TALLER SI – PRÁCTICA 5		
NÚMERO DE GRUPO	**FUNCIÓNS**	**Apelidos, Nome**
	Coordinador/a:	
	Responsable Limpeza:	
	Responsable Documentación:	

ESCENARIO: Rede local. Control de acceso á rede e Internet mediante filtrado MAC

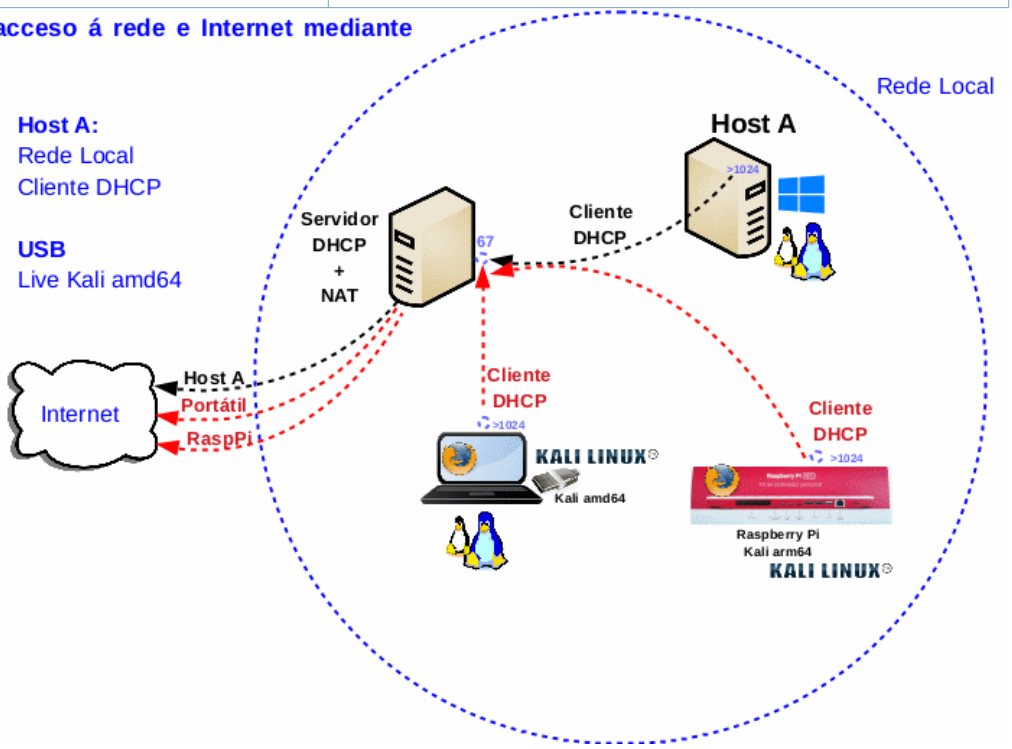
Servidor DHCP + NAT:
Rede Local
Configuración activa por filtrado de MAC

Portátil:
Rede Local
MAC filtrada (sen acceso)

Raspberry Pi:
Rede Local
MAC filtrada (sen acceso)
SO: Kali arm64

Host A:
Rede Local
Cliente DHCP

USB
Live Kali amd64



Material necesario	Práctica: Ataque MAC Spoofing. Conseguir acceso á rede local e Internet
■ Host A (MAC Address con acceso á rede e Internet) ■ Portátil sen acceso á rede local local(material existente no taller) ■ USB Live amd64 Kali GNU/Linux(solicitar ao docente) ■ Raspberry Pi 4 (ou 400) sen acceso á rede local(material que posúe o grupo) ■ [1] Descargas Kali ARM ■ [2] Documentación Kali ARM	(1) Portátil: a) Conseguir acceso á rede local e Internet mediante cambio de MAC Address e solicitude DHCP. b) Descargar a distribución Kali ARM (arm64) e verificar a súa descarga. c) Conectar a tarxeta MicroSD co adaptador SD no portátil d) Crear MicroSD arrancable (2) Raspberry PI a) Arrancar mediante a MicroSD Kali b) Cambiar contrasinais de usuarios c) Conseguir acceso á rede local e Internet

Procedemento:

(1) Portátil:

(a) Arrancar cun USB Live amd64 Kali GNU/Linux

(b) Conseguir acceso á rede local e a Internet. Abrir unha consola e executar:

```
$ setxkbmap es #Configurar teclado en español
$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
  # ip link show eth0 #Amosar información sobre a NIC eth0. Identificar a MAC Address (link/ether)
  # ip link set down dev eth0 #Deshabilitar a NIC eth0
  # ip link set address 11:22:33:44:55:66 dev eth0 #Modificar na NIC eth0 a MAC Address ploa dirección solicitada ao docente, a cal é pertencente a un host da rede con acceso a Internet.
  # ip link set up dev eth0 #Habilitar a NIC eth0
  # ip link show eth0 #Amosar información sobre a NIC eth0. Verificar o cambio correcto de MAC Address
  # dhclient -v eth0 #Solicitar configuración de rede para a NIC eth0. Como agora temos a MAC Address cambiada suplantando a un host real deberiamos obter a mesma configuración de rede dese host, sen impedimento que ese host perda a configuración de rede. Pero, agora teremos na rede 2 hosts coa mesma configuración, provocando que a electrónica de rede envíe comunicación "intermitente" aos 2 hosts.
  # ip addr show eth0 #Amosar información sobre a NIC eth0. Verificar o cambio correcto de MAC Address
  # ping -c4 www.google.es #Enviar 4 paquetes ICMP ECHO_REQUEST a www.google.es, solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede hacia Internet e ao servidor de google.
  # exit #Saír da shell
$
```

(c) Descargar Kali arm64 [1] en `/home/kali`

(d) Verificar descarga mediante comprobación hash. Exemplo:

```
$ pwd #Imprimir directorio de traballo actual
/home/kali
$ sha256sum kali-linux-2021.4-rpi-arm64.img.xz #Calcular Hash sha256
```

(e) Conectar a tarxeta MicroSD mediante o adaptador SD no portátil

```
$ sudo dmesg -w #Antes de conectar executar este comando. A continuación da execución conectar. Pódese verificar o nome do dispositivo conectado, por exemplo: mmcblk0
```

(f) Crear a MicroSD arrancable[2]. Exemplo:

```
$ mount #Importante!: Verificar que o dispositivo non está montado
$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
 # xzcat /home/kali/kali-linux-2021.4-rpi-arm64.img.xz | dd of=/dev/mmcblk0 bs=4M \
status=progress #"Queimar" microSD
 # exit #Saír da shell
$ mount #Importante!: Verificar que o dispositivo non está montado. Se non está montado sacar a tarxeta MicroSD(adaptador SD) do portátil
```

(g) Avisar ao docente para revisión.

(2) Raspberry Pi:

(a) Conectar a MicroSD na Raspberry Pi

(b) Arrancar e verificar o arranque do sistema operativo Kali ARM (arm64)

(c) Modificar contrasinais de usuarios kali e root. Novos contrasinais **abc123.** (Ollo que existe un caracter punto e final no contrasinal!). Exemplo:

```
$ echo -e 'kali\nabc123.\nabc123.' | passwd #Cambiar contrasinal ao usuario kali
$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
 # echo -e 'abc123.\nabc123.' | passwd #Cambiar contrasinal ao usuario root
```

(d) Avisar ao docente para revisión.

(e) Realizar de novo o apartado (1.b). Unha vez rematado avisar de novo ao docente para a revisión.

(3) Contesta e razoa brevemente:

(a) Cantos hosts posúen agora a mesma configuración de rede? Cales?

(b) Vese afectada a electrónica de rede? Existen conflictos?

(c) Envía simultaneamente un ***ping con 100 paquetes ICMP a www.google.es*** dende os 3 hosts: HostA, Portátil, Raspberry Pi. Que acontece? Por que?

```
# ping -c100 www.google.es #Enviar 100 paquetes ICMP ECHO_REQUEST a www.google.es, solicitando 100 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede hacia Internet e ao servidor de google.
```

(d) Realiza de novo o apartado c) pero executando previamente un escaneo de rede mediante Wireshark dende a Raspberry Pi. Podes distinguir a mesma MAC en distintos hosts?

(e) Como poderiamos detectar este ataque? Monitorización MAC Table no Switch onde están conectados os hosts (HostA, Portátil, Raspberry Pi)?

(f) Que contramedidas poderiamos tomar para evitar este ataque? *Switch Port Security*: Asignación Porto Switch – MAC Address? *MAC Lockdown*: Bloqueo de MAC?

Usando só Port Security o enderezo MAC aínda se pode usar noutro porto do mesmo switch. MAC Lockdown, por outra banda, é unha clara relación un a un entre o enderezo MAC e o porto. Unha vez que un enderezo MAC foi bloqueado nun porto, non se pode usar noutro porto do mesmo switch.