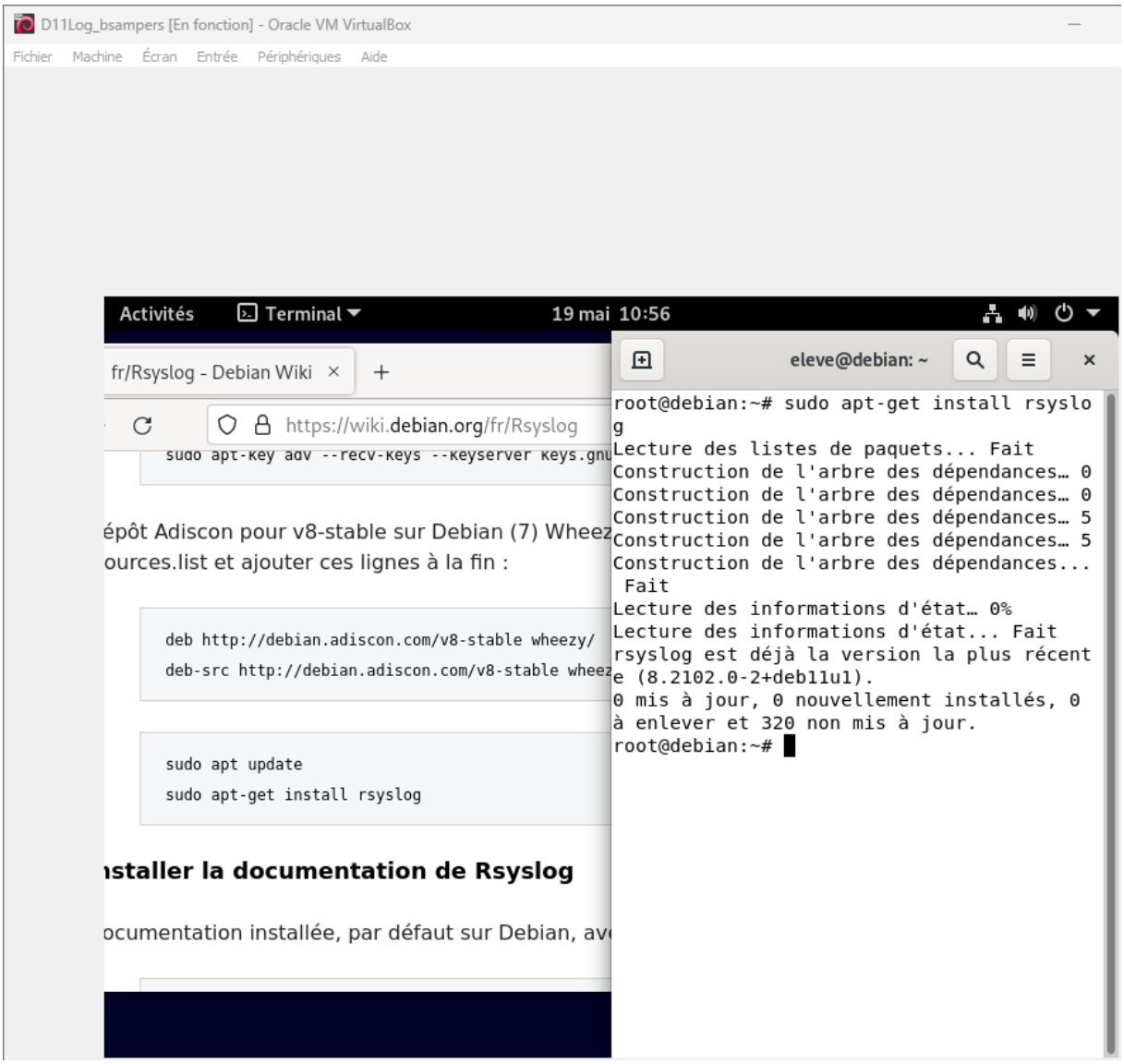
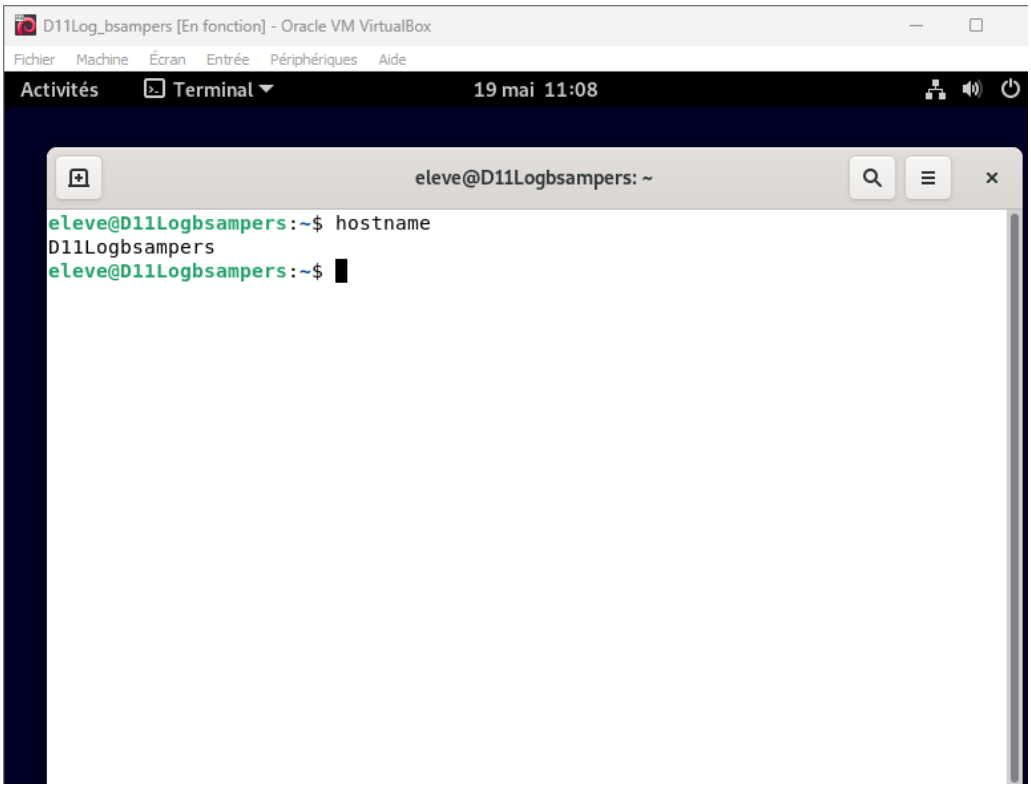
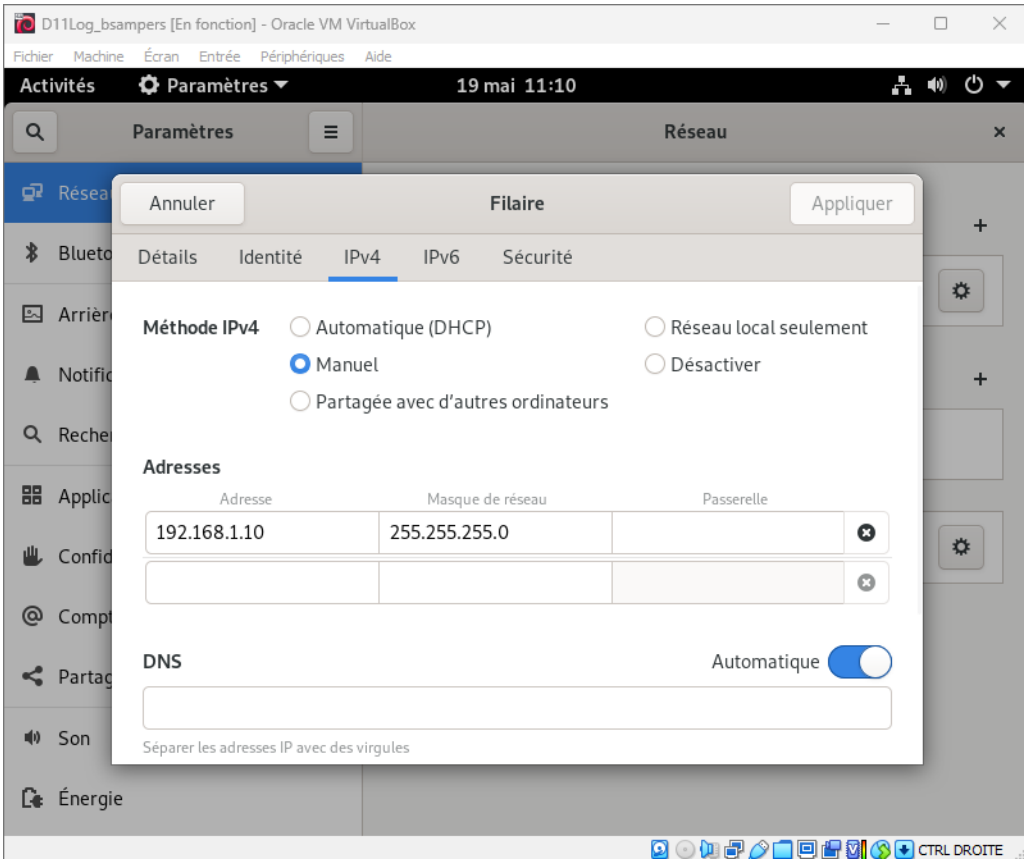
/Benjamin Sampers

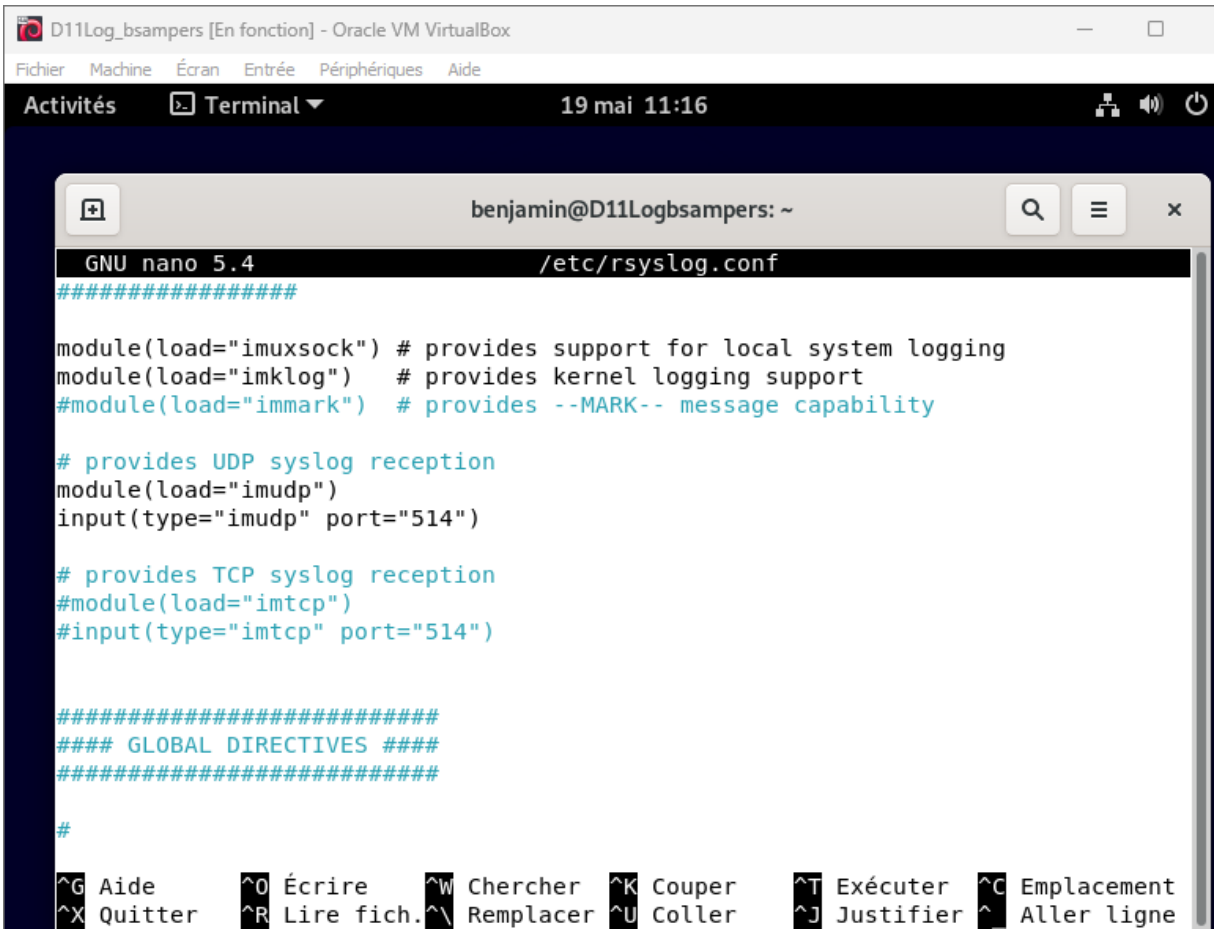
TP6 - Rsyslog



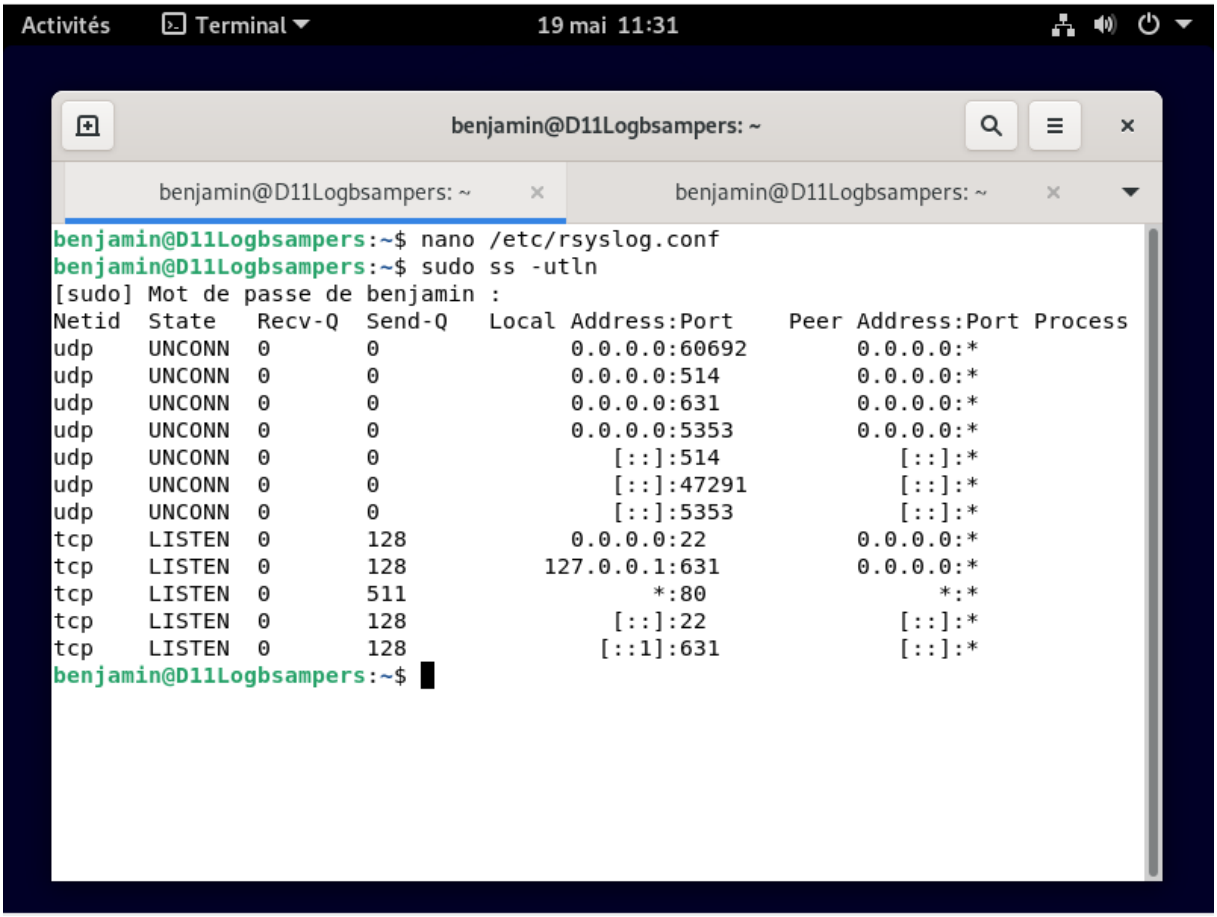
Nous installons tout d'abord rsyslog sur le serveur Log, c'est grâce à cela que nous allons pouvoir centraliser les logs de plusieurs machines sur un seul et même serveur.


D11Log_bsampers [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Activités
Terminal
19 mai 11:08
eleve@D11Logbsampers: ~
eleve@D11Logbsampers:~$ hostname
D11Logbsampers
eleve@D11Logbsampers:~$

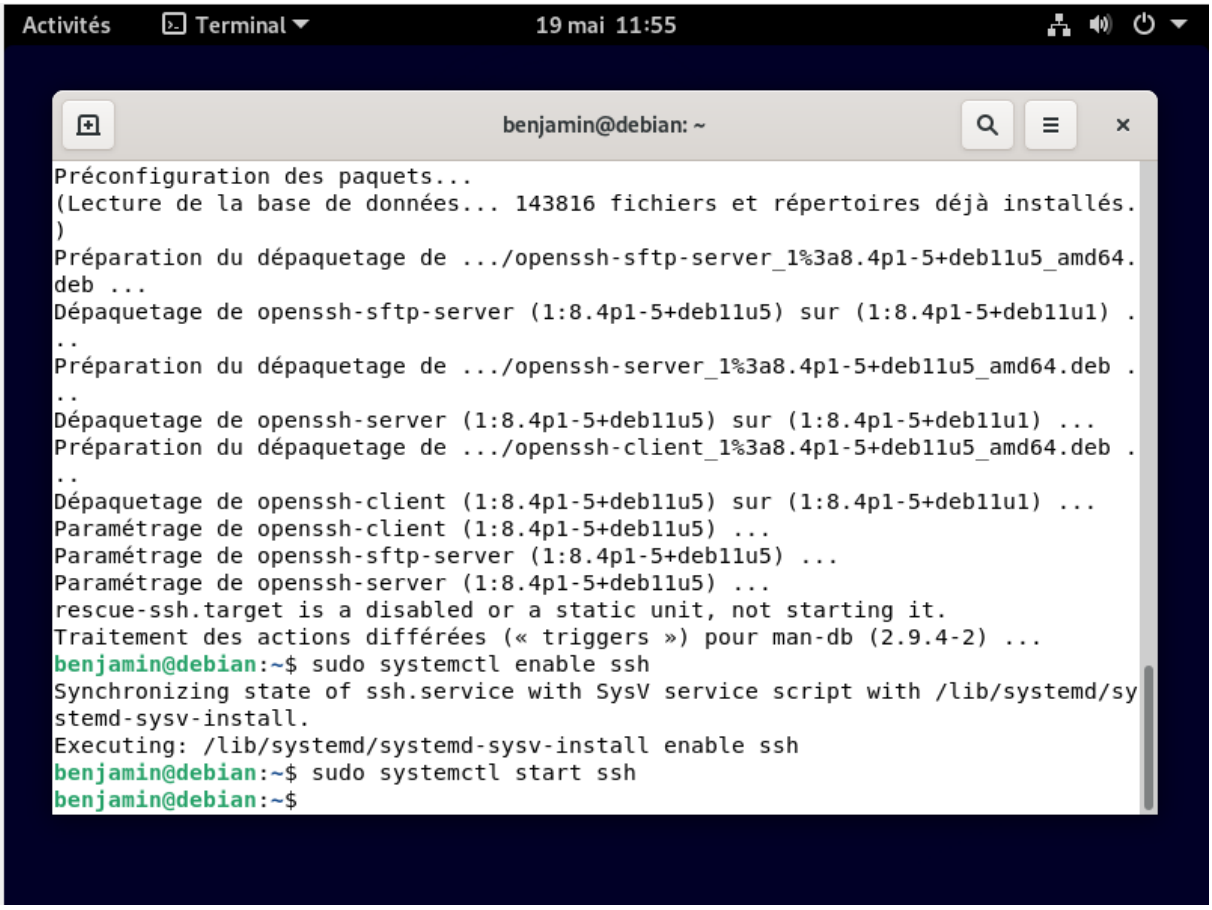

D11Log_bsampers [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Activités
Paramètres
19 mai 11:10
Paramètres
Réseau
Annuler
Filaire
Appliquer
Détails
Identité
IPv4
IPv6
Sécurité
Méthode IPv4
Automatique (DHCP)
Manuel
Partagée avec d'autres ordinateurs
Réseau local seulement
Désactiver
Adresses
Adresse
Masque de réseau
Passerelle
192.168.1.10
255.255.255.0
DNS
Automatique
Séparer les adresses IP avec des virgules
Son
Énergie
CTRL DROITE



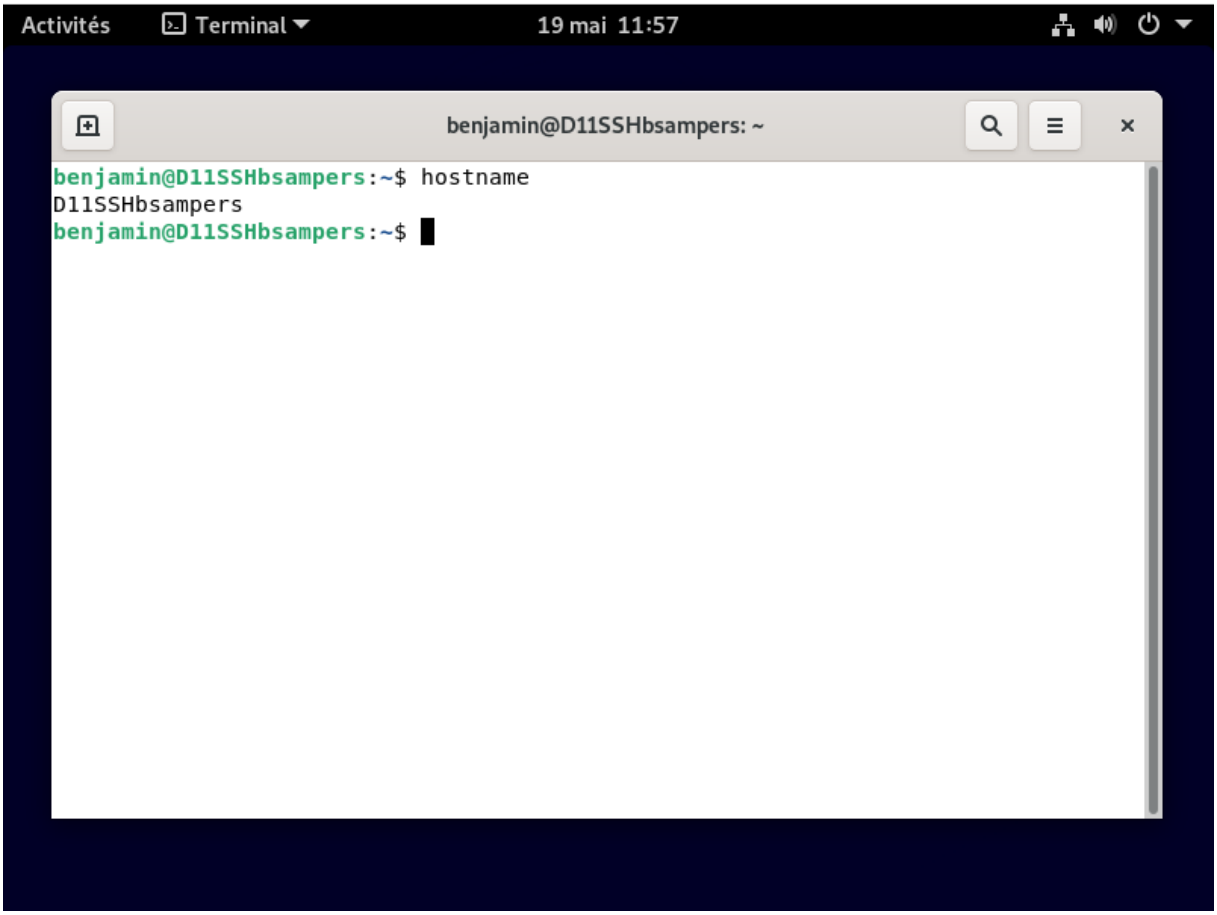
Nous activons le module UDP qui est identifié par le port 514.

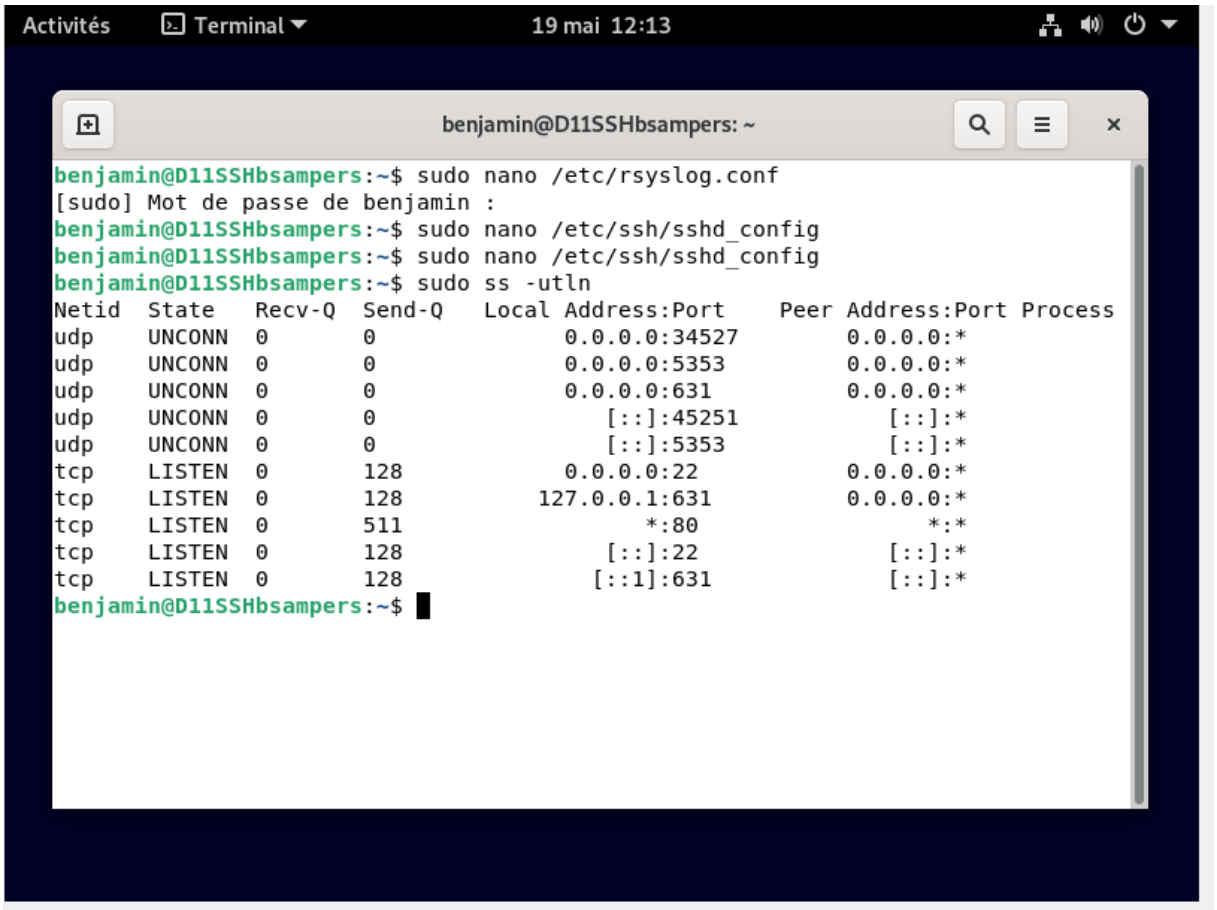


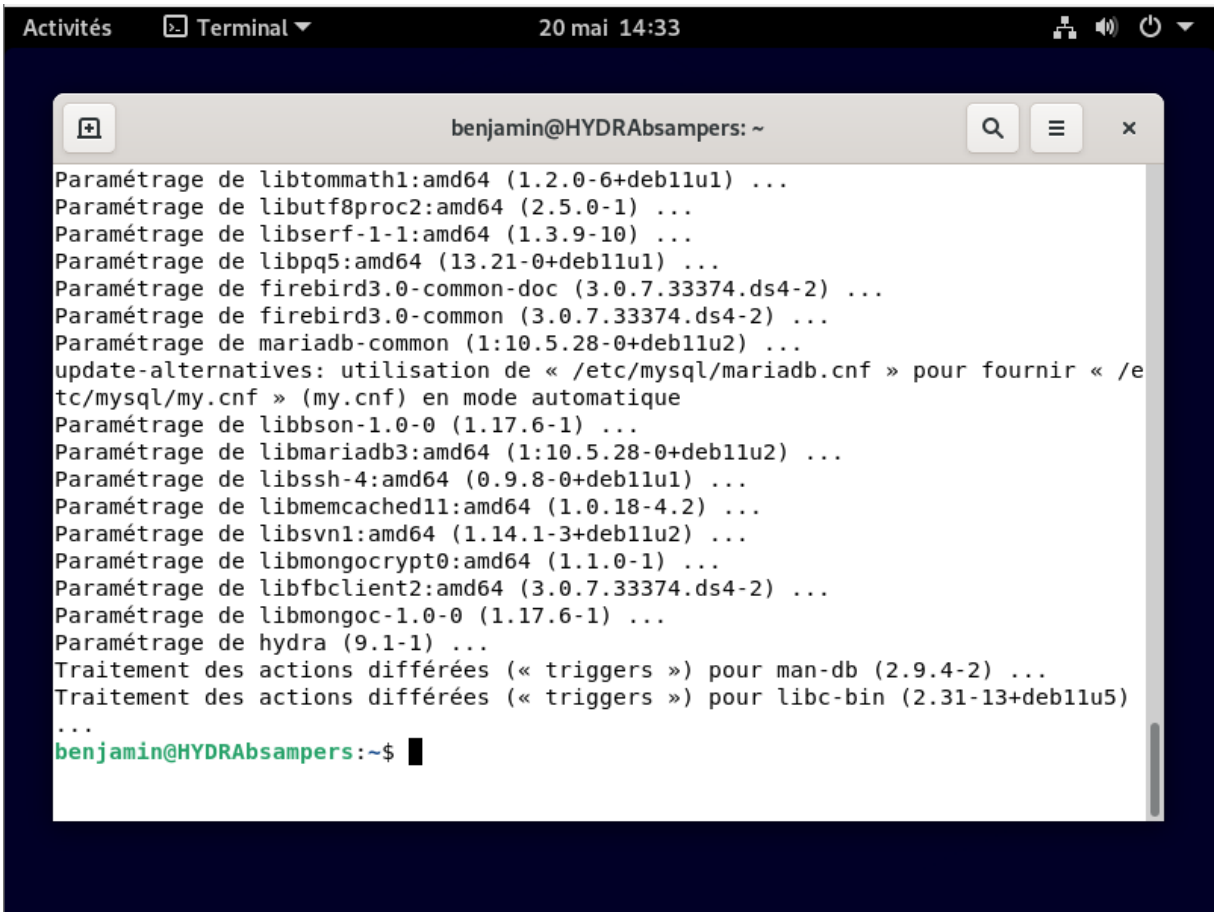
Nous pouvons donc remarquer dans le gestionnaire que le port 514 apparaît bien.



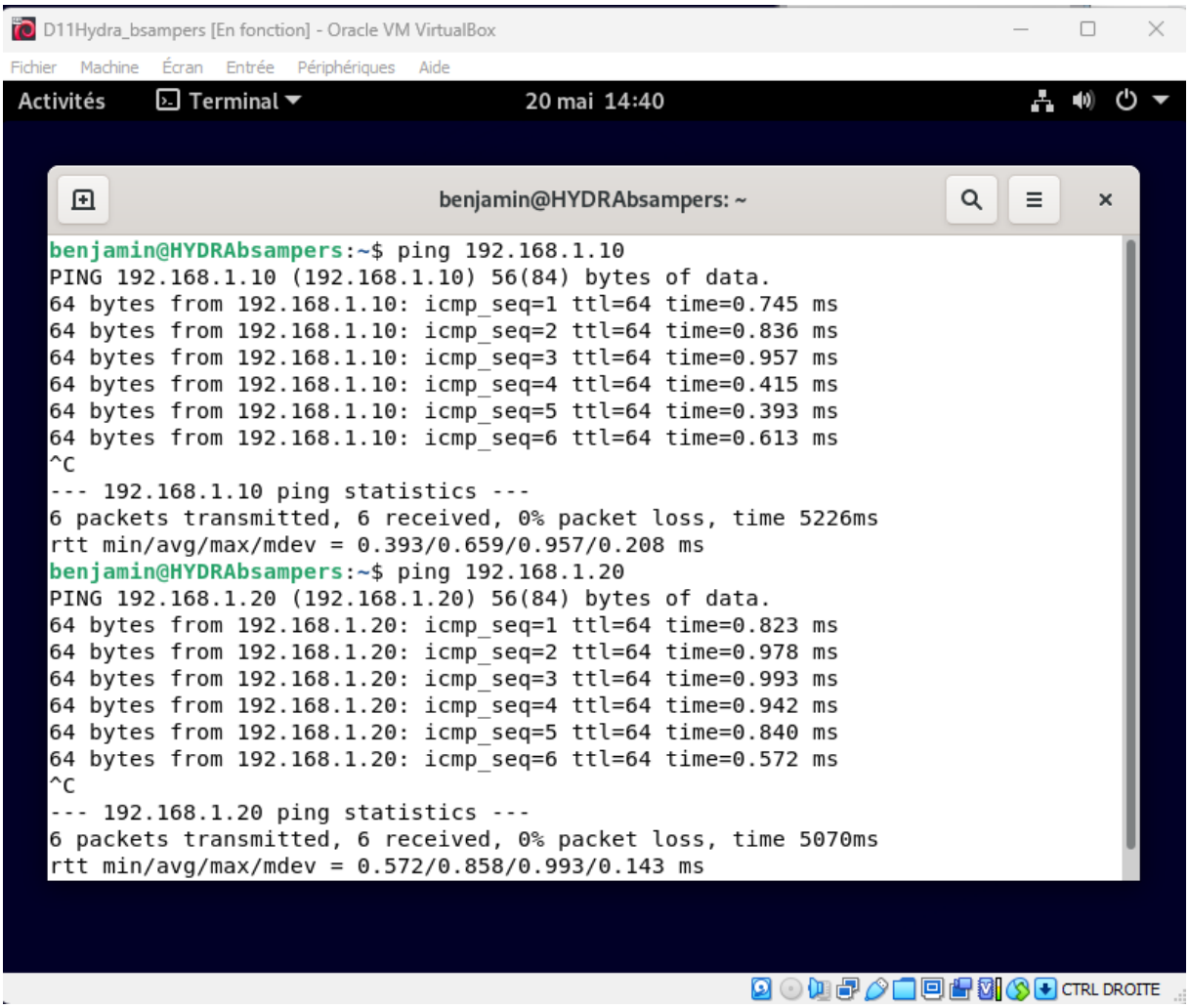
Du côté du serveur SSH, nous installons et démarrons le serveur SSH.


Activités
Terminal
19 mai 11:57
benjamin@D11SSHbsampers: ~
benjamin@D11SSHbsampers:~$ hostname
D11SSHbsampers
benjamin@D11SSHbsampers:~$

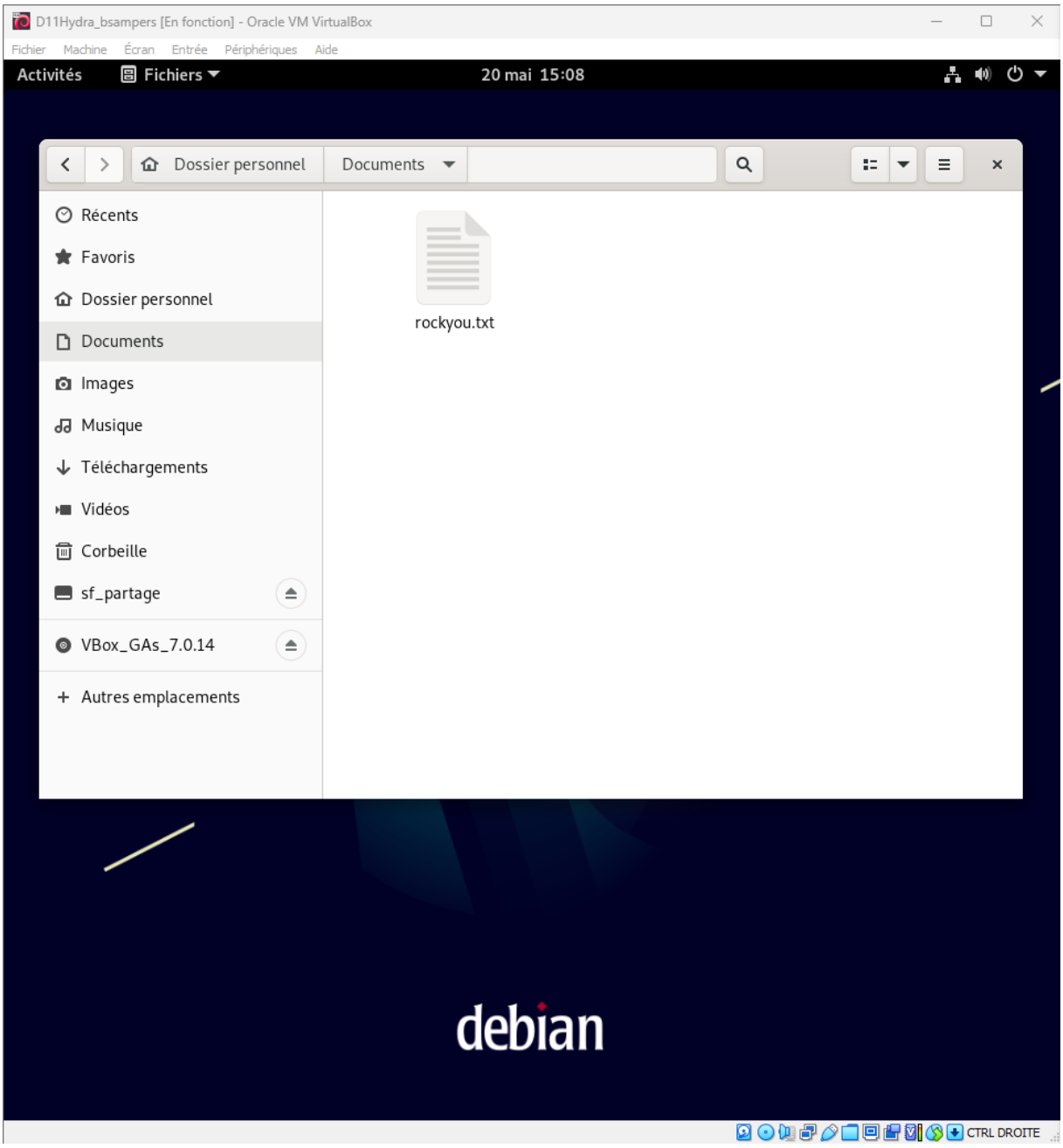

Activités
Terminal
19 mai 12:13
benjamin@D11SSHbsampers: ~
benjamin@D11SSHbsampers:~$ sudo nano /etc/rsyslog.conf
[sudo] Mot de passe de benjamin :
benjamin@D11SSHbsampers:~$ sudo nano /etc/ssh/sshd_config
benjamin@D11SSHbsampers:~$ sudo nano /etc/ssh/sshd_config
benjamin@D11SSHbsampers:~$ sudo ss -utln
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
udp UNCONN 0 0 0.0.0.0:34527 0.0.0.0:*
udp UNCONN 0 0 0.0.0.0:5353 0.0.0.0:*
udp UNCONN 0 0 0.0.0.0:631 0.0.0.0:*
udp UNCONN 0 0 [::]:45251 [::]:*
udp UNCONN 0 0 [::]:5353 [::]:*
tcp LISTEN 0 128 0.0.0.0:22 0.0.0.0:*
tcp LISTEN 0 128 127.0.0.1:631 0.0.0.0:*
tcp LISTEN 0 511 *:80 *:*
tcp LISTEN 0 128 [::]:22 [::]:*
tcp LISTEN 0 128 [::1]:631 [::]:*
benjamin@D11SSHbsampers:~$



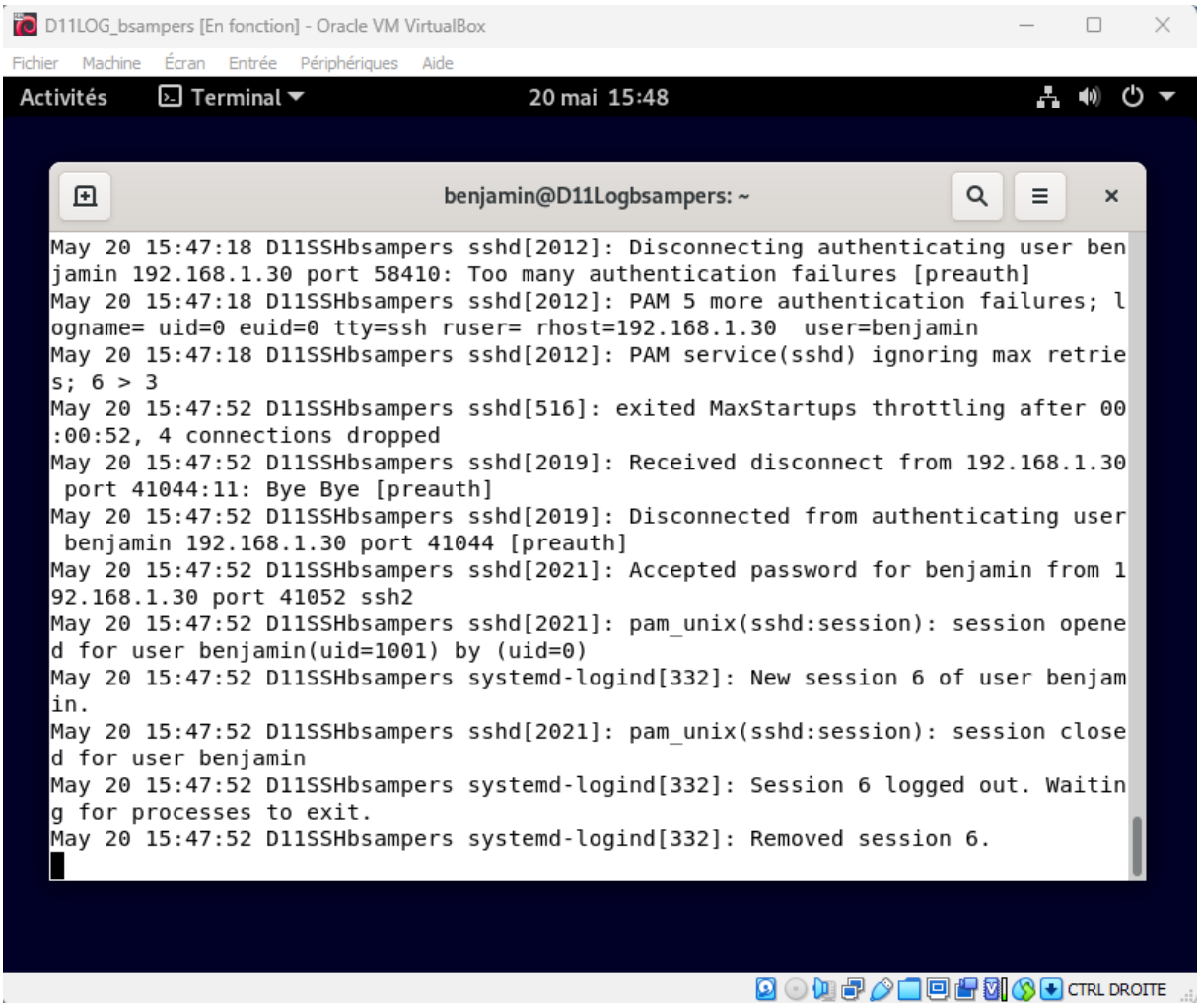
Nous nous occupons d'installer Hydra sur notre dernière machine, elle nous permettra d'envoyer une attaque par force brute par dictionnaire sur le serveur SSH.



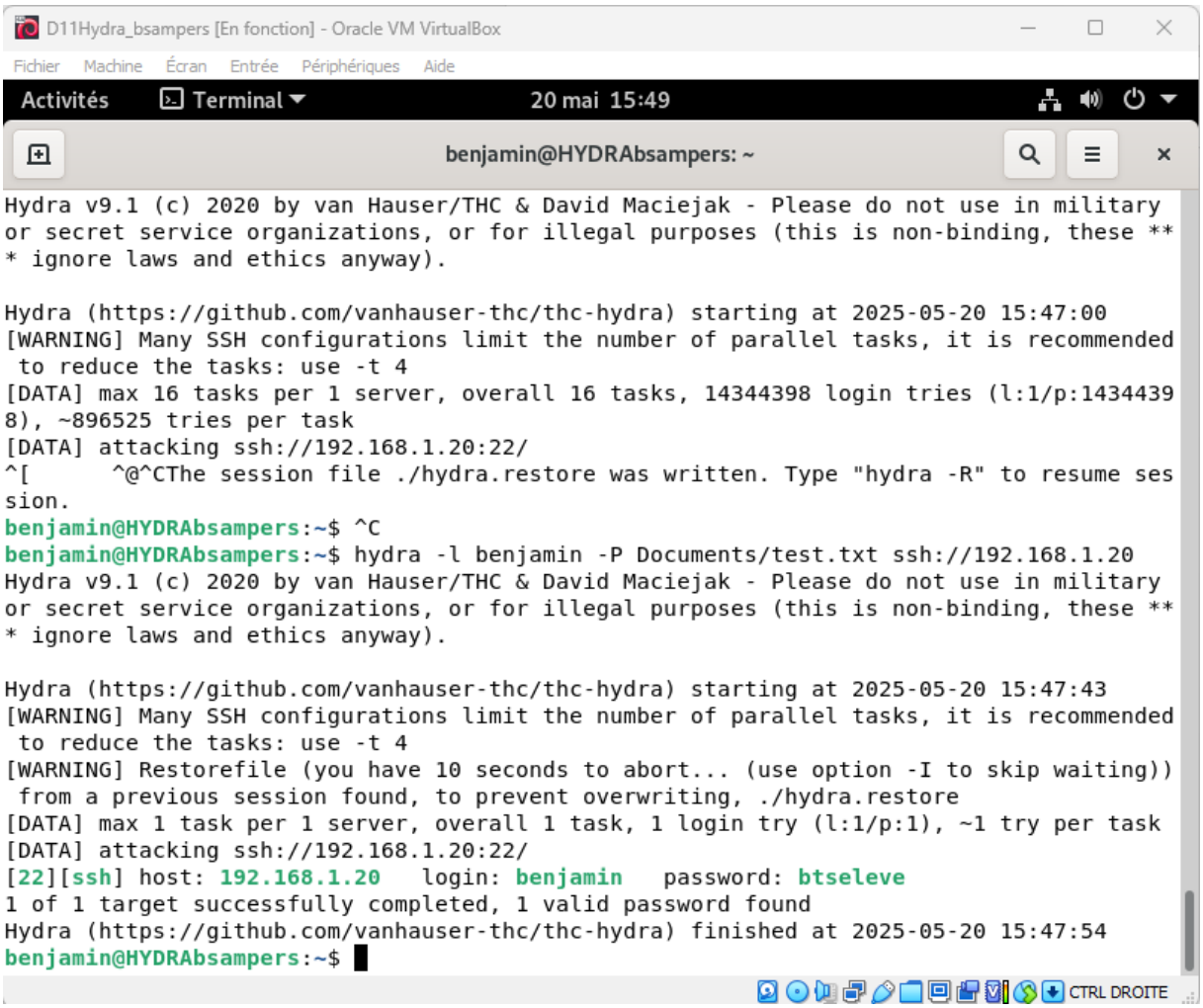
Les ping permettent ici de certifier que les machines communiquent bien entre elles.



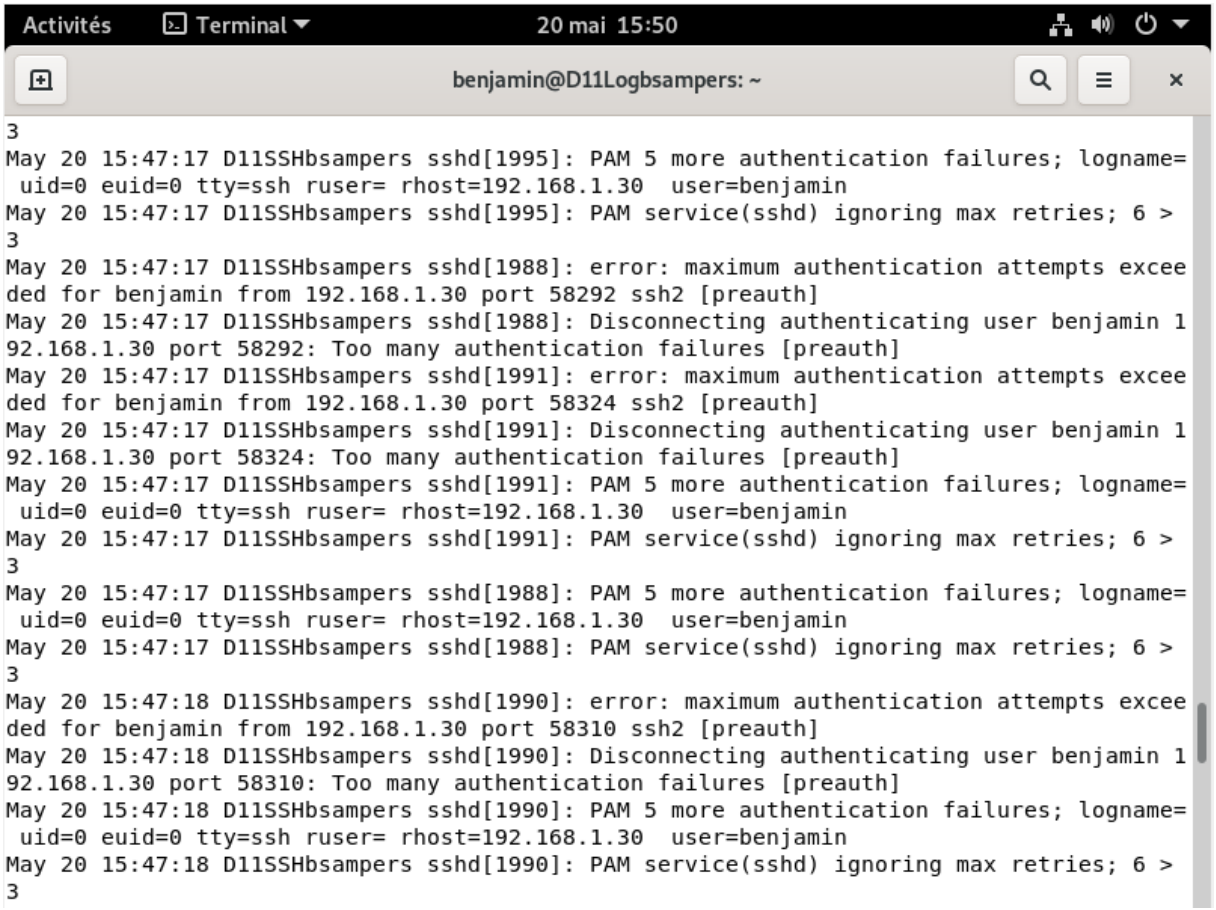
Nous avons créé un dossier partage afin de pouvoir récupérer le fichier rockyou.txt sur la machine Hydra.



Nous pouvons voir sur le serveur Log que nous recevons des logs de la part du serveur SSH concernant l'adresse ip 192.168.1.30 qui a réussi à se connecter au serveur SSH.



Du côté de la machine Hydra, nous avons réussi à casser le code de l'utilisateur 'benjamin'.



Ici, nous voyons que la machine 192.168.1.30 fait de multiples tentatives de connexion frauduleuses, cela indique qu'il y a probablement une attaque en force brute. La solution ici serait de bloquer les adresses IP qui provoquent trop de tentatives frauduleuses à la minute.