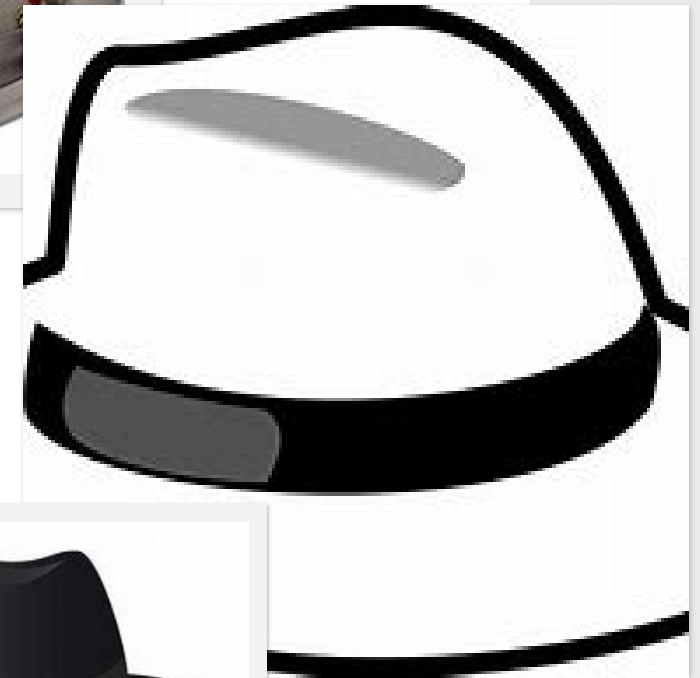




TP- IDENTIFIER LES MENACES

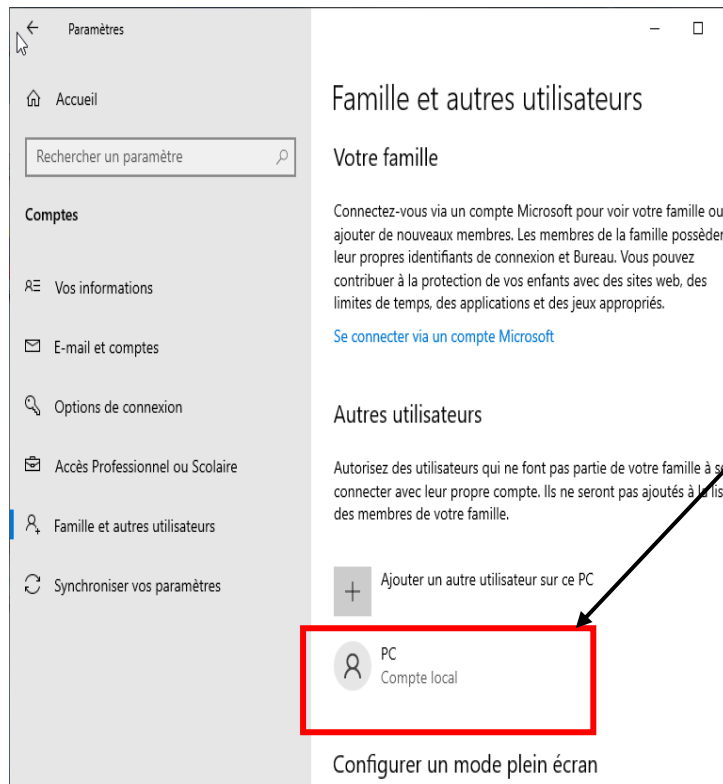
L'audit que je réaliserai pour le DSI sera un audit de style White Hat. Cela signifie que j'effectuerai une série de tests et de simulations pour évaluer la sécurité des systèmes d'information, dans le respect de la loi et des normes éthiques.

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 simulerai 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.



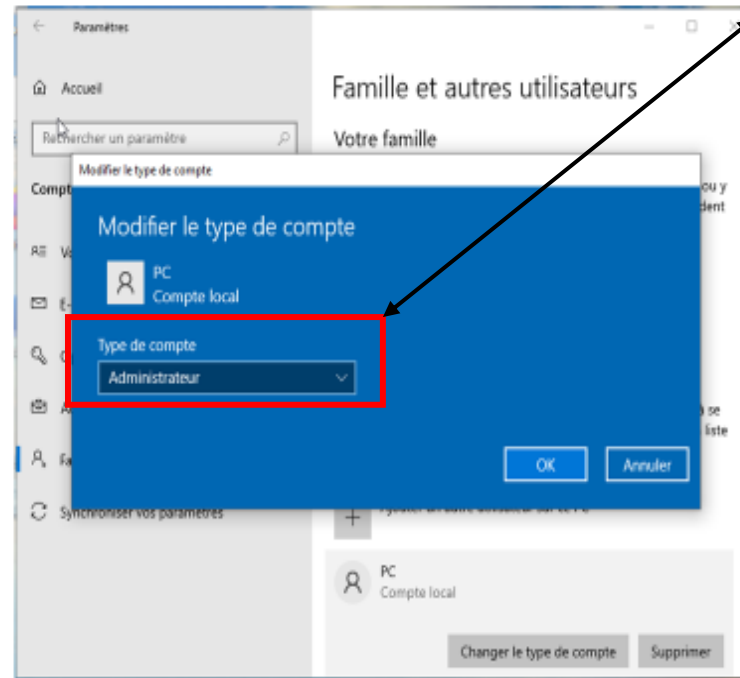
# PRÉPAREZ LA MACHINE VIRTUELLE WINDOWS 10

## Création de l'utilisateur PC



Création d'un utilisateur nommé PC

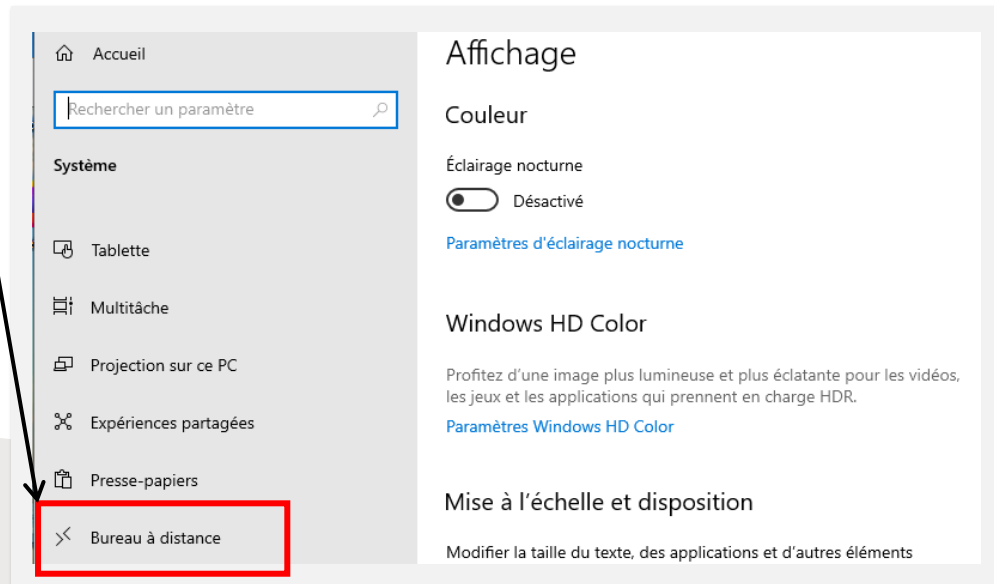
## Modifier le compte en tant que Administrateur



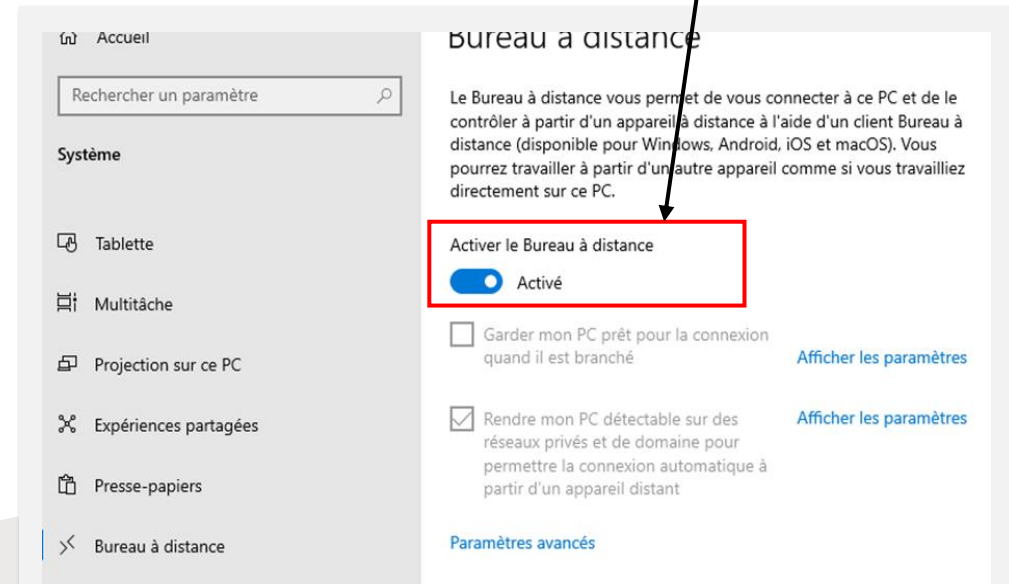
Modifié le type de compte et mettre l'utilisateur PC en mode Administrateur

# ACTIVATION DU BUREAU A DISTANCES (PROTOCOL RDP)

Cliqué sur bureau à distance

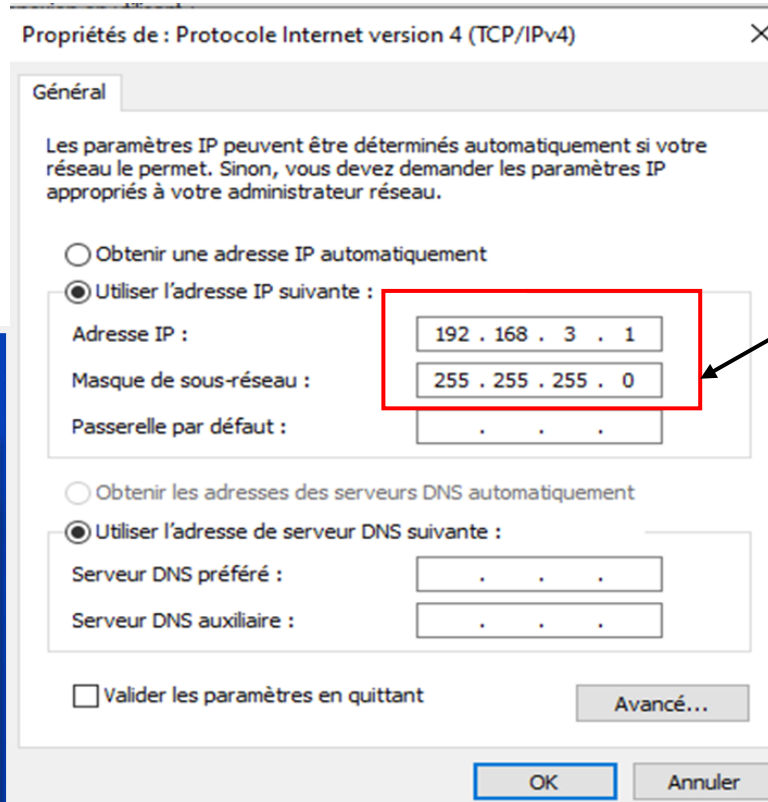
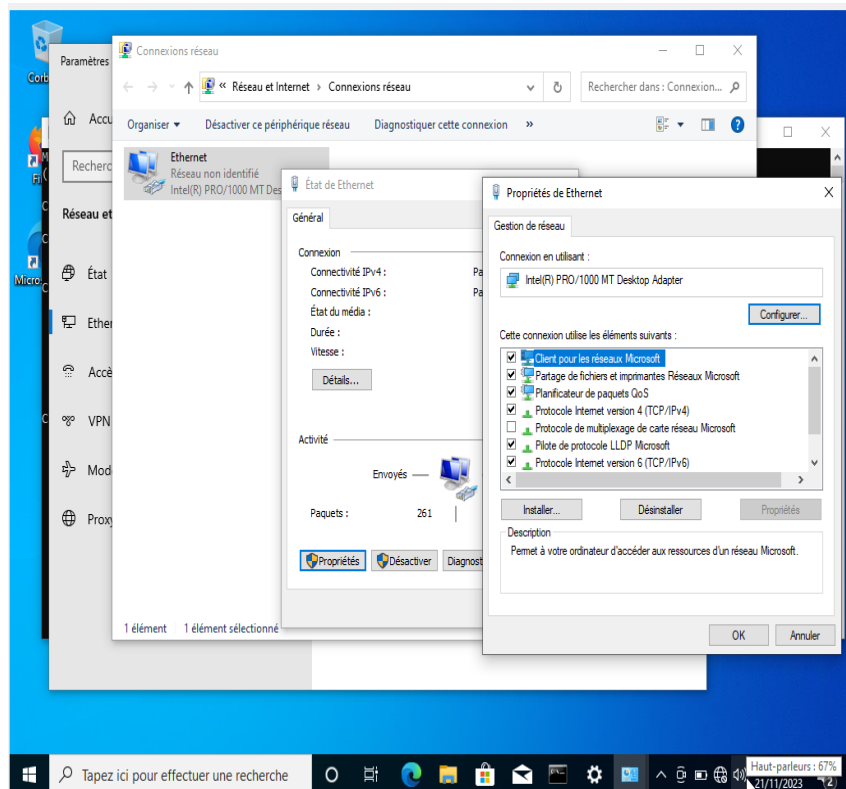


Activé le bureau a distance  
comme ci-dessous





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

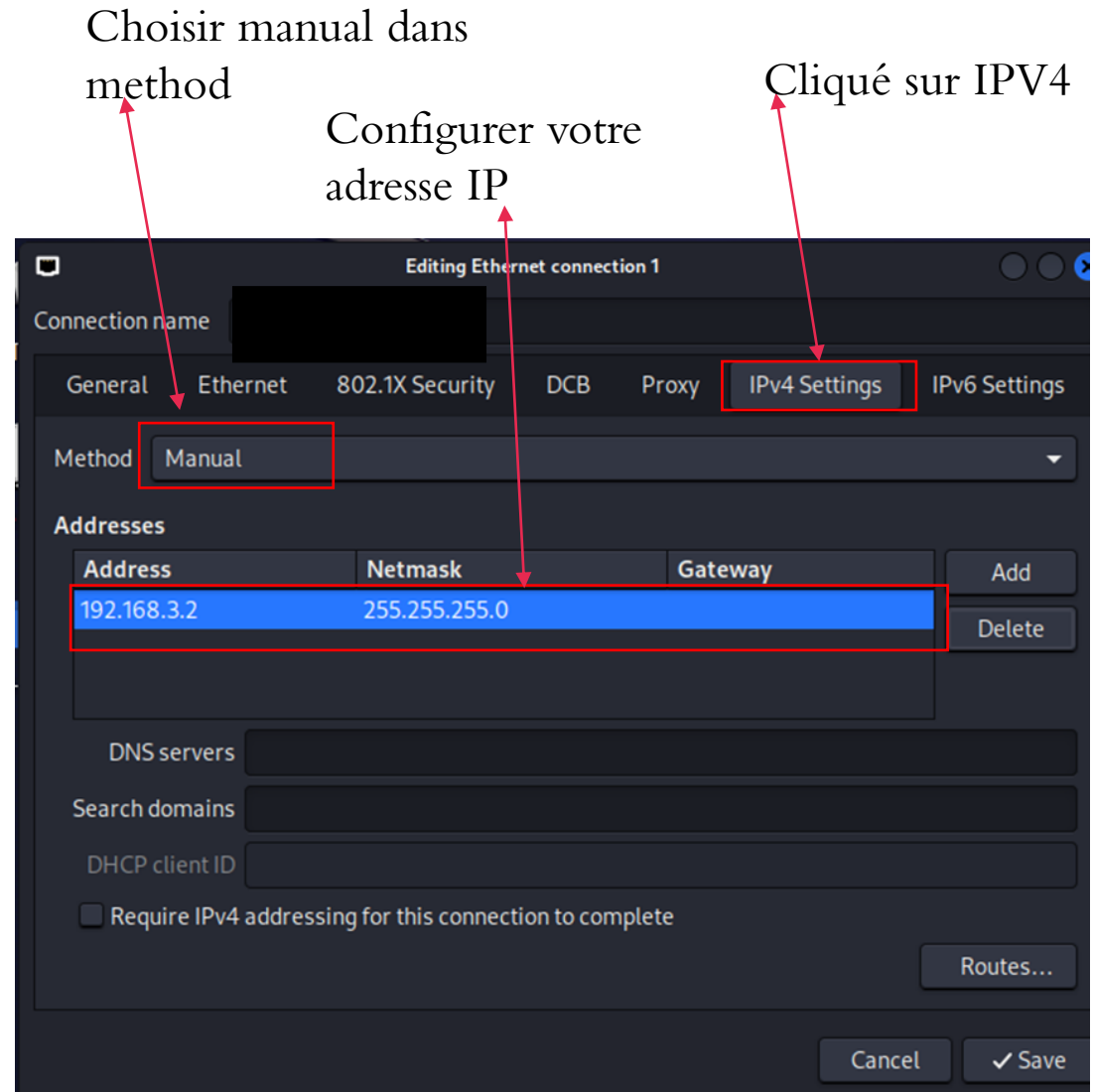
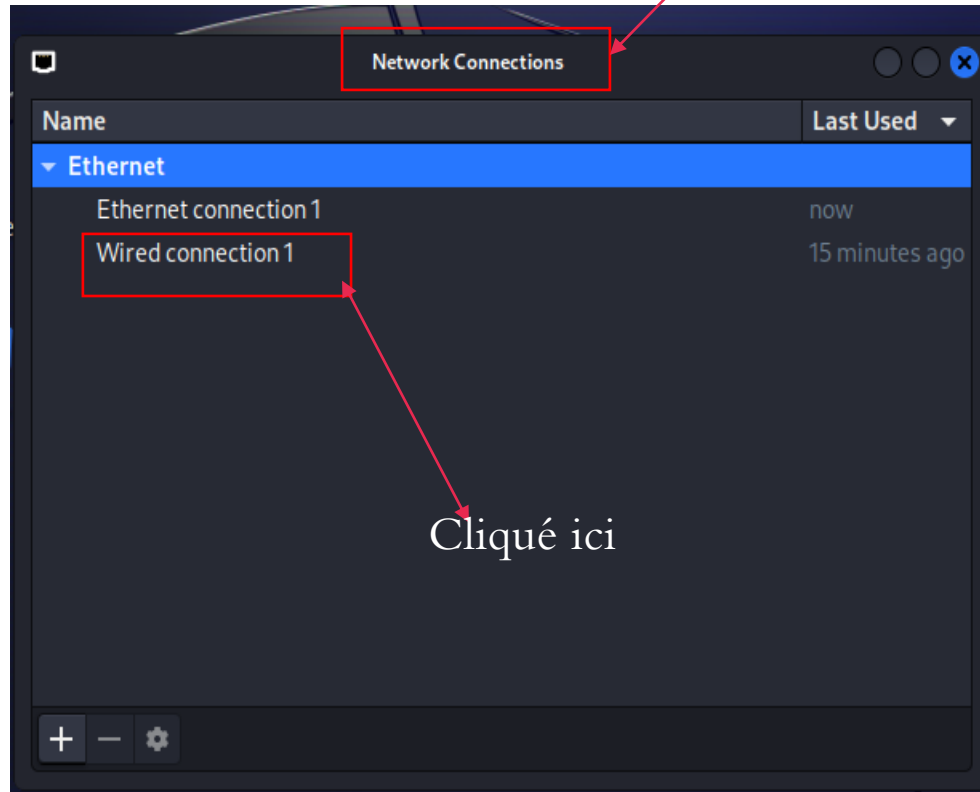


Définition de l'adresse et du masque

Vérifier que l'adresse IP a bien été changée

```
Carte Ethernet Ethernet :  
Suffixe DNS propre à la connexion: . . . :  
Adresse IPv6 de liaison locale. . . . : fe80::f987:fb1c:29c2:6092%15  
Adresse IPv4. . . . . : 192.168.3.1  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle par défaut. . . . . :
```

# MACHINE KALI-LINUX



```
sahara@sahara: ~  
File Actions Edit View Help  
(sahara@sahara)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:91:39:a3 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.3.2/24 brd 192.168.3.255 scope global noprefixroute eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::306c:856c:7b6b:eff4/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
(sahara@sahara)-[~]  
$
```

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

```
sahara@sahara: ~  
File Actions Edit View Help  
(sahara@sahara)-[~]  
$ nmap 192.168.3.1  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-21 14:06 CET  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers  
Nmap scan report for 192.168.3.1  
Host is up (0.028s latency).  
Not shown: 996 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
3389/tcp   open  ms-wbt-server  
Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds  
(sahara@sahara)-[~]  
$
```

Le protocole rdp est bien actif

# RECUPERATION DU DICTIONNAIRES DE MOTS PASSE



500-worst-passwords.txt

Completed — 3.4 KB

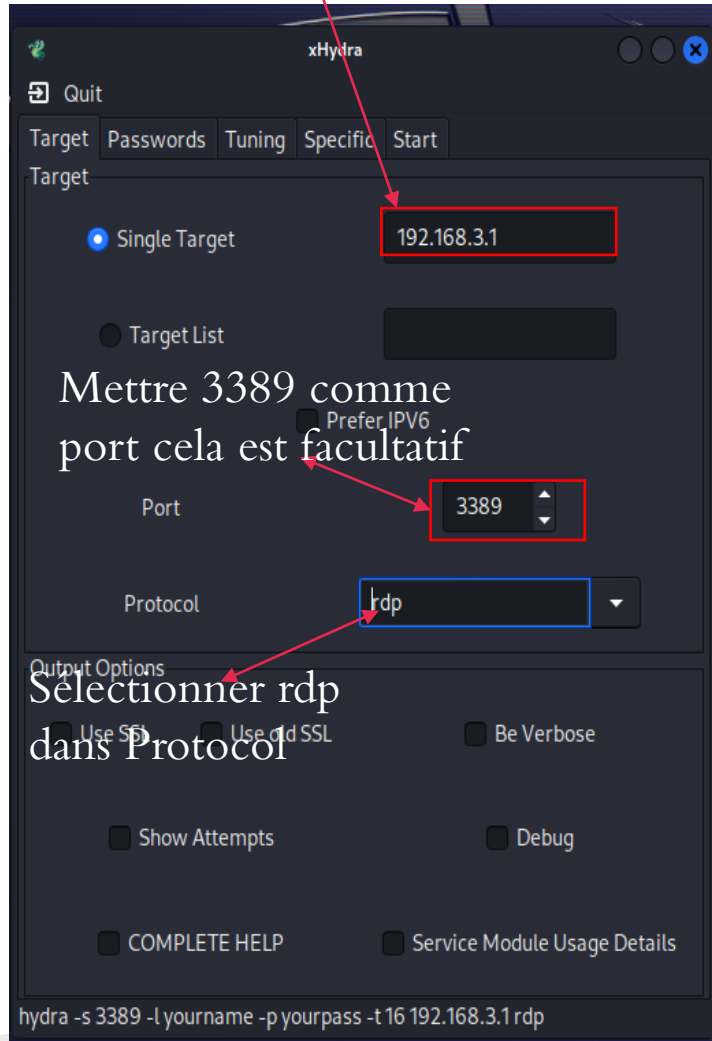


[Show all downloads](#)

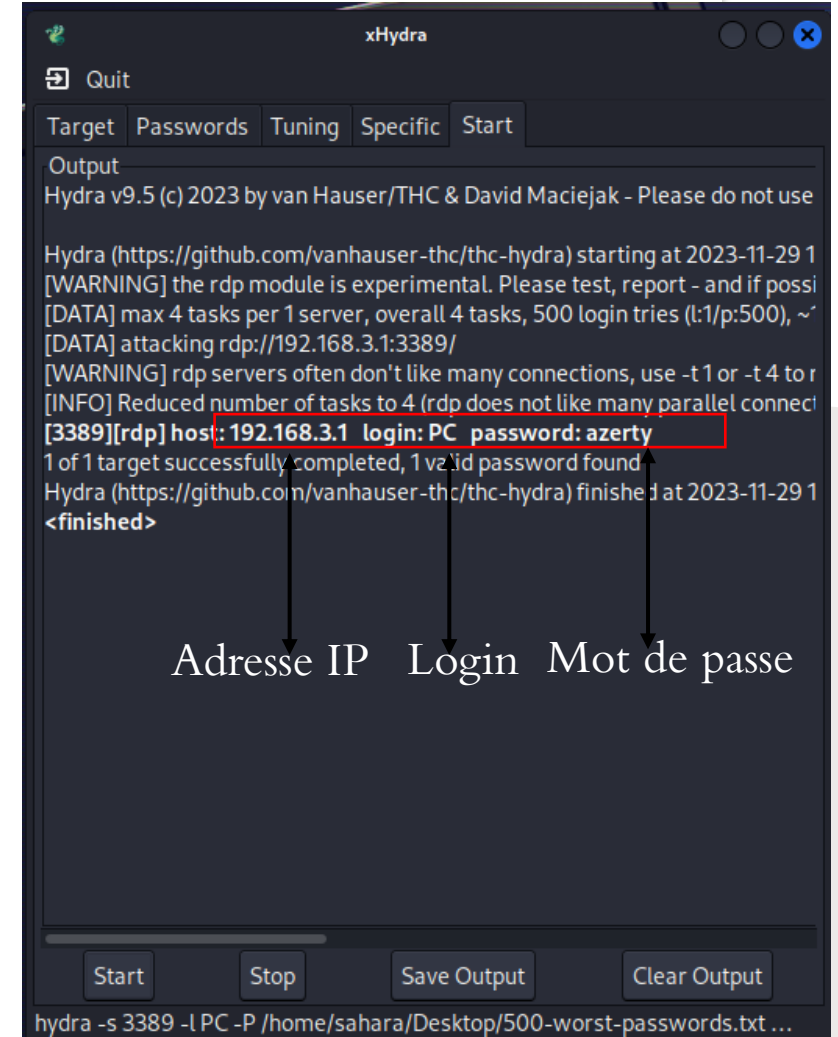
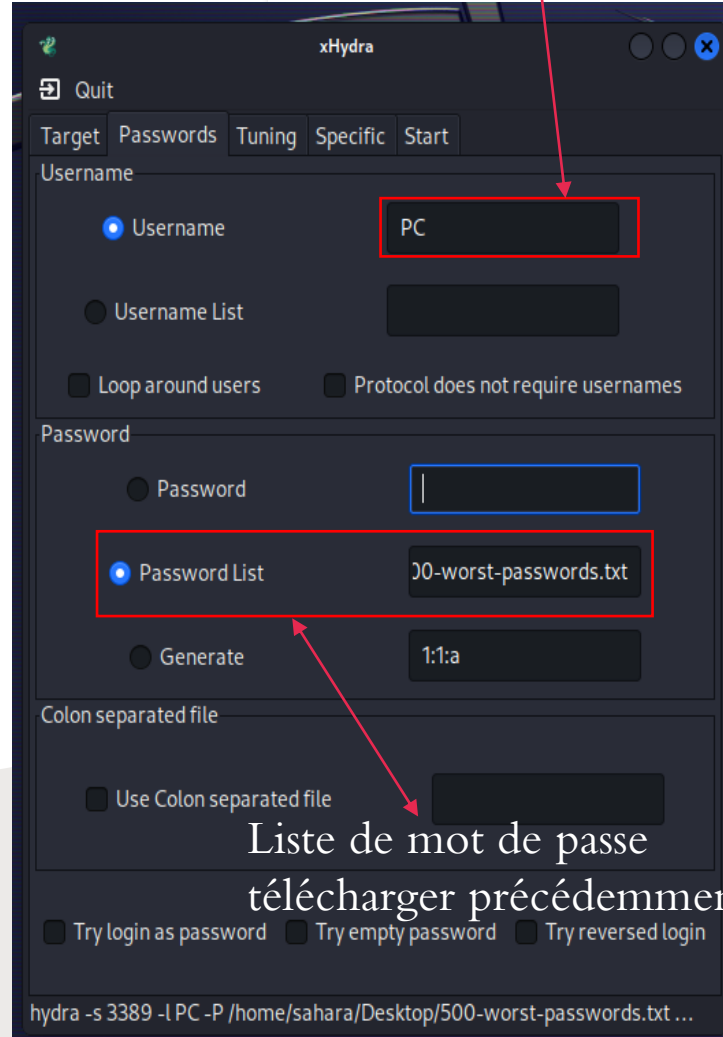


# Utilisation de l'outil xhydra

Adresse IP de notre machine Windows

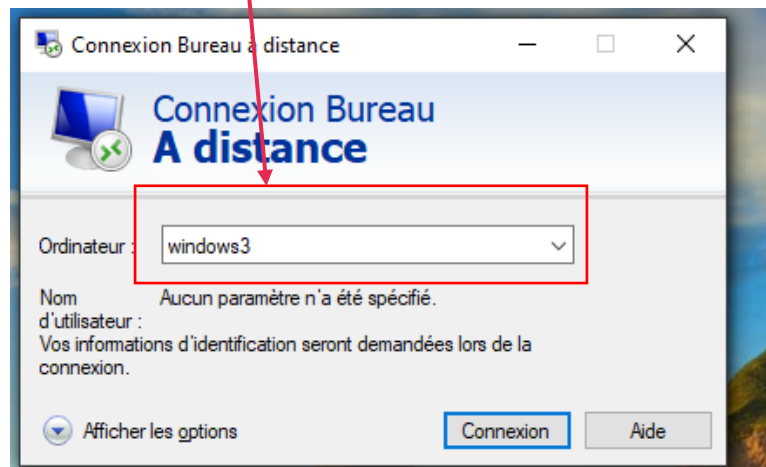


Nom de l'utilisateur de la machine Windows

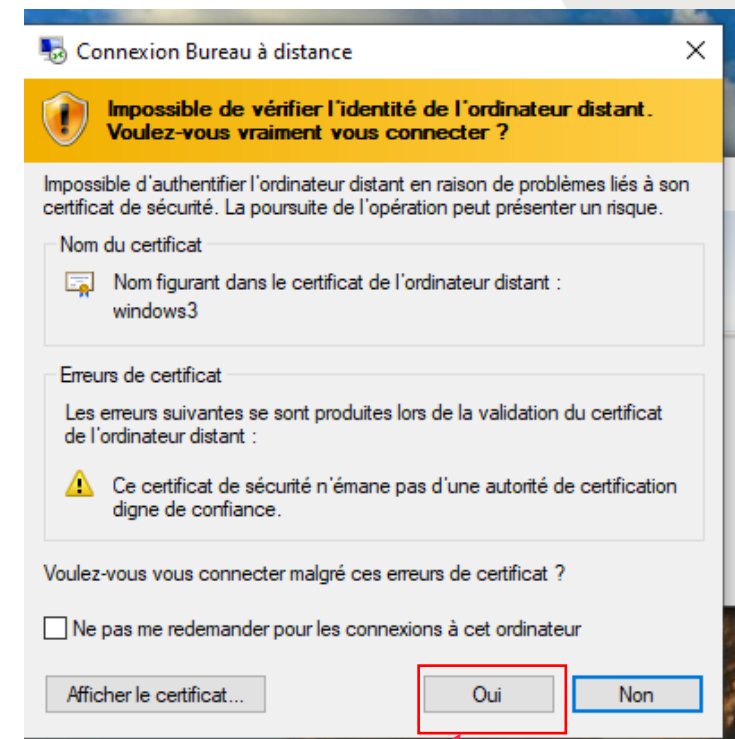
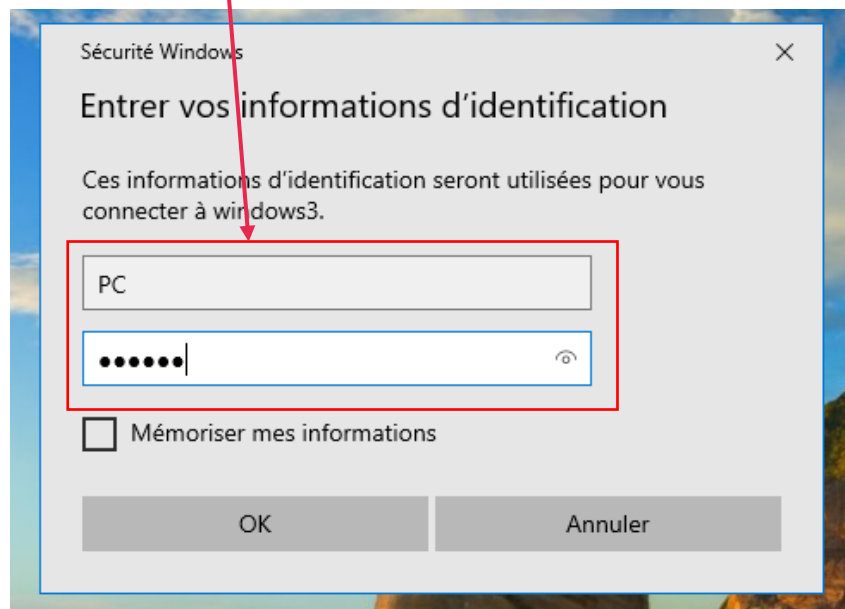


# TESTE DE CONNEXION SUR LE BUREAU A DISTANCE

Nom de la machine sur laquelle nous souhaitons nous connecter



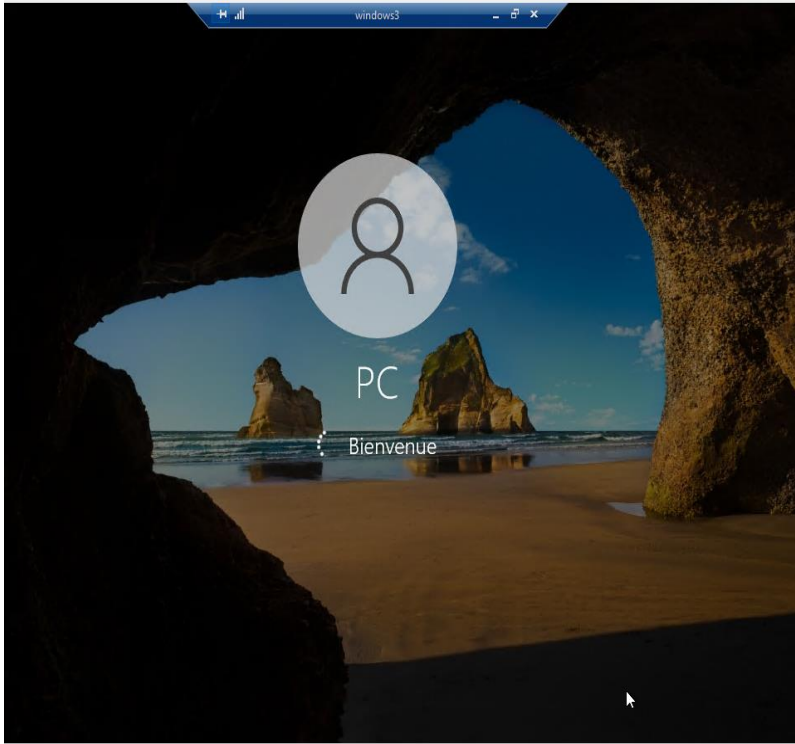
Nom d'utilisateur et le mot de passe que nous avons récupéré précédemment avec Xhydra



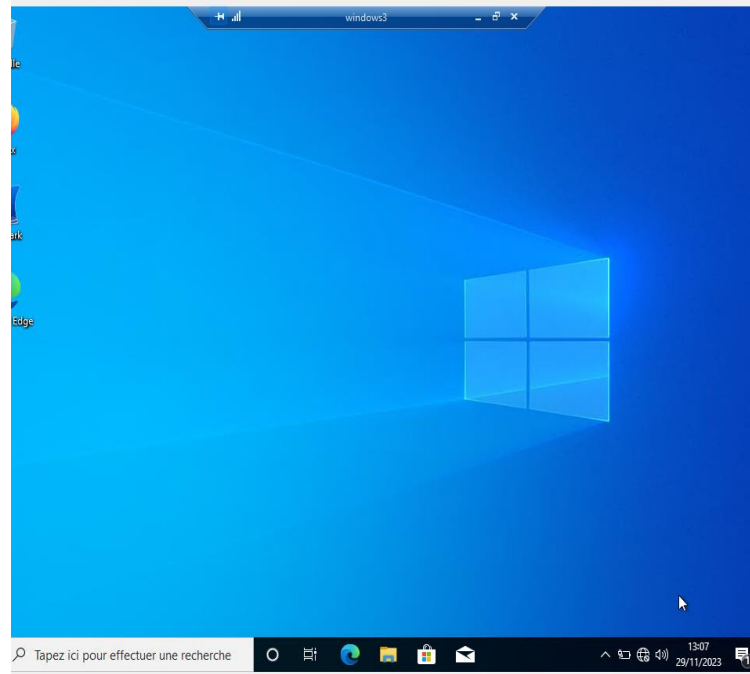
Cliqué sur oui

# CONNEXION RÉUSSIE

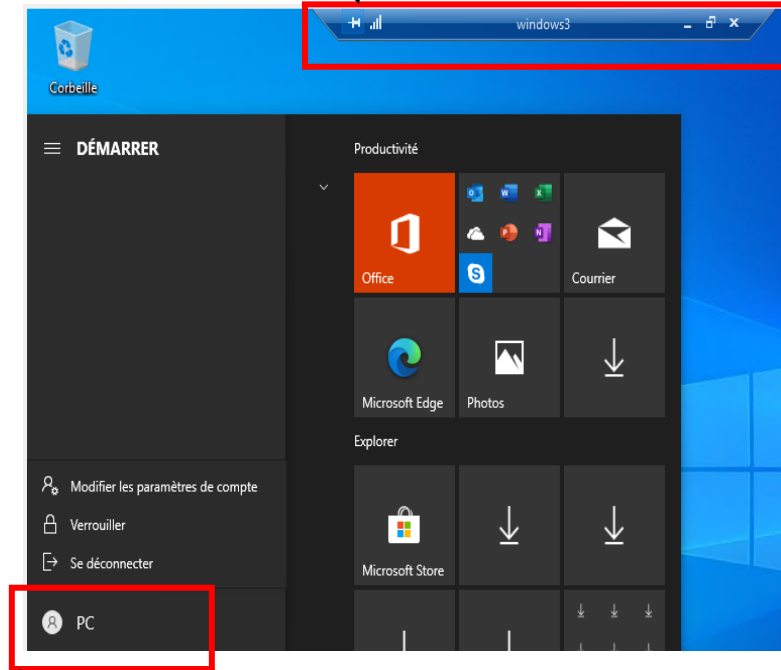
La connexion est en cours



Nous sommes bien connectés à distance



Le nom de la machine sur laquelle on est connecté



Le nom de l'utilisateur sur lequel nous sommes connecté