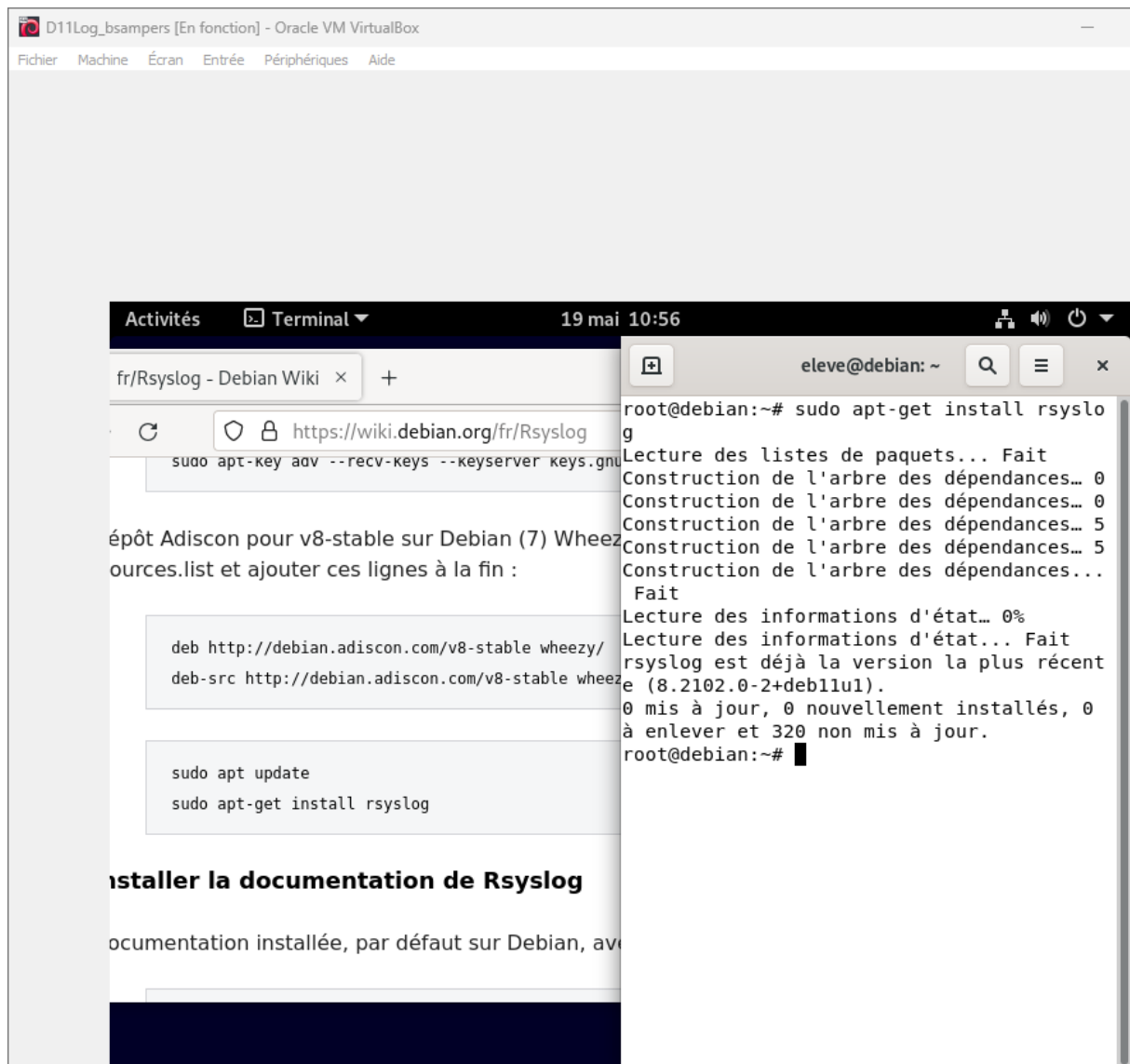
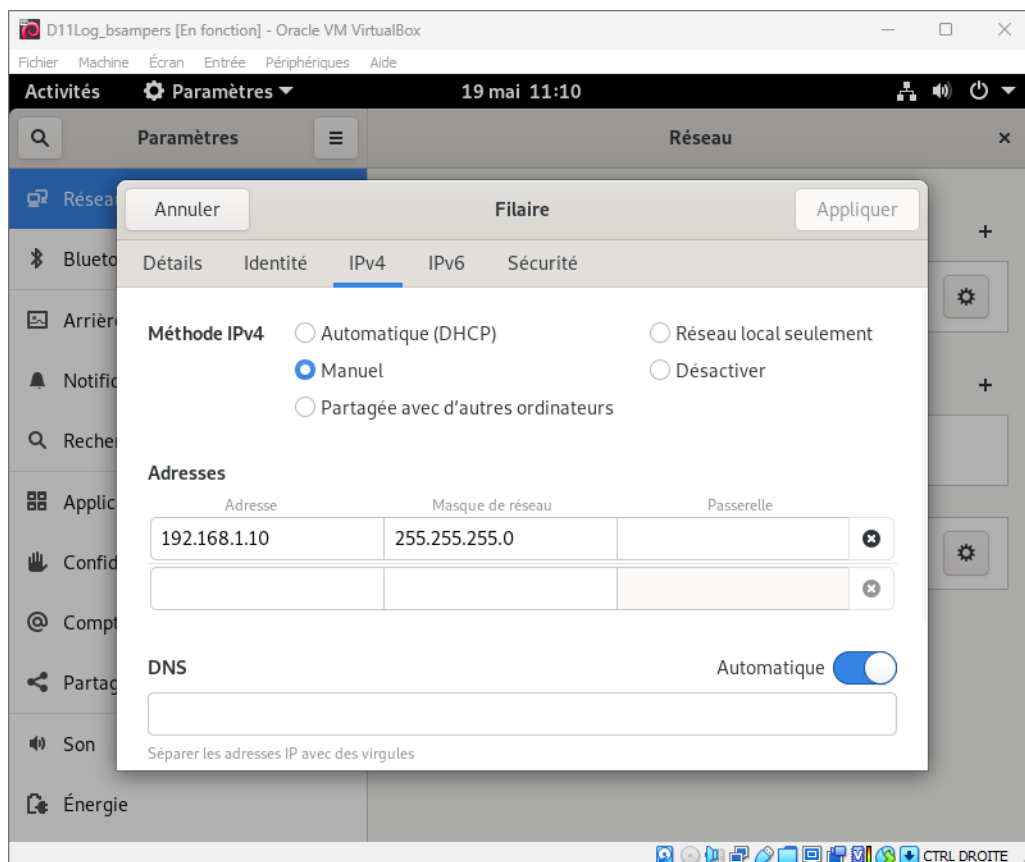
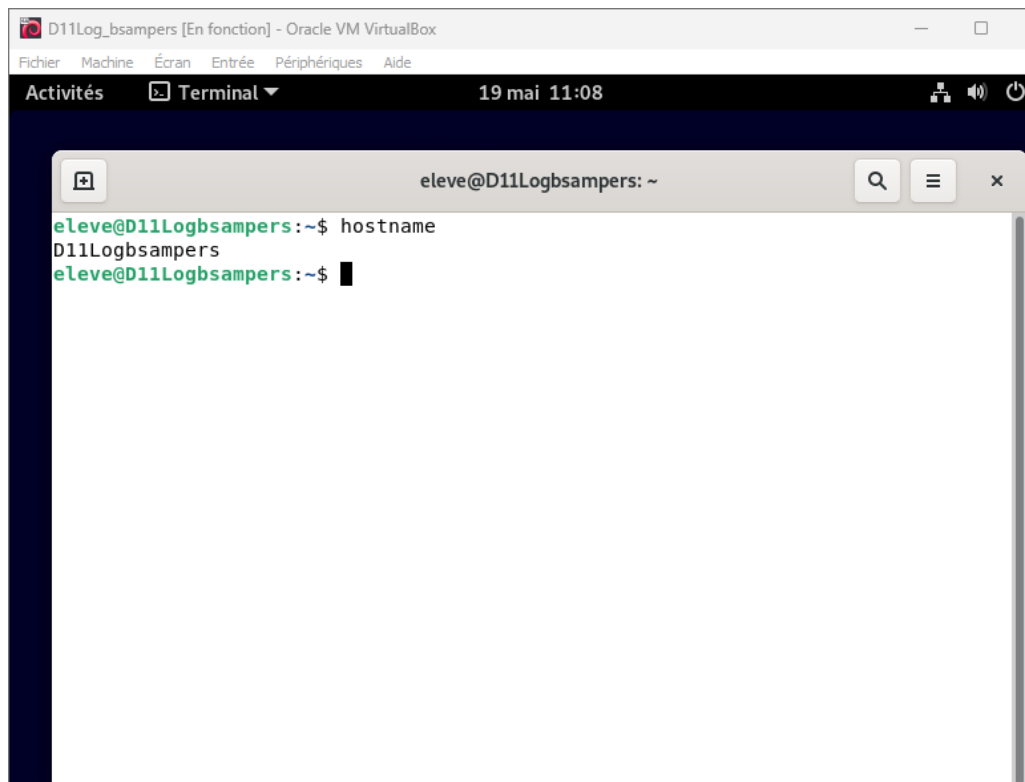


TP6 - Rsyslog



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 11:16

benjamin@D11Logbsampers: ~
GNU nano 5.4 /etc/rsyslog.conf
#####

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

#####
#### GLOBAL DIRECTIVES ####
#####

#

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^_ Aller ligne
```

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

```
Activités Terminal 19 mai 11:31
```

```
benjamin@D11Logbsampers: ~
```

```
benjamin@D11Logbsampers:~$ nano /etc/rsyslog.conf
```

```
benjamin@D11Logbsampers:~$ sudo ss -utln
```

```
[sudo] Mot de passe de benjamin :
```

Netid	State	Recv-Q	Send-Q	Local	Address:Port	Peer	Address:Port	Process
udp	UNCONN	0	0		0.0.0.0:60692		0.0.0.0:*	
udp	UNCONN	0	0		0.0.0.0:514		0.0.0.0:*	
udp	UNCONN	0	0		0.0.0.0:631		0.0.0.0:*	
udp	UNCONN	0	0		0.0.0.0:5353		0.0.0.0:*	
udp	UNCONN	0	0		:::514		:::*	
udp	UNCONN	0	0		:::47291		:::*	
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@D11Logbsampers:~$
```

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

```
Activités Terminal 19 mai 11:55

benjamin@debian: ~
Préconfiguration des paquets...
(Lecture de la base de données... 143816 fichiers et répertoires déjà installés.
)
Préparation du dépaquetage de .../openssh-sftp-server_1%3a8.4p1-5+deb11u5_amd64.
deb ...
Dépaquetage de openssh-sftp-server (1:8.4p1-5+deb11u5) sur (1:8.4p1-5+deb11u1) .
..
Préparation du dépaquetage de .../openssh-server_1%3a8.4p1-5+deb11u5_amd64.deb .
..
Dépaquetage de openssh-server (1:8.4p1-5+deb11u5) sur (1:8.4p1-5+deb11u1) ...
Préparation du dépaquetage de .../openssh-client_1%3a8.4p1-5+deb11u5_amd64.deb .
..
Dépaquetage de openssh-client (1:8.4p1-5+deb11u5) sur (1:8.4p1-5+deb11u1) ...
Paramétrage de openssh-client (1:8.4p1-5+deb11u5) ...
Paramétrage de openssh-sftp-server (1:8.4p1-5+deb11u5) ...
Paramétrage de openssh-server (1:8.4p1-5+deb11u5) ...
rescue-ssh.target is a disabled or a static unit, not starting it.
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
benjamin@debian:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/sy
stemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
benjamin@debian:~$ sudo systemctl start ssh
benjamin@debian:~$
```

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         [::]:*
```

```
Activités Terminal 20 mai 14:33

benjamin@HYDRAbsampers: ~

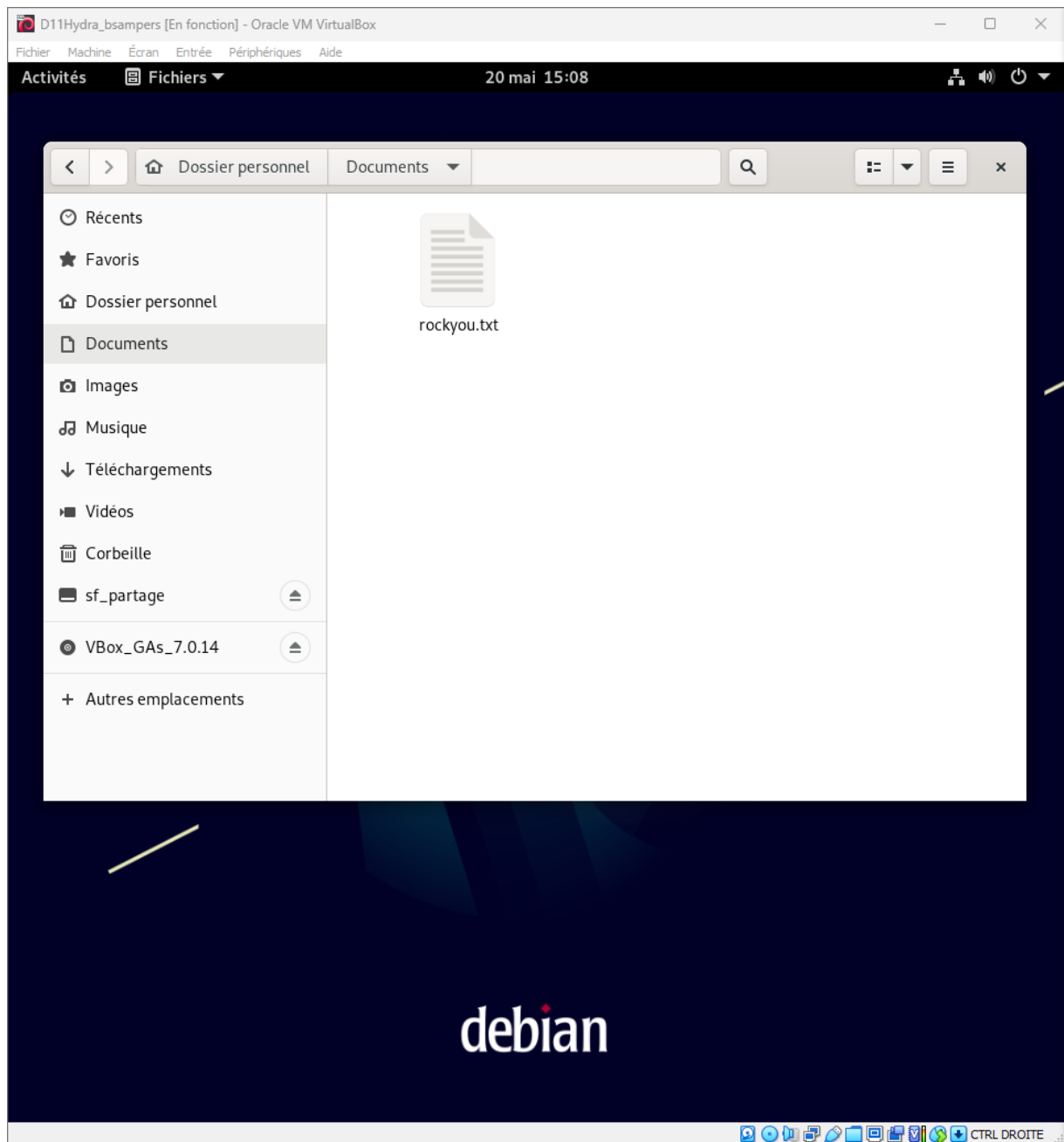
Paramétrage de libtommath1:amd64 (1.2.0-6+deb11u1) ...
Paramétrage de libutf8proc2:amd64 (2.5.0-1) ...
Paramétrage de libserf-1-1:amd64 (1.3.9-10) ...
Paramétrage de libpq5:amd64 (13.21-0+deb11u1) ...
Paramétrage de firebird3.0-common-doc (3.0.7.33374.ds4-2) ...
Paramétrage de firebird3.0-common (3.0.7.33374.ds4-2) ...
Paramétrage de mariadb-common (1:10.5.28-0+deb11u2) ...
update-alternatives: utilisation de « /etc/mysql/mariadb.cnf » pour fournir « /e
tc/mysql/my.cnf » (my.cnf) en mode automatique
Paramétrage de libbson-1.0-0 (1.17.6-1) ...
Paramétrage de libmariadb3:amd64 (1:10.5.28-0+deb11u2) ...
Paramétrage de libssh-4:amd64 (0.9.8-0+deb11u1) ...
Paramétrage de libmemcached11:amd64 (1.0.18-4.2) ...
Paramétrage de libsvn1:amd64 (1.14.1-3+deb11u2) ...
Paramétrage de libmongocrypt0:amd64 (1.1.0-1) ...
Paramétrage de libfbclient2:amd64 (3.0.7.33374.ds4-2) ...
Paramétrage de libmongoc-1.0-0 (1.17.6-1) ...
Paramétrage de hydra (9.1-1) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.31-13+deb11u5)
...
benjamin@HYDRAbsampers:~$
```

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.

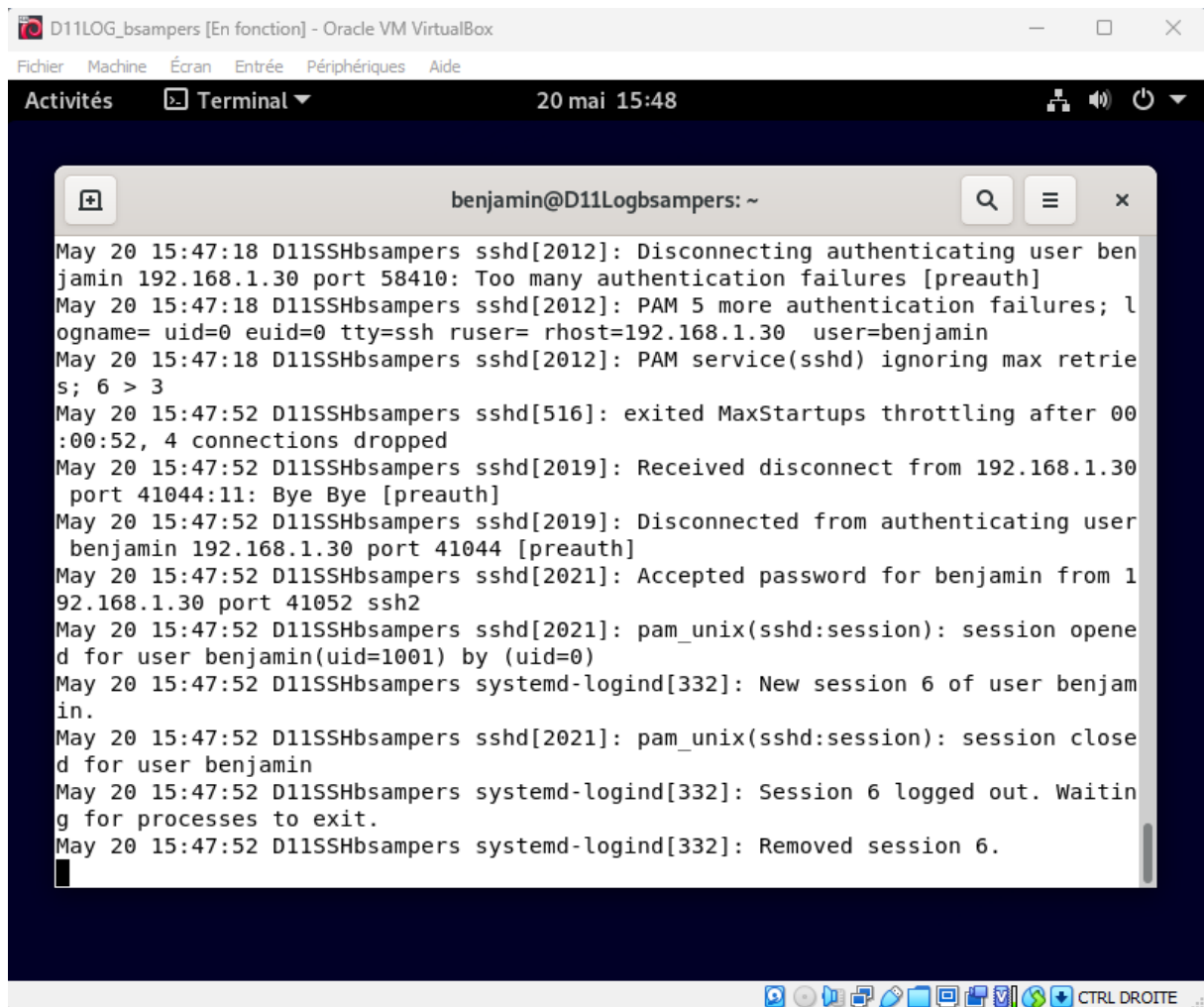
The screenshot shows a terminal window titled "benjamin@HYDRABsampers: ~" within an Oracle VM VirtualBox environment. The terminal displays two ping commands and their results. The first command is "ping 192.168.1.10", which shows six successful pings with times ranging from 0.393 ms to 0.957 ms. The second command is "ping 192.168.1.20", which also shows six successful pings with times ranging from 0.572 ms to 0.993 ms. Both tests show 0% packet loss and a total time of approximately 5226ms and 5070ms respectively. The terminal window is part of a larger interface with a menu bar (Fichier, Machine, Écran, Entrée, Périphériques, Aide) and a status bar (20 mai 14:40, system icons, CTRL DROITE).

```
benjamin@HYDRABsampers:~$ ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=0.745 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=0.836 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=64 time=0.957 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=64 time=0.415 ms
64 bytes from 192.168.1.10: icmp_seq=5 ttl=64 time=0.393 ms
64 bytes from 192.168.1.10: icmp_seq=6 ttl=64 time=0.613 ms
^C
--- 192.168.1.10 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5226ms
rtt min/avg/max/mdev = 0.393/0.659/0.957/0.208 ms
benjamin@HYDRABsampers:~$ ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=64 time=0.823 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=64 time=0.978 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=64 time=0.993 ms
64 bytes from 192.168.1.20: icmp_seq=4 ttl=64 time=0.942 ms
64 bytes from 192.168.1.20: icmp_seq=5 ttl=64 time=0.840 ms
64 bytes from 192.168.1.20: icmp_seq=6 ttl=64 time=0.572 ms
^C
--- 192.168.1.20 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5070ms
rtt min/avg/max/mdev = 0.572/0.858/0.993/0.143 ms
```

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



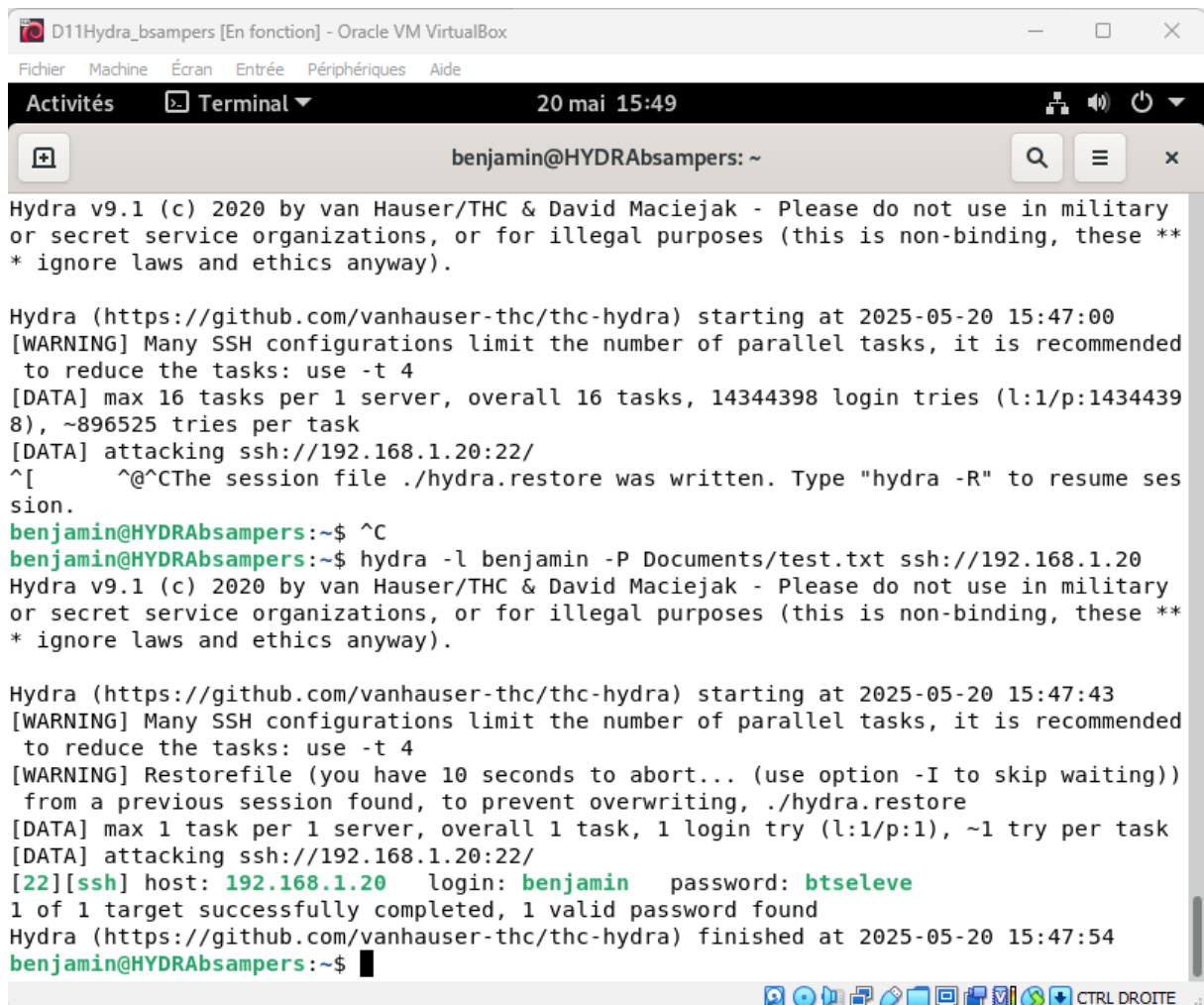
Nous avons créé un dossier partage afin de pouvoir récupérer le fichier rockyou.txt sur la machine Hydra.



The screenshot shows a VirtualBox window titled "D11LOG_bsampers [En fonction] - Oracle VM VirtualBox". The interface includes a menu bar with "Fichier", "Machine", "Écran", "Entrée", "Périphériques", and "Aide". Below the menu is a toolbar with "Activités" and a "Terminal" button. The main area displays a terminal window titled "benjamin@D11Logbsampers: ~". The terminal output shows a series of SSH-related log messages from May 20, 15:47:18 to 15:47:52. The logs indicate that a user named "benjamin" from IP 192.168.1.30 attempted to connect via SSH. The first attempt failed due to too many authentication failures. The second attempt was successful, and a session was established. The session was then closed, and the user was logged out.

```
May 20 15:47:18 D11SSHbsampers sshd[2012]: Disconnecting authenticating user benjamin 192.168.1.30 port 58410: Too many authentication failures [preauth]
May 20 15:47:18 D11SSHbsampers sshd[2012]: PAM 5 more authentication failures; loginname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30 user=benjamin
May 20 15:47:18 D11SSHbsampers sshd[2012]: PAM service(sshd) ignoring max retries; 6 > 3
May 20 15:47:52 D11SSHbsampers sshd[516]: exited MaxStartups throttling after 00:00:52, 4 connections dropped
May 20 15:47:52 D11SSHbsampers sshd[2019]: Received disconnect from 192.168.1.30 port 41044:11: Bye Bye [preauth]
May 20 15:47:52 D11SSHbsampers sshd[2019]: Disconnected from authenticating user benjamin 192.168.1.30 port 41044 [preauth]
May 20 15:47:52 D11SSHbsampers sshd[2021]: Accepted password for benjamin from 192.168.1.30 port 41052 ssh2
May 20 15:47:52 D11SSHbsampers sshd[2021]: pam_unix(sshd:session): session opened for user benjamin(uid=1001) by (uid=0)
May 20 15:47:52 D11SSHbsampers systemd-logind[332]: New session 6 of user benjamin.
May 20 15:47:52 D11SSHbsampers sshd[2021]: pam_unix(sshd:session): session closed for user benjamin
May 20 15:47:52 D11SSHbsampers systemd-logind[332]: Session 6 logged out. Waiting for processes to exit.
May 20 15:47:52 D11SSHbsampers systemd-logind[332]: Removed session 6.
```

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.



```
D11Hydra_bsampers [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Activités Terminal 20 mai 15:49
benjamin@HYDRABsampers: ~

Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military
or secret service organizations, or for illegal purposes (this is non-binding, these **
* ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-20 15:47:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:1434439
8), ~896525 tries per task
[DATA] attacking ssh://192.168.1.20:22/
^[ ^@^CThe session file ./hydra.restore was written. Type "hydra -R" to resume ses
sion.
benjamin@HYDRABsampers:~$ ^C
benjamin@HYDRABsampers:~$ hydra -l benjamin -P Documents/test.txt ssh://192.168.1.20
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military
or secret service organizations, or for illegal purposes (this is non-binding, these **
* ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-20 15:47:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting))
from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.20:22/
[22][ssh] host: 192.168.1.20 login: benjamin password: btseleve
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-20 15:47:54
benjamin@HYDRABsampers:~$
```

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

```
Activités Terminal 20 mai 15:50
benjamin@D11Logbsampers: ~
3
May 20 15:47:17 D11SSHbsampers sshd[1995]: PAM 5 more authentication failures; logname=
uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30 user=benjamin
May 20 15:47:17 D11SSHbsampers sshd[1995]: PAM service(sshd) ignoring max retries; 6 >
3
May 20 15:47:17 D11SSHbsampers sshd[1988]: error: maximum authentication attempts excee
ded for benjamin from 192.168.1.30 port 58292 ssh2 [preauth]
May 20 15:47:17 D11SSHbsampers sshd[1988]: Disconnecting authenticating user benjamin 1
92.168.1.30 port 58292: Too many authentication failures [preauth]
May 20 15:47:17 D11SSHbsampers sshd[1991]: error: maximum authentication attempts excee
ded for benjamin from 192.168.1.30 port 58324 ssh2 [preauth]
May 20 15:47:17 D11SSHbsampers sshd[1991]: Disconnecting authenticating user benjamin 1
92.168.1.30 port 58324: Too many authentication failures [preauth]
May 20 15:47:17 D11SSHbsampers sshd[1991]: PAM 5 more authentication failures; logname=
uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30 user=benjamin
May 20 15:47:17 D11SSHbsampers sshd[1991]: PAM service(sshd) ignoring max retries; 6 >
3
May 20 15:47:17 D11SSHbsampers sshd[1988]: PAM 5 more authentication failures; logname=
uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30 user=benjamin
May 20 15:47:17 D11SSHbsampers sshd[1988]: PAM service(sshd) ignoring max retries; 6 >
3
May 20 15:47:18 D11SSHbsampers sshd[1990]: error: maximum authentication attempts excee
ded for benjamin from 192.168.1.30 port 58310 ssh2 [preauth]
May 20 15:47:18 D11SSHbsampers sshd[1990]: Disconnecting authenticating user benjamin 1
92.168.1.30 port 58310: Too many authentication failures [preauth]
May 20 15:47:18 D11SSHbsampers sshd[1990]: PAM 5 more authentication failures; logname=
uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30 user=benjamin
May 20 15:47:18 D11SSHbsampers sshd[1990]: PAM service(sshd) ignoring max retries; 6 >
3
```

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.