# Sécurité des Systèmes d’Information

# TP1: Écoute d'une connexion

## Sommaire

CentOS (**Community ENTerprise Operating System**) est une distribution GNU/Linux principalement destinée aux serveurs et dont tous les paquets sont compilés à partir des sources de RHEL (**Red Hat Enterprise Linux**).

Depuis janvier 2012, c'est la seconde distribution la plus utilisée (27,5 %) sur les serveurs web, derrière Debian (32,6 %) et devant Ubuntu (21,9 %).

CentOS

Une fois connecté en tant que **root,** exécutez la commande suivante pour installer les paquets nécessaires :

```
# yum -y install telnet telnet-server
```

Il faut maintenant démarrer Xinetd, démon chargé de « réveiller » Telnet lorsqu'il y a une demande de connexion :

```
# service xinetd start
# chkconfig xinetd on
```

Il faut autoriser une connexion **root** depuis l'extérieur :

```
# echo pts/0 >> /etc/securetty
```

Il ne reste plus qu'à désactiver le pare-feu :



```
# service iptables stop
```

Wireshark est un **analyseur de paquets libre** utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie.

Son appellation d'origine (Ethereal) est modifiée en mai 2006 pour des questions relatives au droit des marques.

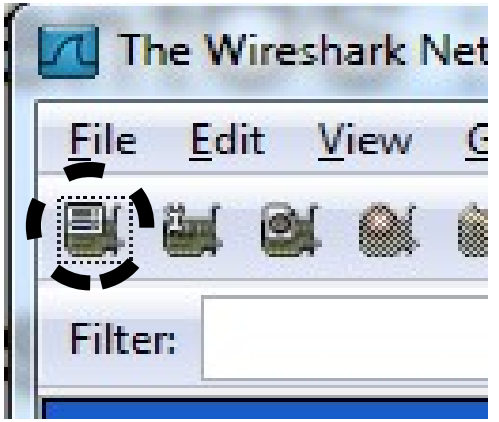

Pour l'installer, rien de plus simple :

# yum -y install wireshark wireshark-gnome

Pour lancer Wireshark, tapez la commande suivante :

# wireshark &

Cliquez sur le bouton ci-dessous pour ouvrir la fenêtre de sélection d'une carte réseau. **Sélectionnez** la carte sur laquelle les paquets vont circuler, généralement **eth0**.

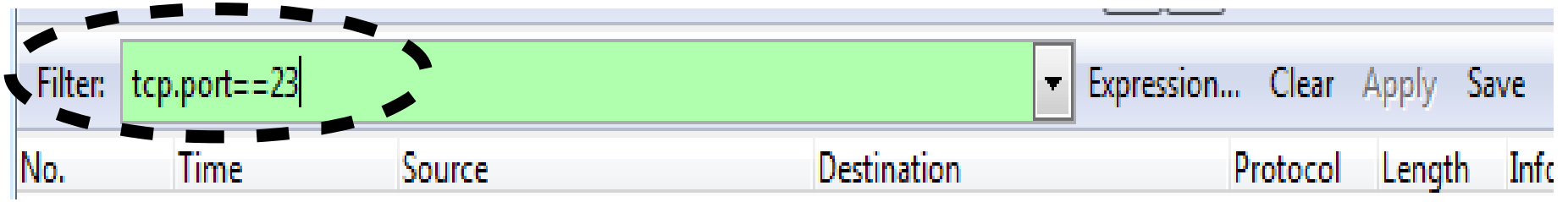



Appuyer sur le bouton 

pour démarrer la capture.

On peut améliorer la lecture en effectuant un filtrage.

Telnet utilise le protocole TCP sur le port 23, nous allons donc spécifier que seuls les paquets respectant ce critère nous intéressent :




Maintenant que tout est prêt, nous pouvons initier la connexion Telnet !!!

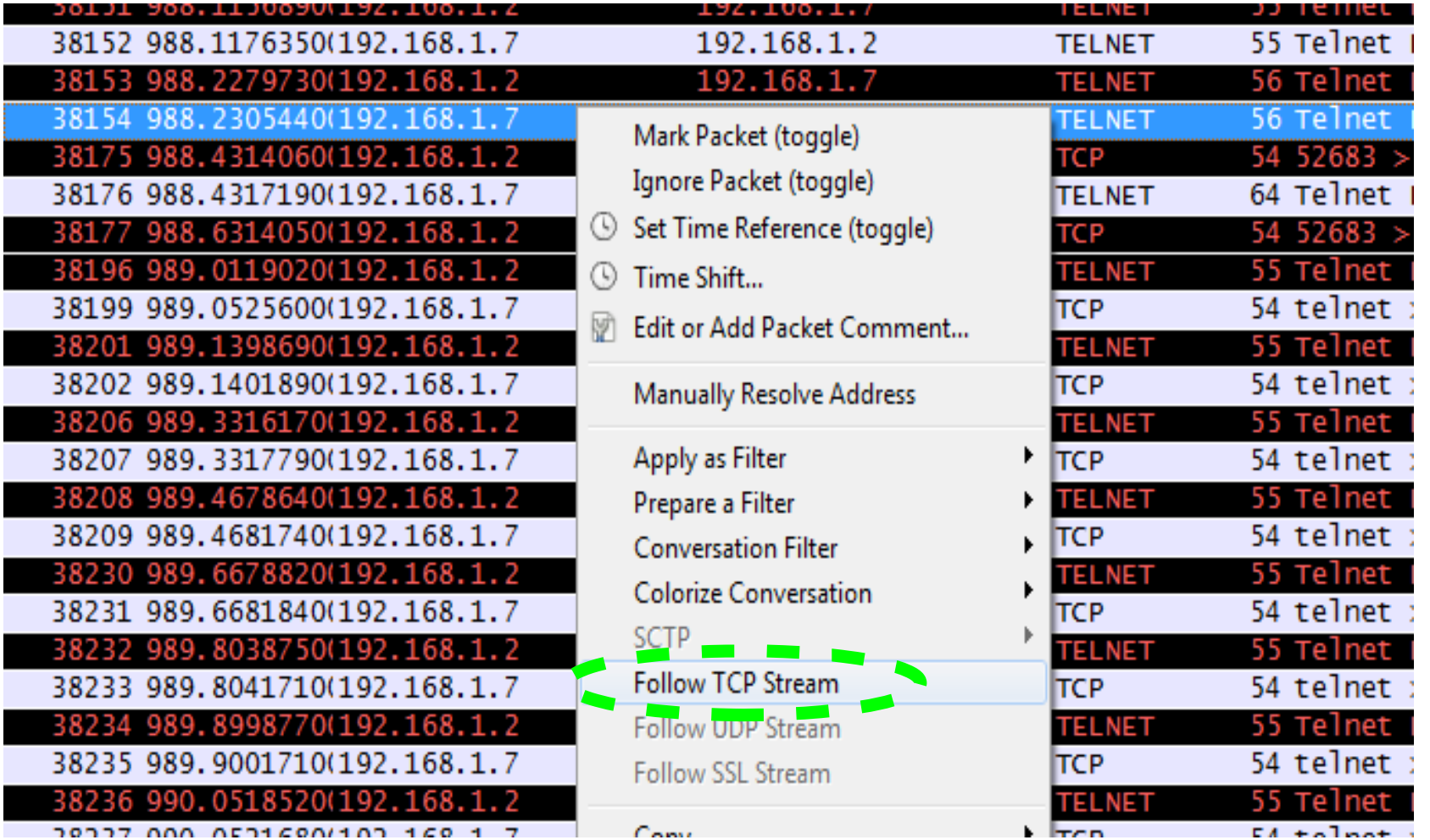
Dans un terminal, tapez la commande suivante :

# telnet 192.168.1.7 23

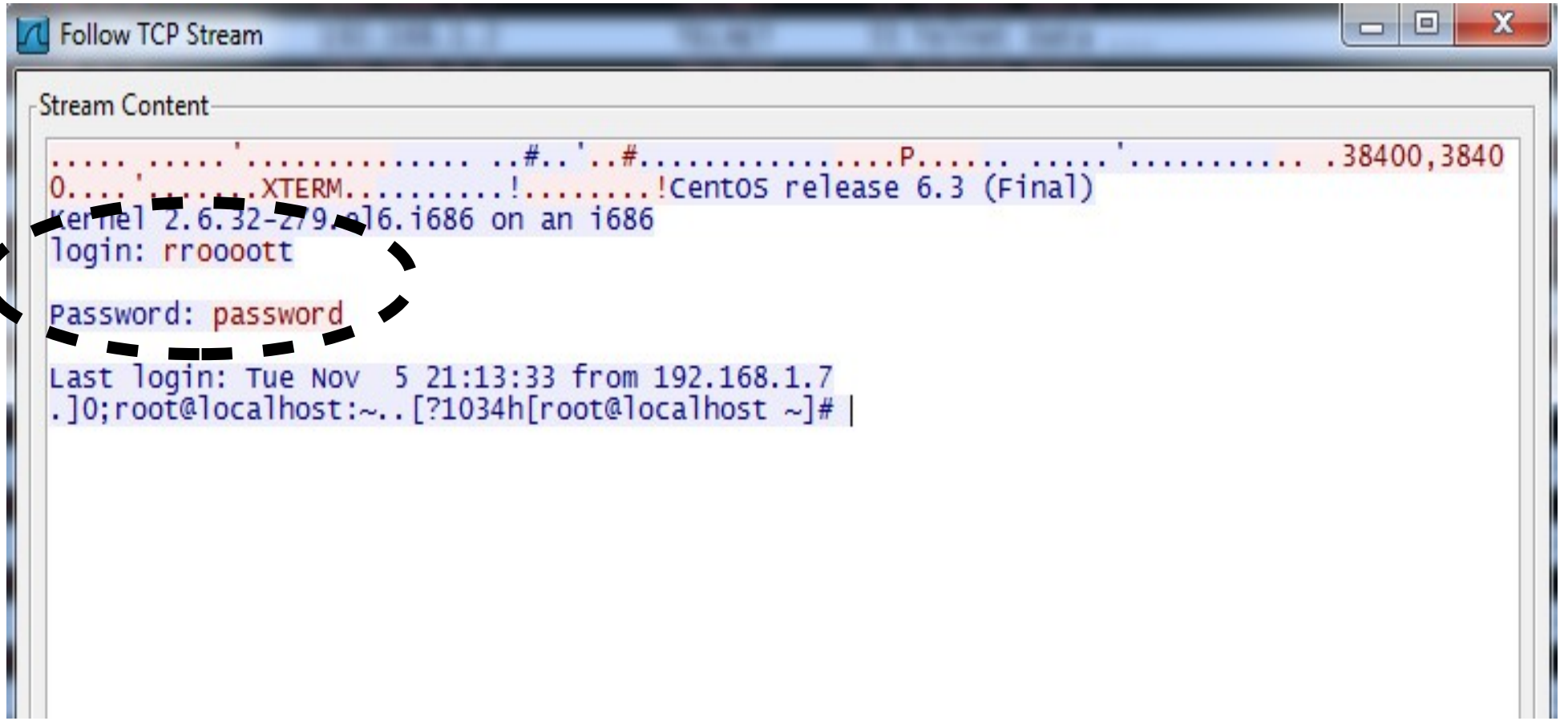
Il faudra remplacer « 192.168.1.7 » par l'adresse IP de l'ordinateur de l'un de vos camarades.

Trying 192.168.1.7...
Connected to 192.168.1.7.
Escape character is '^]'.
CentOS release 6.3 (Final)
Kernel 2.6.32-279.el6.i686 on an i686
**login: root**
**Password:**
Last login: Tue Nov  5 20:49:12 from 192.168.1.2
#

Dans votre fenêtre Wireshark, sélectionnez un paquet Telnet (TCP23) et dans le menu contextuel, sélectionnez « **Follow TCP Stream** »...



On peut se demander si Telnet respecte la **confidentialité** ?!?



Sur quasiment tous les Linux, un serveur SSH (Secure Shell) est activé par défaut.

Le protocole de connexion impose un échange de clés de chiffrement en début de connexion et, par la suite, tous les segments TCP sont **authentifiés** et **chiffrés**.

**Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur... nous allons quand même essayer !**

Tout d'abord, installez SSH :

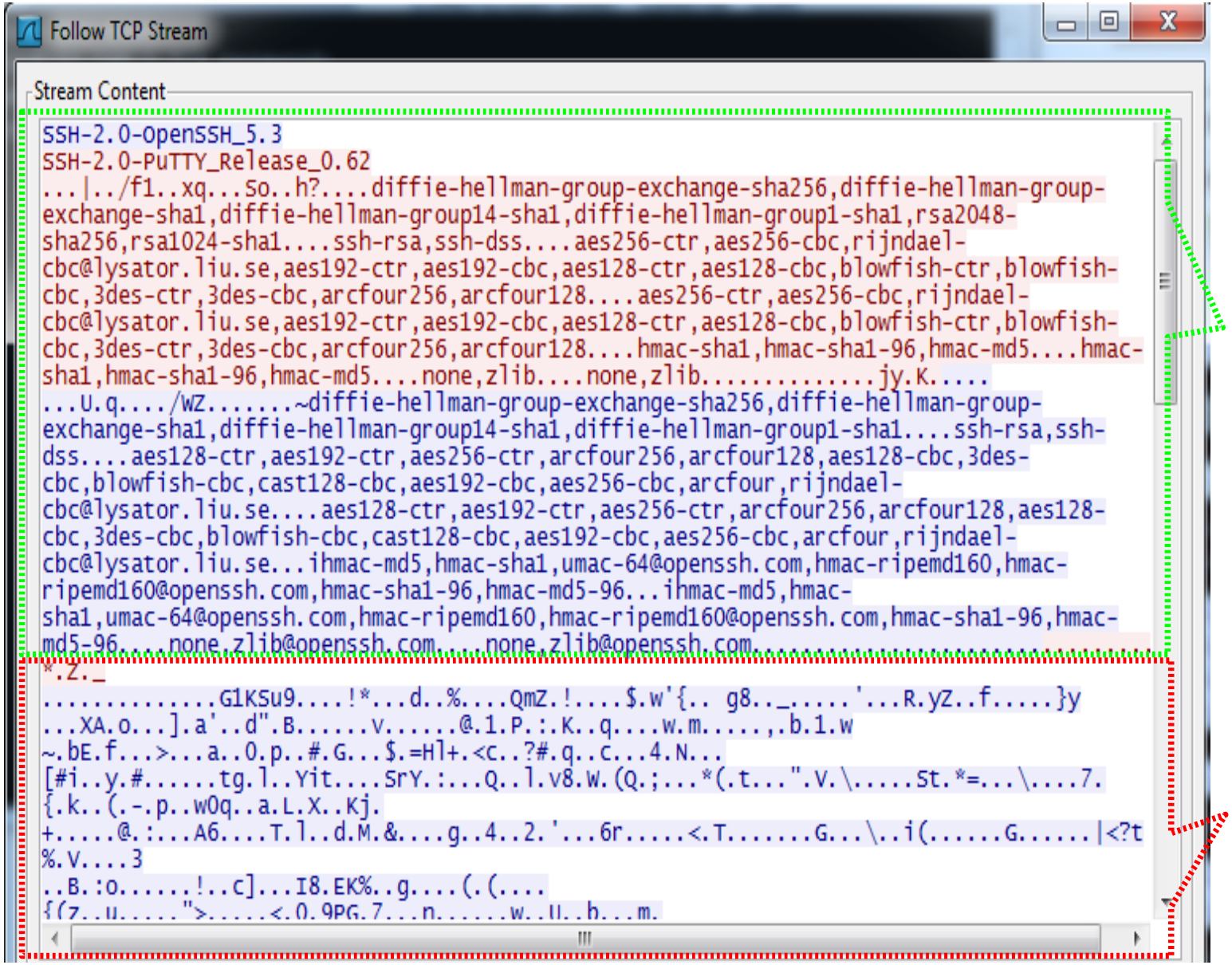
# yum -y install openssh-clients

On peut utiliser SSH grâce à la commande du même nom et de manière similaire à Telnet :

# ssh 192.168.1.7

SSH vous demande si vous souhaitez ajouter la clé de la machine distante à votre trousseau :

The authenticity of host '192.168.1.7 (192.168.1.7)' can't be established.
RSA key fingerprint is ce:c0:04:b9:91:63:47:12:78:89:32:52:12:04:f8:aa.
Are you sure you want to continue connecting (yes/no)? yes
**Warning: Permanently added '192.168.1.7' (RSA) to the list of known hosts.**
root@192.168.1.7's password:
Last login: Tue Nov  5 21:17:37 2013 from 192.168.1.2

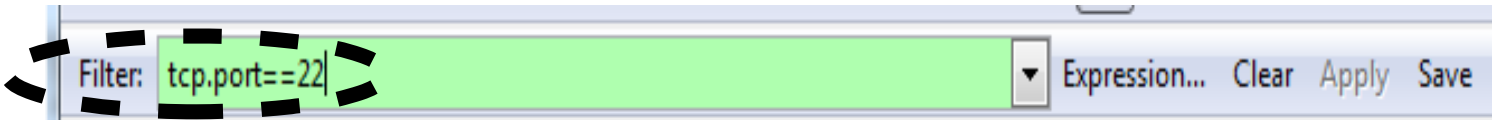



L'échange commence en clair pour négocier les clés

Une fois les clés négociées, la connexion est cryptée...

Essayons maintenant de suivre le flux TCP grâce à Wireshark.

Tout d'abord, il faut changer notre filtre pour l'adapter au protocole SSH qui utilise le port TCP 22 (et non 23 comme telnet) :




Il ne nous reste plus qu'a sélectionner un paquet TCP et dans le menu contextuel, sélectionnez « **Follow TCP Stream** »...

## Tout d'abord il faut générer une paire de clés :

## # ssh-keygen

```
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
df:30:9b:dc:6b:71:91:9d:4d:88:8c:58:bd:1f:ca:92 root@localhost.localdomain
The key's randomart image is:
+--[ RSA 2048]----+
|         o.+ . . |
|        . . + . .|
|             . +o|
|            . +.o|
|        S oo o o |
|         oEB+ o  |
|          =.oo   |
|            ..   |
|            ..   |
+-----------------+
```

Une fois la clé générée, il faut copier la clé publique sur la machine distante :

# ssh-copy-id -i .ssh/id_rsa.pub root@192.168.1.7

root@192.168.1.7's password:
Now try logging into the machine, with "ssh 'root@192.168.1.7'", and check in:

.ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.

Essayez maintenant de vous connecter :

**plus besoin de mot de passe !!**