

Travaux pratiques – Accès distant

Objectifs

Comparez SSH et Telnet pour l'accès à un hôte distant.

Contexte/Scénario

Vous utiliserez SSH et Telnet pour établir des connexions distantes à un hôte. SSH est une méthode sécurisée pour assurer des accès distants à un hôte SSH. Telnet est une méthode non sécurisée pour accéder à un hôte Telnet.

Ressources requises

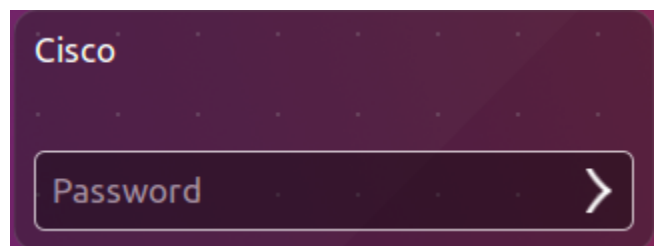
- Ordinateur équipé d'Ubuntu 16.04 Desktop LTS dans une machine virtuelle VirtualBox or VMware

Étape 1 : Ouvrez une fenêtre de terminal dans Ubuntu.

- Connectez-vous à Ubuntu à l'aide des informations d'identification suivantes :

Utilisateur : **cisco**

Mot de passe : **password**



- Cliquez sur l'icône du terminal pour ouvrir une fenêtre de terminal.



Étape 2 : De Telnet à localhost

- À l'invite de commandes, saisissez la commande suivante :

```
cisco@ubuntu:~$ telnet localhost
```

- b. Vous êtes invités à saisir un identifiant et un mot de passe pour un compte existant sur l'hôte.

Identifiant Ubuntu : **cisco**

Mot de passe : **password**

```
cisco@ubuntu:~$ telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 16.04 LTS
ubuntu login: cisco
Password:
Last login: Fri Jun  3 22:22:43 PDT 2016 from localhost on pts/22
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

13 packages can be updated.
7 updates are security updates.

cisco@ubuntu:~$
```

Vous vous êtes correctement connecté à votre machine à l'aide de Telnet.

- c. À l'invite de commandes, saisissez la commande suivante pour quitter cette session Telnet :

cisco@ubuntu:~\$ **exit**

```
cisco@ubuntu:~$ exit
logout
Connection closed by foreign host.
cisco@ubuntu:~$
```

Étape 3 : De SSH à localhost

- a. Saisissez la commande suivante dans le terminal pour accéder au localhost en utilisant SSH :

cisco@ubuntu:~\$ **ssh localhost**

```
cisco@ubuntu:~$ ssh localhost
cisco@localhost's password:
```

Remarque : s'il s'agit de votre première connexion avec SSH, les clés de sécurité devront être enregistrées dans le système. Si vous êtes invité à confirmer la procédure de connexion, saisissez **yes** pour poursuivre.

- b. Utilisez le mot de passe **password** pour l'utilisateur **cisco**.

```
cisco@localhost's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

13 packages can be updated.
7 updates are security updates.

Last login: Fri Jun  3 22:29:58 2016 from localhost
cisco@ubuntu:~$
```

- c. Vous vous êtes correctement connecté à votre machine à l'aide de SSH.

Étape 4 : Accès à un hôte distant


- a. Choisissez un partenaire, puis modifiez les adaptateurs réseau de vos machines virtuelles respectives afin de les connecter en mode pont. Pour ce faire, vous devez éloigner votre curseur de la machine virtuelle, puis accéder à **Machine > Paramètres**, cliquez sur **Réseau** et remplacer **Attachée à : NAT** par **Attachée à : Adaptateur pont**. Attendez que le réseau se reconnecte. Vérifiez votre adresse IP en saisissant la commande suivante :

```
cisco@ubuntu:~$ ifconfig
```

```
cisco@ubuntu:~$ ifconfig
ens33  Link encap:Ethernet  HWaddr 00:0c:29:f9:1f:e3
        inet addr:192.168.68.130  Bcast:192.168.68.255  Mask:255.255.255.0
        inet6 addr: fe80::8b70:7396:899:7dc1/64  Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:4499 errors:0 dropped:0 overruns:0 frame:0
        TX packets:484 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:774294 (774.2 KB)  TX bytes:313660 (313.6 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128  Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:5900 errors:0 dropped:0 overruns:0 frame:0
        TX packets:5900 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:345057 (345.0 KB)  TX bytes:345057 (345.0 KB)

cisco@ubuntu:~$
```

Remarque : si vous n'avez pas reçu de nouvelle adresse IP, cliquez sur l'icône de réseau (). Déconnectez la connexion filaire, puis reconnectez-la.

- b. Exécutez à nouveau les commandes SSH et Telnet, mais en utilisant l'adresse IP de votre partenaire plutôt que localhost.