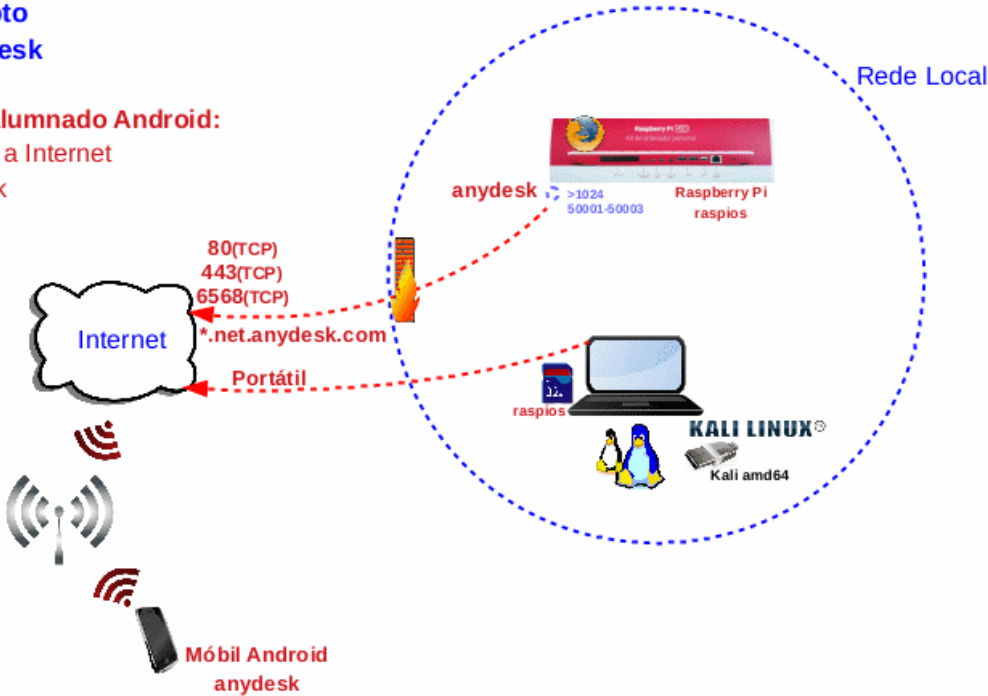


NÚMERO DE GRUPO	FUNCIÓNS	Apellidos, Nome
<div></div>	Coordinador/a:	
	Responsable Limpieza:	
	Responsable Documentación:	

ESCENARIO: Acceso Control Remoto
Impedir acceso á rede local a AnyDesk

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 Control Remoto. Impedir acceso á rede local a Anydesk
<ul style="list-style-type: none">■ Prerrequisito: [1] Práctica 14■ Raspberry Pi 4 (ou 400) con acceso á rede local e Internet (material que posúe o grupo)■ [2] Firewall iptables■ [3] Documentación AnyDesk firewall■ [4] Comandos e SHELL bash 1■ [5] Scripts SHELL bash	<ul style="list-style-type: none">(1) Raspberry PI: Realizar Práctica 14[1](2) Móbil alumnado: Acceso remoto co anydesk é posible (bypass firewall)(3) Raspberry Pi: Regras iptables[2] → Impedir acceso anydesk(4) Móbil alumnado: Acceso remoto co anydesk non é posible(5) Raspberry Pi: Eliminar Regras iptables[2] → Permitir acceso anydesk(6) Raspberry Pi: Script SHELL bash + CRON → Impedir acceso anydesk(7) Móbil alumnado: Acceso remoto co anydesk non é posible



Procedemento:

(1) Raspberry Pi:

(a) Realizar a Práctica 14 [2] → Acceso remoto co anydesk é posible

(b) Abrir un novo terminal(a partir de agora chamado **terminal1**) e executar:

```
$ pkill anydesk #Matar calquera execución do programa anydesk
```

```
$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando  
sudo (/etc/sudoers, visudo)
```

(c) **iptables** [2]

i. Impedir o acceso remoto **AnyDesk** → **Filtrado de portos TCP: 80, 443**

Executar no **terminal1**:

```
# command -v iptables ; [ $? -ne 0 ] && apt update && apt -y install iptables  
#Instalar o paquete iptables no caso que non estar instalado  
  
# iptables -L -line-numbers #Listar de forma numerada todas as regras das cadeas da táboa  
filter, é dicir, amosar de forma numerada todas as regras das cadeas INPUT, FORWARD e OUTPUT  
  
# iptables -I OUTPUT -p tcp -m multiport --dports 80,443 -j DROP #Denegar acceso aos  
portos 80 (http) e 443 (https). Coa opción -I a regra insértase como a primeira regra da cadea  
correspondente, neste caso a cadea OUTPUT  
  
# iptables -L -line-numbers #Listar de forma numerada todas as regras das cadeas da táboa  
filter, é dicir, amosar de forma numerada todas as regras das cadeas INPUT, FORWARD e OUTPUT
```

ii. Acceder á páxina <http://www.edu.xunta.gal> Que acontece? Por que? Capturar unha imaxe.

iii. Acceder á páxina gmail.com Que acontece? Por que? Capturar unha imaxe.

iv. Acceder a calquera páxina que permita o acceso mediante o protocolo HTTP (http://) Que acontece? Por que? Capturar unha imaxe.

v. Acceder a calquera páxina que permita o acceso mediante o protocolo HTTPS (https://) Que acontece? Por que? Capturar unha imaxe.

vi. Executar no **terminal1**:

```
# iptables -L -v -line-numbers #Listar de forma numerada todas as regras das cadeas da táboa  
filter, é dicir, amosar de forma numerada todas as regras das cadeas INPUT, FORWARD e OUTPUT. Coa  
opción -v actívase o modo "verbose" no cal tamén se amosa o número de paquetes e bytes afectados por  
esta regra. É dicir, coa opción -v se os contadores non posúen valor cero quere dicir que a regra está  
afectando a algunha/s conexións
```

vii. Abrir un novo terminal(a partir de agora chamado **terminal2**) e executar:

```
$ anydesk & #Executar anydesk
```

viii. Capturar unha imaxe da GUI AnyDesk

(2) Móbil alumnado:

(a) Comprobar que o acceso remoto a **AnyDesk** segue sendo posible. Por que?

(b) Capturar unha imaxe da pantalla do móbil

(3) Raspberry Pi:

(a) Capturar unha imaxe da pantalla da Raspberry Pi.

(b) Avisar ao docente para revisión.

(4) Raspberry Pi:

(a) Executar no **terminal1**:

```
# pkill anydesk #Matar calquera execución do programa anydesk
```

(b) **iptables** [2]

i. Impedir o acceso remoto **AnyDesk** → **Filtrado de porto TCP: 6568**

Executar no **terminal1**:

```
# iptables -I OUTPUT -p tcp --dport 6568 -j DROP #Denegar acceso ao porto TCP 6568. Coa  
opción -I a regra insértase como a primeira regra da cadea correspondente, neste caso a cadea OUTPUT  
  
# iptables -L -v -line-numbers #Listar de forma numerada todas as regras das cadeas da táboa  
filter, é dicir, amosar de forma numerada todas as regras das cadeas INPUT, FORWARD e OUTPUT. Coa  
opción -v actívase o modo "verbose" no cal tamén se amosa o número de paquetes e bytes afectados por  
esta regra. É dicir, coa opción -v se os contadores non posúen valor cero quere dicir que a regra está  
afectando a algunha/s conexións
```

ii. Executar no **terminal2**:

```
$ anydesk & #Executar anydesk
```

iii. Capturar unha imaxe da GUI AnyDesk

Connecting to the AnyDesk network... → Could not connect to the AnyDesk network (result_timeout)

(5) **Móbil alumnado**: Comprobar que o acceso remoto a **AnyDesk** non é posible

(a) Capturar unha imaxe da pantalla do móbil

(b) Avisar ao docente para revisión.

(6) **Raspberry Pi**:

(a) Matar proceso/s anydesk:

Executar no **terminal1**:

```
# pkill anydesk #Matar calquera execución do programa anydesk
```

(b) Eliminar regras iptables:

Executar no **terminal1**:

```
# iptables -F #Eliminar regras iptables

# iptables -L -v -line-numbers #Listar de forma numerada todas as regras das cadeas da táboa filter, é dicir, amosar de forma numerada todas as regras das cadeas INPUT, FORWARD e OUTPUT. Coa opción -v actívase o modo "verbose" no cal tamén se amosa o número de paquetes e bytes afectados por esta regra. É dicir, coa opción -v se os contadores non posúen valor cero quere dicir que a regra está afectando a algunha/s conexións
```

(c) **Script SHELL bash** [4] [5]

i. Impedir o acceso remoto **AnyDesk** → **Script SHELL bash + CRON** → Xerar un script que "mate" calquera proceso *anydesk* e sexa executado a cada minuto.

Executar no **terminal1**:

```
# cat > /root/control-remoto.sh << EOF
> #!/bin/bash
> pgrep anydesk
> while [ $? -eq 0 ]; do
>   pkill anydesk
>   sleep 4
>   pgrep anydesk
> done
> EOF
# echo '* * * * * root /bin/bash /root/control-remoto.sh' >> /etc/crontab
```

ii. Executar no **terminal2**:

```
$ anydesk & ; sleep 60 #Executar anydesk e logo esperar 60 segundos
```

iii. Capturar unha imaxe da GUI AnyDesk:

i. Antes que rematen os 60 segundos de espera.

ii. Logo que rematen os 60 segundos de espera. Que acontece?

iv. Executar no **terminal1**:

```
# tail -f /var/log/syslog #Deixar aberto o ficheiro /var/log/syslog para lectura, comenzando a ver polas 10 últimas liñas.
```

v. Executar no **terminal2**:

```
$ anydesk & ; sleep 60 #Executar anydesk e logo esperar 60 segundos
```

vi. Capturar unha imaxe da GUI AnyDesk:

i. Antes que rematen os 60 segundos de espera.

ii. Logo que rematen os 60 segundos de espera. Que acontece? Capturar unha imaxe do **terminal1**

(7) **Móbil alumnado:** Comprobar que o acceso remoto a **AnyDesk** non é posible

- (a) Capturar unha imaxe da pantalla do móbil
- (b) Avisar ao docente para revisión

(8) **Raspberry Pi:** Comentar a liña do CRON (/etc/crontab) para non executar o script `bash control-remoto.sh`:

No **terminal1** premer <Ctrl>+<C> e executar:

```
# sed -i 's|^*\ * \* \* \* root /bin/bash /root/control-remoto.sh|#&|' /etc/crontab
```

(9) Contesta e razoa brevemente:

(a) Que acontece co programa *anydesk* se reinicias a Raspberry Pi? Execútase? A que crees que é debido?

(b) No **terminal1** premer <Ctrl>+<C> e executar:

```
# find / -iname "*anydesk*service*" 2>/dev/null | xargs ls -l #Buscar o patrón  
*anydesk*service* en todo o sistema e a cada referencia atopada executarlle o comando ls -l (listado  
extendido)
```

```
# /etc/init.d/anydesk status #Ver o estado do servizo anydesk
```

Que acontece? Por que?

(c) No **terminal1** executar:

```
# systemctl status anydesk #Ver o estado do servizo anydesk
```

```
# systemctl stop anydesk #Parar o servizo anydesk
```

```
# ls -l /etc/systemd/system/multi-user.target.wants/anydesk.service #Listar de forma  
extendida
```

```
# systemctl disable anydesk #Deshabilitar o servizo anydesk. Terá efecto no próximo inicio do  
sistema operativo.
```

```
# ls -l /etc/systemd/system/multi-user.target.wants/anydesk.service #Listar de forma  
extendida
```

Que acontece? Pasou algo con ese ficheiro?

(d) No **terminal1** executar:

```
# reboot #Reiniciar
```

Logo de reiniciar execútase *anydesk*? Por que?

(e) Por que empregar un script bash para denegar o acceso remoto a *anydesk* se xa co bloqueo de portos 80, 443 e 6568 xa estaría bloqueado?

(f) Por que empregar un script bash para denegar o acceso remoto a *anydesk* se xa con soamente o bloqueo do porto TCP 6568 poderíase bloquear?

(g) Cada vez que conectamos a *anydesk* faresh unha resolución DNS a algún host pertencente ao subdominio *.net.anydesk.com*, polo que cada vez conectamos a unha máquina distinta para o control de acceso remoto. Entón:

- i. Se tiveramos todos os hosts do subdominio de *anydesk* poderíamos bloquear anydesk engadido todas ás IPs que apuntan eses hosts nunha ACL?
- ii. Se limpamos a caché DNS, montamos un servidor DNS e creamos unha zona DNS *net.anydesk.com* que apuntara á interface *loopback* poderíamos bloquear *anydesk*?