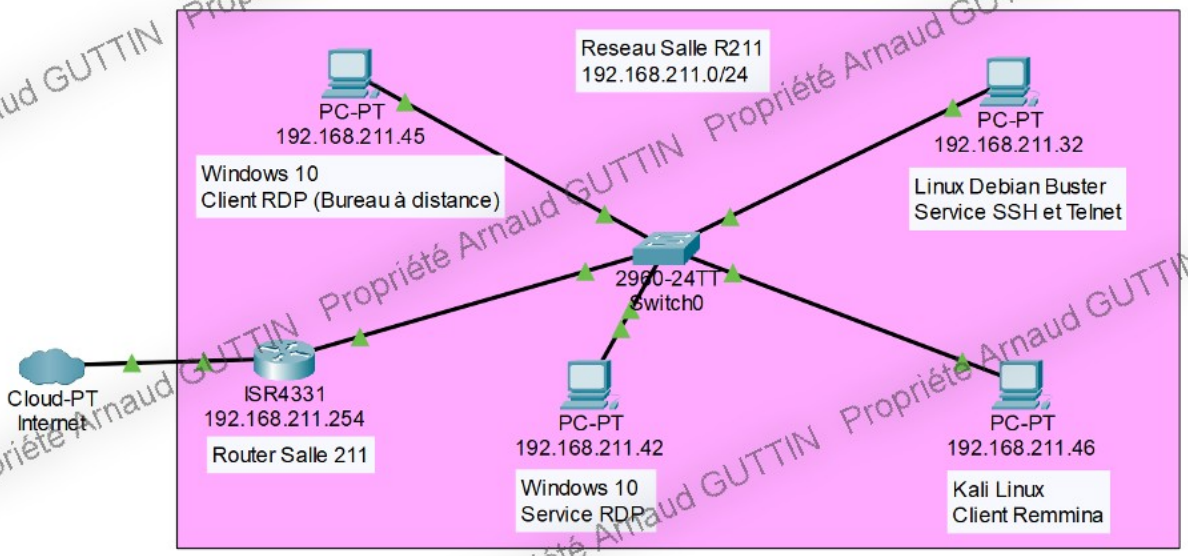
Les différentes méthodes de connexion à distance

Schéma réseau du laboratoire de test

Le réseau est constitué de quatre machines, une machine Windows équipé du service RDP, une autre machine Windows avec le client RDP. Une machine Debian équipée des services Telnet et SSH, et une machine Kali Linux équipée du client Remmina. Le réseau est relié au routeur pour rejoindre internet.



A quoi servent les connexions à distance ?

La connexion à distance est le principe de ce connecter à partir d'une machine hôte à un autre appareil connecté à un réseau.
Il est possible de se connecter à distance pour superviser l'appareil, le contrôler, faire du "helpdesk", ou transférer des données.
Cela permet donc à un utilisateur de se connecter à un ordinateur distant et d'interagir avec lui comme s'il était physiquement présent devant celui-ci.

Pour ce connecter il existe différents protocoles ou services de connexions à distance, tels que SSH, FTP (protocole de transfert de fichiers), Telnet, RDP, RFB (Remote Framebuffer, utilisé par VNC).

Telnet

Telnet (TErminaL NETwork) est un protocole permettant de se connecter à une machine à distance. On l'utilise le plus souvent pour l'administration à distance, la supervision des routeurs, switchs, pare-feu, mais aussi d'une simple machine.

Telnet à le désavantages, de ne pas sécurisé, c'est à dire que l'intégralité des données transmises sur le réseau, dont les mots de passes, sont transmis en clair, et lisible pour

toute personnes analysant le réseau. Il a donc été remplacé par le protocole SSH qui lui est sécurisé.

Telnet étant un protocole, il peut être mis en place sur n'importe quel système d'exploitation. Telnet fonctionne sous l'architecture, client-serveur, c'est à dire que lors de la connexion, la machine voulant se connecter cera le client, et la machine sur lequel on se connecte sera le serveur.

Lorsque la connexion Telnet est établie, les commandes entrées dans un terminal seront envoyées au serveur distant Telnet, qui traitera les commandes et renvoie les résultats au client.

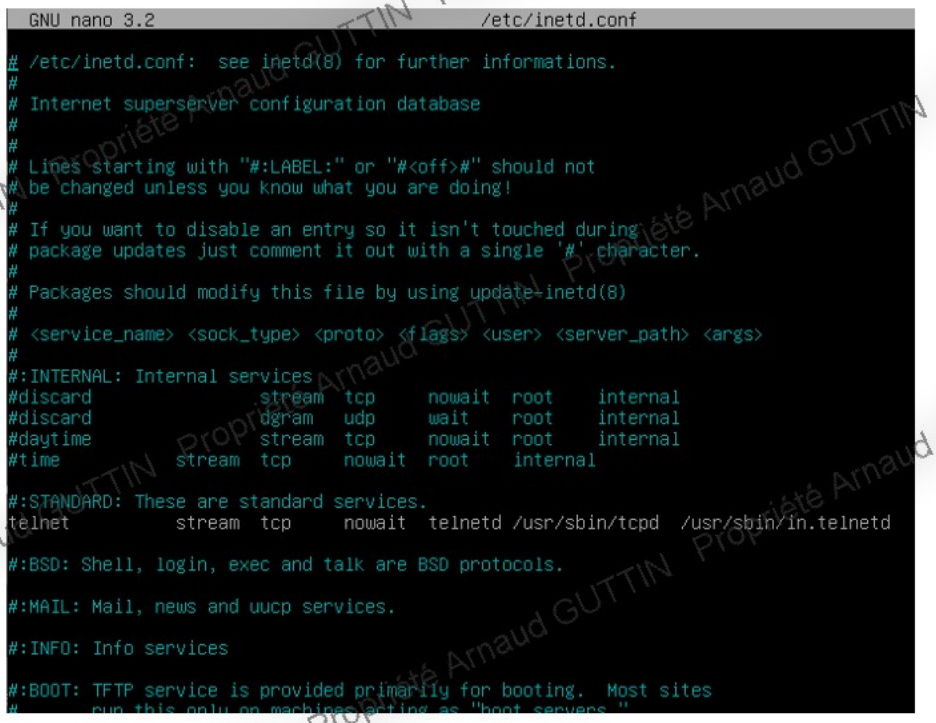
Installation de Telnet

Pour installer le service telnet sur une machine debian, il faut actualiser les liste de paquets avec la commande `apt update`.
Ensuite, il faudra entrer la commande `apt install telnetd`, (vous pouvez ajouter le paramètres -y pour valider l'installation par défaut).

```
root@buster:~# apt update -y && apt install telnetd -y
```

Si vous souhaitez modifier la configuration du service telnet, comme interdir certaines connexions venant d'un réseau ou autre, vous pouvez éditer le fichier de configuration avec l'éditeur nano et au chemin /etc/inetd.conf, (voir ci dessous).

Commande: `nano /etc/inetd.conf`



Une fois la modification du fichier de configuration modifié, il faudra redémarrer le service telnet, grâce à la commande, `systemctl restart inetd`.

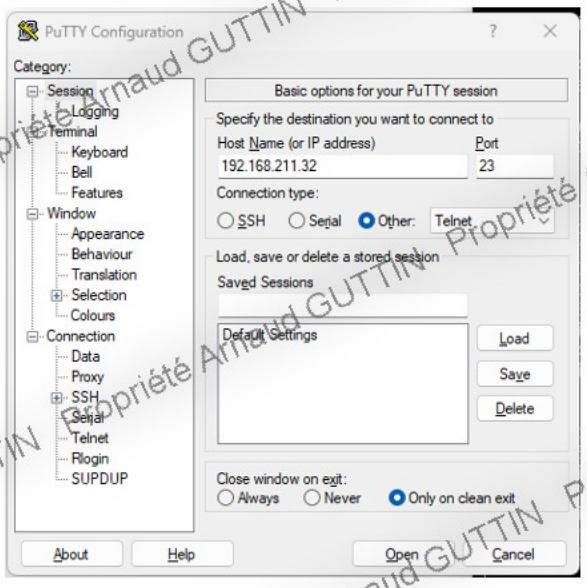
Lorsque l'installation est terminée, il faudra activer le service avec la commande systemctl enable inetd.
Si vous souhaitez vérifier l'état de fonctionnement du service , vous pouvez entrez la commande, `systemctl status inetd`, (voir ci-dessous).

```
root@buster:~# systemctl restart inetd
root@buster:~# systemctl enable inetd
root@buster:~# systemctl status inetd
● inetd.service - Internet superserver
   Loaded: loaded (/lib/systemd/system/inetd.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-09-05 15:01:29 CEST; 18s ago
     Docs: man:inetd(8)
 Main PID: 1041 (inetd)
    Tasks: 1 (limit: 2359)
   Memory: 496.0K
   CGroup: /system.slice/inetd.service
           └─1041 /usr/sbin/inetd

sept. 05 15:01:29 buster systemd[1]: Starting Internet superserver...
sept. 05 15:01:29 buster systemd[1]: Started Internet superserver.
root@buster:~# _
```

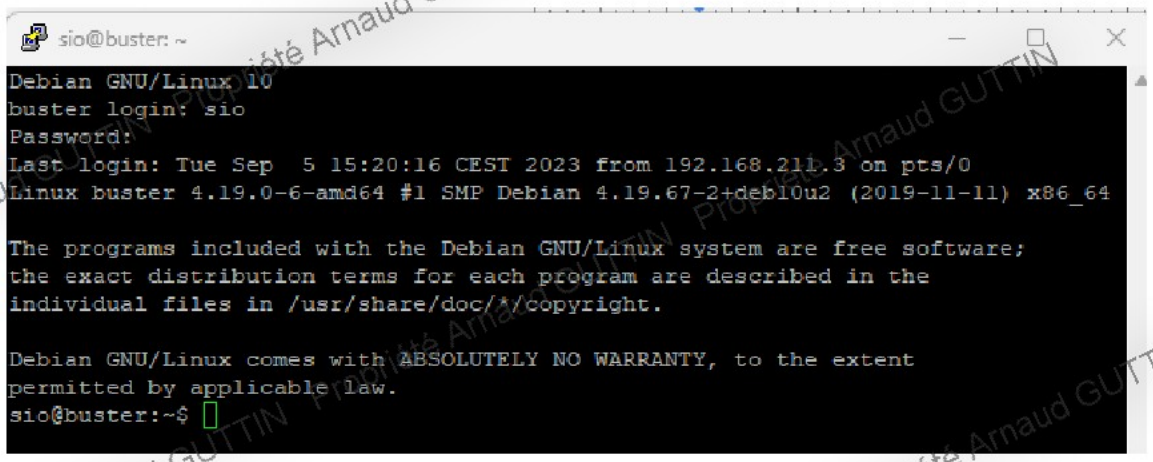
Connexion avec un client Telnet

Pour vous connecter à une machine grâce à Telnet, vous aurez besoin d'avoir un client telnet.
Il est possible de le télécharger dans un Terminal ou d'installer un logiciel tier, comme ici Putty.

Il faudra ensuite entrer l'adresse IP de la machine distante, puis préciser le port, Telnet utilise le port 23, (voir ci-dessous).



Vous pouvez ensuite vous connecter en entrant le login et mot de passe d'un utilisateur local, (voir ci-dessous). Attention ! Vous ne pouvez pas vous connecter avec l'utilisateur root pour des raisons de sécurité.



SSH

Le protocole SSH, (Secure Shell) est un protocole de communication utilisé pour sécuriser les communications à distance sur des réseaux.
SSH certifie la confidentialité des données transmises car il utilise le chiffrement asymétrique grâce à des clés de chiffrement. Il certifie aussi l'exactitude et l'intégrité des données car la connexion SSH est basée sur le protocole TCP qui s'assurera que les données sont bien transmises.
Il est utilisé pour l'accès à distance à des systèmes, la gestion de serveurs, le transfert de fichiers sécurisé, et d'autres.

Ce protocole est basé sur l'architecture client-serveur. Il faudra donc que la machine à distance soit équipée du service SSH et que la machine se connectant possède un client SSH.

Installation et configuration de SSH

Pour installer SSH sur Debian, il faut tout d'abord actualiser les liste des paquets puis ensuite installer le service SSH.
Pour ce faire entrez la commande: `apt update -y && apt install openssh-server -y`
Le paramètres -y permet de valider les autorisations requise par défaut, les symboles && permettent d'enchaîner plusieurs commandes à la suite pour ne pas attendre chaque exécution de commande.

```
root@buster:~# apt update -y && apt install openssh-server -y
```

Pour vérifier l'état du service SSH, il faudra entrer la commande, `systemctl status sshd`.
Si le service n'est pas démarré, vous pouvez entrer la commande `systemctl start sshd`, (voir ci-dessous).

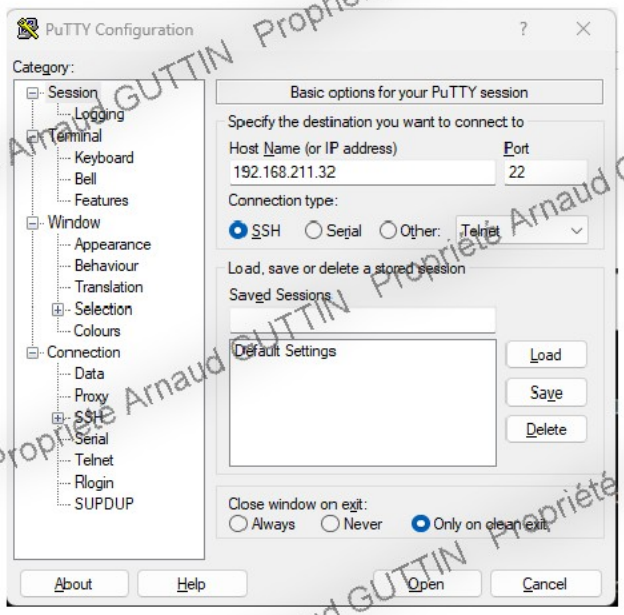
```
root@buster:~# systemctl start sshd
root@buster:~# systemctl enable sshd
Failed to enable unit: Too many levels of symbolic links
root@buster:~# systemctl start sshd
root@buster:~# systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2023-09-08 13:58:58 CEST; 1min 0s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 1039 (sshd)
    Tasks: 1 (limit: 2359)
   Memory: 2.9M
   CGroup: /system.slice/ssh.service
           └─1039 /usr/sbin/sshd -D

sept. 08 13:58:58 buster systemd[1]: Starting OpenBSD Secure Shell server...
sept. 08 13:58:58 buster sshd[1039]: Server listening on 0.0.0.0 port 22.
sept. 08 13:58:58 buster sshd[1039]: Server listening on :: port 22.
sept. 08 13:58:58 buster systemd[1]: Started OpenBSD Secure Shell server.
```

Vous avez aussi la possibilité de configurer le service SSH pour le rendre plus personnalisable. Pour ce faire il faudra modifier le fichier au chemin /etc/ssh/sshd_config.
Il est possible d'ajouter différentes fonctionnalités, comme l'autorisation de connexion avec l'utilisateur root (refusé par défaut) en ajoutant le paramètres "PermitRootLogin" dans le fichier.

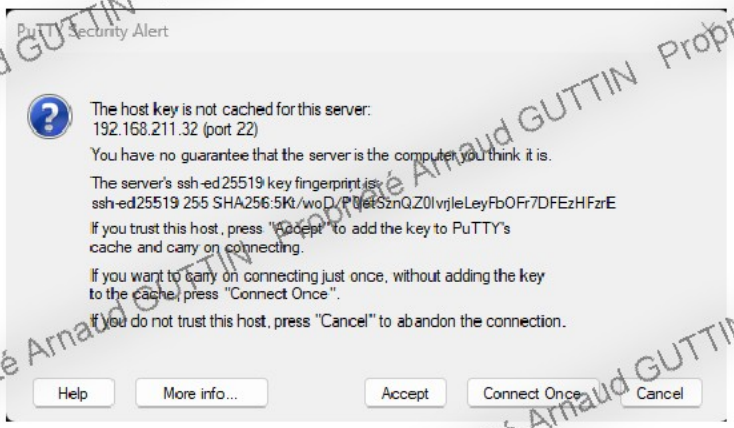
Connexion avec un client SSH

Pour se connecter à une machine possédant le service SSH, il faudra pocéder un client SSH. Il est souvent installé par défaut sur le Terminal, vous pouvez aussi installer un logiciel tier tel que Putty.

Vous pouvez entrer les informations de connexions tel que l'adresse IP et le port qu'utilise SSH (port 22), (voir ci-dessous).



Lors d'une connexion SSH il vous sera souvent demandé d'accepter le certificat de chiffrement, (voir ci-dessous).



Vous pouvez ensuite vous connecter avec un utilisateur local de votre machine distante, (voir ci-dessous).
Attention, si vous échouez plus de trois fois lors de l'authentification de la session, il faudra renouveler la connexion SSH avec la machine distante.

RDP

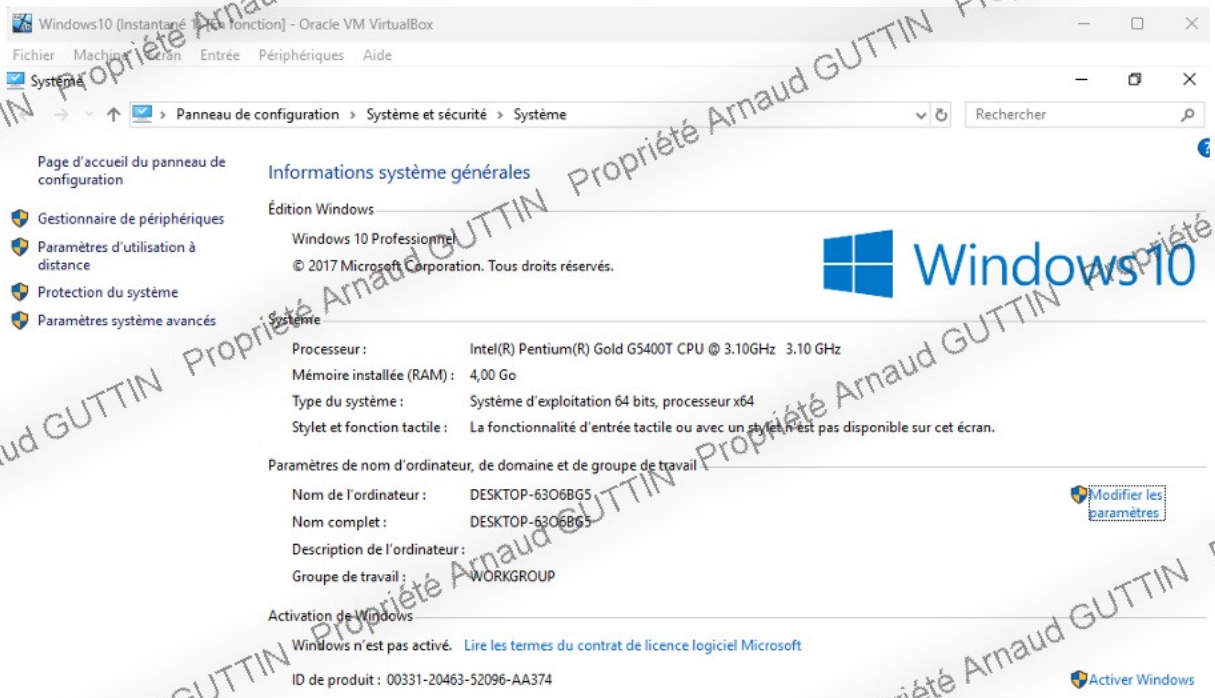
Le protocole RDP (Remote Desktop Protocol) est un protocole de connexion à distance. Il permet de se connecter à un hôte distant grâce à une interface graphique. Ce protocole est la propriété de Microsoft, il est donc utilisable uniquement par les machines Windows (depuis Windows NT4.0).

Ce protocole fonctionne sous l'architecture client-serveur, il utilise le port 3389 pour effectuer la connexion.

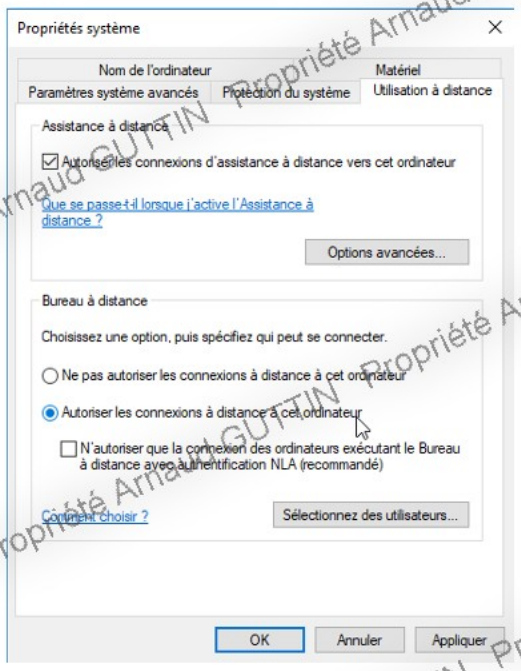
RDP est aussi utilisé par le service Remote Desktop Services anciennement Terminal Services de Windows Server, il permet la centralisation des sessions utilisateurs.
Souvent le serveur héberge une application et les utilisateurs se connecte depuis RDP. Cela est utile lorsqu'une application est lourde au fonctionnement et que les ressources matérielles sont limitées.

Installation et configuration de RDP

Par défaut, sur les machines Windows (client et serveur) le service d'utilisation à distance est déjà installé mais désactivé. Pour l'activer, il faudra vous rendre dans le Panneau de configuration, puis Système et sécurité puis Système. Ensuite, il faudra cliquer sur Modifier les paramètres (en bas à droite), (voir ci-dessous).



Il faudra ensuite ce rendre dans l'onglets Utilisation à distance, puis cocher la case, "Autoriser les connexions à distance vers cet ordinateur", (voir ci-dessous).



Connexion avec un client RDP

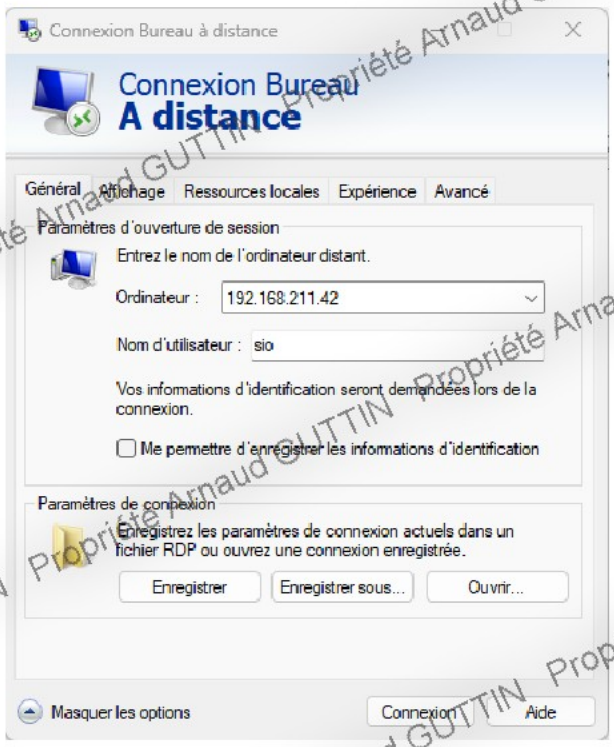
Pour vous connecter, si vous ne connaissez pas l'adresse ip de votre machine distante, vous pouvez ouvrir l'invite de commande puis entrer la commande ipconfig sur celle-ci. L'adresse IP est écrite à la ligne adresse IPv4, (voir ci dessous).

```
C:\Users\sio>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : BTSSIO.LOCAL
   Adresse IPv6 de liaison locale. . . . .: fe80::4817:8a77:35d1:114b%2
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.211.42
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.211.254

C:\Users\sio>
```

Sur toutes les machines Windows, le client RDP est déjà installé, pour ce faire, il faut ouvrir l'application Bureau à distance. Vous pouvez ensuite entrer l'adresse IP de votre machine Windows distante, entrer le nom d'utilisateur puis vous connecter, (voir ci-dessous).

Attention, lors de l'ouverture de la session RDP, la session locale sur la machine distante sera fermée.

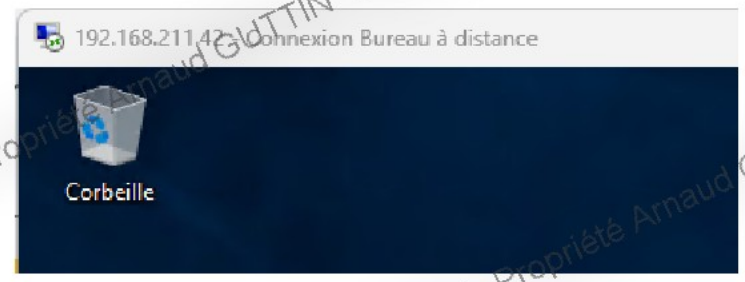
Vous avez aussi la possibilité d'enregistrer cette connexion en cliquant sur Enregistrer pour ne pas avoir à remplir les informations une nouvelle fois.



Il vous sera ensuite demandé d'entrer le mot de passe de la session locale sur laquelle vous vous connectez, (voir ci-dessous).

Il sera nécessaire d'autoriser le certificat de chiffrement pour se connecter à l'appareil distant, (voir ci-dessous).

Une fois la connexion réussie, une nouvelle fenêtre s'ouvrira pour laisser place à l'interface graphique de votre session distante, (voir ci-dessous).



VNC

VNC est une application de connexion à distance grâce à une interface graphique. C'est-à-dire que lors de la connexion, nous pouvons voir l'interface graphique de la machine distante.

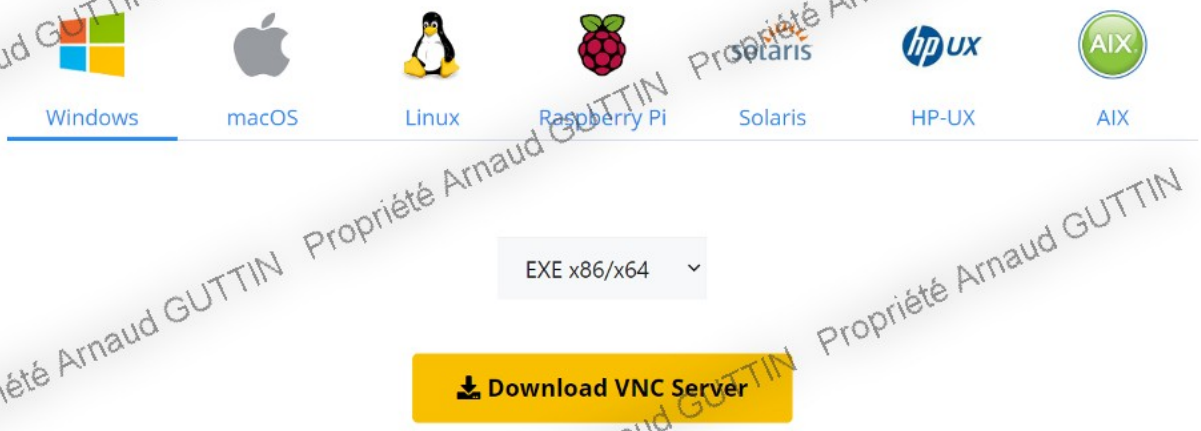
Il existe d'autres services similaires comme TeamViewer, Bureau à distance, Teams…

VNC est principalement utilisé pour faire du helpdesk (assistance à distance). Il est possible de l'installer sur différents systèmes d'exploitations, comme, Windows, Linux, MacOS, IOS, Android…

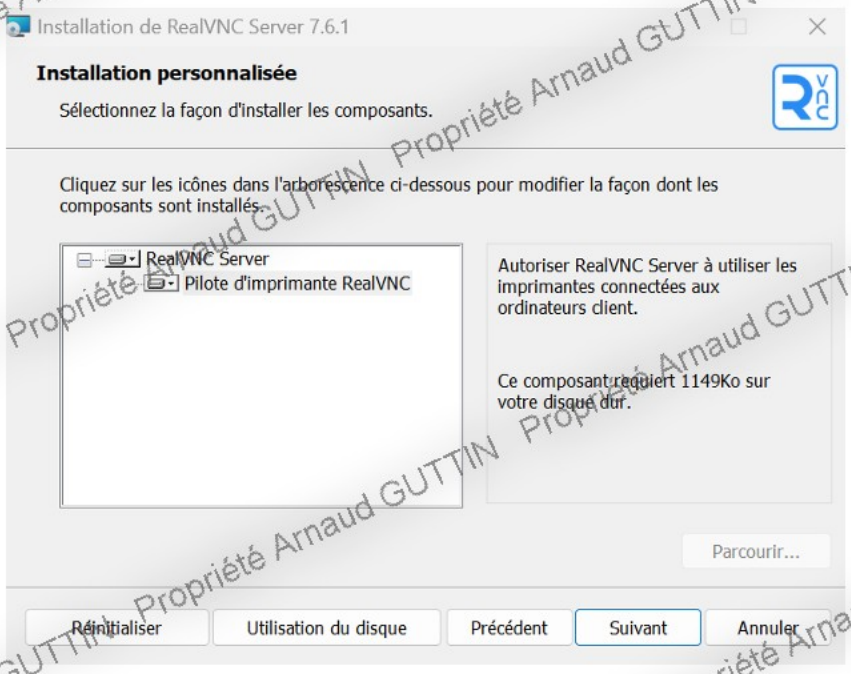
Ce service fonctionne sous l'architecture client-serveur; pour l'utiliser il faudra donc un service VNC et un client VNC. Les données sont transmises par le protocole d'application RFB, Remote Framebuffer. Ce protocole permet le transfert de l'image, la gestion de la souris et des entrées claviers.

Installation et configuration de VNC

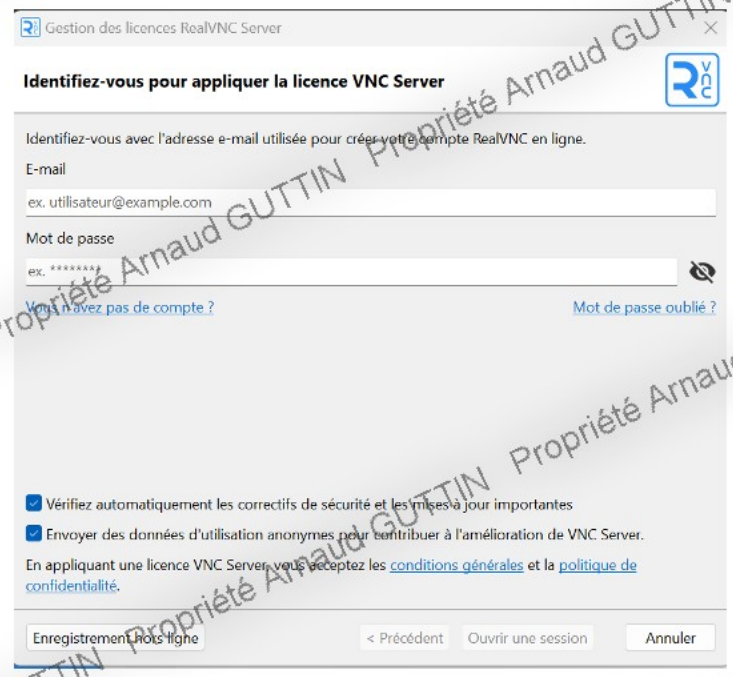
Pour télécharger VNC Server, veuillez vous rendre sur le site de VNC. Vous pouvez ensuite sélectionner le système d'exploitation sur lequel vous souhaitez installer votre serveur VNC, puis le télécharger, (voir ci-dessous).



Vous pouvez ensuite exécuter le fichier .exe, accepté le contrat de licence, puis validé l'installation personnalisé, (voir ci-dessous).

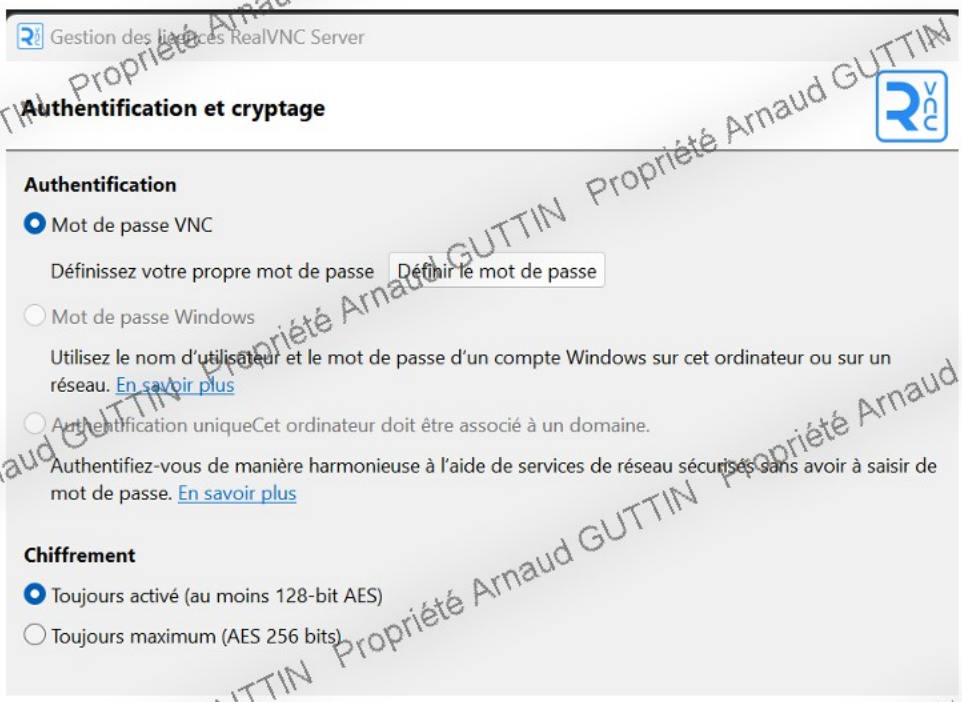


Une fois l'installation terminée, il vous sera demandé de vous connecter ou d'entrer une clé de licence, (voir ci-dessous).

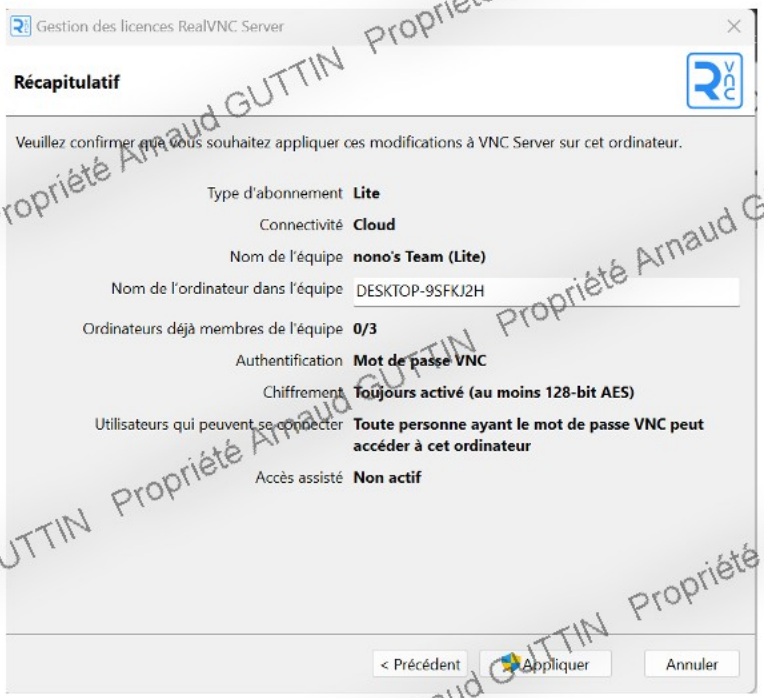


Il faudra alors vous créer un compte, vous rendre sur les paramètres de votre compte sur l'interface web et activer une licence, (il existe la licence Léger ou Home pour une utilisation non commercial), comme ci-dessous.

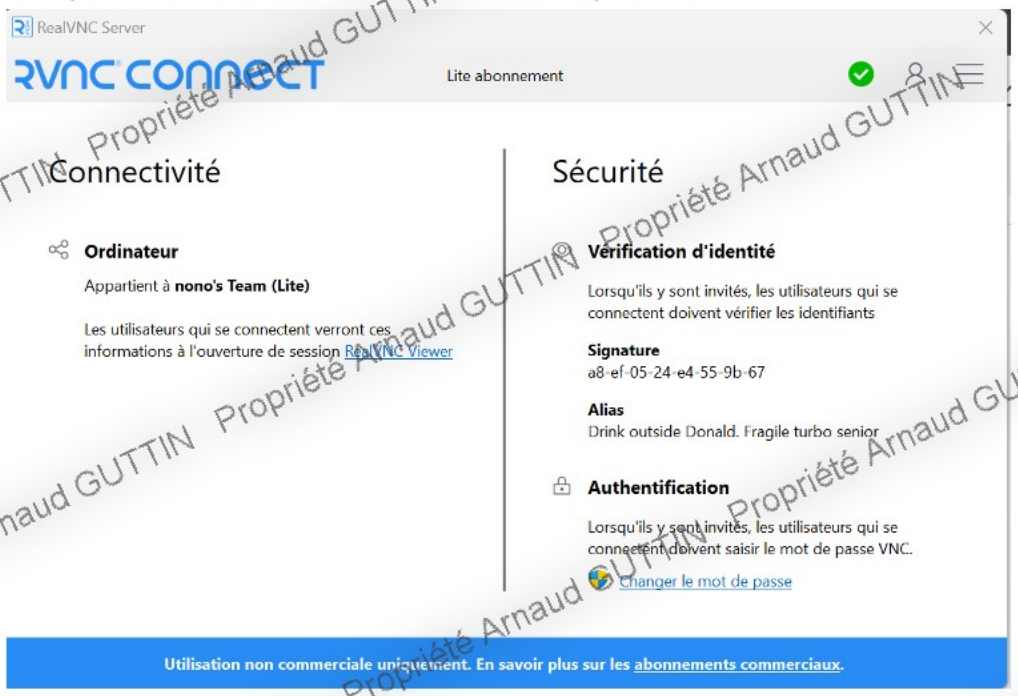
Une fois authentifié, sur VNC Server, il vous sera demandé de créer un mot de passe. Celui-ci permettra l'authentification des personnes voulant se connecter sur cette machine. Il est aussi possible de sélectionner le type de chiffrement voulu pour la connection entre le client et le serveur.



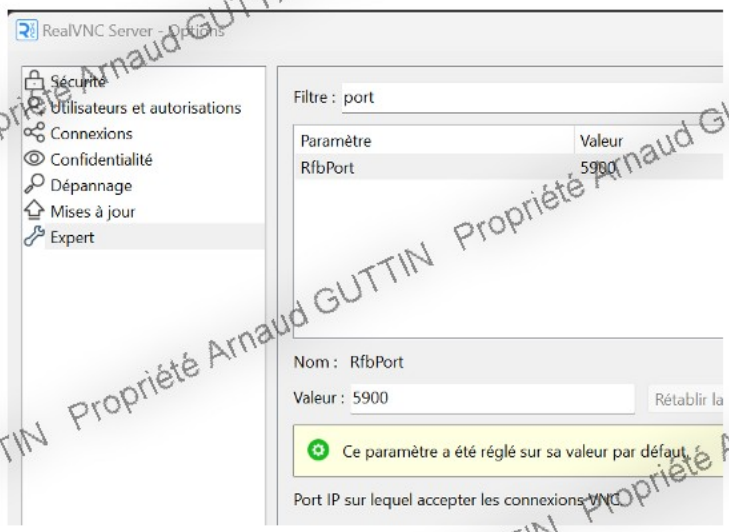
Lors de la fin de la configuration vous aurez une fenêtre vous résumant l'intégralité de la configuration de VNC Server pour cette machine, (voir exemple ci-dessous).



Si la page d'accueil de VNC Server indique le valide vert en haut a droite, c'est que la configuration est réussie. Vous pouvez noter la signature indiquer, celle-ci permet de se connecter à partir d'un réseau distant directement depuis internet.



Attention !
Certaines machines comme Windows ont un pare-feu activé, il faudra alors ouvrir le port 5900, (port par défaut), pour que les utilisateurs puissent se connecter à la machine distante.
Vous pouvez aussi changer le port, dans Option, Expert, et modifier le paramètre RfbPort, (voir ci-dessous).

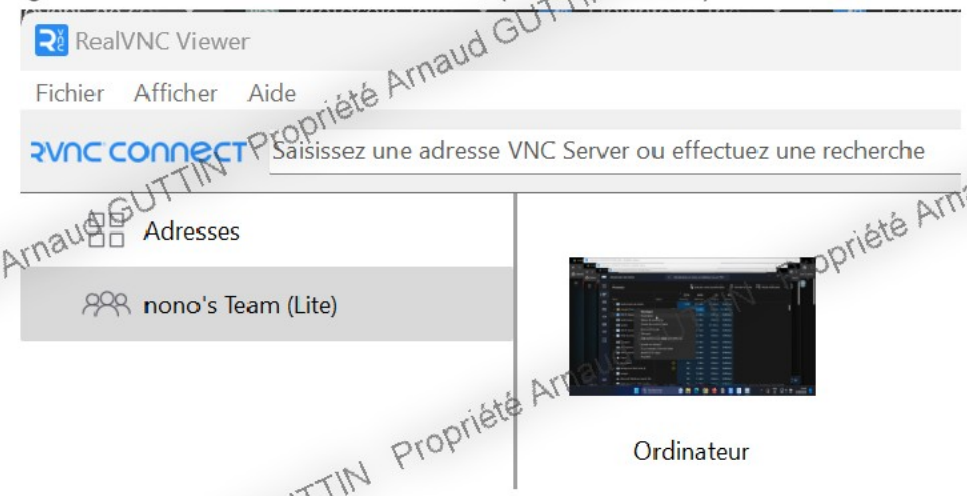


Connexion avec un client VNC

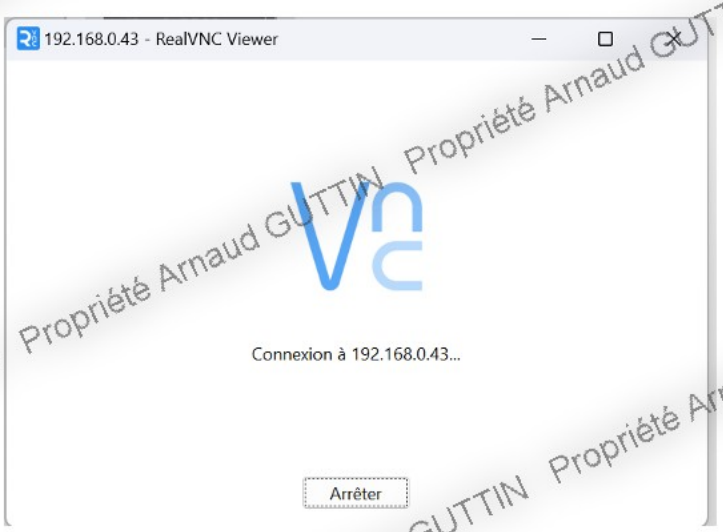
Pour installer le client VNC Viewer, veuillez vous rendre sur le site de RealVNC, ensuite, exécutez le fichier téléchargé.

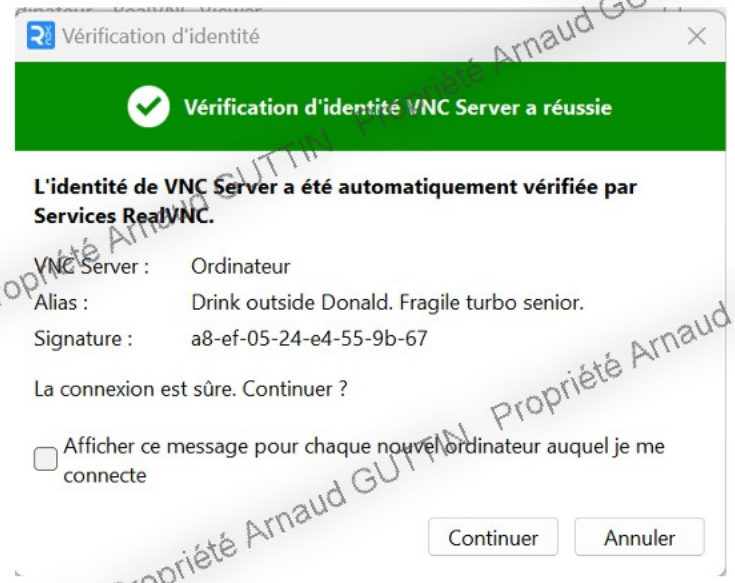
Il sera nécessaire de vous connecter avec le compte utilisé lors de l'installation de VNCServer.

Une fois arrivé sur la page d'accueil de VNC Viewer, vous retrouverez dans le volet à gauche, l'intégralité de vos machines connectées à ce compte.
Vous pouvez aussi vous connecter à une machine VNC directement en entrant son adresse IP ou sa signature VNC dans la barre frontale, (voir ci-dessous).



Vous pouvez ensuite vous connecter, vous pouvez enfin valider la signature de la machine distante.





Remmina

Remmina est un client de bureau à distance open-source qui permet aux utilisateurs de se connecter à des machines distantes. Il prend en charge plusieurs protocoles de connexion à distance, (vu précédemment) comme RDP (Remote Desktop Protocol), VNC (Virtual Network Computing) et SSH (Secure Shell).
Remmina réserve la possibilité d'installer des plugins pour prendre en charge plus de protocoles.

Installation et configuration de Remmina

Pour installer Remmina sur un système Linux, veuillez actualiser les listes de paquets grâce à la commande `apt update -y`, (le paramètres sudo est nécessaire sur certaines distributions Linux pour obtenir les droits de super utilisateur).

```
~ $ sudo apt update -y
```

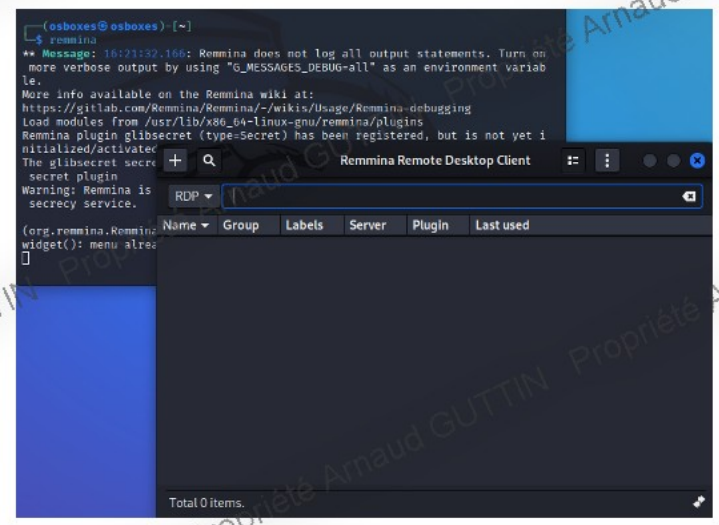
Ensuite, veuillez entrer la commande ci-dessous:

```
sudo apt install -y remmina remmina-plugin-rdp remmina-plugin-secret remmina-plugin-spice
```

Les paramètres remmina-plugin… permettent d'installer les différents plugins qui seront disponibles lors de l'utilisation de Remmina. Par exemple, grâce au plugin RDP, il sera possible d'accéder à une machine en RDP.

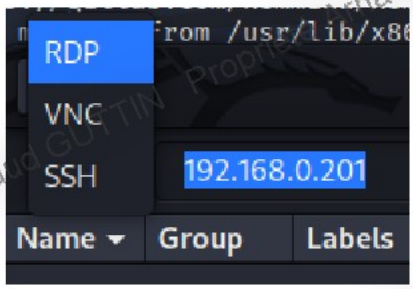
Sur le site web de Remmina, il existe une liste de différents plugins permettant d'installer des extensions, (voir ci-dessous).

Une fois l'installation terminée, vous pouvez exécuter dans le Terminal la commande `remmina`, cela va ouvrir la fenêtre de gestion, (voir ci-dessous).

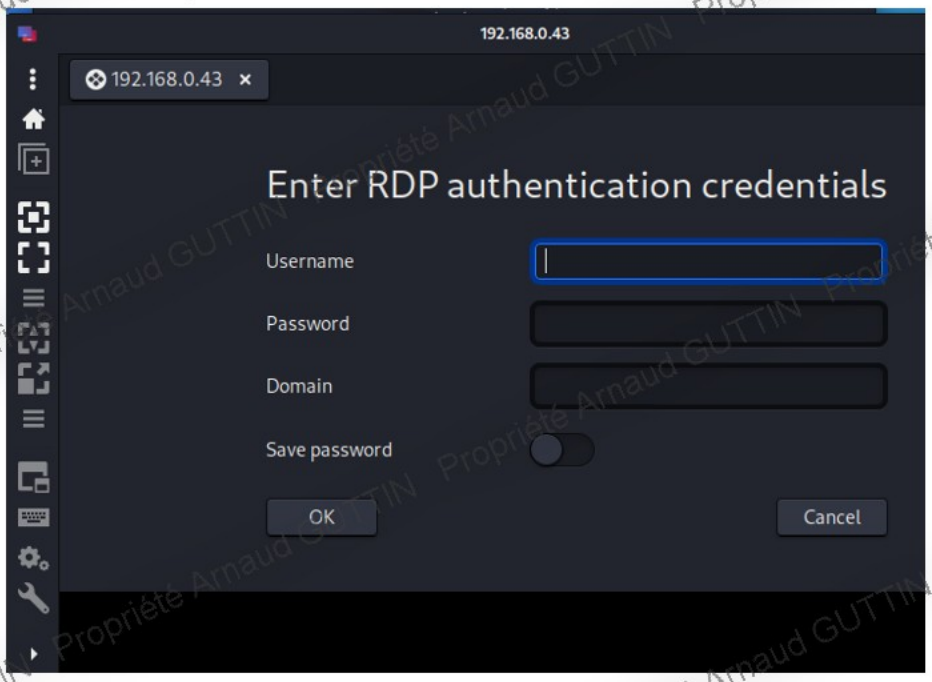


Connexion à une machine distante avec Remmina

Pour vous connecter à distance, veuillez tout d'abord sélectionner le protocole voulu dans le menu déroulant en haut à gauche. Ensuite, entrez l'adresse IP de votre machine distante.



Pour la connexion RDP, il faudra entrer le nom d'utilisateur et le mot de passe de la session distante, (voir ci-dessous).



Pour la connexion SSH, il sera aussi nécessaire de s'identifier pour accéder à la machine. Attention, vous ne pouvez pas vous connecter avec l'utilisateur root. Pour des problèmes de sécurité, ce compte est désactivé pour SSH.