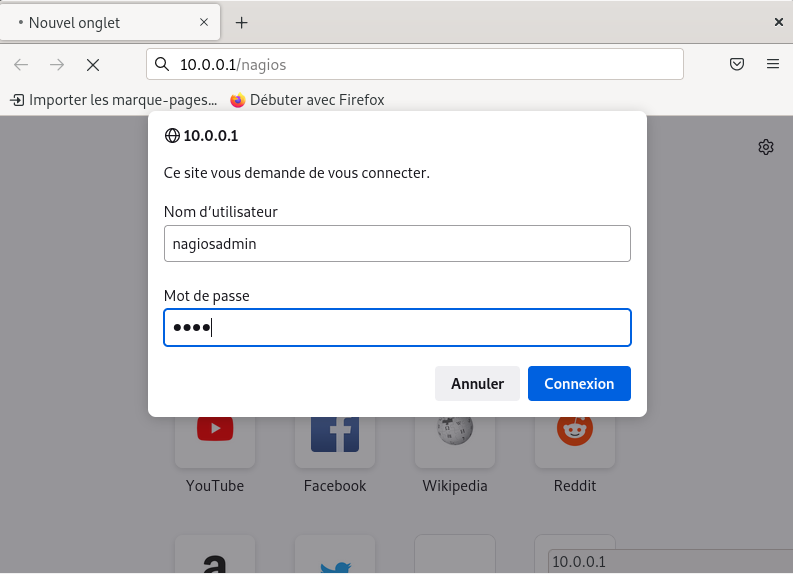
**TECH. HACKING**

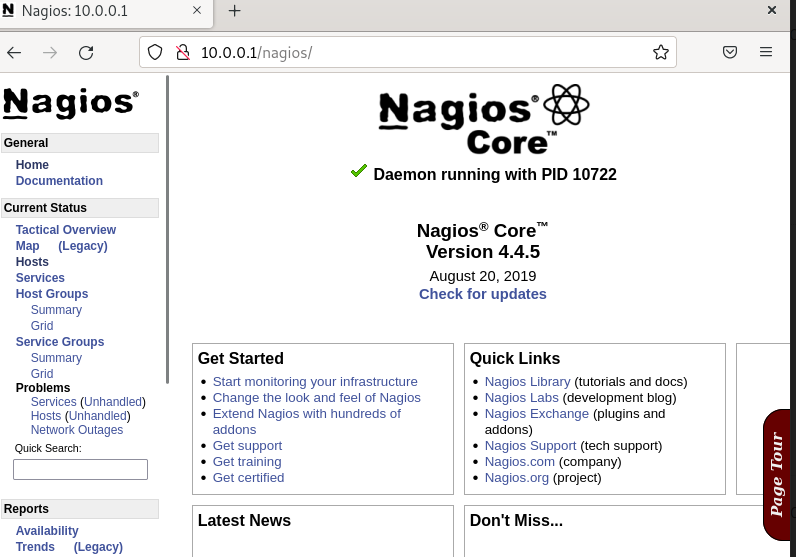
1°) **Nagios**

Nagios est un système de surveillance réseau et de gestion d’alertes. Il est utilisé pour surveiller l’état et la disponibilité des ressources, des services et des hôtes sur un réseau informatique.

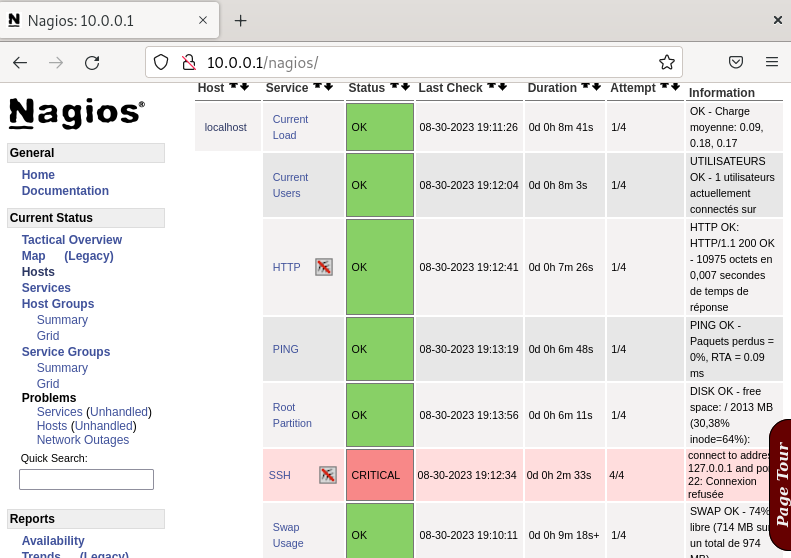
L’installation de nagios se trouve dans le fichier pdf de cours Tech. Hacking et sécurité.



Ici on va se connecter sur nagios.



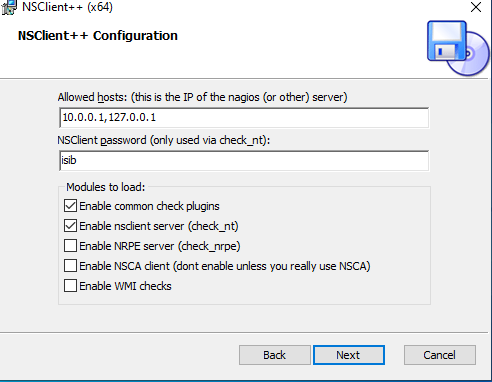
On aura ceci.



Tous les status c’est ok .

2°) **NSclient**

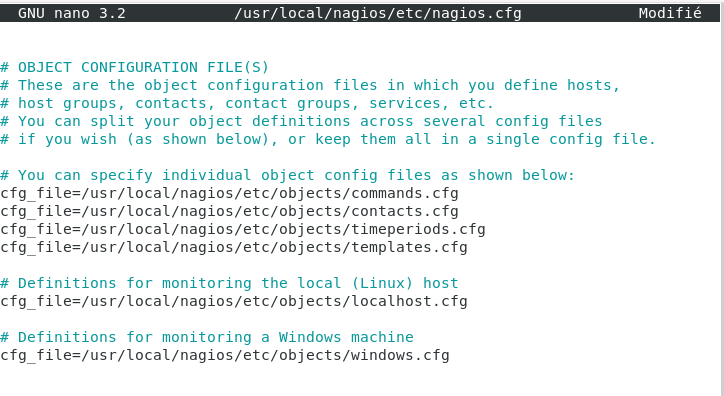
Le NSclient est un logiciel qui agit comme un agent de surveillance pour les systèmes d’exploitation Windows.



Ici on va configurer le NSclient.

Puis lorsque l’installation a été fini, on va aller sur la machine debian où y a Nagios pour activer la surveillance sur des machines windows distants donc on va écrire cette commande:

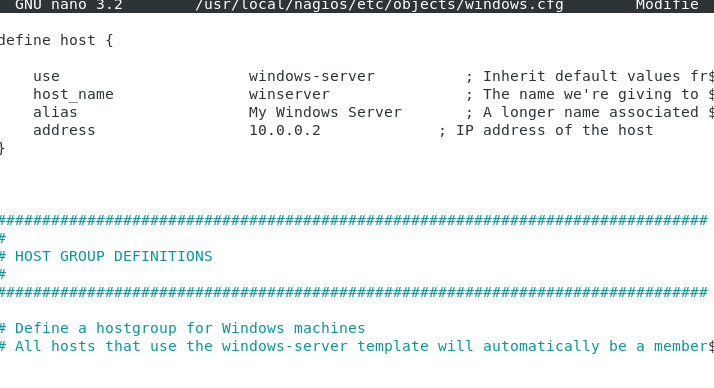




On va décommentez **cfg\_file=/usr/local/nagios/etc/onjects/windows.cfg**

Puis on s’y rend dedans:



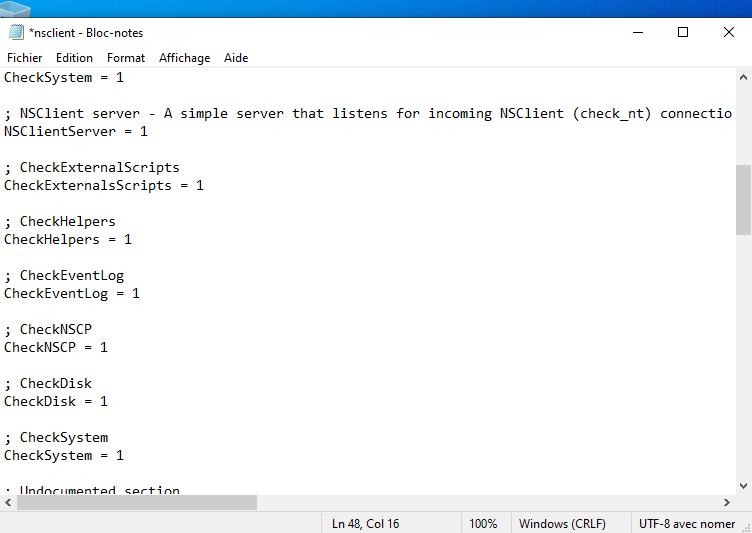


Du coup ici on aura changé l’adresse IP pour mettre l’adresse IPv4 de la machine cliente.

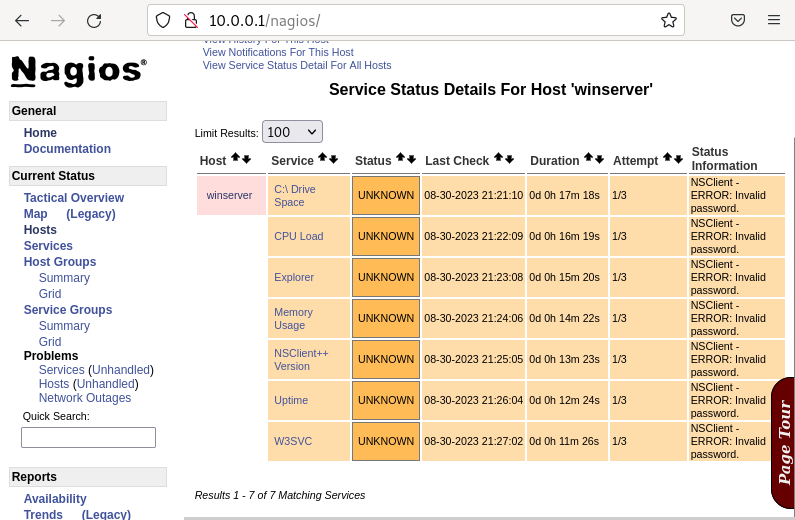


Puis on redémarre le service nagios.

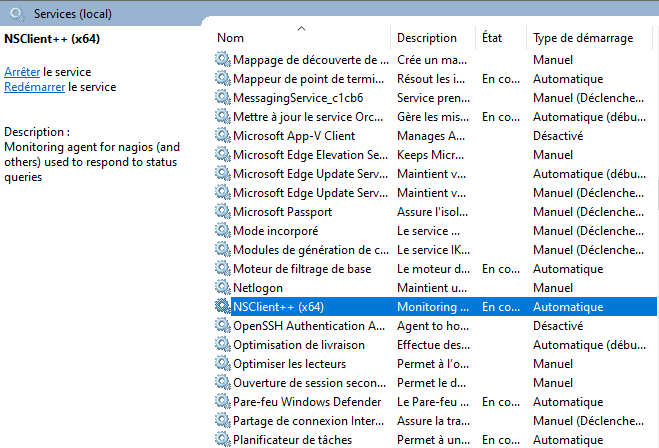
Puis on va dans la machine client pour configurer dans nsclient.init



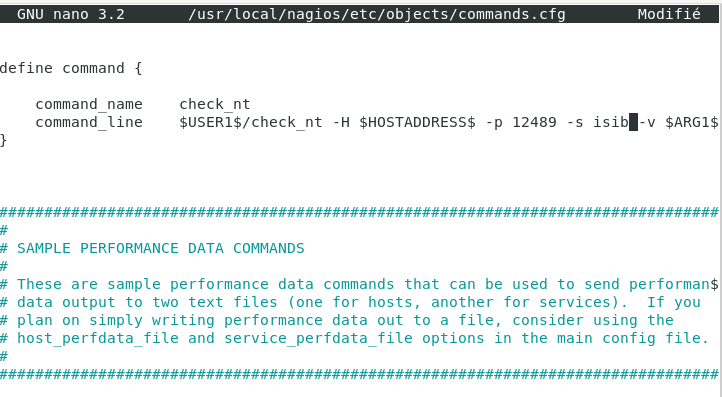
Puis on s’y rend nagios pour voir des changements



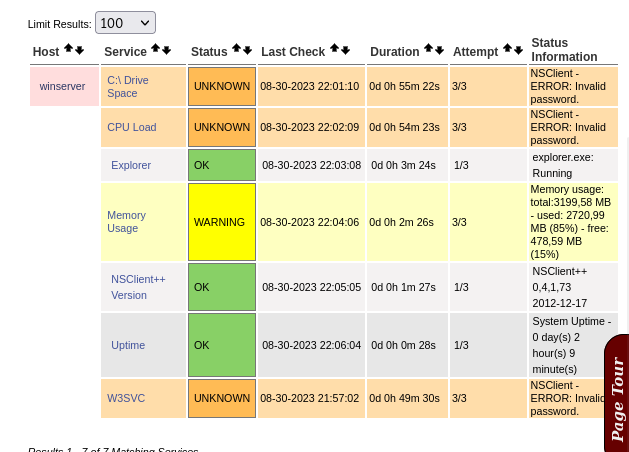
Il y a le status UNKNOWN , on va essayer de redémarrer le service NSclient dans la machine cliente.



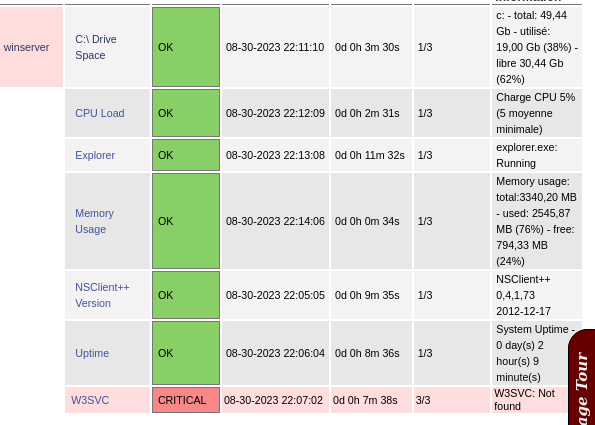
J’ai redémarré le service mais ça ne marche toujours pas, et l’erreur c’est “NSClient - ERROR : Invalid password”

D’après des recherches 

Fallait mettre dans define command de check\_nt => notre mot de passe

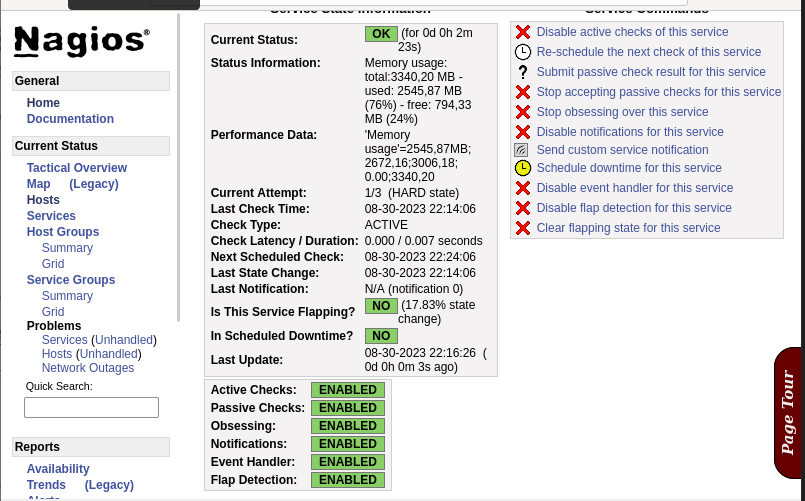


La ca commence à venir petit à petit.



Après un certain temps tous les modules activés sont en status OK.

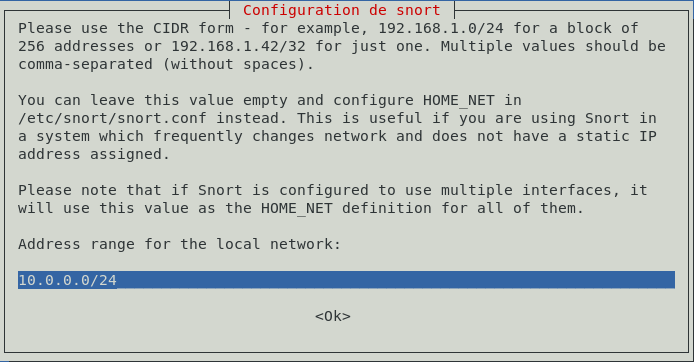
On peut voir les informations de la mémoire RAM.



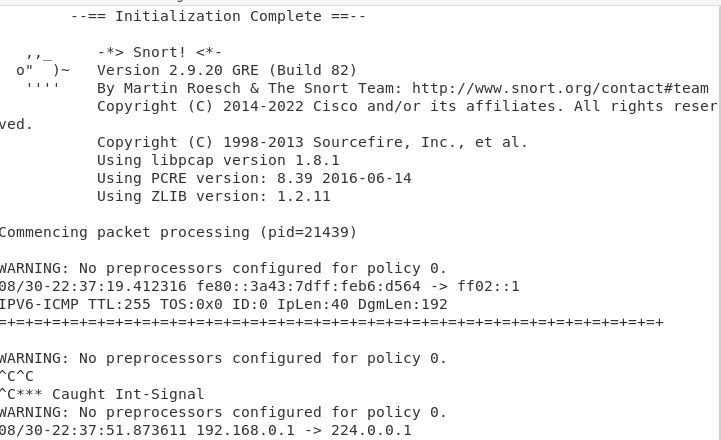
3°) **SNORT**

Snort est un système de détection d’intrusion pour surveiller et analyser le trafic réseau en temps réel.

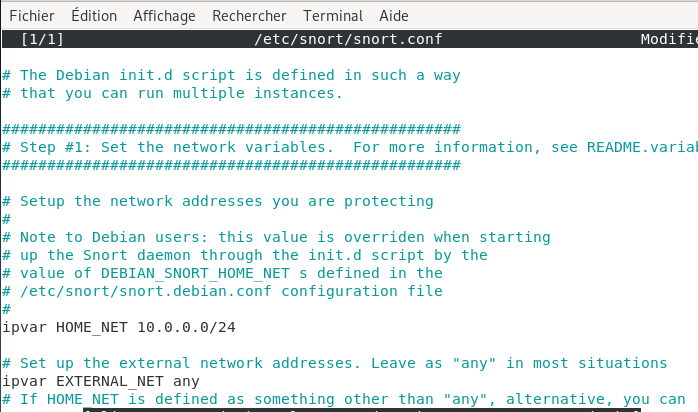




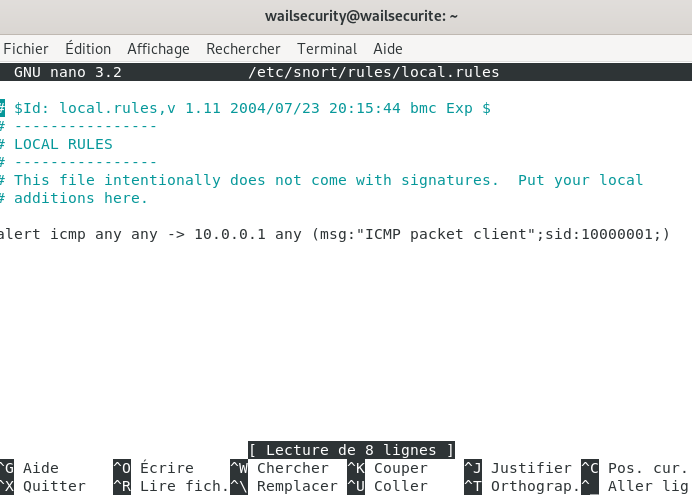
On va configurer ici



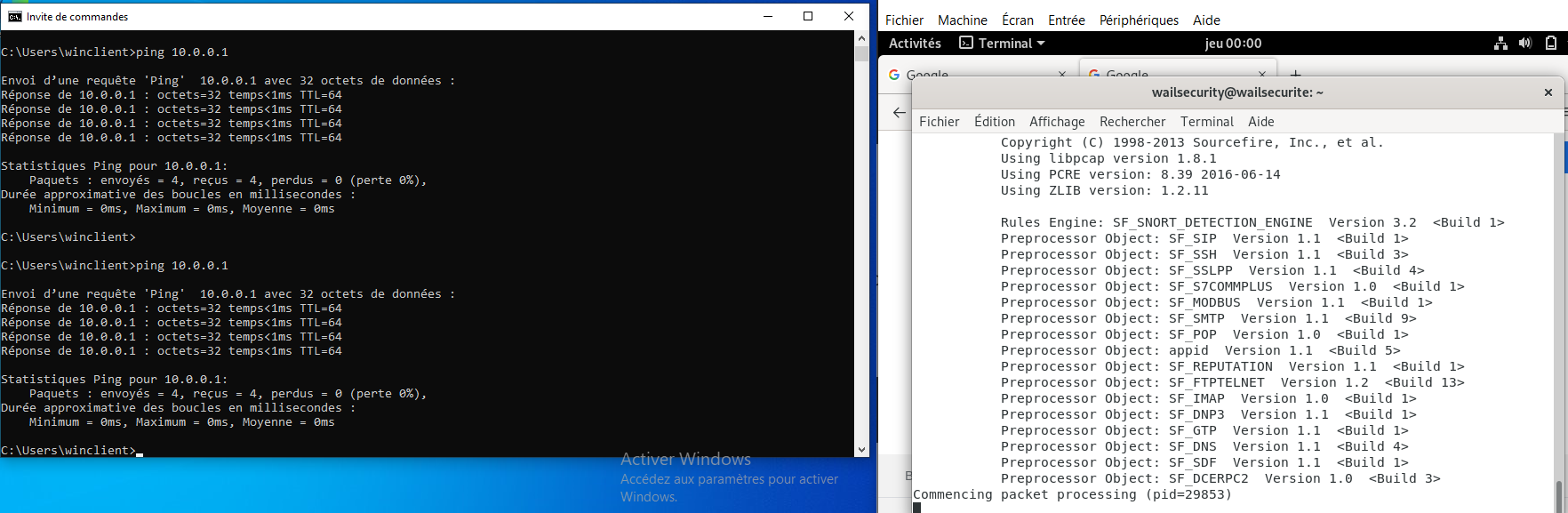
Mise en application de snort



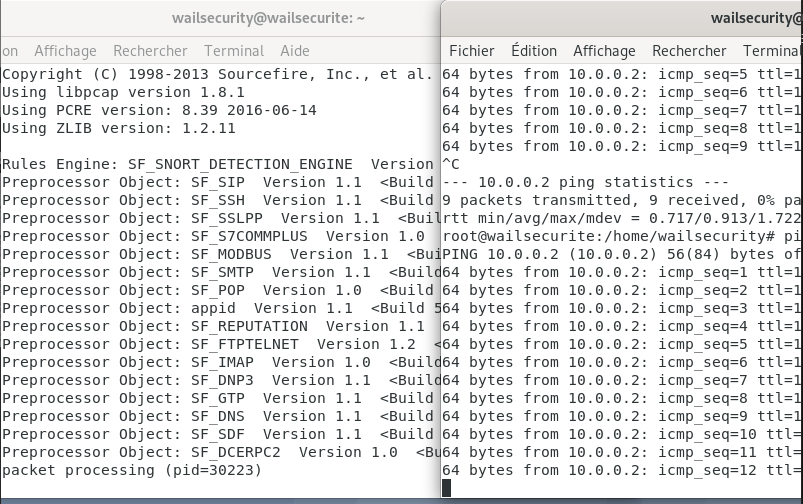
On va configurer ici la même



On va tester :

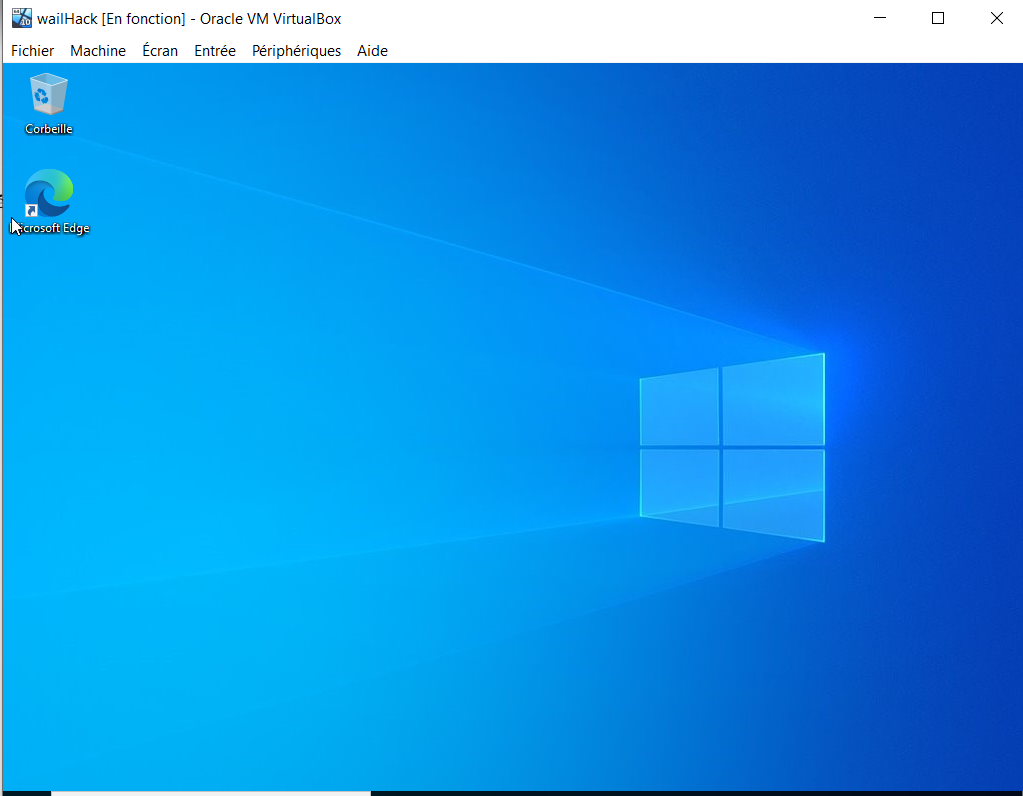


On fait de l’autre côté

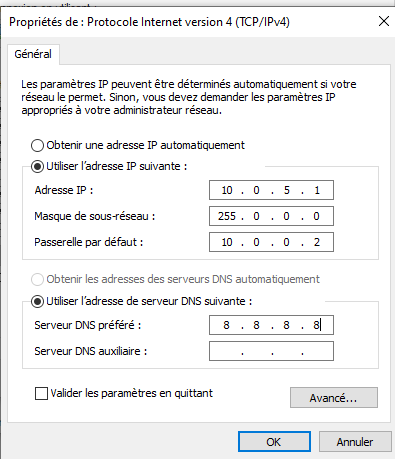


Ca ne marche pas .

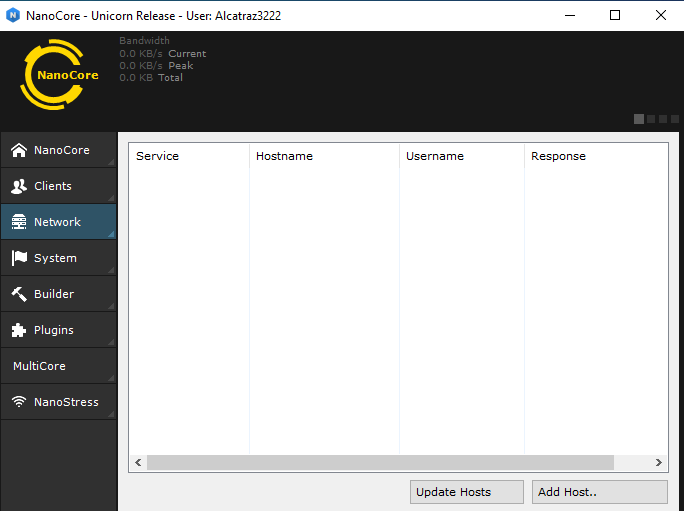
**4°) Deploiement de Trojan RAT sur la machine cliente**



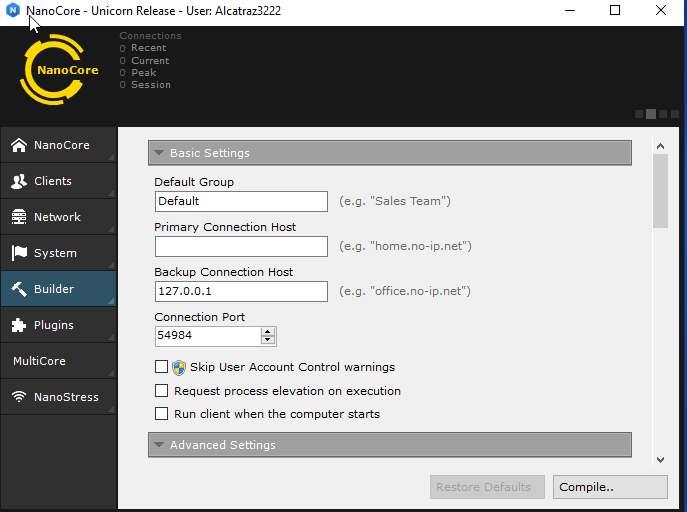
On a créé une machine où on va télécharger le malware.



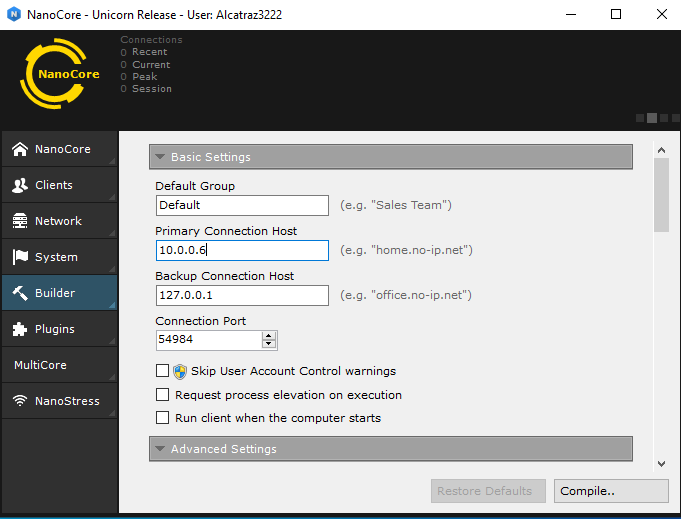
Ici on a configuré notre carte réseau

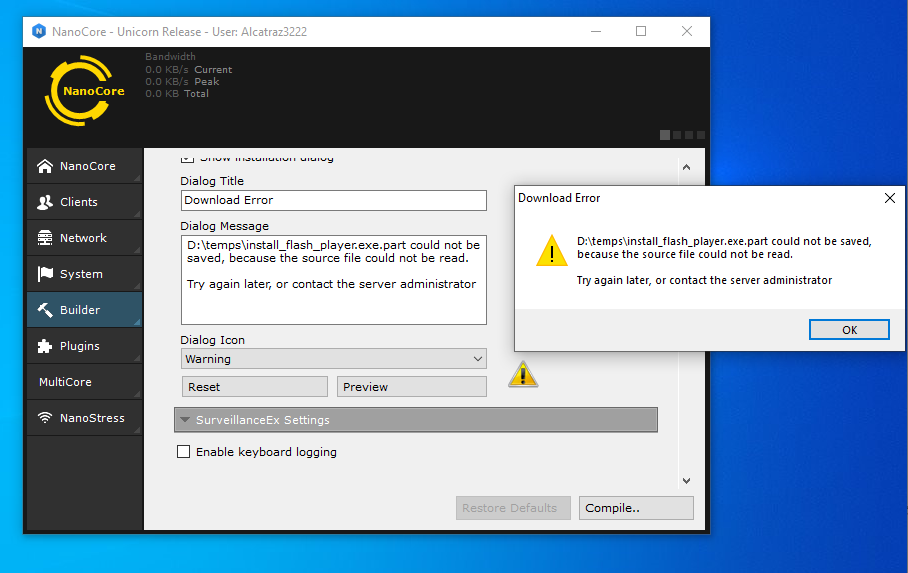


On aura installé Nanocore est un malware de type RAT.



Ici on va faire la configuration de l’adresse hôte

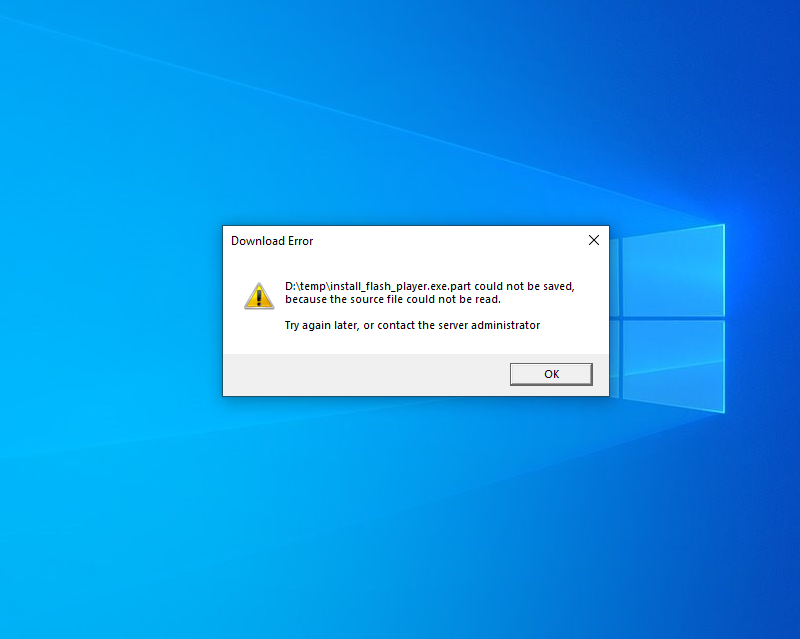




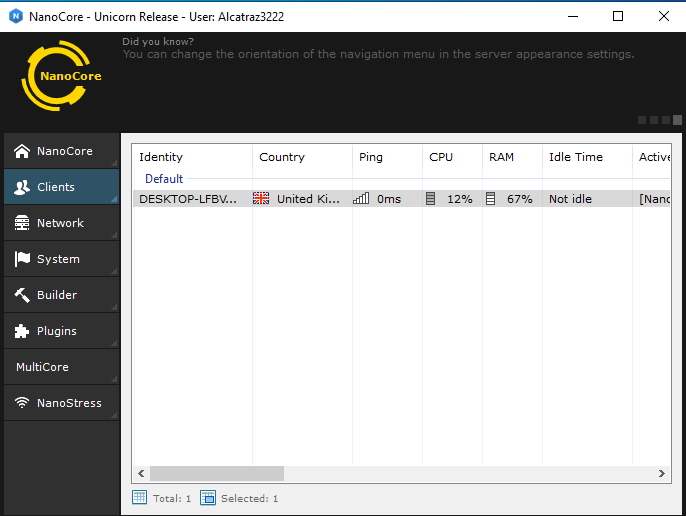
On va créer ici une page pop-up qui va dire que le fichier source n’a pas pu être lu

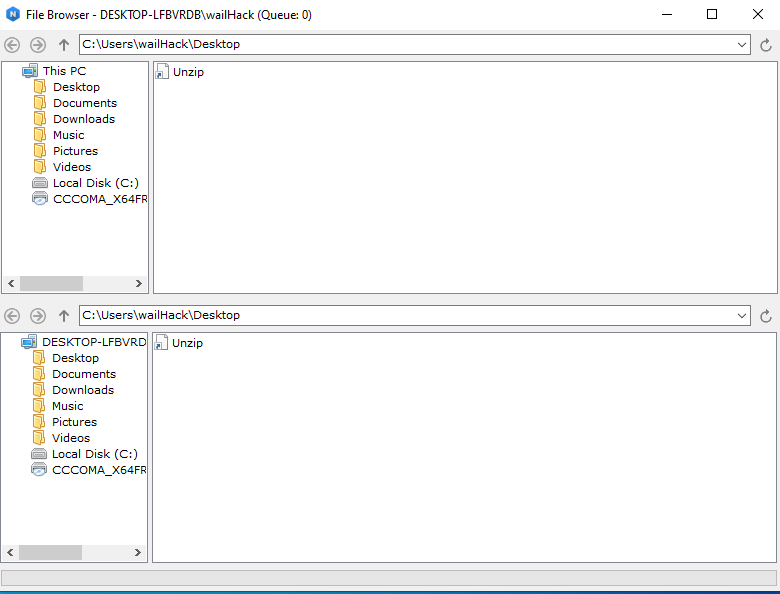
On va utiliser la méthode **ingénierie sociale** on va envoyer la personne sur gmail une mise à jour de flash player dans son entreprise.

La personne va cliquer en voyant que cette appli est importante pour l’entreprise.

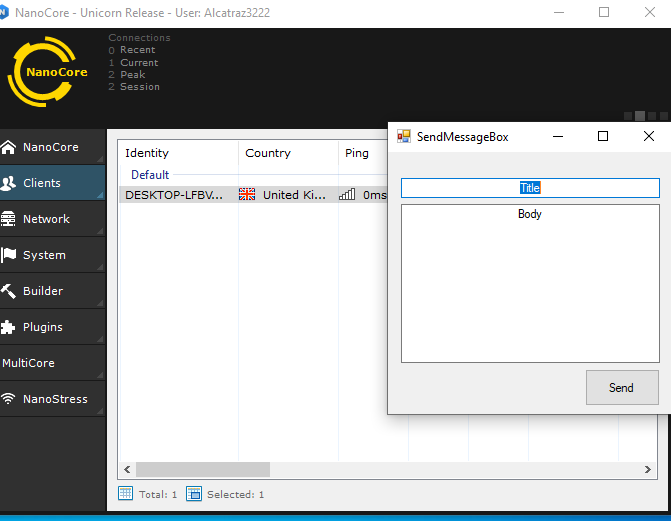


Puis lors de clique le hackeur a pu se connecter sur son pc

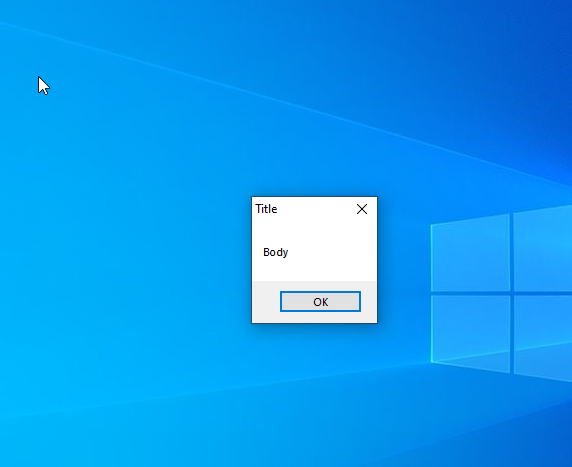


Et là il peut faire ce qu’il veut 

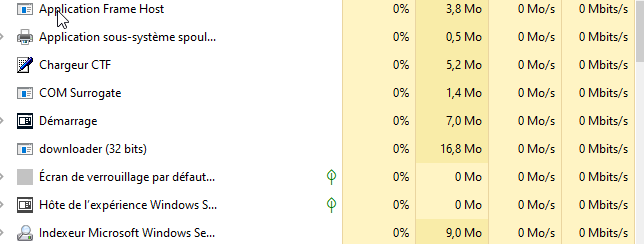
Il a accès à ses dossiers,fichiers,etc...



Il peut envoyer un message depuis son pc



Et pleins de trucs aussi à l’accès de son cmd.



Ici on peut voir que l’application tourne en arrière plan.



Cependant la vue à distance prend beaucoup de ressources.

**5°) Kali Linux et Attaque Hydra**

Le Kali Linux est une distribution de système d’exploitation basée sur Linux donc il est conçu pour les tests de pénétration, la sécurité informatique et les activités d'hacking.



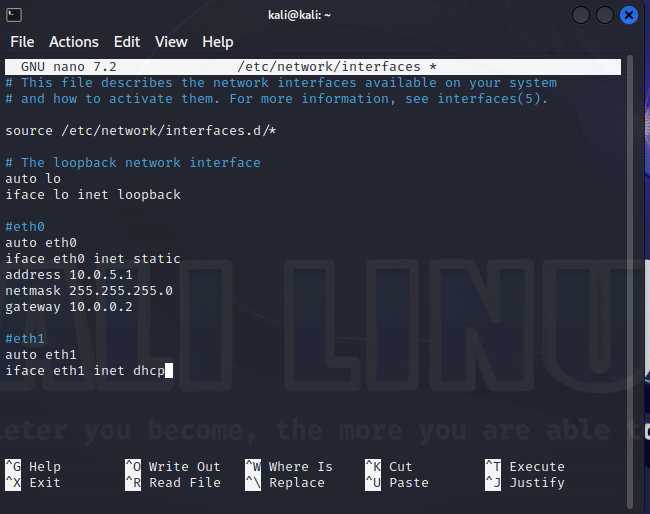
On a l’installation puis



Plusieurs choix intéressant



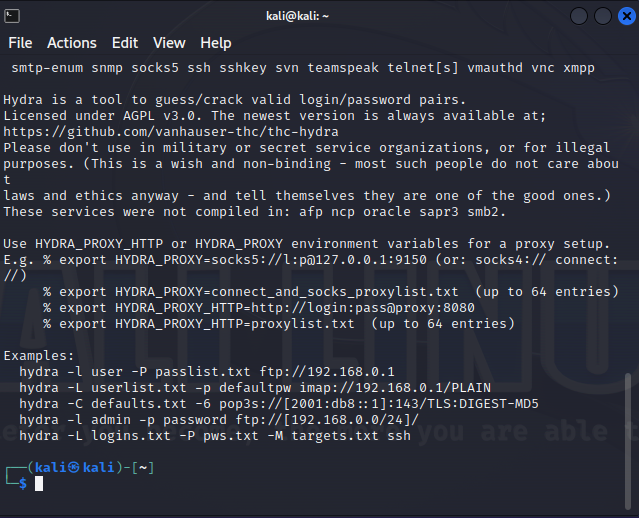
Les appli hacking proposé par kali



Ici j’ai configuré

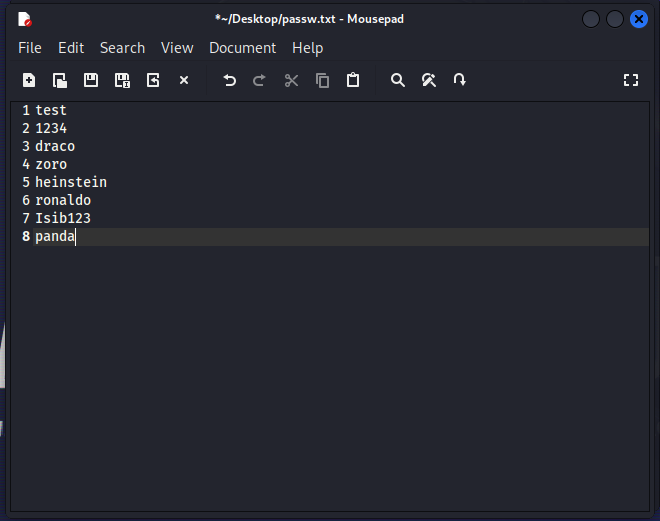
J'ai activé aussi le routage :

On va faire l’attaque hydra , donc appelé “brute force attack” est une attaque utilisé en sécurité informatique pour tenter de trouver des mot de passe ou des clés en testant systématiquement toutes les combinaisons possible.



Ici Kali Linux nous donne des exemples d’attaque.

D'abord on va créer une liste



Par exemple on va se connecter dans la machine client où y a NSclient



Et du coup il va chercher le mot de passe du coup faut toujours faire des mot de passe complexe.