# Utiliser nmap pour la découverte du réseau

**Correction**

Il faut trouver le serveur friedshrimp comme on ne connait pas son ip, on va lancer nmap pour découvrir les machines autour qui ont les ports entre 2000-3000 ouverts

En effet un **nslookup** ne nous retourne rien avec le nom friedshrimp seul

nmap -A -p 2000-3000 172.25.0.1-255



On constate que le service ssh est ouvert sur

nmap-discovery.friedshrimp.student.intranet (172.25.0.5)

2732/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)

Le port est donc **2732** et l’IP **172.25.0.5**

ssh -p 2732 172.25.0.5 permet d’accéder à la machine friedshrimp



Une fois que vous avez accès au serveur friedshrimp, vous pouvez lire le fichier souhaité

>ls

friedshrimp.txt

>cat friedshrimp.txt

Une autre possibilité (non comptabilisée dans le lab) depuis l’ordinateur « client »

ubuntu@mycomputer:~$ scp -P 2706 ubuntu@172.25.0.5:~/friedshrimp.txt ./friedshrimp.txt

ou

ubuntu@mycomputer:~$ scp -P 2706 ubuntu@nmap-discovery.friedshrimp.student.intranet:~/friedshrimp.txt ./friedshrimp.txt