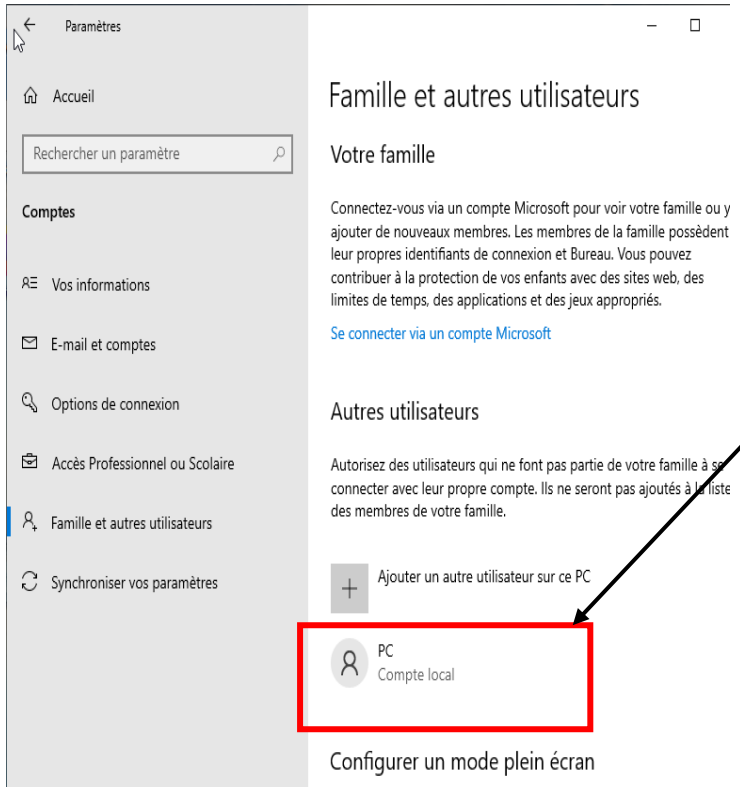
TP– IDENTIFIER LES MENACES

L'audit que je réaliserai pour le DSI sera un audit de style White Hat. Cela signifie que j'effectuerai une série de tests et de simulations pour évaluer la sécurité des systèmes d'information, dans le respect de la loi et des normes éthiques.

1. **Identification des actifs :** je commencerais par identifier tous les actifs informatiques de l'organisation, tels que les serveurs, les postes de travail, les applications et les données.
2. **Évaluation de la vulnérabilité :** Ensuite, j'évaluerai les vulnérabilités potentielles de ces actifs. Cela peut impliquer l'utilisation d'outils automatisés ainsi que de techniques manuelles pour tester la résistance du système à différents types d'attaques.
3. **Simulation d'attaque :** en tant que pentester, je simulerais des attaques directes et indirectes pour voir comment le système réagit. Les attaques directes visent à exploiter des vulnérabilités connues, tandis que les attaques indirectes utilisent des méthodes plus sophistiquées, comme le phishing ou l'ingénierie sociale.
4. **Rapport et recommandations** : Enfin, je fournirai un rapport détaillé de mes constatations, ainsi que des recommandations sur la manière d'améliorer la sécurité du système d'information.

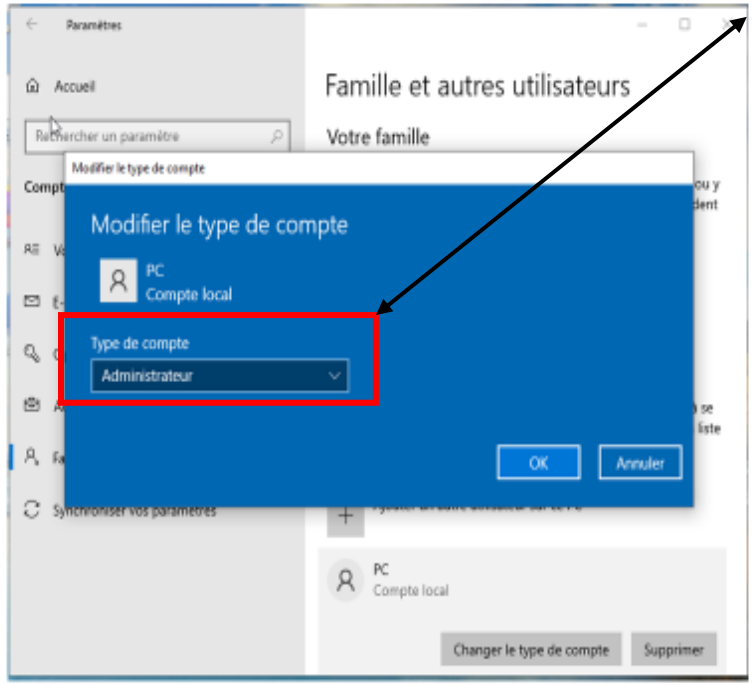
PRÉPAREZ LA MACHINE VIRTUELLE WINDOWS 10

Création de l'utilisateur PC



Création d'un utilisateur nommé PC

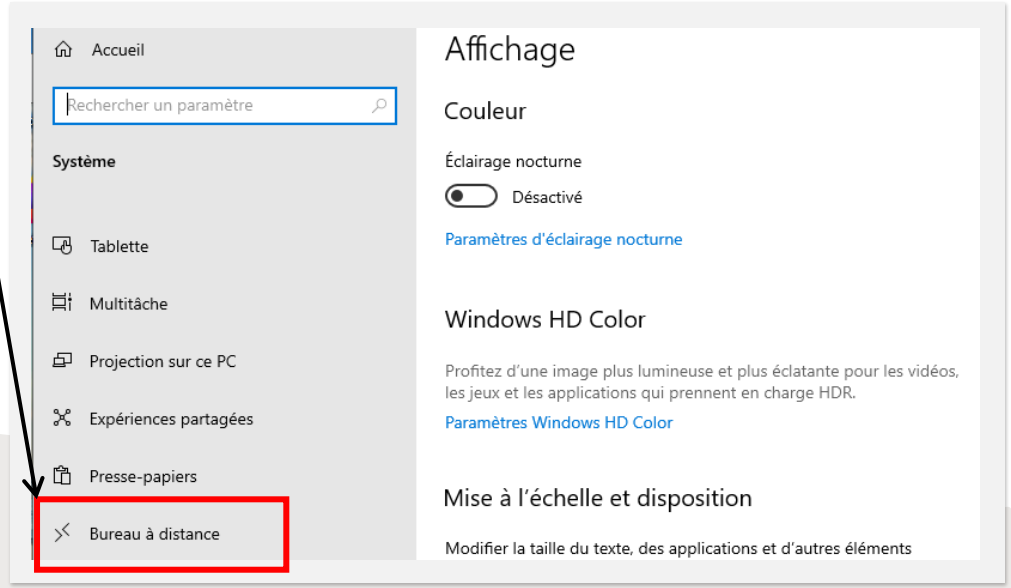
Modifier le compte en tant que Administrateur



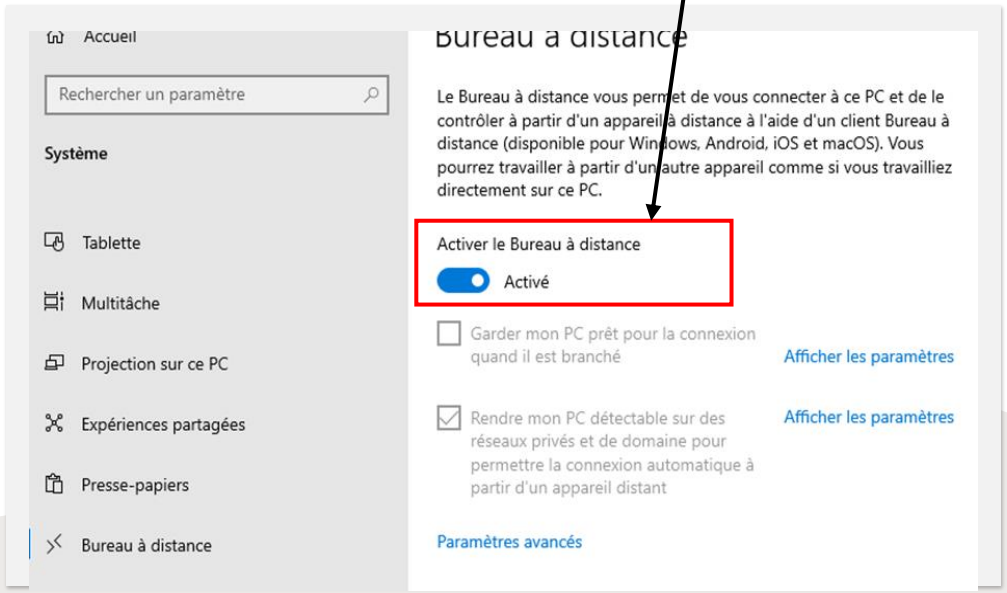
Modifié le type de compte et mettre l'utilisateur PC en mode Administrateur

ACTIVATION DU BUREAU A DISTANCES (PROTOCOL RDP)

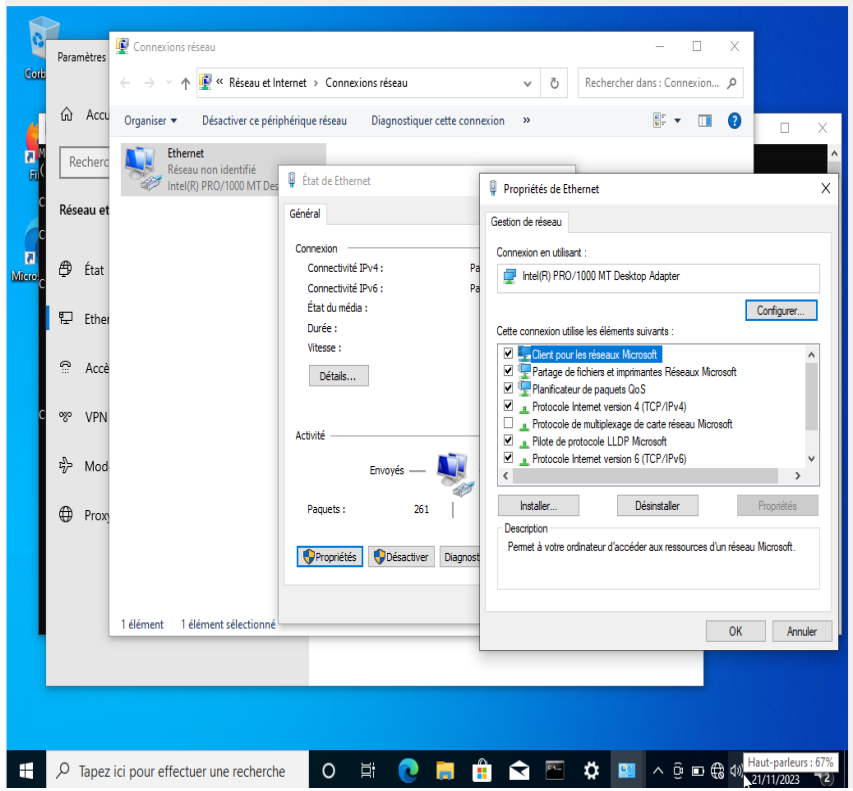
Cliqué sur bureau à distance

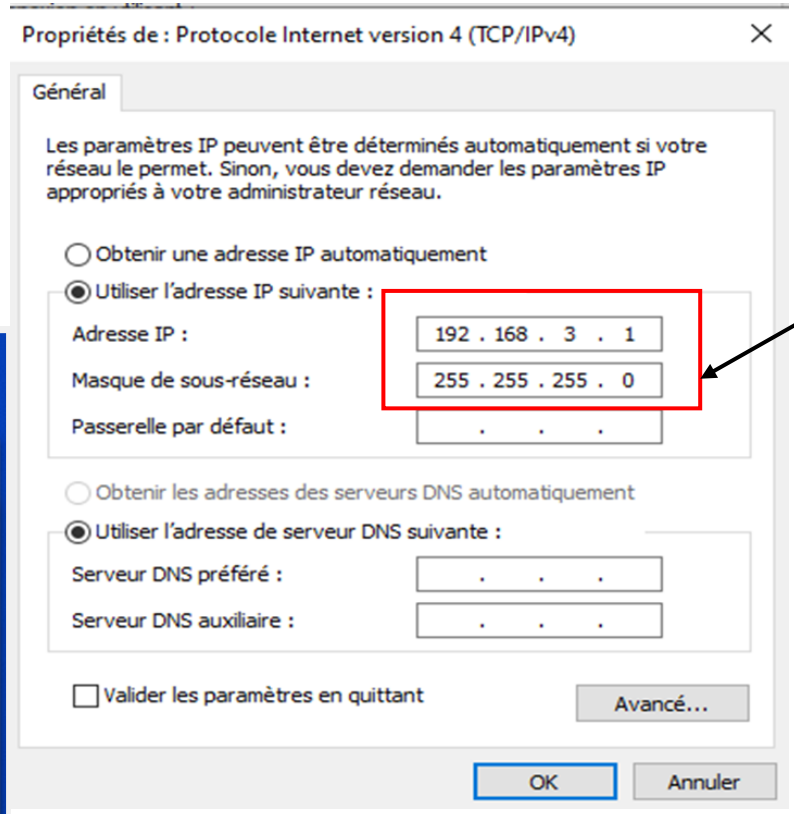


Activé le bureau a distance comme ci-dessous



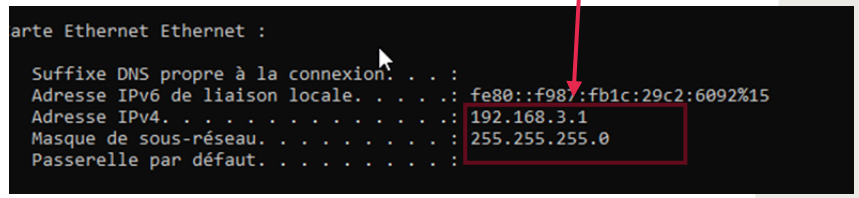
MISE EN PLACE EN RÉSEAU INTERNET ET CONFIGURATION DE L'ADRESSE IP DES MACHINES





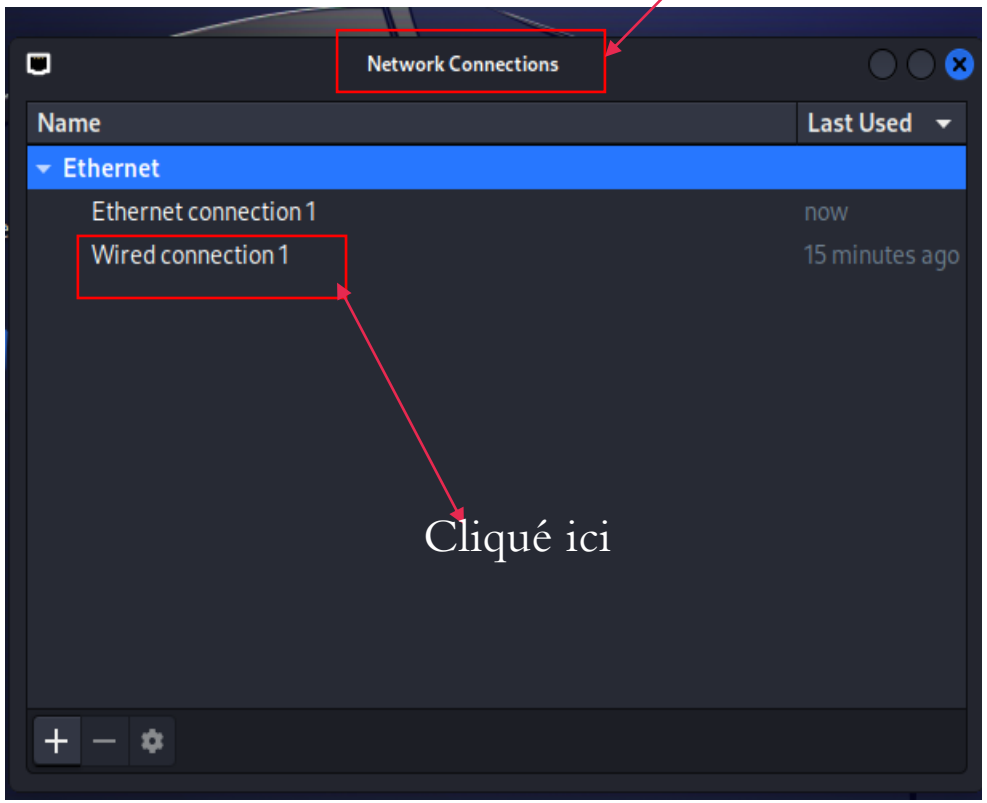
Définition de l'adresse et du masque

Vérifier que l'adresse IP a bien été changer



MACHINE KALI-LINUX

Accéder à network connections.

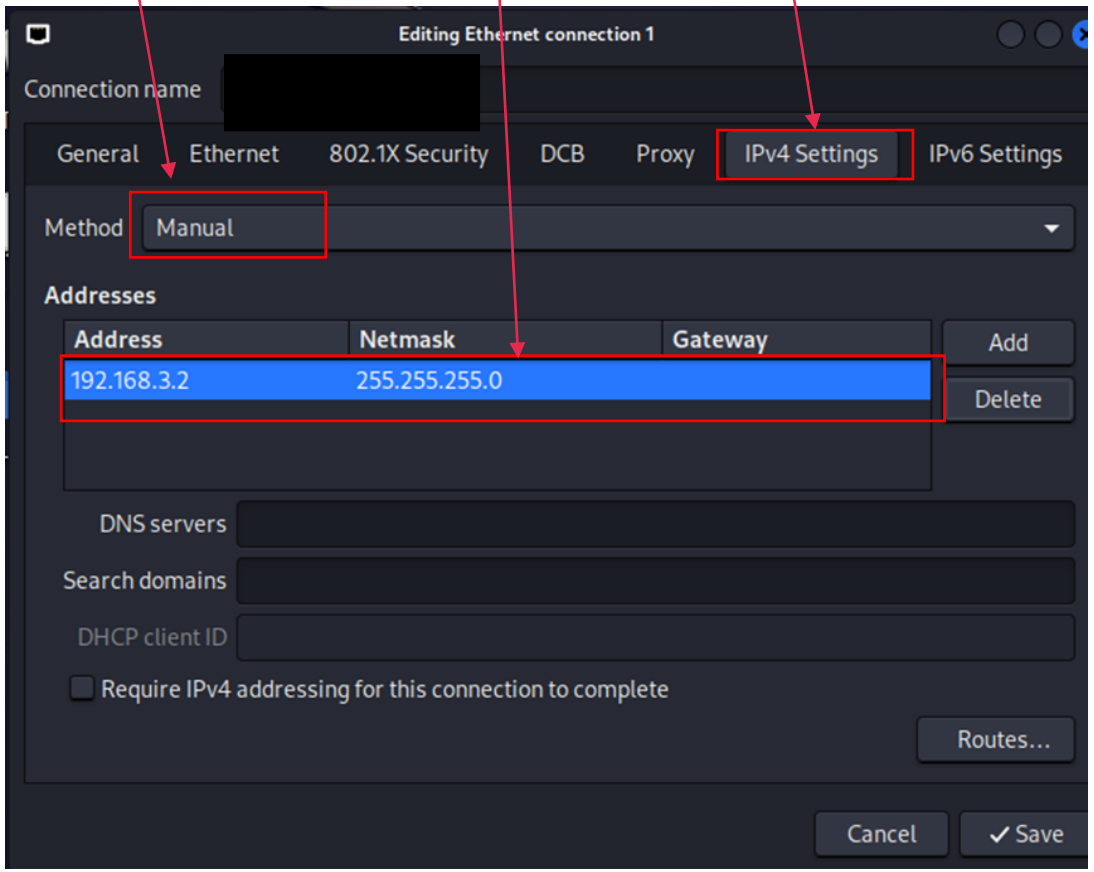


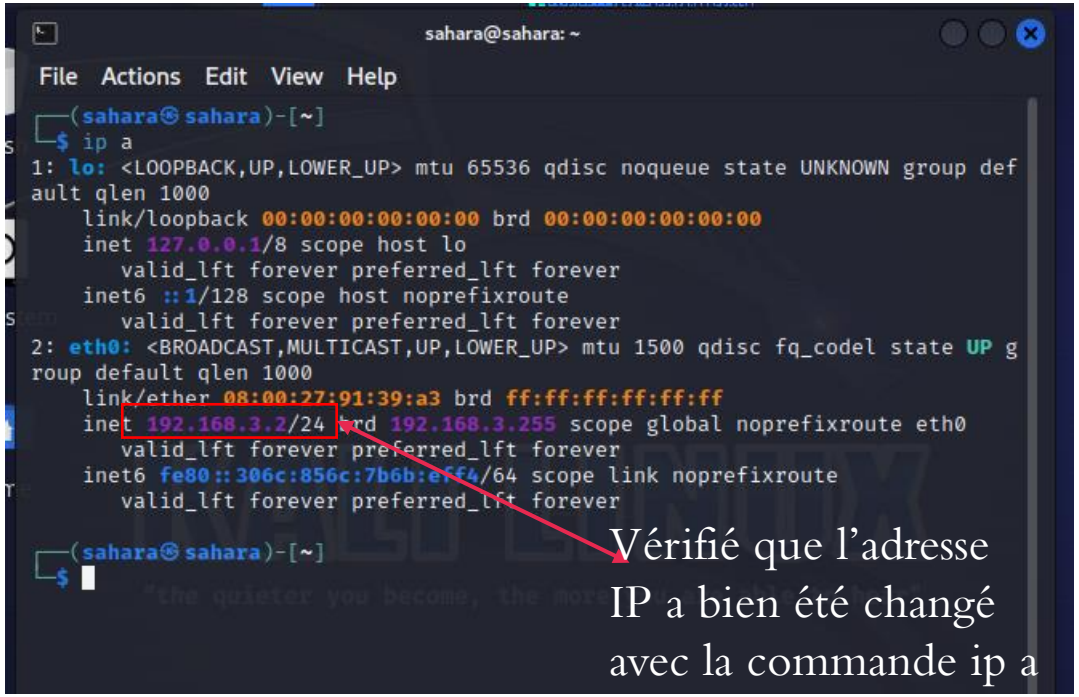
Cliqué ici

Choisir manual dans method

Configurer votre adresse IP

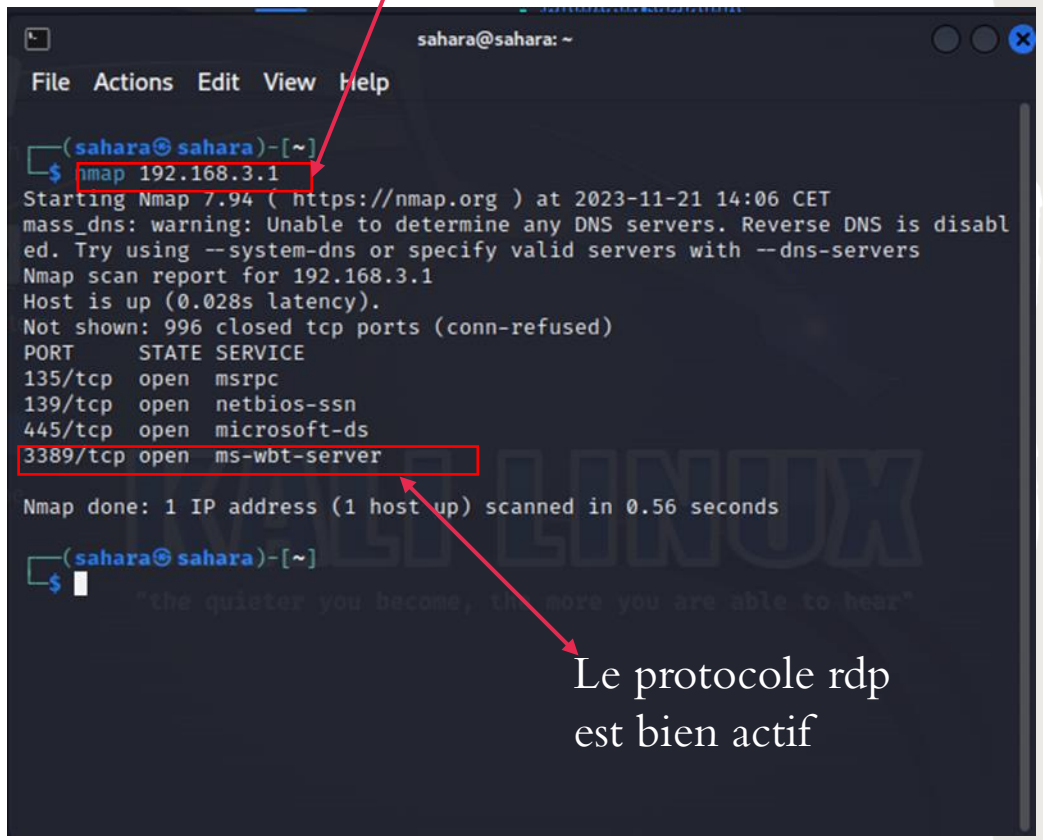
Cliqué sur IPV4





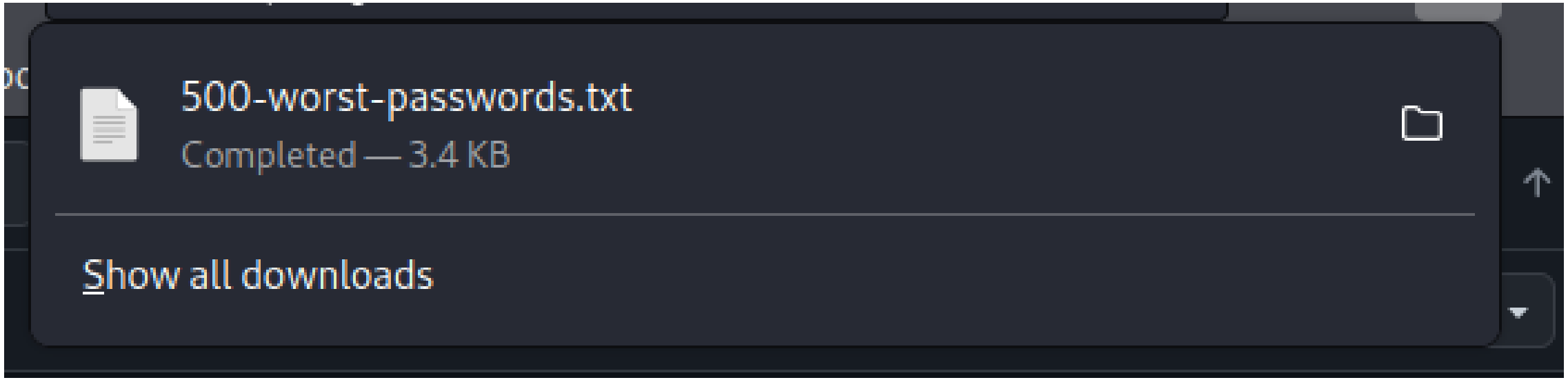
Vérifié que l'adresse IP a bien été changé avec la commande ip a

Nmap la machine Windows afin de vérifier si le protocole RDP est bien actif sur celle-ci



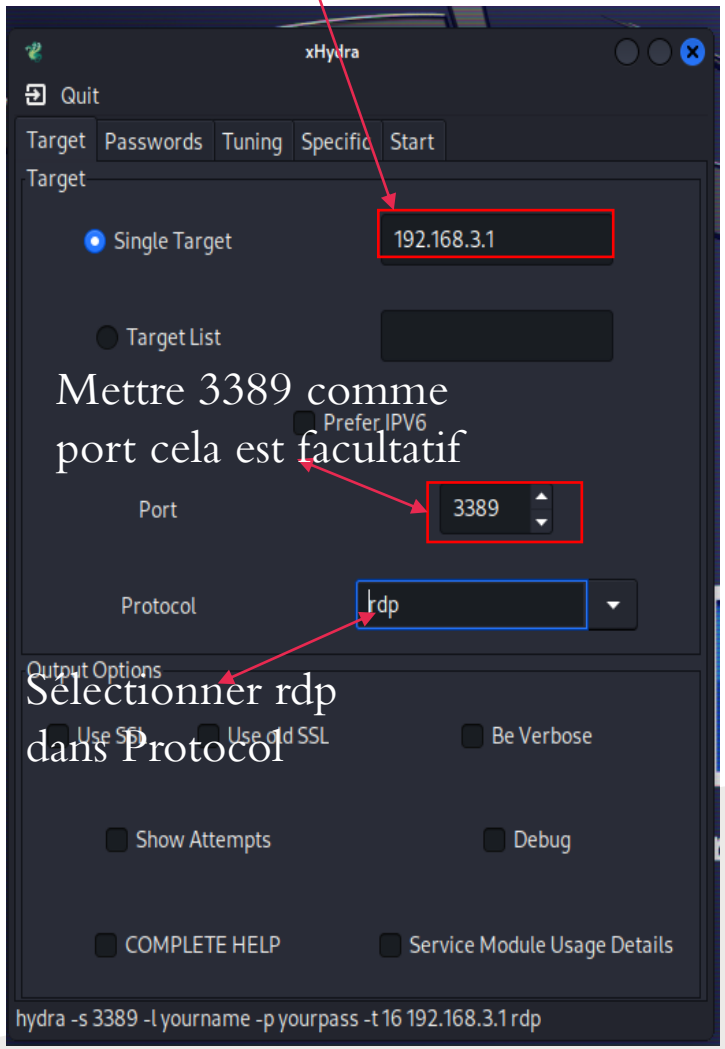
Le protocole rdp est bien actif

RECUPERATION DU DICTIONARIES DE MOTS PASSE



Utilisation de l'outil xhydra

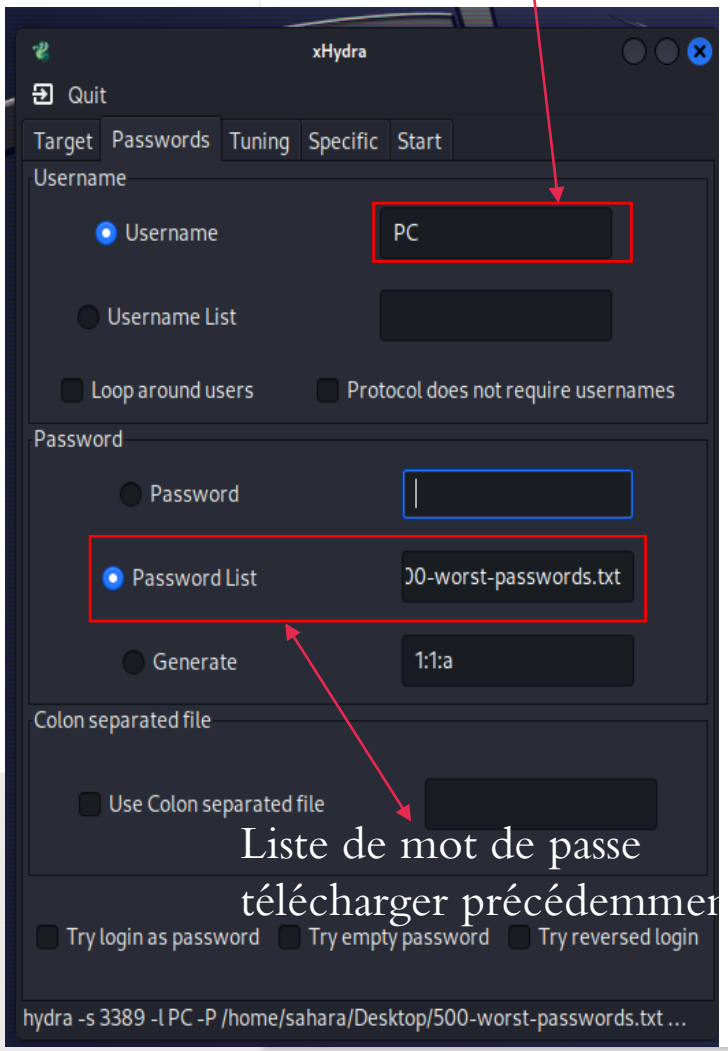
Adresse IP de notre machine Windows



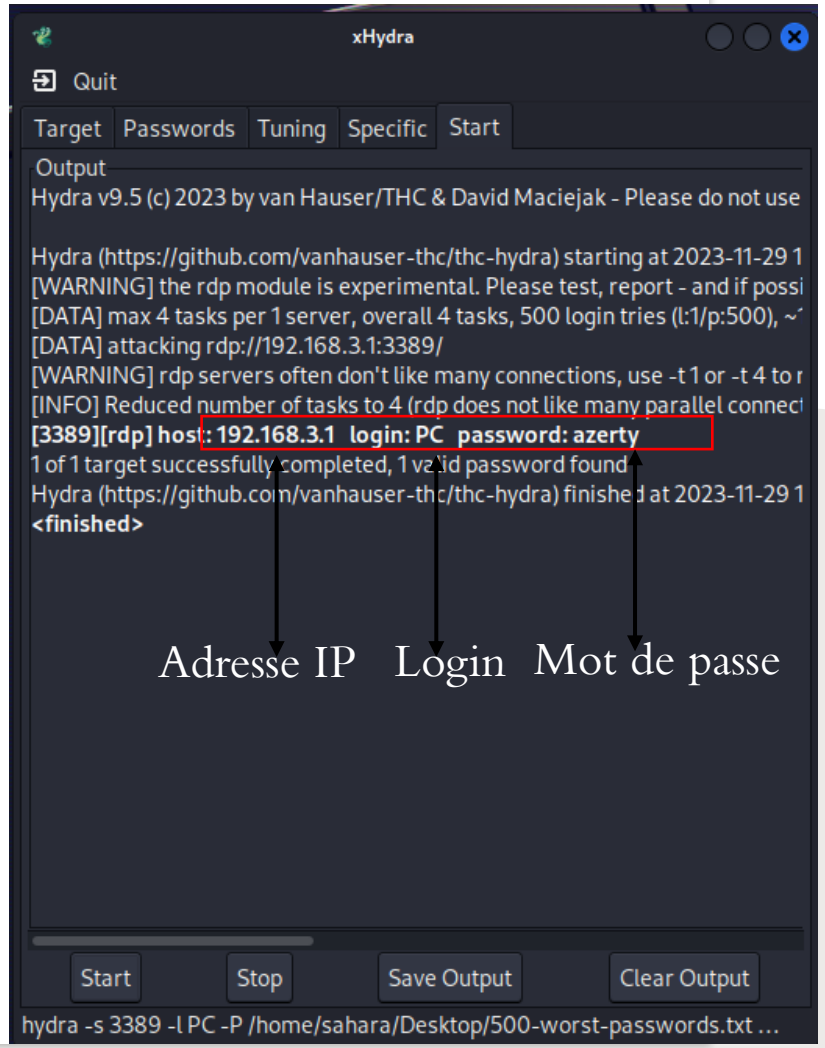
Mettre 3389 comme port cela est facultatif

Sélectionner rdp dans Protocol

Nom de l'utilisateur de la machine Windows



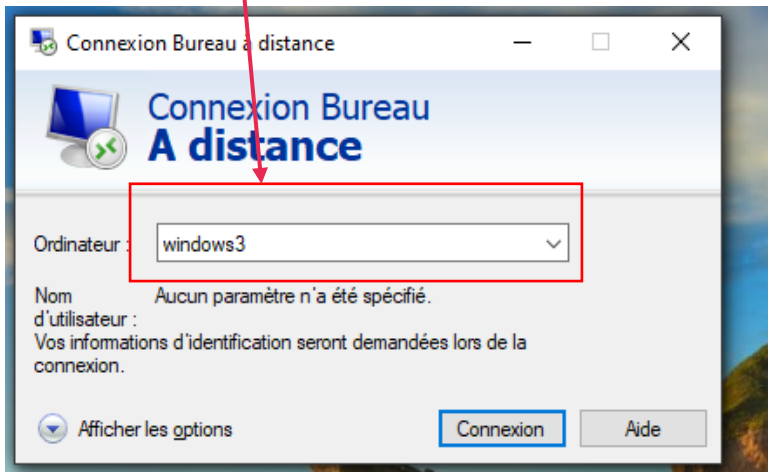
Liste de mot de passe télécharger précédemmer



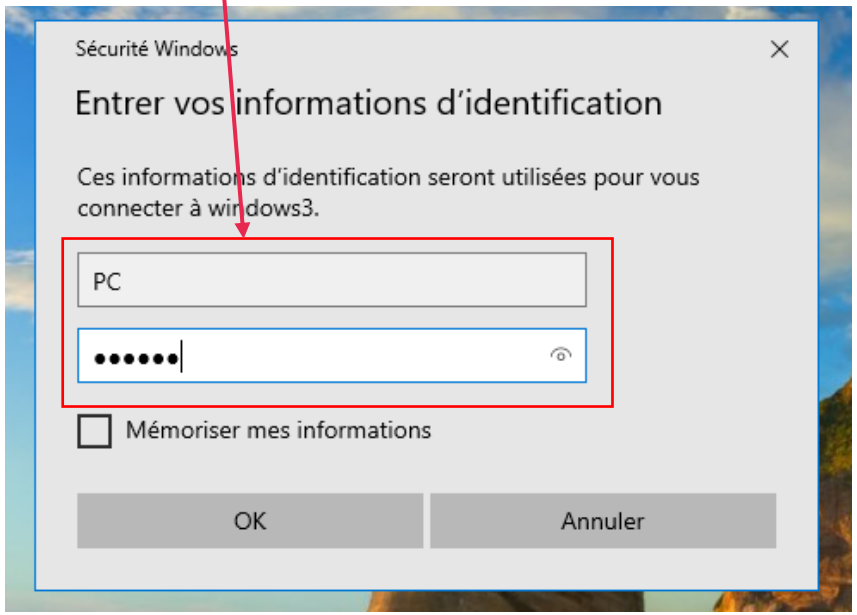
Adresse IP Login Mot de passe

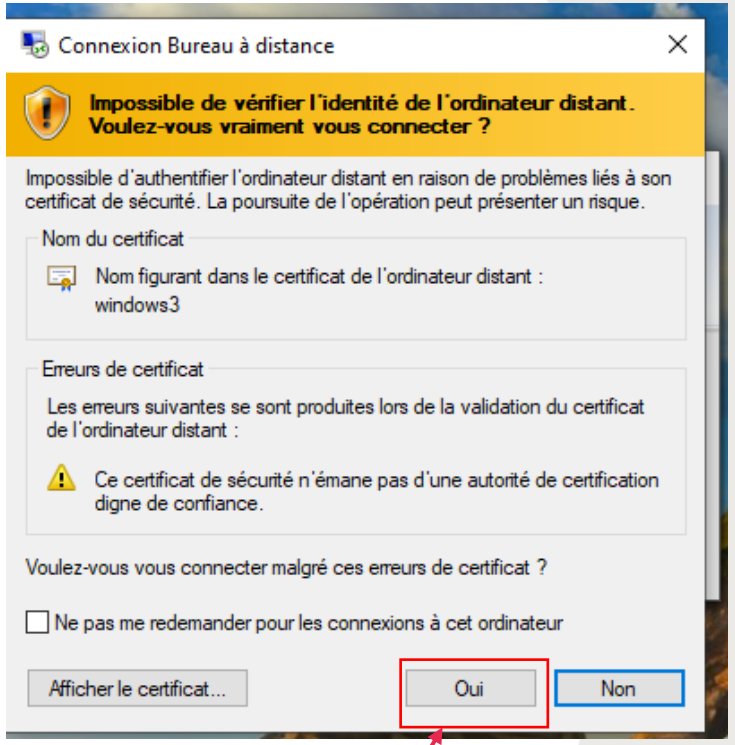
TESTE DE CONNEXION SUR LE BUREAU A DISTANCE

Nom de la machine sur laquelle nous souhaitons nous connecter



Nom d'utilisateur et le mot de passe que nous avons récupéré précédemment avec Xhydra

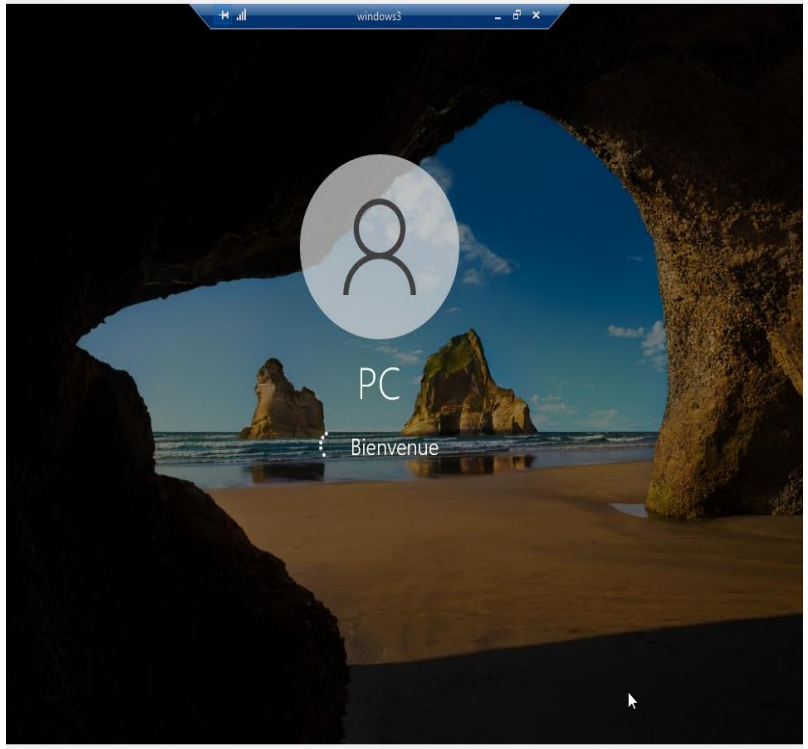




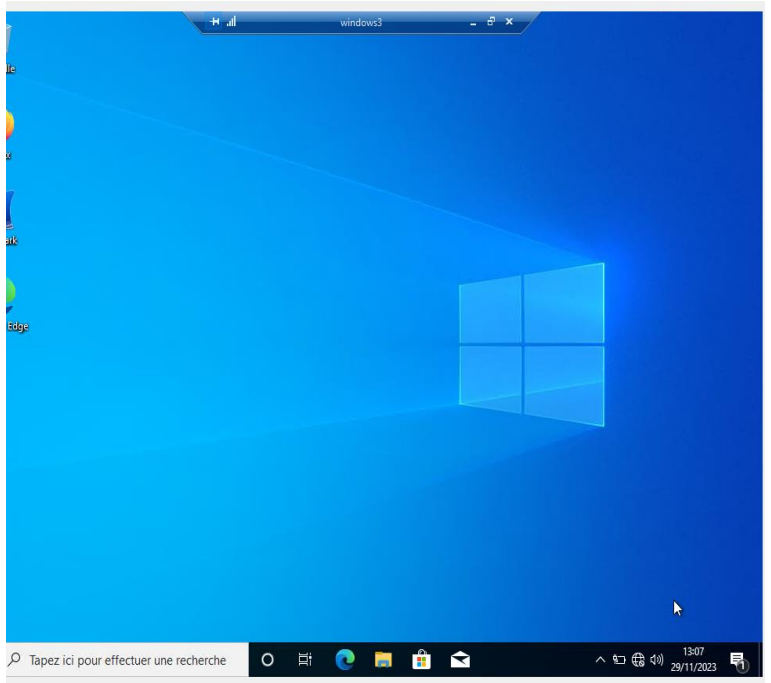
Cliqué sur oui

CONNEXION RÉUSSIE

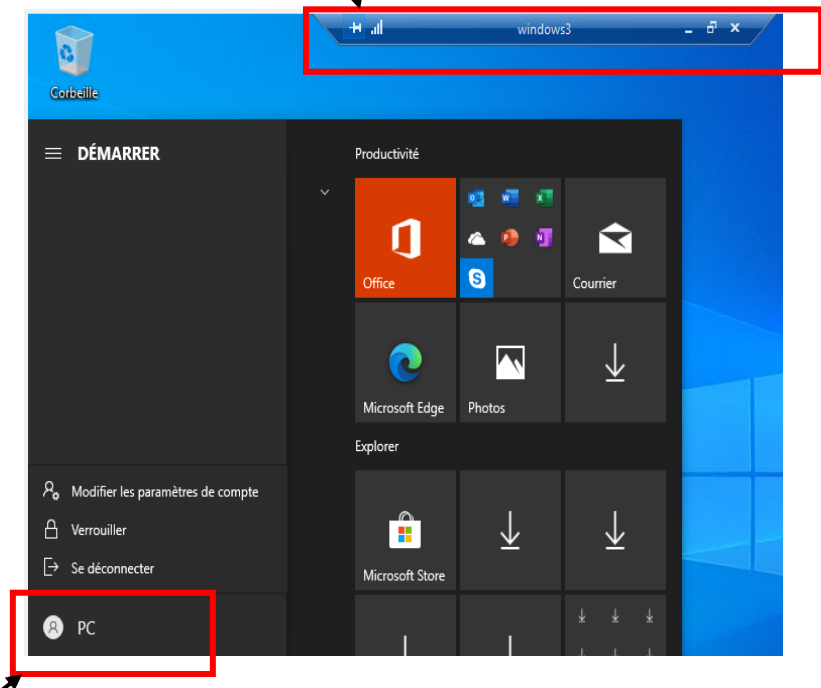
La connexion est en cours



Nous sommes bien connectés à distance



Le nom de la machine sur laquelle on est connecté



Le nom de l'utilisateur sur lequel nous somme connecté