Tema 1
Sniffer: espiando conversaciones

Recopilación de información

- Lo primero es poner nuestra máquina virtual con Kali en modo bridge (no NAT)
- Vamos a descubrir qué clientes hay conectados en la red en la que nos encontramos
- Para ello hay muchas herramientas pero una de ellas es netdiscover
- Pero primero veremos cuál es nuestra dirección IP en Linux con ifconfig (ojo, ipconfig en Windows)

Recopilación de información

- Si nuestra dirección IP es 192.168.1.14 deberíamos ver qué equipos hay en esta red (192.168.1.0/24)
- ¿Qué es ese /24? Notación CIDR

Recopilación de información

- **Netdiscover**
- Para ello:
- Para ello hay muchas herramientas pero una de ellas es netdiscover
- netdiscover -r 192.168.1.0/24
- Según se vayan conectando irán apareciendo por aquí
- Todos ellos son potenciales víctimas

Recopilación de información

- ¿Voy a poder capturar todos los paquetes que haya en esta red Wi-Fi, vayan o no a mí?
- Necesito tener el interfaz wi-fi en modo monitor
- Desde la máquina virtual no puedo hacerlo porque no accede directamente a la tarjeta de red, sino a una virtual
- Debería usar una tarjeta externa Wireless USB que admita modo monitor

Recopilación de información

- Las tarjetas internas no suelen soportar el modo monitor
- Para ver si la mía lo soporta hacer lsusb –vv. Fijarse en el chipset que utiliza y ver en la siguiente lista si soporta modo monitor
- https://www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dongles.html

Recopilación de información

- En este ejemplo el chipset es Ralink RT5372, que sí esta soportado

```
lsusb -vv

Bus 001 Device 002: ID 148f:5372 Ralink Technology, Corp. RT5372 Wireless Adap
Device Descriptor:
  bLength                18
  bDescriptorType         1
  bcdUSB               2.00
  bDeviceClass            0 (Defined at Interface level)
  bDeviceSubClass         0
  bDeviceProtocol         0
  bMaxPacketSize0        64
  idVendor           0x148f Ralink Technology, Corp.
  idProduct          0x5372 RT5372 Wireless Adapter
  bcdDevice            1.01
  iManufacturer           1 Ralink
  iProduct                2 802.11 n WLAN
  iSerial                 3 (error)
  bNumConfigurations      1
```

- Si no lo tenemos no pasa nada, pero tendremos que hacer un ataque man in the middle para espiar conversaciones

Recopilación de información

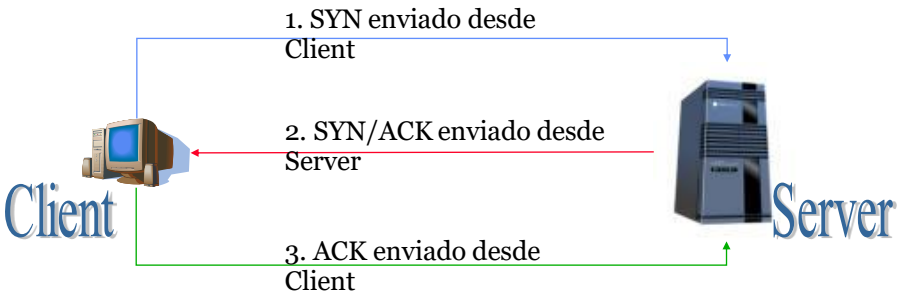
- En este ejemplo el chipset es Ralink RT5372, que sí esta soportado

```
lsusb -vv

Bus 001 Device 002: ID 148f:5372 Ralink Technology, Corp. RT5372 Wireless Adap
Device Descriptor:
  bLength                18
  bDescriptorType         1
  bcdUSB               2.00
  bDeviceClass            0 (Defined at Interface level)
  bDeviceSubClass         0
  bDeviceProtocol         0
  bMaxPacketSize0        64
  idVendor           0x148f Ralink Technology, Corp.
  idProduct          0x5372 RT5372 Wireless Adapter
  bcdDevice            1.01
  iManufacturer           1 Ralink
  iProduct                2 802.11 n WLAN
  iSerial                 3 (error)
  bNumConfigurations      1
```

Comunicación cliente-servidor

TCP three-way handshake



TCP three-way handshake

- **Paquete #1 - Cliente**: Envía un paquete sin datos con el flag SYN activado (“Quiero hablar contigo”)
- **Paquete # 2 - Servidor** – Envía un paquete con el flag ACK activado (“Recibido”) y el SYN también activado (“vale, yo también quiero hablar contigo”)

TCP three-way handshake

- **Paquete # 3 - Cliente** – El servidor está esperando a que el cliente le diga que ha recibido su paquete. Al recibirlo tiene que decirle al servidor que lo ha recibido. Para ello el cliente envía un paquete ACK.
- Se cierra la negociación: “empecemos a hablar”.

Conversación HTTP

- Conversación http
- **Paquete # 4 – Cliente:** El cliente manda un GET http (http request)

Conversación HTTP

- **Paquete #5 – Servidor:** El servidor manda su OK o Recibido
- **Paquete #6 – Servidor:** El servidor manda la respuesta a la petición HTTP del cliente

Conversación HTTP

- **Paquete #7 – Cliente:** El cliente debe decirle al servidor que ha recibido su respuesta (la página web)

Conversación HTTP

- **Cierre de conexión (four way handshake)**
- **Cliente:** Manda un paquete con el flag FIN activado (“ya no quiero hablar más”
- **Servidor**: Manda un paquete con el flag ACK activado (“recibido, me doy por enterado”) y otro paquete con el flag FIN activado también (“me parece bien, yo tampoco quiero hablar más contigo”)
- Este paso anterior se puede hacer en uno o en dos pasos (mandando uno o dos paquetes con cada flag)

Espiando conversaciones

- **Práctica – captura de contraseñas http**
- Vamos a realizar nuestra primera acción de hacking
- Realizar una conexión http para ver una página web cualquiera que tenga un login mediante http (Buscar en Google http)
- Capturar los paquetes de la conexión mediante wireshark
- Para ello instalar primero el wireshark

TCP three-way handshake

- **Acciones:**
- Capturar los paquetes de la conexión mediante wireshark
- Identificar los tres paquetes del three-way handshake
- Capturar el usuario y la contraseña introducida
- Identificar los cuatro paquetes de cierre de conexión

TCP three-way handshake

- Ayuda: filtrar http contains “password” -> ver paquete POST
- Botón derecho / conversation filter para ver el Three way handshake

TCP three-way handshake

- Preguntas para responder:
  - Identifica los paquetes involucrados en el three way handshake o inicio de conexión
  - ¿Qué IP tiene el servidor? ¿Y el cliente?
  - Puertos del cliente y del servidor
  - Identifica los valores de los sequence y acknowledge numbers en el three way handshake
  - Identifica los paquetes involucrados en el four way handshake o fin de conexión
  - Identifica el paquete que lleva la contraseña