

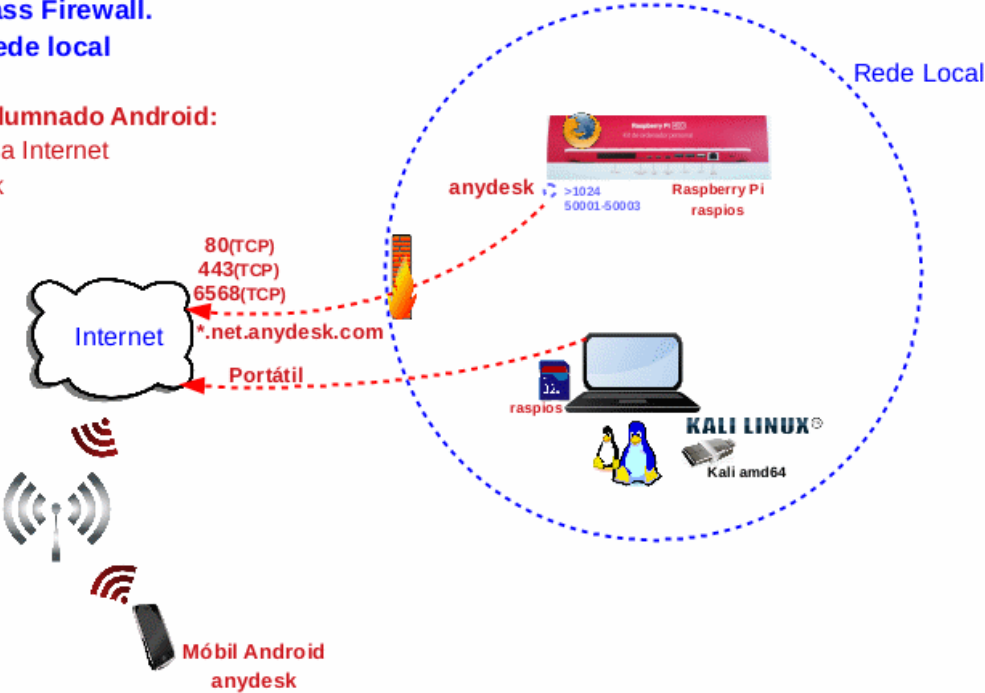
TALLER SI – PRÁCTICA 14

NÚMERO DE GRUPO	FUNCIÓNS	Apellidos, Nome
<div></div>	Coordinador/a:	
	Responsable Limpieza:	
	Responsable Documentación:	

ESCENARIO: Acceso Remoto. Bypass Firewall.
Conseguir acceso á rede local

Raspberry Pi:
Rede Local
Acceso a Internet
SO: Raspberry Pi OS(armhf)
anydesk

Móbil alumnado Android:
Acceso a Internet
anydesk



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

Material necesario	Práctica: Acceso Remoto. Bypass Firewall Conseguir acceso á rede local.
<ul style="list-style-type: none">■ Raspberry Pi 4 (ou 400) con acceso á rede local e Internet (material que posúe o grupo)■ [1] Descargas Rasperry Pi OS■ [2] Documentación Raspberry Pi OS■ Móbil alumnado■ [3] AnyDesk■ [4] AnyDesk Raspberry Pi■ [5] AnyDesk, el software de escritorio remoto Google Play■ [6] wireshark■ [7] 03-Exercicio3-Wireshark-ICMP-ARP.pdf	<ul style="list-style-type: none">(1) Raspberry PI<ul style="list-style-type: none">a) Arrancar mediante a MicroSD RaspiOSb) Acceso á rede local e Internetc) Instalar programa acceso remoto[3][4]d) Arrancar ese programa: anydesk(2) Móbil alumnado<ul style="list-style-type: none">a) Acceso a Internet por datosb) Instalar programa acceso remoto[3][5]c) Conectar por acceso remoto: anydeskd) Acceso na rede local (bypass firewall)(non foi necesario facer NAT(PNAT) no router)



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 pola
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 deberíamos 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 [RaspiOS](#) [1] en /home/kali

(d) Verificar descarga mediante comprobación hash. Exemplo:

```
$ pwd #Imprimir directorio de traballo actual
/home/kali
$ sha256sum 2021-10-30-raspios-bullseye-armhf-full.zip #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
$ unzip -p /home/kali/2021-10-30-raspios-bullseye-armhf.zip | sudo dd
of=/dev/mmcblk0 bs=4M conv=fsync status=progress #"Queimar" microSD
$ 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. ☐ 1

(2) Raspberry Pi:

(a) Conectar a MicroSD na Raspberry Pi

(b) Arrancar e verificar o arranque do sistema operativo Raspberry Pi OS (armhf)

Next → Country: Spain → Language: Galician → Timezone: Madrid → Next

Change password user pi → abc123. → Next → Next → Skip → Skip → Done

(c) Modificar contrasinal do usuario **root**. Novo contrasinal **abc123**. (Olo que existe un carácter punto e final no contrasinal!). Exemplo:

```
$ 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
# exit #Saír da consola de root
$
```

(d) Avisar ao docente para revisión. ☐ 2

(3) Raspberry Pi: AnyDesk [3]

(a) Descargar [4]:

```
$ wget https://download.anydesk.com/rpi/anydesk_6.1.1-1_armhf.deb  
-O /tmp/anydesk-_armhf.deb #Descargar anydesk
```

(b) Instalar [4]:

```
$ sudo dpkg -i /tmp/anydesk_armhf.deb #Instalar anydesk  
$ sudo apt -f -y install #Instalar dependencias anydesk  
$ sudo dpkg -i /tmp/anydesk_armhf.deb #Instalar anydesk  
$ sudo apt -y install libgles-dev # Instalar dependencias anydesk
```

Solucionar Problema shared librarías → <https://raspberrypi.stackexchange.com/questions/116996/anydesk-error-while-loading-shared-libraries-libbrcmglesv2-so>

```
$ sudo ln -s /usr/lib/arm-linux-gnueabihf/libGLv2.so /usr/lib/libbrcmGLv2.so  
$ sudo ln -s /usr/lib/arm-linux-gnueabihf/libEGL.so /usr/lib/libbrcmEGL.so
```

(c) Executar:

```
$ anydesk &  
New Session → This Desk: XXX XXX XXX
```

NOTA:

XXX XXX XXX → *Identificador que permitirá a conexión dende o móbil*

(4) Móbil alumnado: AnyDesk [3]

(a) Instalar [5]

Google Play → [5] → Instalar

(b) Conseguir Acceso remoto á Raspberry Pi:

Abrir app anydesk → Aceptar Licenza (Política de Privacidad) → OK → Descartar instalación plugin que permite control de acceso remoto ao Móbil → CANCELAR → Premer fóra da zona azul → Dirección remota: XXX XXX XXX → Premer icono CONECTAR

(5) Raspberry Pi: GUI AnyDesk

Aceptar a conexión solicitada dende o móbil → **Accept**

Seleccionar o terminal aberto → Premer na icona situada á dereita e escoller: Opciones de entrada → Mostrar teclado.

Executar no terminal:

```
$ ls  
$ id
```

- Se non é posible realizar a conexión:
 - i. Indicar que acontece?
 - ii. A que crees que pode ser debido que non se realice a conexión?
- Se é posible realizar a conexión:
 - i. Capturar unha imaxe da pantalla da Raspberry Pi.
 - ii. Capturar unha imaxe da pantalla do móbil
 - iii. Probar a interface de anydesk do móbil.
 - iv. Premer na aspa (X) e pechar a conexión.

(6) Avisar ao docente para revisión. ☐

(7) Raspberry Pi: **wireshark** [6][7]

Identificar co sniffer *wireshark* as conexións que intenta establecer *anydesk*:

(a) Abrir un novo terminal e executar:

```
$ sudo wireshark -i eth0 & #Sniffer wireshark lanzado esperando comunicacións coa NIC eth0
```

(b) **Menú → Start capturing packets (Premer na aleta do “tiburón”)**

(c) Realizar de novo os apartados (3c) , (4b) e (5)

(d) Unha vez capturados os paquetes da conexión deter o **Wireshark**:

Menú → Stop capturing packets (Premer no cadrado de fondo vermello)

(e) Identificar os sockets da conexión e achegar as imaxes do *wireshark* correspondentes.

(8) Avisar ao docente para a entrega e revisión da práctica. ☐ 4

Revisión:

☐ ¹ ☐ ² ☐ ³ ☐ ⁴