TALLER SR – PRÁCTICA 43 – RAC Microsoft Windows Acceso usuarios sen permisos de administrador		
NÚMERO DE GRUPO	**FUNCIÓNS**	**Apelidos, Nome**
	Coordinador/a:	
	Responsable Limpeza:	
	Responsable Documentación:	

ESCENARIO:

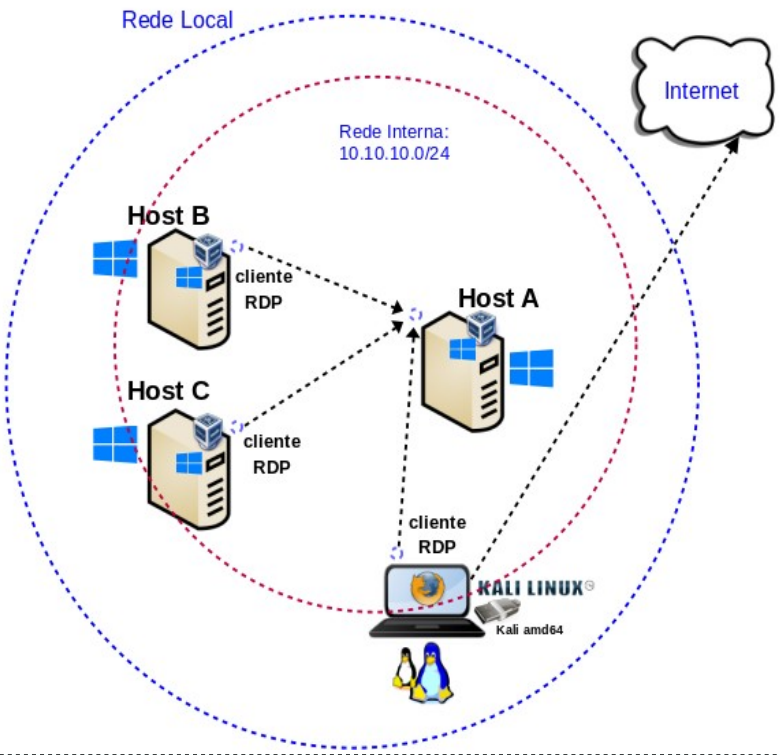
Portátil:
Intranet, Internet
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB
ISO: Kali Live amd64
Cliente RDP (remmina, xfreerdp)
IP/MS: 10.10.10.10/24

USB
Live Kali amd64

Hosts A, B, C:
∈ Intranet
⊃ Máquina virtual

Máquinas virtuais Microsoft Windows:
⊂ Host
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
Rede: Bridge
Disco duro: Windows amd64
IP/MS: 10.10.10.XY/24

Máquina virtual do Host A:
RAC activado (usuario, administrador)



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 Microsoft Windows – Acceso usuarios sen permisos de administrador
■ Portátil ■ Regleta ■ Switch 5-Port Gigabit ■ USB Live amd64 Kali ■ Hosts alumnado ■ Cableado de rede ■ [1] Microsoft Windows – Escritorio remoto ■ [2] Remmina ■ [3] FreeRDP ■ [4] Práctica 1 ■ [5] Actualizacións CredSSP ■ [6] Práctica Wireshark	(1) Prerrequisito: Ter realizada a Práctica 1 [4] (2) **NON conectar o switch á roseta da aula.** (3) Conectar portátil e hosts do alumnado ao switch. (4) Hosts alumnado: a) Crear máquinas virtuais coa rede en modo “bridge” e especificacións según escenario. b) Arrancar máquina virtual. c) Configurar a rede según o escenario. (5) Host A alumnado: Máquina virtual: RAC - Permitir control de acceso remoto a usuarios sen permiso de administrador. (6) Portátil: a) Arrancar co USB Live amd64 Kali b) Instalar Remmina e FreeRDP c) Acceso de forma remota á máquina virtual do host A mediante Remmina e FreeRDP. (7) Hosts B, C alumnado: Máquinas virtuais: Acceso de forma remota á máquina virtual do host A.

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 [4] .

(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) Instalar Remmina. Executar na consola anterior:

```
$ echo 'sudo apt update
sudo apt -y install snapd
sudo systemctl start snapd
sudo snap install remmina
sudo snap connect remmina:avahi-observe :avahi-observe # servers discovery
sudo snap connect remmina:cups-control :cups-control # printing
sudo snap connect remmina:mount-observe :mount-observe # mount management
sudo snap connect remmina:password-manager-service :password-manager-service # password manager
sudo snap connect remmina:audio-playback :audio-playback # audio sharing
sudo snap connect remmina:audio-record :audio-record # microphone
sudo snap connect remmina:ssh-keys :ssh-keys # ssh-keys
sudo snap connect remmina:ssh-public-keys :ssh-public-keys #ssh-public-keys' > install-remmina.sh
$ bash install-remmina.sh
```

(d) Instalar FreeRDP. Executar na consola anterior:

```
# apt update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
# apt search freerdp #Buscar calquera paquete que coincida co patrón de búsqueda freerdp
# apt -y install freerdp2-x11 #Instalar o paquete freerdp2-x11. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
```

(e) Avisar ao docente para a revisión. ☐[1]

(3) **Conectar no mesmo segmento de rede o portátil e os hosts do alumnado.**

(a) **NON conectar o switch á roseta da aula.**

(b) Conectar os vosos equipos de alumnado ao switch.

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

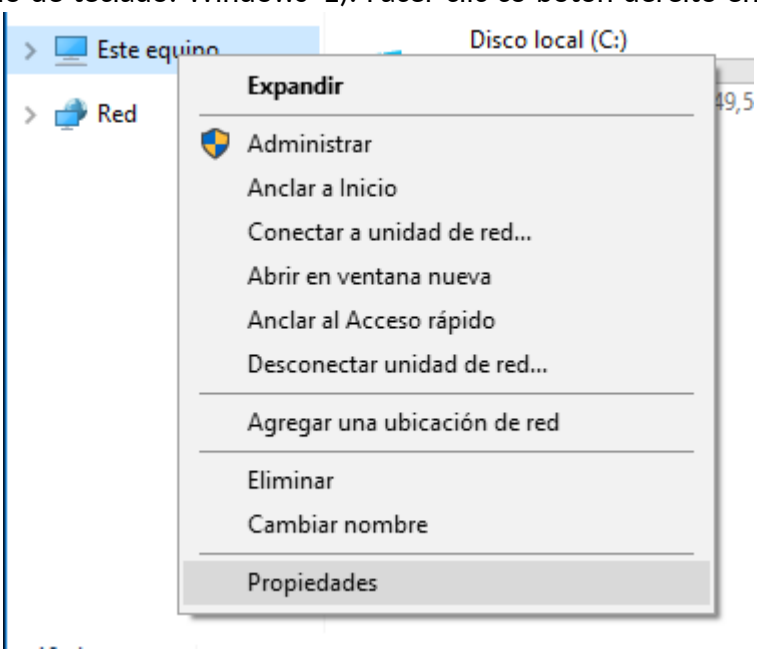
I. RAM ≥ 2048MB
II. CPU ≥ 2
III. PAE/NX habilitado
IV. Rede: Soamente unha tarxeta activada en modo bridge (ponte)
V. Disco duro: Microsoft Windows 10
VI. Nome: Practica43-RAC-MW-AlumnoXY, *o valor XY é o valor do PC que tedes asignado. Así, o alumno 17 terá como nome da máquina virtual: Practica43-RAC-MW-Alumno17*

(5) Host A alumnado:

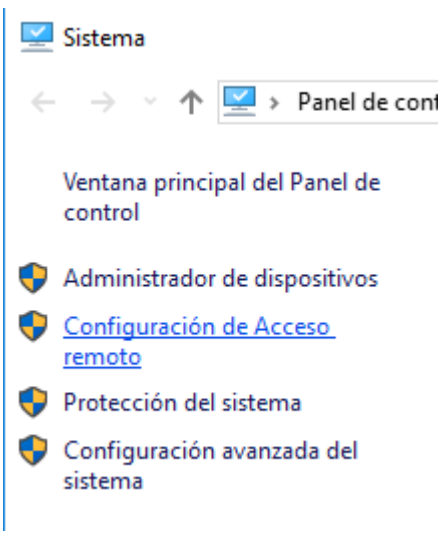
(a) Arrancar a máquina virtual.

(b) Configurar a tarxeta de rede según o escenario → Rede: 10.10.10.XY/24, *o valor XY é o valor do PC que tedes asignado. Así, o alumno 17 terá como IP a IP: 10.10.10.17*

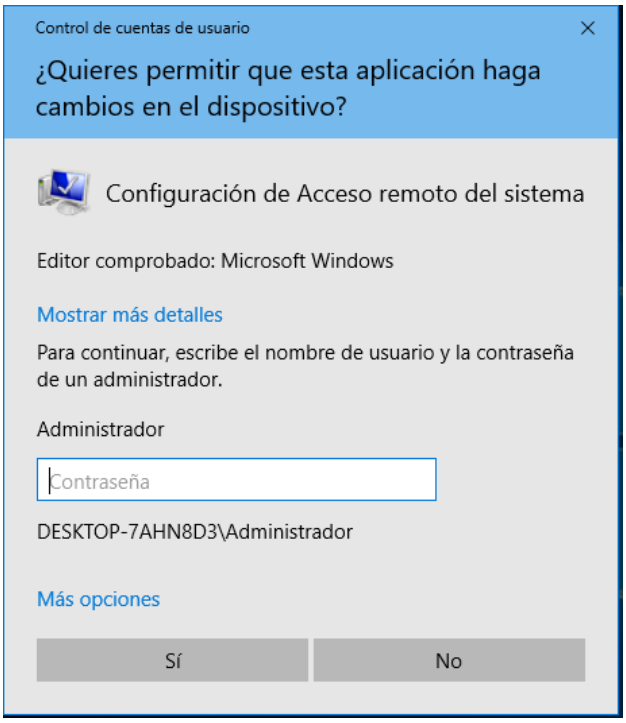
(c) Abrir un explorador de arquivos (Atallo de teclado: Windows+E). Facer clic co botón dereito en "Este Equipo" e seleccionar "Propiedades".



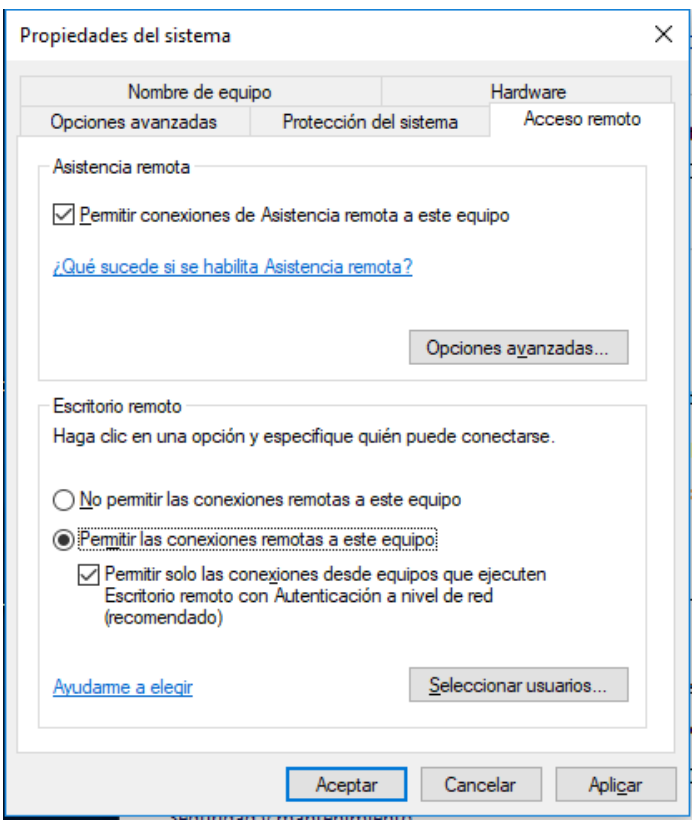
(d) Seleccionar "Configuración de Acceso remoto".



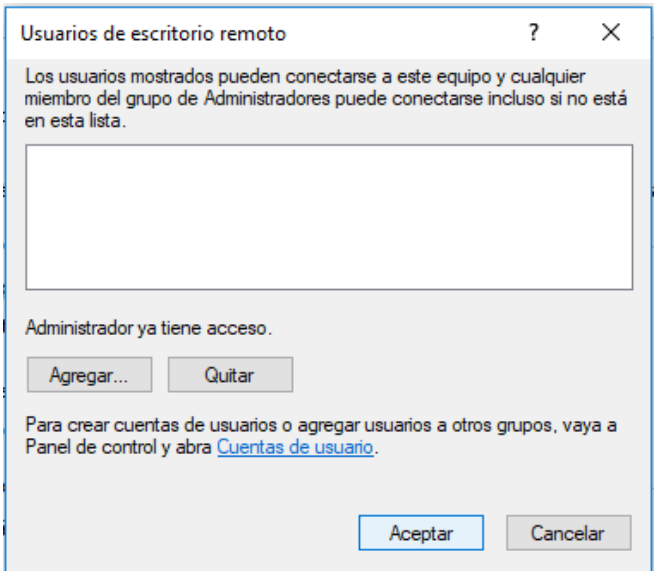
(e) Permitir o acceso á configuración introducindo o contrasinal do usuario con permisos de administración.



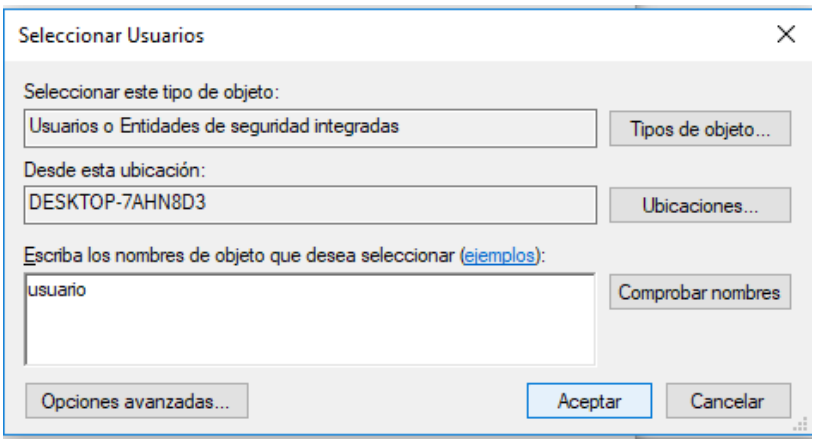
(f) Na sección "Escritorio remoto", seleccionar "Permitir las conexiones remotas a este equipo".



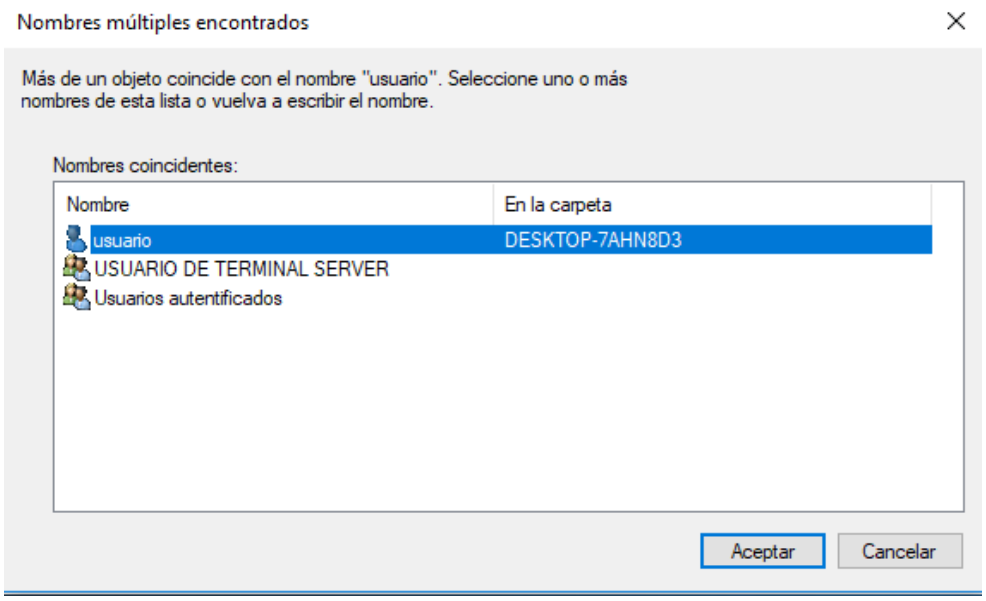
(g) Picar en “Seleccionar usuarios”.



(h) Premer en “Agregar” para permitir o acceso aos usuarios de sistema. Escribir ou buscar o usuario a permitir o accceso (neste caso o usuario de sistema de nome: usuario).

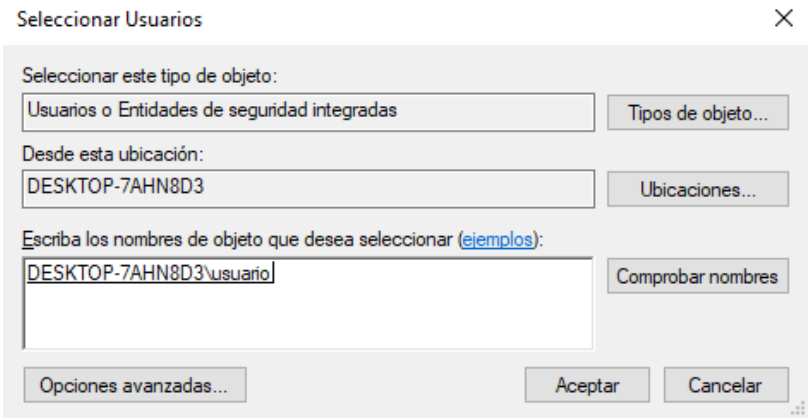


(i) Facer clic en “Comprobar nombres”.

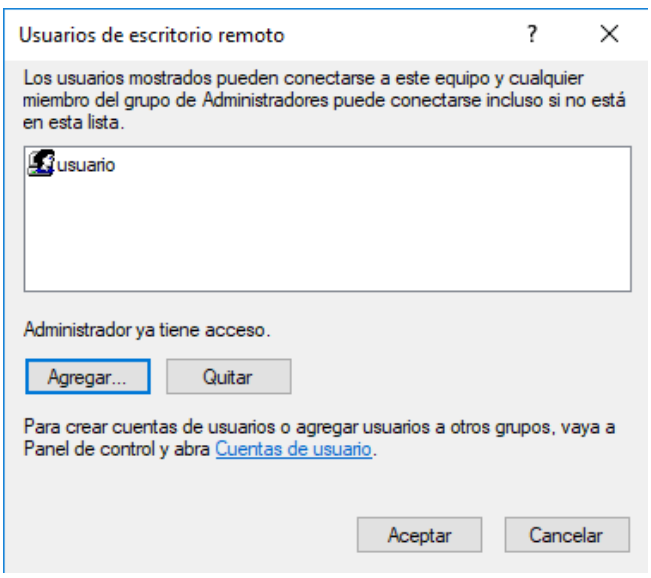


(j) Aceptar

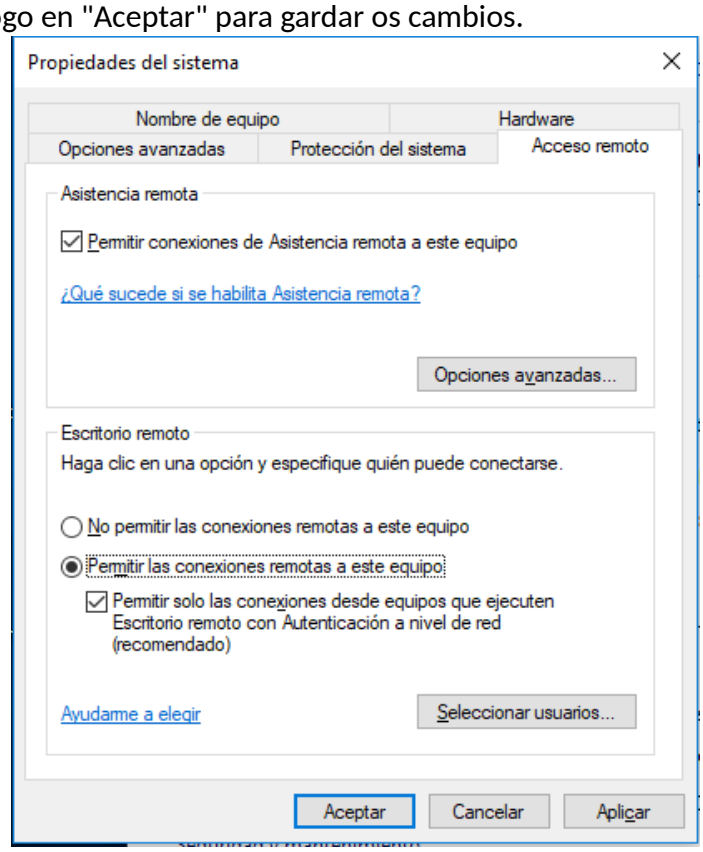
(k) Agora debe aparecer o nome do usuario escollido para otorgarlle o permiso de acceso a Escritorio Remoto. Entón, facer clic en “Aceptar”.



(l) Aceptar.



(m) Facer clic en "Aplicar" e logo en "Aceptar" para gardar os cambios.



(n) Se é o caso permitir o acceso a distancia a través dun firewall de Windows.

(6) Portátil: Configurar a rede según o escenario. 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)
# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.
# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.
# ip addr add 10.10.10.10/24 dev eth0 #Configurar a tarxeta de rede eth0, coa IP: 10.10.10.10 e máscara de subrede: 255.255.255.0.
# ip addr show eth0 #Amosar información sobre a NIC eth0. Verificar a configuración de rede para a NIC eth0
```

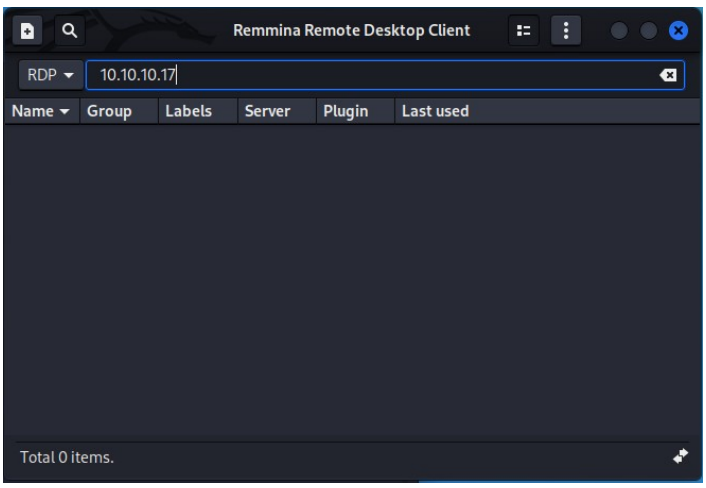
(7) Portátil:

(a) Arrancar o cliente Remmina. Executar nunha consola:

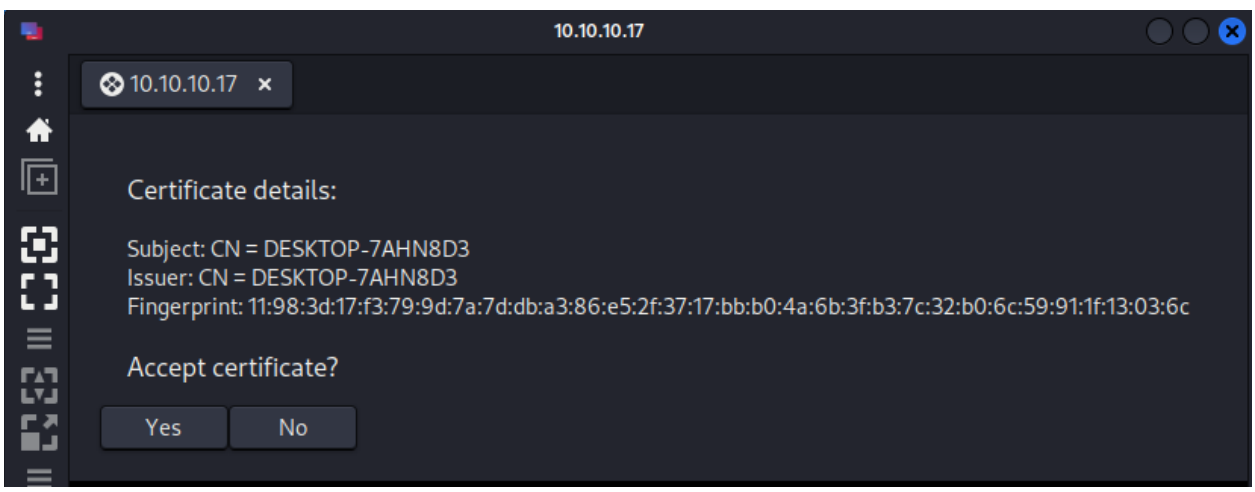
```
$ /snap/bin/remmina &
```

(b) Acceder de forma remota a cada máquina virtual `Practica43-RAC-MW-AlumnoXY`

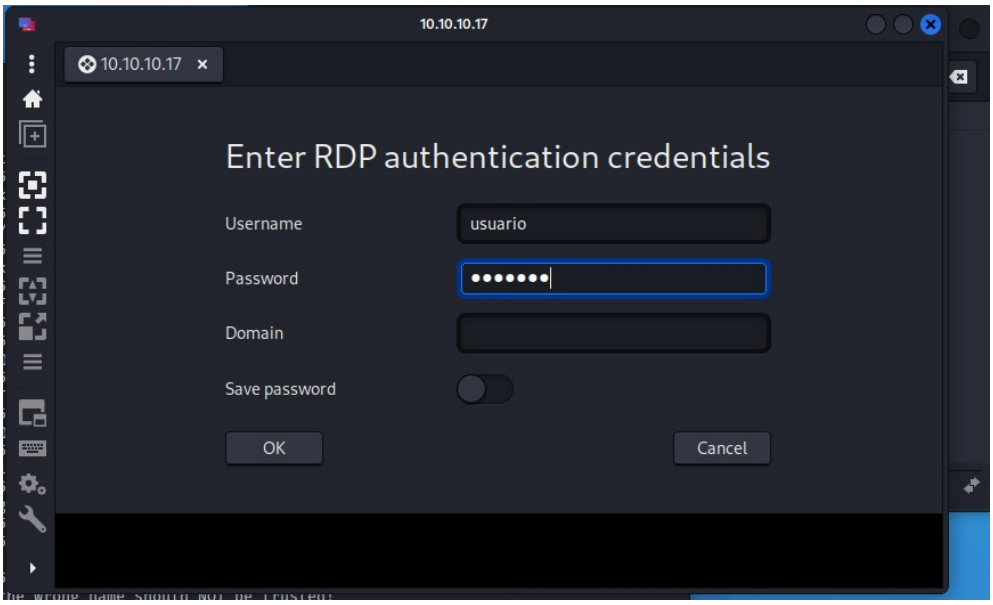
I. Escribir a dirección IP do equipo Microsoft Windows a conectar de forma remota: 10.10.10.XY



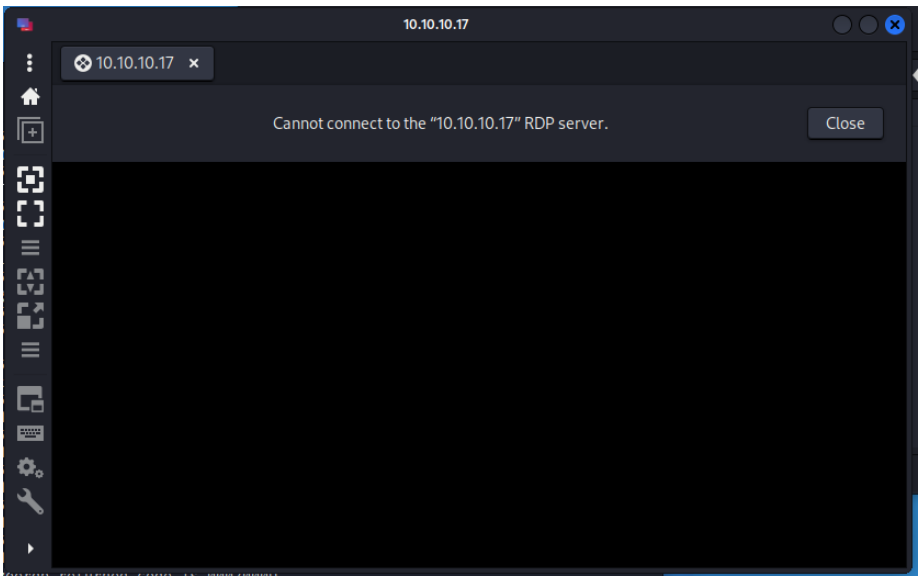
II. Confiar no certificado.



III. Introducir as credenciais de inicio de sesión cun usuario sen permisos de administrador.

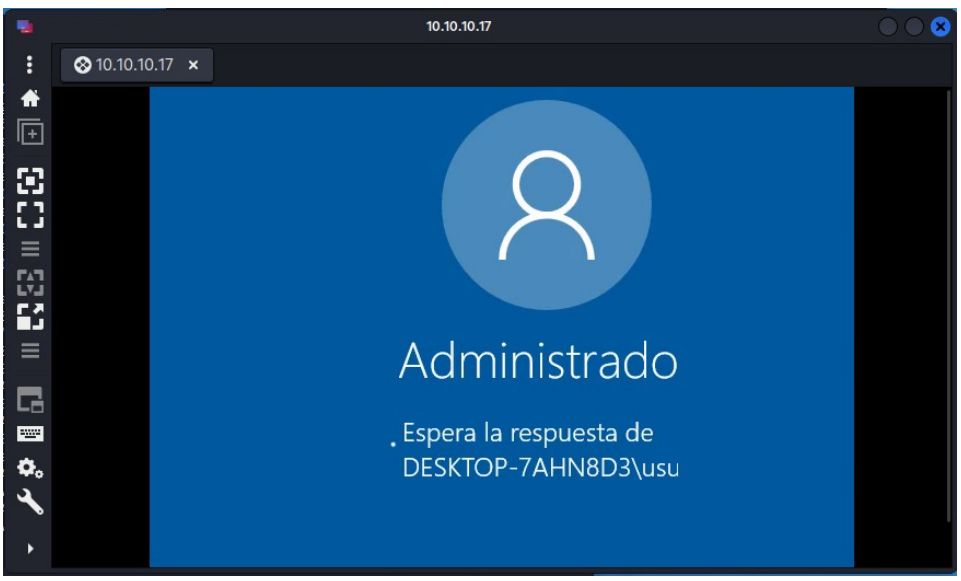


IV. Facer clic en "OK".



NOTA: Agora a conta usuario sen permisos de administrador si ten permitido o acceso de conexión remota.

V. Acceso concedido.



(c) Avisar ao docente para revisión. ☐ 2

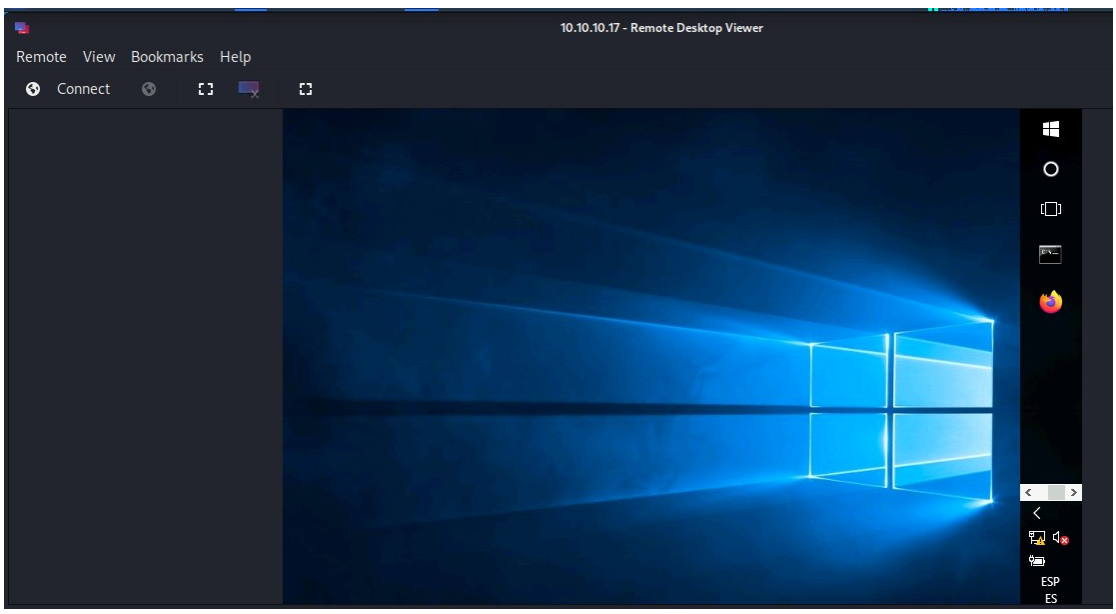
(d) Cliente FreeRDP: Acceder de forma remota a cada máquina virtual Practica42-RAC-MW-AlumnoXY

I. Executar nunha consola (escribir a dirección IP do equipo Microsoft Windows a conectar de forma remota: 10.10.10.XY e introducir as credenciais de inicio de sesión cun usuario sen permisos de administrador.)

```
$ xfreerdp /u:usuario /p:abc123. /v:10.10.10.17
...
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) Y
...
```

NOTA: Agora a conta usuario sen permisos de administrador si ten permitido o acceso de conexión remota.

I. Acceso concedido.



(e) Avisar ao docente para revisión. ☐ 3

(8) Hosts B e C do alumnado: Máquinas virtuais dos hosts do alumnado.

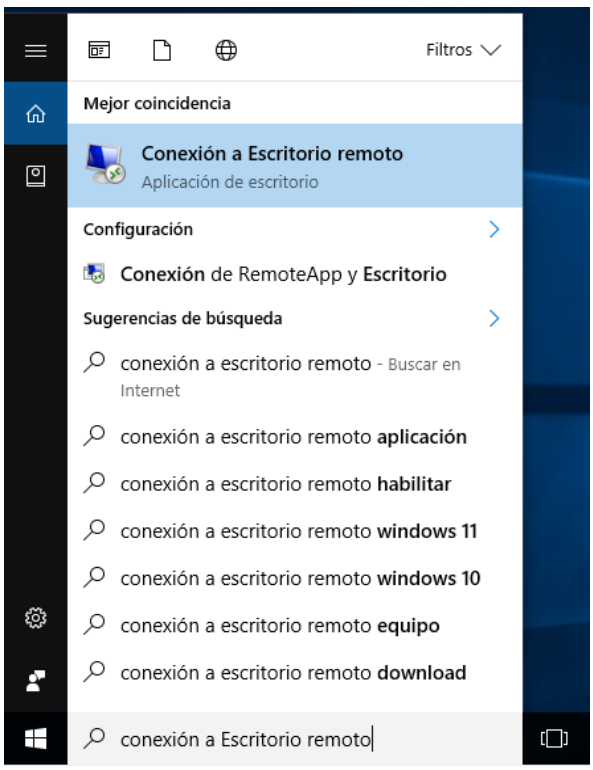
(a) Configurar a rede según o escenario.

(b) Comprobar a conectividade de rede coa máquina virtual do Host A. Executar nunha consola:

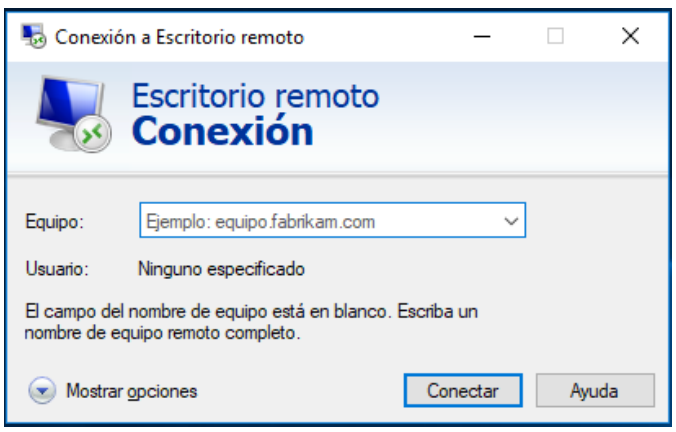
```
> ping 10.10.10.XY #O valor XY é o valor do PC que tedes asignado no host A. Así, o alumno 17 terá como IP: 10.10.10.17 Enviar 4 paquetes ICMP ECHO_REQUEST a 10.10.10.17, solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede hacia a máquina virtual do host A.
```

(c) Acceder de forma remota á máquina virtual do Host A:

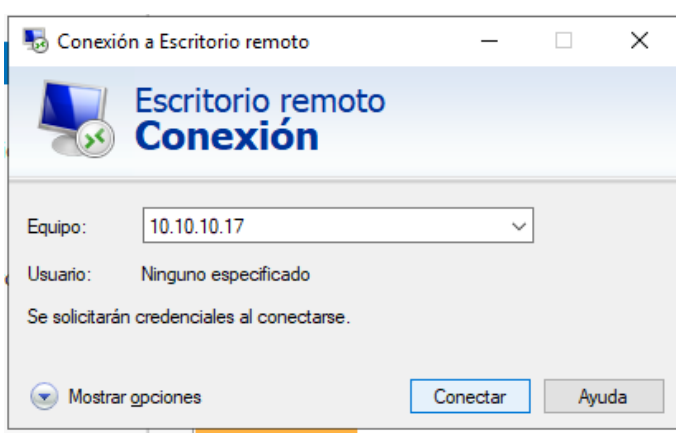
I. No recrado de búsqueda na barra de tarefas, escribir: Conexión a Escritorio remoto.



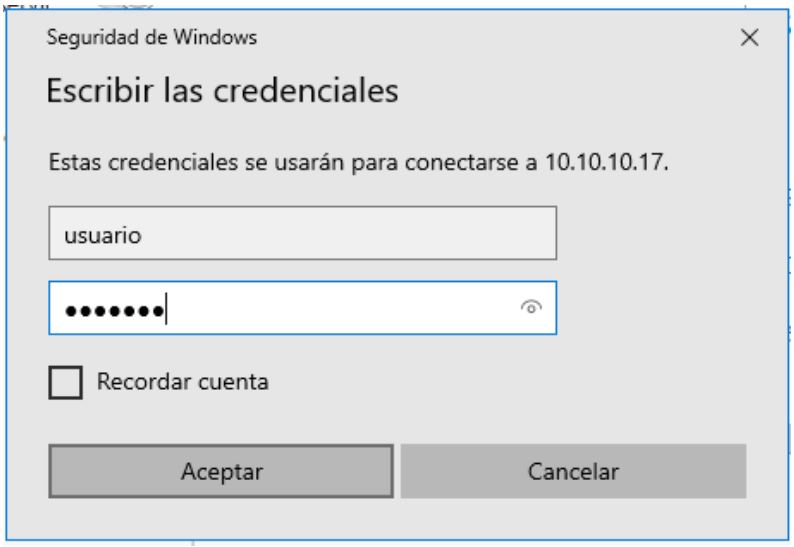
II. Seleccionar Conexión a Escritorio remoto.



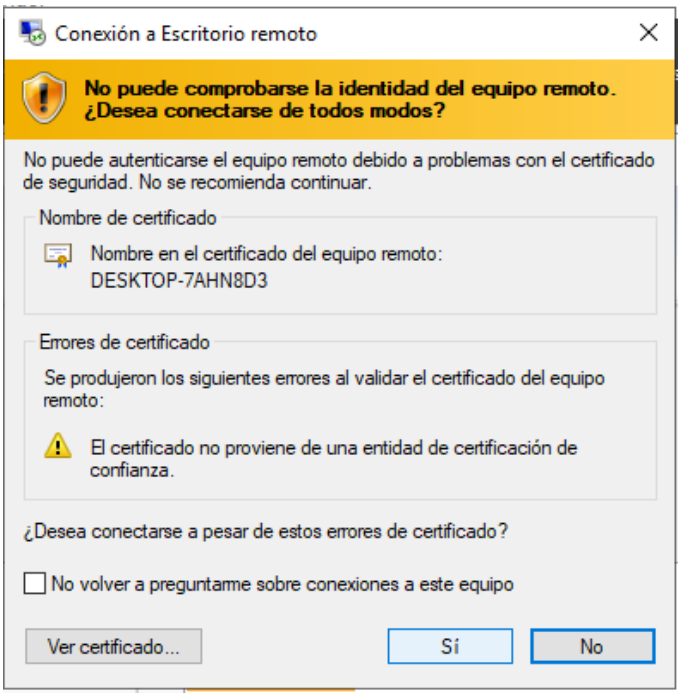
III. Escribir a dirección IP, ou nome, do equipo Microsoft Windows a conectar de forma remota: 10.10.10.XY



IV. Introducir as credenciais de inicio de sesión cun usuario sen permisos de administrador.



V. Confiar no certificado.



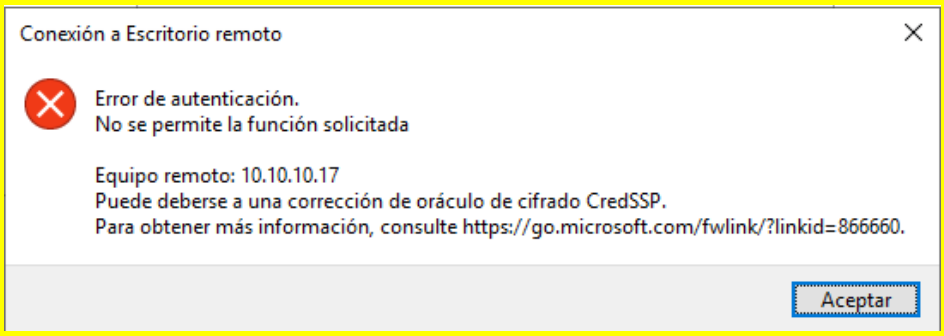
VI. Facer clic en "Sí".

NOTA: Agora a conta usuario sen permisos de administrador si ten permitido o acceso de conexión remota.

VII. Acceso concedido.

(d) Avisar ao docente para revisión. ☐ 4

NOTA: Pode darse o caso que o cliente de Microsoft Windows amose o seguinte erro:



Neste caso revisar a ligazón do erro [5], buscar a solución e documentala.

(9) Razoa e contesta brevemente:

(a) Que pasa co usuario logueado cando se accede co mesmo usuario por acceso remoto? 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) 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) Na sesión de acceso remoto teremos acceso a todos os recursos e ficheiros do equipo? É seguro?

(d) Cantas conexións de acceso remoto permite un equipo windows 10? Windows 10 Home permite soamente unha conexión de acceso remoto simultánea?

(e) Se se desexa permitir mais dunha conexión simultánea, débese utilizar a edición Pro ou Enterprise de Windows 10? Estas edicións permiten ata 2 conexións simultáneas por defecto? E poden admitir ata 256 conexións mediante a configuración adicional de licenzas de Terminal Server?

(f) Portátil:

I. Comprobar que non existe ningunha conexión a Escritorio Remoto. Sé é o caso pechar esa/s conexión/s.

II. 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.
```

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

IV. Play (icono azul aleta tiburón) en wireshark [6], é dicir, arrancamos o wireshark.

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

VI. Identificar no Wireshark [6]:

(1) Cales son os paquetes necesarios para establecer unha comunicación entre cliente e servidor RDP.

(2) Cales son os portos empregados polos clientes e servidor para establecer a comunicación Conexión a Escritorio Remoto (RDP)?

(g) Pódese modificar o porto para o establecemento de conexión RDP? Se é o caso describe o procedemento e realiza as capturas de pantalla necesarias.

(h) Avisar ao docente para a entrega e revisión da práctica. ☐ 5

Revisión:

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5