Tema 2
Ataques man in the middle

Ataques man in the middle

Protocolo ARP

Protocolo ARP

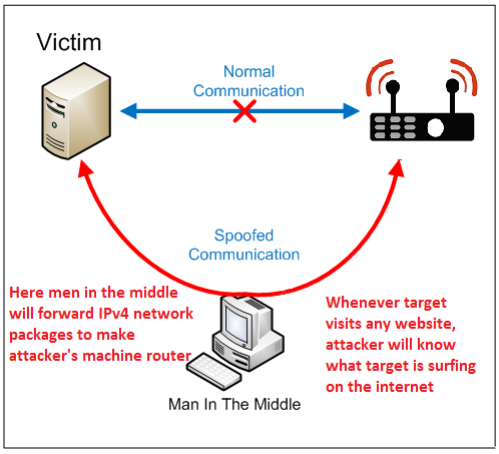
- Address Resolution Protocol
- Usado para resolver la dirección IP a la dirección física
- Necesario para por ejemplo para conectarse a un router wifi que nos dé salida a Internet

ARP

- En efecto, en una LAN (Red de área local) para comunicarse con un equipo (por ejemplo el router que nos da salida a Internet) se debe realizar una resolución ARP
- ARP: Address Resolution Protocol
- Resuelve la dirección IP a su dirección física o dirección MAC por broadcast
- Y se lo apunta en la caché ARP
- Para ver la caché ARP: arp -a

Ataques man in the middle

Configurar Linux como router



Linux como router

- Primero tenemos que saber cómo hacer que mi equipo sea un router
- Activar el IP_forward
  - Cambiar el valor ip_forward a 1 en /etc/sysctl.conf y guardar los cambios (sysctl –p)

Ataques man in the middle

ARP poisoning con arpspoof

ARP poisoning

- **Vamos a envenenar la caché ARP de los equipos víctima para obligarles a que pasen por mí**
- **Si tenemos en nuestro equipo un sniffer como Wireshark o como otros que veremos posteriormente podremos espiar sus conversaciones**
- **Y capturar usuarios, contraseñas, etc…**
- Este ataque es clave en el ámbito de la Seguridad

ARP poisoning

- **Práctica**: ARP cache poisoning mediante arpspoof (dsniff)
- Espiar una conversación http con wireshark entre mi Windows y el router
  - Buscar http login (CELFI por ejemplo) o vulnweb.com (y hacer login arriba a la derecha)

Ataques man in the middle

Detección del ARP spoofing

XArp

- **¿Cómo saber si nos están envenenando la caché ARP?**
- Aplicación: Xarp (www.xarp.net)
- Para Windows y para Linux (Ubuntu)
- Te avisa si detecta que están envenenando tu caché
- Para ello chequea la caché ARP para ver si hay entradas duplicadas
- Te avisa cuando cambian esta caché y aparecen macs raras o duplicadas

Wireshark

- ¿Cómo me protejo?
- Añadiendo una entrada estática para la mac del router
- Claro, el problema es que hay que cambiarlo según me conecto a cada red diferente

Ataques man in the middle

Bettercap

Bettercap

- **Instalación**
  - sudo apt install bettercap
  - bettercap (--iface eth0, pero no es necesario, solo si tenemos varias tarjetas)
  - help
  - net.probe on (y hace un netdiscover)
  - net.show

Bettercap

- **Ataques man in the middle con bettercap**
- Hay un módulo llamado arp.spoof
  - help arp.spoof (fijarse también que hay un arp.ban on para matar conexiones)
  - arp.spoof.fullduplex – así no hace falta dar la ip del router, la pilla automáticamente (set arp.spoof.fullduples true)
  - set arp.spoof.targets 192.168.1.18 (la 192.168.1.1 la pilla automáticamente) Ver las Ips de los objetivos de net.show
  - arp.spoof on

Bettercap

- **Comprobación**
  - Ver arp -a en la víctima, para ver cómo se envenena la caché arp

Bettercap

- **Espiar las conversaciones**
- net.sniff on
- Como antes, ir a vulnweb.com
- Ir al primer enlace y clic en login (arriba derecha, vale cualquier usuario y cualquier contraseña)
- Esto mandará la password sin cifrar puesto que no es https y podremos verlo en bettercap.
- Si no buscar un login http website en Google (CELFI por ejemplo)