

TALLER SR – PRÁCTICA 44 – RAC Sistemas operativos – TeamViewer

Resolución tickets incidencias

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

ESCENARIO:

Portátil:

Intranet, Internet

RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado

BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

ISO: Kali Live amd64

Cliente RAC (teamviewer)

USB

Live Kali amd64

Hosts A, B, C:

∈ Intranet

⊃ Máquina virtual

Máquinas virtuais Microsoft Windows:

⊂ Host

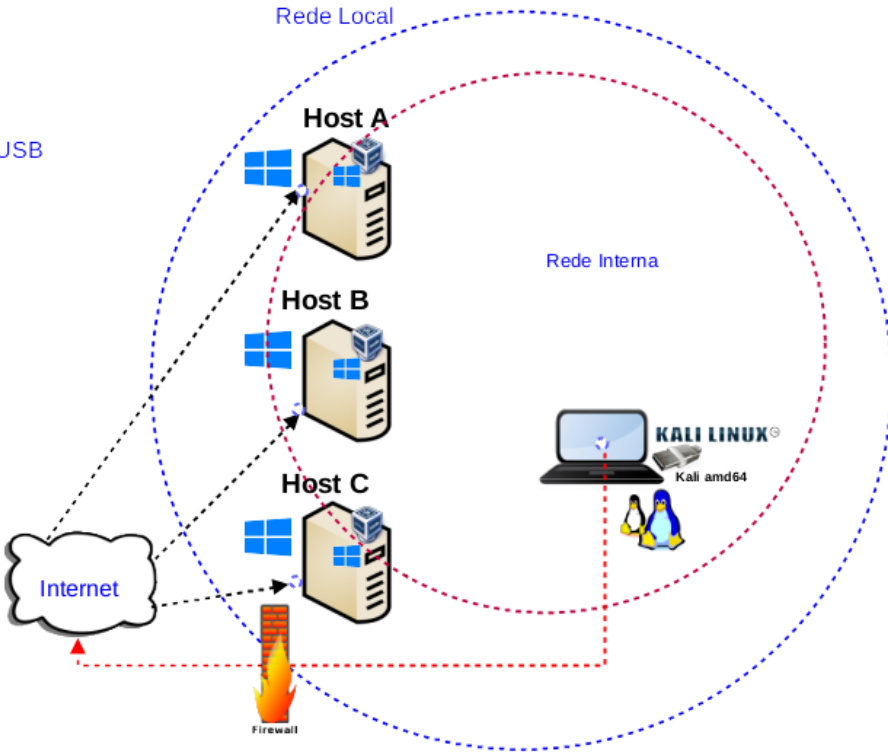
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado

Rede: NAT

Disco duro: Windows amd64

RAC activado (TeamViewer)

IP/MS: 10.0.2.15/24



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: RAC Sistemas operativos – TeamViewer Resolución tickets incidencias
<div>■ Portátil</div> <div>■ Regleta</div> <div>■ Switch 5-Port Gigabit</div> <div>■ USB Live amd64 Kali</div> <div>■ Hosts alumnado</div> <div>■ Cableado de rede</div> <div>■ [1] Práctica 1</div> <div>■ [2] TeamViewer</div> <div>■ [3] wireshark</div> <div>■ [4] Práctica Wireshark</div> <div>■ [5] Práctica SI 13 - Bypass Firewall - Conseguir acceso á rede local</div> <div>■ [6] Práctica SI Firewall iptables</div>	<div>(1) Prerrequisito: Ter realizada a Práctica 1 [1]</div> <div>(2) Conectar o switch á roseta da aula.</div> <div>(3) Conectar o portátil ao switch.</div> <div>(4) NON conectar os hosts do alumnado ao switch.</div> <div>(5) Hosts alumnado:<div>a) Crear máquinas virtuais coa rede en modo “NAT” e especificacións según escenario.</div><div>b) Arrancar máquina virtual.</div><div>c) Configurar a rede según o escenario.</div><div>d) Instalar/arrancar programa de acceso remoto teamviewer[2]</div></div> <div>(6) Portátil:<div>a) Instalar programa acceso remoto[2]</div><div>b) Conectar por acceso remoto (teamviewer) ás máquinas virtuais dos hosts do alumnado.</div><div>c) Acceso na rede local (bypass firewall)(non foi necesario facer NAT(PNAT) no router)</div></div>



Procedemento:

- (1) **NON conectar no mesmo segmento de rede o portátil e os hosts do alumnado.**
 - (a) Conectar a regleta á corrente eléctrica na vosa zona de traballo.
 - (b) Conectar o switch á regleta.
 - (c) Conectar o portátil ao switch co cableado de rede creado na [Práctica 1](#) [1] .
 - (d) **Conectar o switch á roseta da aula.**
 - (e) **NON conectar os vosos equipos de alumnado ao switch.**

(2) Portátil:

- (a) Arrancar co USB Live Kali amd64.
- (b) Comprobar que tedes acceso á rede local e a Internet. Abrir unha consola e executar:

```
$ setxkbmap es #Configurar teclado en español
$ ip addr show eth0 #Amosar información sobre a NIC eth0. Verificar a configuración de rede para a NIC eth0
$ ip route #Amosar a táboa de enrutamento.
$ cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, no cal configúranse os servidores DNS mediante a directiva nameserver.
$ 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.
```

Cubrir a seguinte táboa:

Host	IP	Máscara Subrede	Gateway	IP Servidores DNS (/etc/resolv.conf)
Portátil				

- (c) Avisar ao docente para a revisión. ☐1

- (3) **NON conectar no mesmo segmento de rede o portátil e os hosts do alumnado, é dicir, non conectar os vosos equipos de alumnado ao switch.**



(4) Hosts alumnado.

(a) Crear unha máquina virtual en cada equipo do alumnado coas seguintes características (ver escenario):

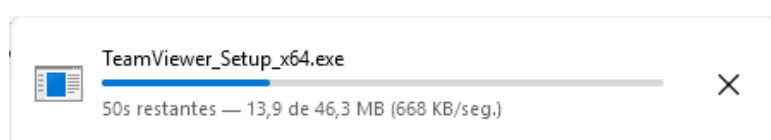
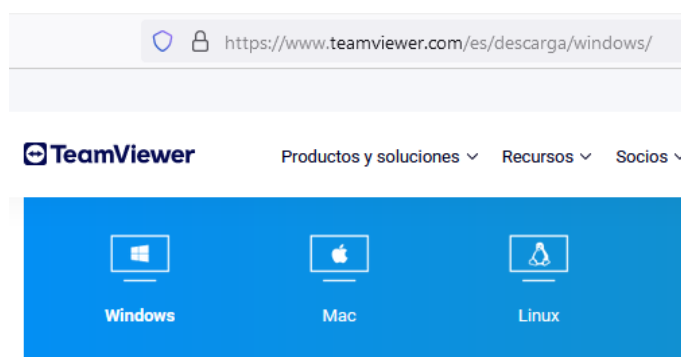
- I. RAM \geq 2048MB
- II. CPU \geq 2
- III. PAE/NX habilitado
- IV. Rede: Soamente unha tarxeta activada en modo NAT
- V. Disco duro: Microsoft Windows 10
- VI. Nome: Practica44-RAC-MW-AlumnoXY, o valor XY é o valor do PC que tedes asignado. Así, o alumno 17 terá como nome da máquina virtual: Practica44-RAC-MW-Alumno17

(b) Arrancar máquina virtual.

(5) Máquinas virtuais dos host de alumnado: TeamViewer[2]

(a) Abrir un navegador na URL: <https://www.teamviewer.com/es/descarga/windows/>

(b) Descargar [2]:



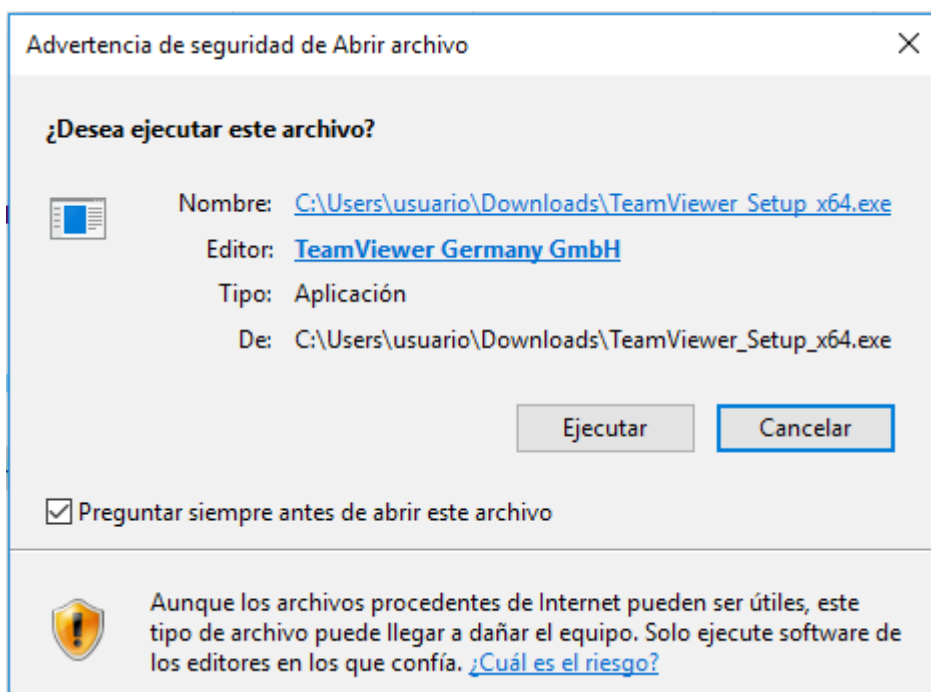
TeamViewer para Windows

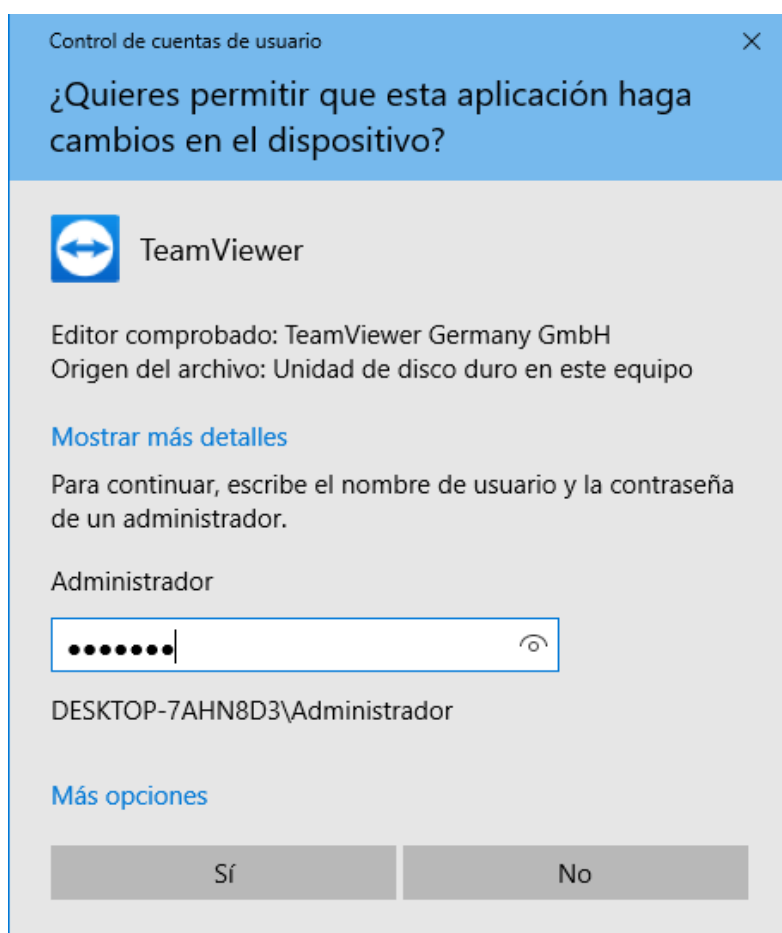
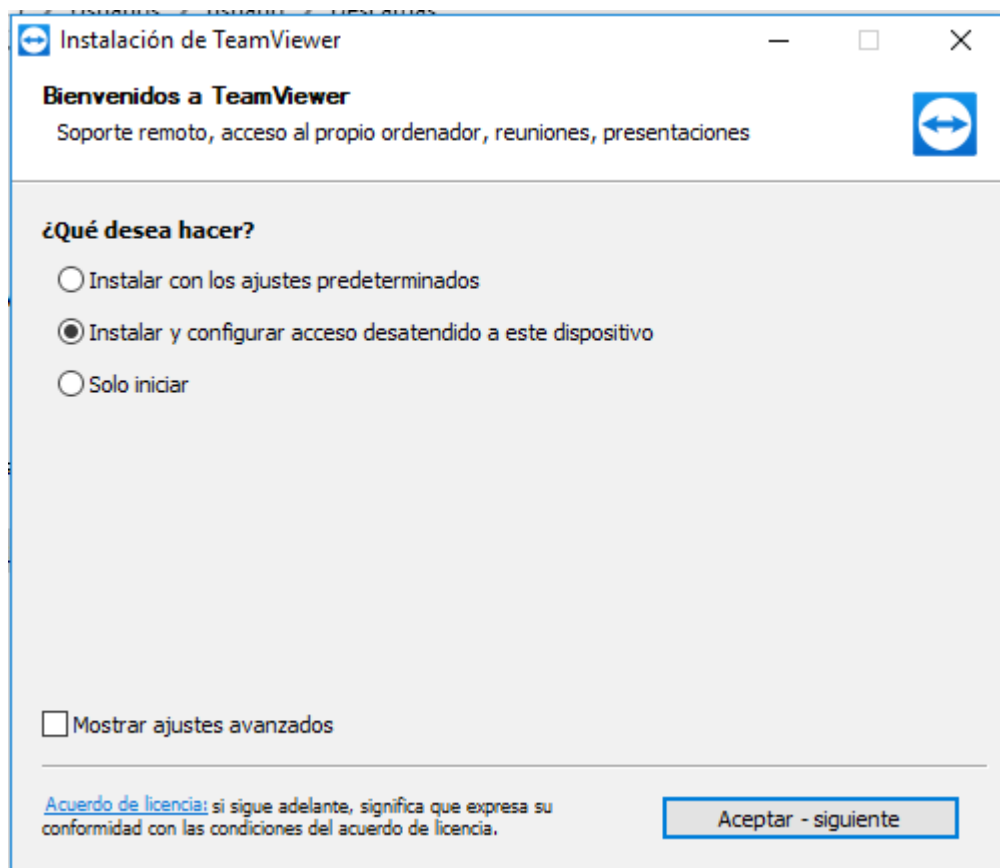
- Establece conexiones entrantes y salientes entre dispositivos
- Acceso y asistencia en tiempo real
- Colabora online, participa en reuniones y chats

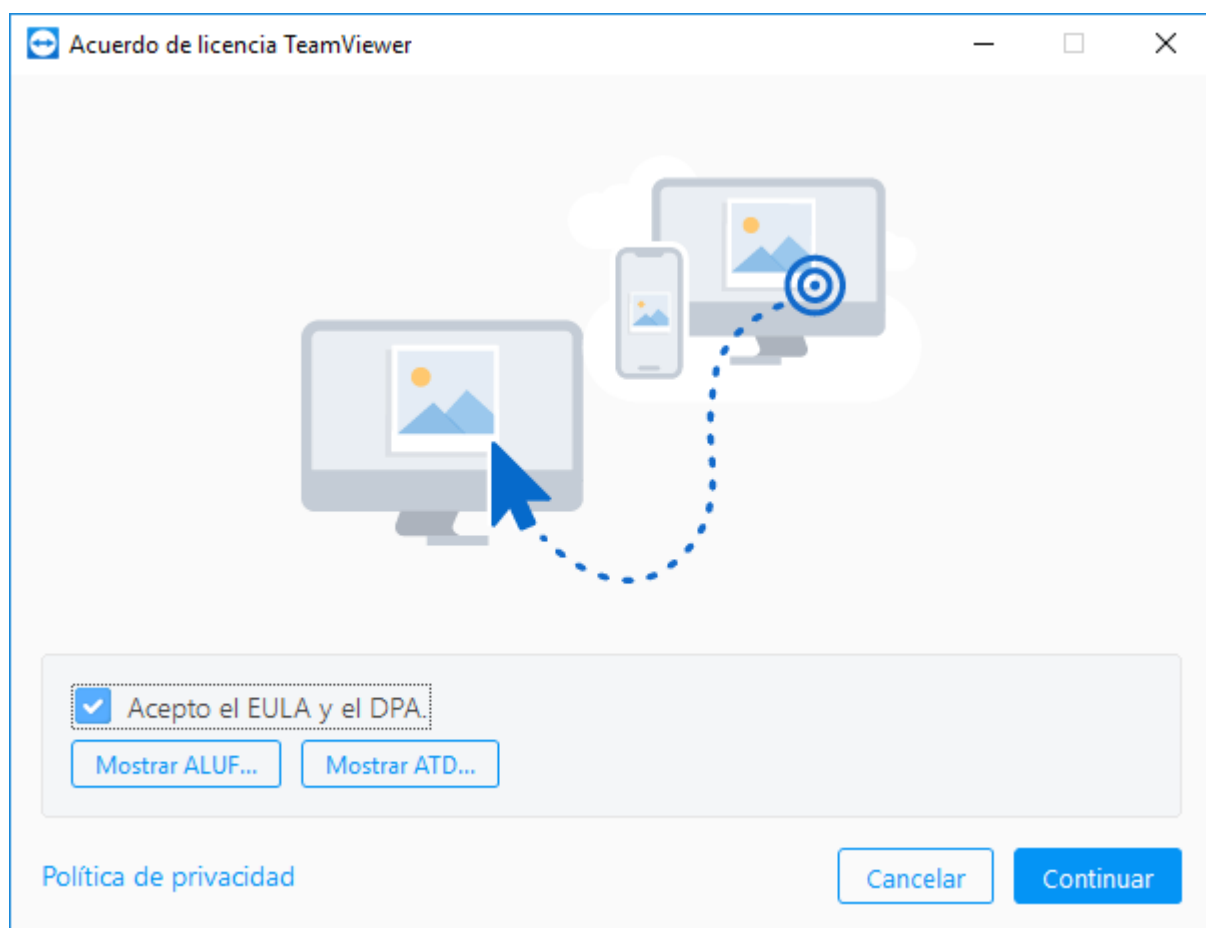
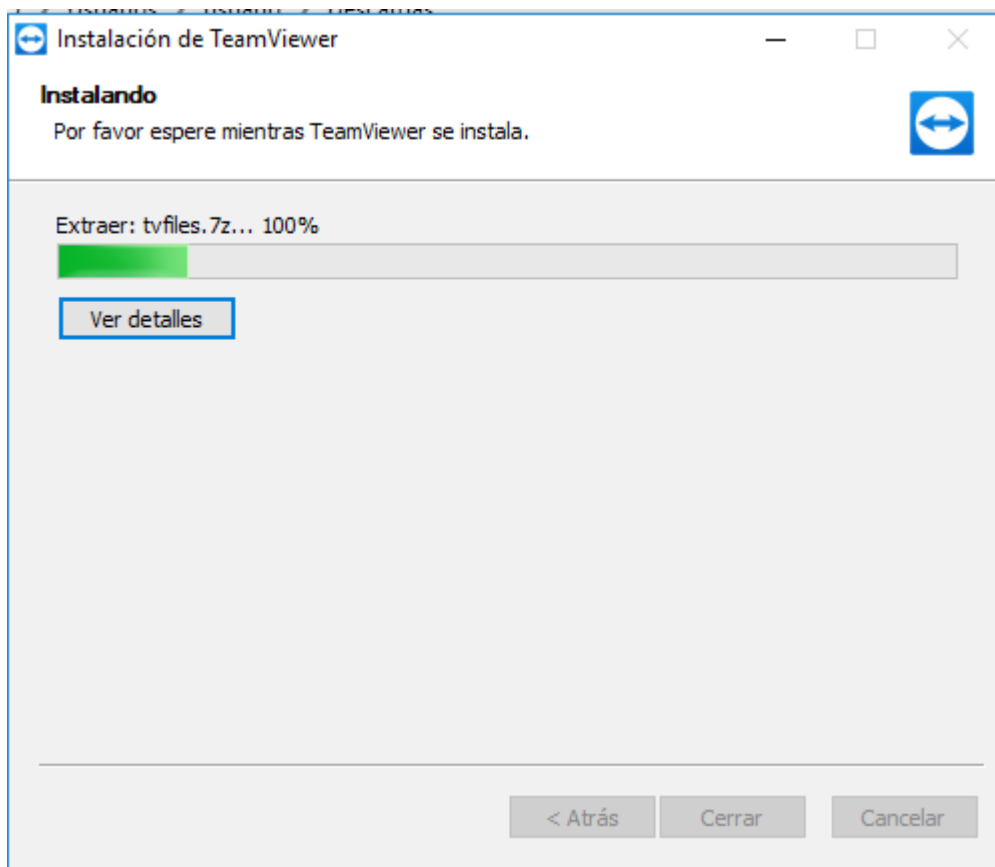
Descargar 64-bit Version

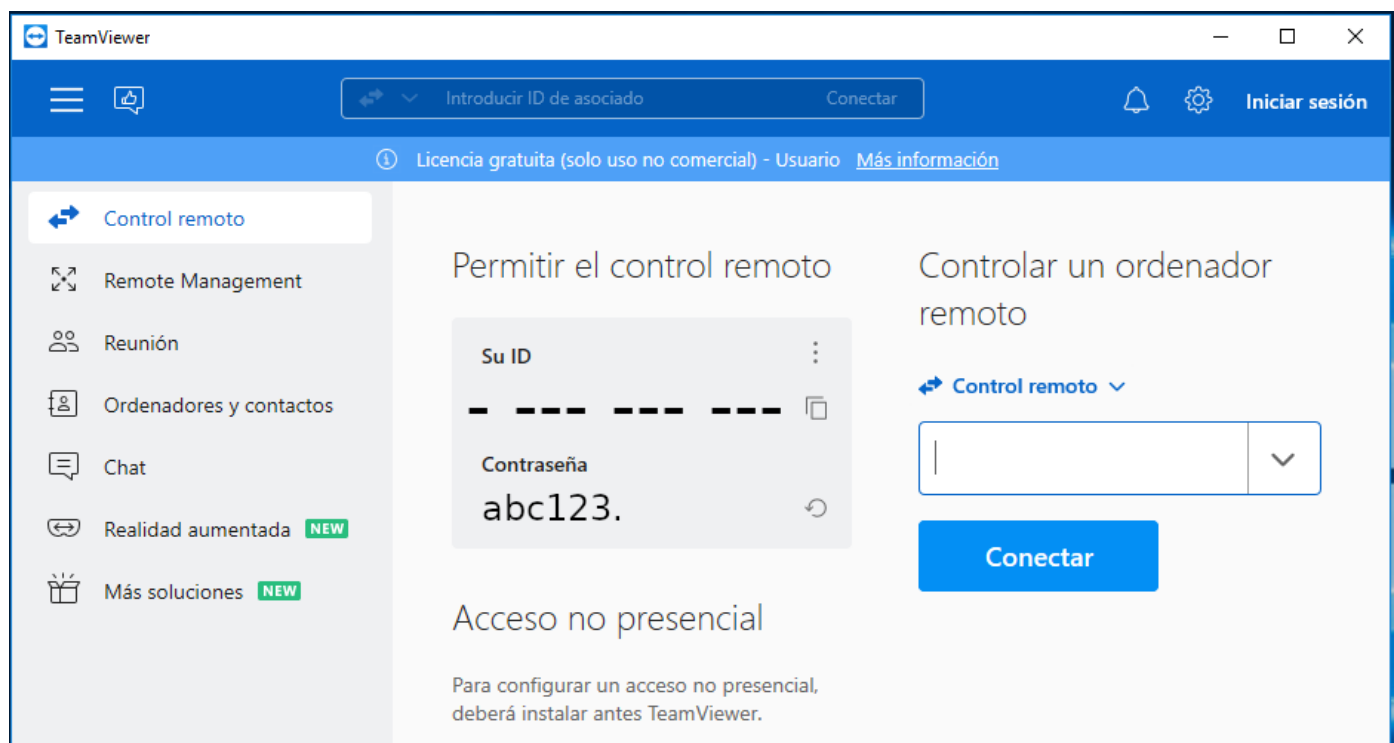
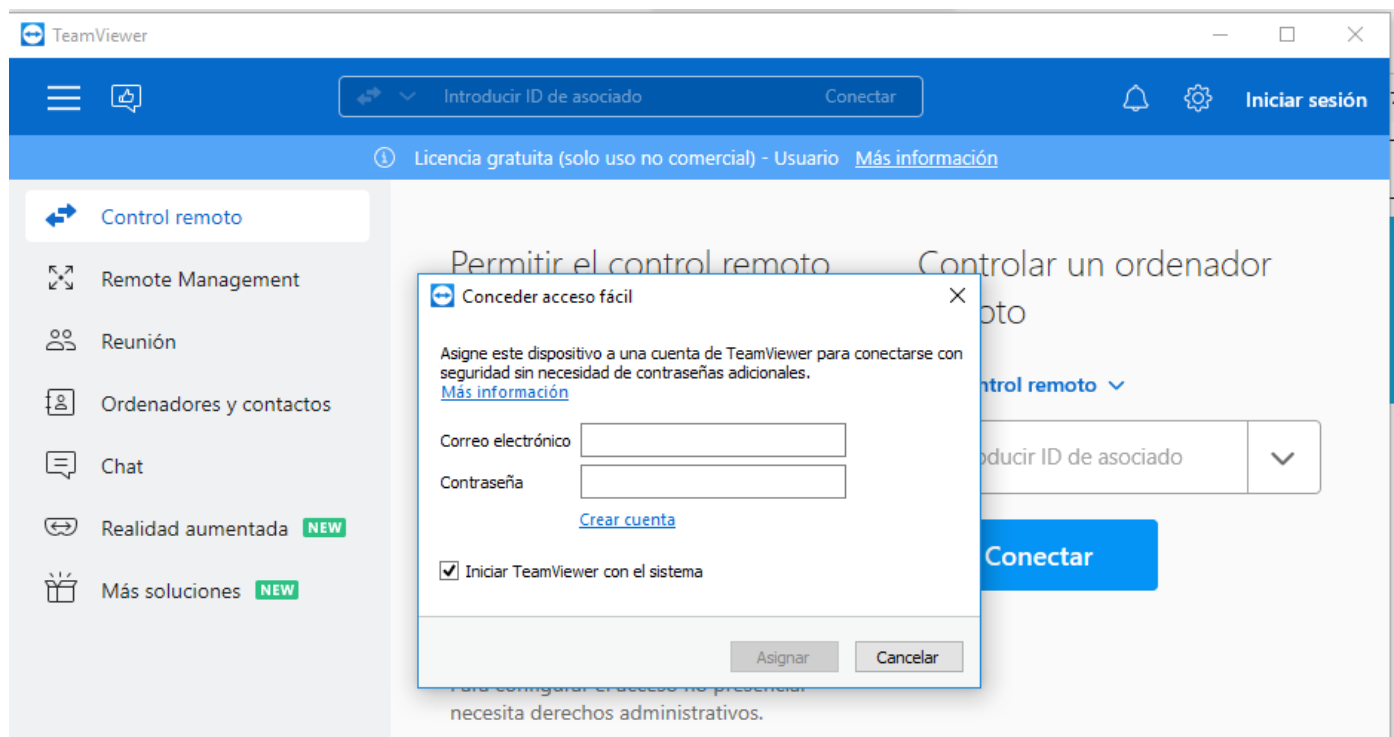
Descargar 32-bit Version

(c) Instalar [2]:









NOTA:

Su ID=- - - - - → *Identificador que permitirá a conexión dende o portátil ás máquinas virtuais Practica44-RAC-MW-AlumnoXY*

Contraseña=abc123. → *Contrasinal solicitada no acceso remoto logo de introducir o ID*

(6) Portátil: TeamViewer [2]

(a) Descargar [2]: Executar nunha consola

```
$ wget https://download.teamviewer.com/download/linux/teamviewer_amd64.deb  
-O /tmp/teamviewer_amd64.deb #Descargar teamviewer
```

(b) Instalar [2]:

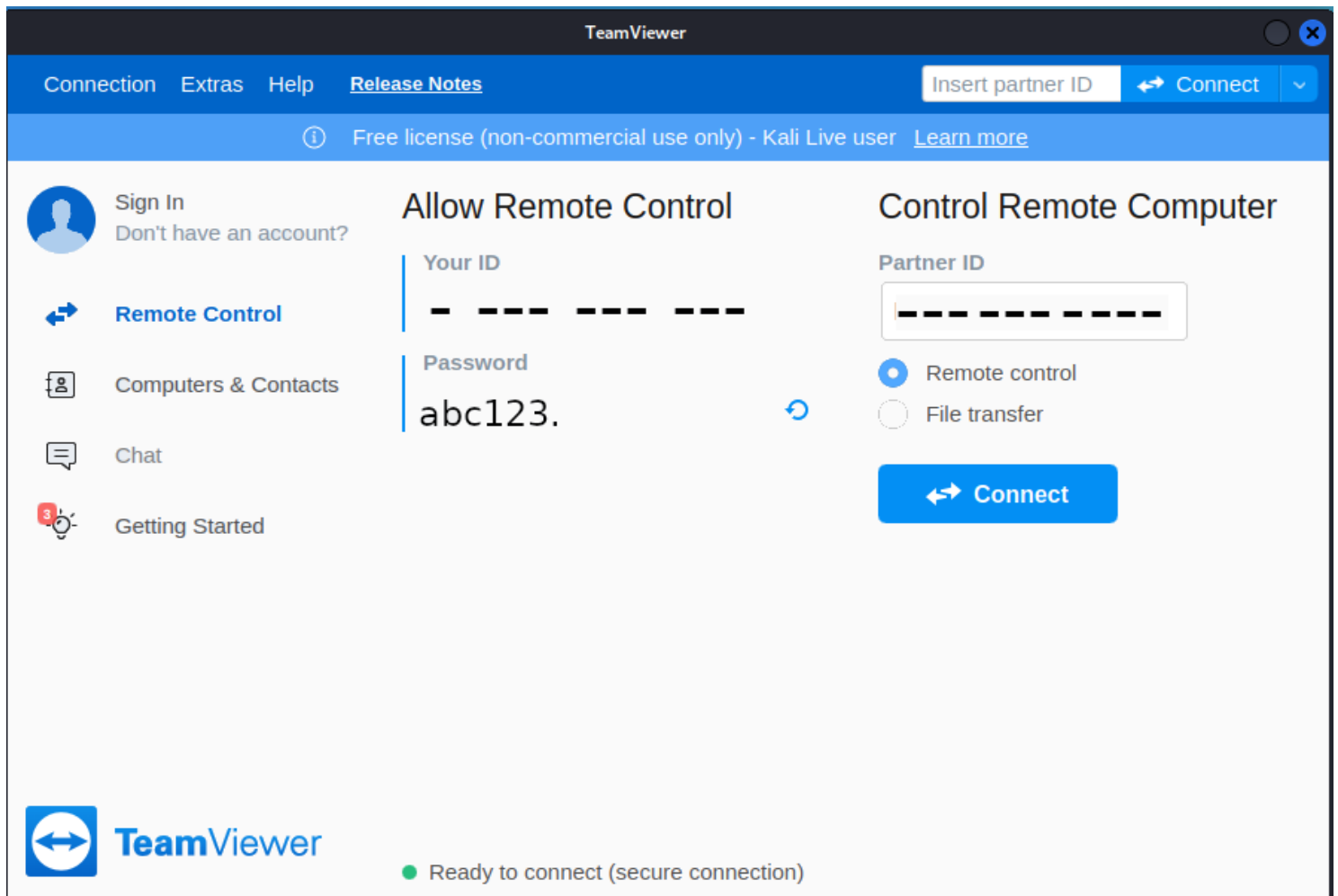
```
$ sudo dpkg -i /tmp/teamviewer_amd64.deb #Instalar teamviewer  
Accept License (I accept the EULA and the DPA) → Continue
```

(c) Executar:

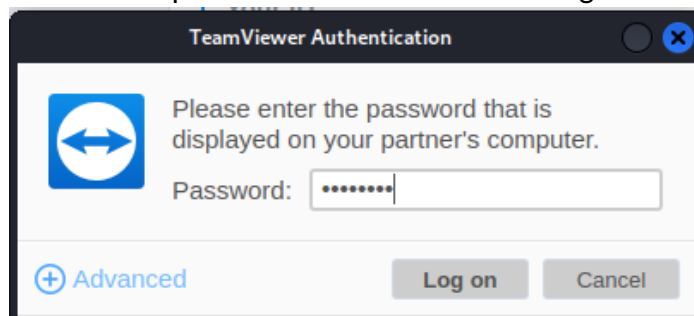
```
$ teamviewer &
```

(d) Acceder de forma remota a cada máquina virtual Practica44-RAC-MW-AlumnoXY mediante o ID conseguido en cada máquina virtual realizando o apartado (5c):

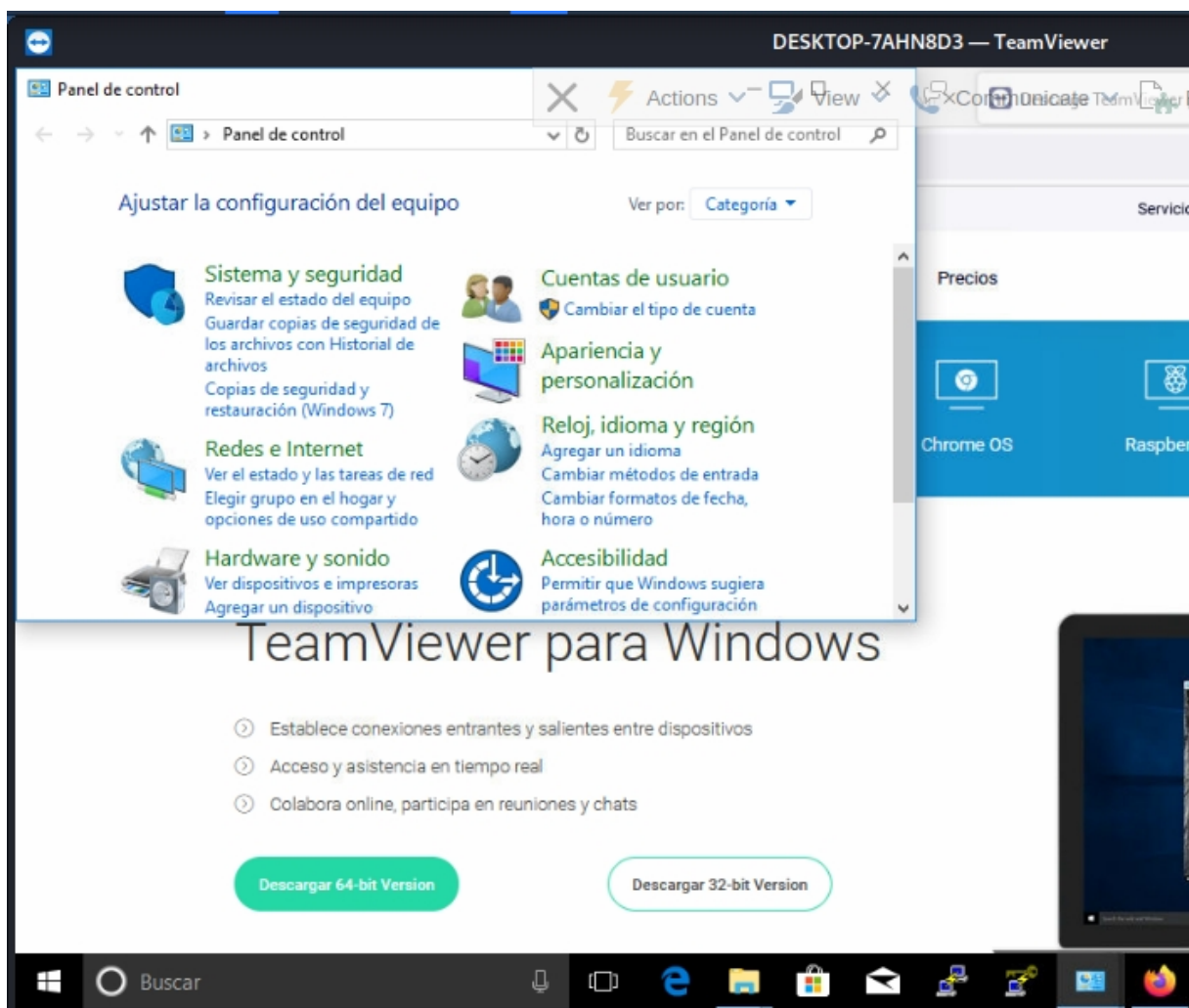
- I. Escribir o ID do apartado (5c) e picar en Connect:



- II. Introducir a password de teamviewer conseguida no apartado (5c) e facer clic en "Log on":



III. Agora deberíamos acceder de forma remota sen pechar a sesión do usuario conectado:



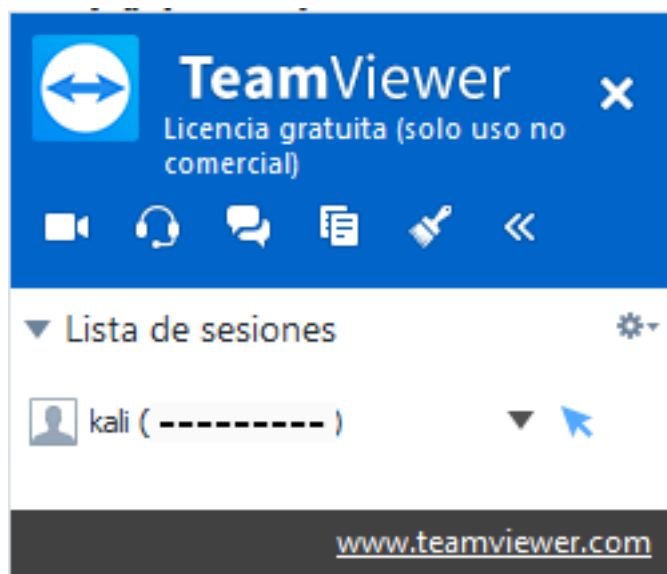
Acceso concedido.

Se non é posible realizar a conexión:

(1)Indicar que acontece?

(2)A que crees que pode ser debido que non se realice a conexión?

(e) Revisar o panel de TeamViewer.



(f) Avisar ao docente para revisión. ☐ 2

(7) Razoa e contesta brevemente:

- (a) Se foi posible a conexión, que pasa co usuario logueado cando se accede mediante TeamViewer? A sesión do usuario logueado será minimizada e bloqueada? E non poderá interactuar coa pantalla ata que a sesión de acceso remoto se peche?
- (b) Se foi posible a conexión, que pasa co usuario logueado cando se accede por acceso remoto con outro usuario distinto ao logueado? A sesión do usuario logueado será minimizada e bloqueada? E non poderá interactuar coa pantalla ata que a sesión de acceso remoto se peche?
- (c) Se foi posible a conexión, na sesión de acceso remoto teremos acceso a todos os recursos e ficheiros do equipo? É seguro?
- (d) Cantas conexións de acceso remoto permite TeamViewer?
- (e) Se se desexa permitir mais dunha conexión simultánea, débese utilizar outra edición distinta á gratuita?
- (f) Se foi posible a conexión, se dende o portátil intentamos comprobar a conectividade de rede coas máquinas virtuais dos hosts do alumnado Practica44-RAC-MW-AlumnoXY executando nunha consola o seguinte comando:

```
$ ping -c4 10.0.2.15 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede hacia unha máquina virtual configurada como NAT.
```

A que máquina virtual estamos a facer ping? É posible conectar? No caso de non ser posible, entón, como é factible ter control remoto desas máquinas dende o portátil empregando TeamViewer?

- (g) Portátil: Comprobar que non existe ningunha conexión mediante TeamViewer. Sé é o caso pechar esa/s conexión/s.

I. Executar o analizador de protocolos Wireshark[6] nunha consola:

```
$ sudo wireshark & #Lanzar o programa wireshark (sniffer) para poder visualizar o que acontece na rede (protocolos, paquetes). O comando sudo permite executar o programa wireshark con permisos de root(administrador) e o caracter & serve para executar en segundo plano o programa e así devolver o prompt da consola para poder seguir traballando nela.
```

II. Na interface do Wireshark [6] escoller para a escoita na rede a NIC eth0

III. Play (icono azul aleta tiburón) en wireshark [6], é dicir, arrancam os wireshark.

IV. Realizar de novo os apartados (7a) e (7b).

V. Identificar no Wireshark [6]:

(1) Cales son os paquetes necesarios para establecer unha comunicación mediante TeamViewer.

(2) Cales son os portos empregados para establecer a comunicación remota mediante TeamViewer?

- (h) Pódese modificar o porto para o establecemento de conexión mediante TeamViewer? Se é o caso describe o procedemento e realiza as capturas de pantalla necesarias.

- (i) Avisar ao docente para a entrega e revisión da práctica. ☐ 3

Revisión:

☐ ¹ ☐ ² ☐ ³