seguridad, pero ahora que conozco todo esto, yo también me he comenzado a volverme obsesivo con la seguridad en todos lados.