

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Shell - ssh Première partie

Renaud TALERoy

27 septembre 2016

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Plan

1 Présentation générale du shell

Les différents shell

Présentation du terminal

Comment ça marche ?

2 Présentation du protocole ssh

3 Et donc, en pratique ?

4 Commandes de base

5 Conclusion

6 Amusons-nous un peu

Qu'est ce qu'un shell ?

Le shell

Les différents shell

Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

shell

Couche logicielle qui fournit l'interface utilisateur d'un système d'exploitation. Il correspond à la couche la plus externe du système d'exploitation.

- interface en ligne de commande dite *CLI*, *Command Line Interface*, où l'utilisateur lance des instructions sous forme de texte ;
- interface graphique dite *GUI*, *Graphical User Interface*, où l'utilisateur utilise sa souris.

Les différentes espèces de shell Unix

Le shell

Les différents shell

Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

Il existe de nombreux shell :

- Shell de Stephen BOURNE
 - BOURNE shell (`/bin/sh`) : ancien shell par défaut, souvent shell par défaut pour `root` ;
 - BOURNE-Again shell (`/bin/bash`) : interprète par défaut (par défaut pour Mac OS X, Cygwin) ;
- Z shell (`/usr/bin/zsh`) : sorte de BOURNE shell étendu reprenant les fonctionnalités les plus pratiques de `bash`, `ksh` et `csh`, par défaut au CRANS.
- ...et bien d'autres encore (`csh`, `ksh`, `fish`, `dash`)...

Le terminal nu

Le shell

Les différents shell

**Présentation du
terminal**

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

```
Last login: Sun Sep 25 11:31:58 on ttys006
-bash-3.2$ █
```

Un terminal habillé

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Message of the day

Dossier courant
~ ⇔ /home/utilisateur

Terrain de jeu !!

\$: utilisateur
: super-utilisateur

Machine

Utilisateur

Code d'erreur
0 ⇔ tout va bien

```
##### /
##### /
/# / /
/ / /
/ / /
## ## /### ### ### /### /##
## ## / ### / ### ###/ #### / / ###
## ## / ###/ ## ## ###/ / ###
## ## ## ## ## ## ## ##
## ## ## ## ## ## #####
# ## ## ## ## ## #####
# ## ## ## ## ## ##
/##/ / ## ## ## ## ##### /
/ #####/ ##### ### / ### #####/
/ ##### ### ##/ ## #####
#
##
```

(15:27:18) ~ > [0]

taleroyr@loire \$

La configuration : mais pourquoi ?

Le shell

Les différents shell

**Présentation du
terminal**

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Intérêts :

- savoir où on est et qui on est
- voir les choses plus clairement (coloration des commandes et résultats)
- (personnaliser sa machine)

Format d'une commande shell

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigation

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

- Une commande simple est une séquence de mots séparés par un séparateur blanc (une espace).
- Le premier mot désigne le nom de la commande à exécuter, les mots suivants sont passés en arguments de la commande.
- On peut placer des drapeaux (*flags*) entre la commande et son argument. Les drapeaux sont généralement introduits par un ou deux tirets.
- La valeur retournée par la commande est celle de son code de retour.

Format d'une commande shell : exemple

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clés

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

```
user@host $ ls -a -l -h /etc/
```

- `ls` est le nom de la commande
- `-a -l -h` sont les drapeaux de la commande
- `/etc/` est l'argument de la commande

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Plan

1 Présentation générale du shell

2 Présentation du protocole ssh
Sécurité et chiffrement
La connexion

3 Et donc, en pratique ?

4 Commandes de base

5 Conclusion

6 Amusons-nous un peu

ssh, *secure shell*

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clés

Commandes

La base

Navigaison

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

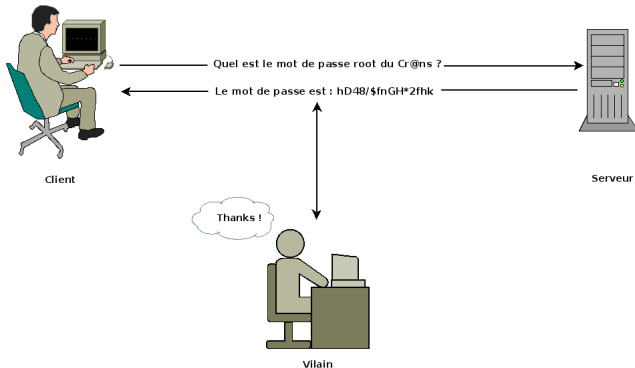
ssh

ssh désigne :

- une commande ;
- un protocole de communication sécurisée (les données sont chiffrées) entre un client et un serveur distant.

Le ssh permet de se connecter à une machine distante et d'y travailler.

Communication avec telnet



→ telnet est simple mais dangereux

→ nécessité de chiffrer ses données

Le shell

Les différents shell
Présentation du terminal
Comment ça marche ?

ssh

Sécurité et chiffrement
La connexion

TD1

Connexion ssh à zamok
Création d'un couple de clefs

Commandes

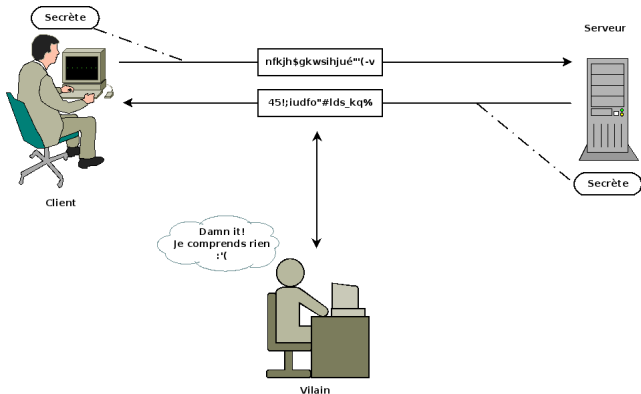
La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de configuration
wget, screen et IRC

Chiffrement symétrique (1/2)



→ parfait le chiffrement symétrique, non ?

Le shell

Les différents shell
Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

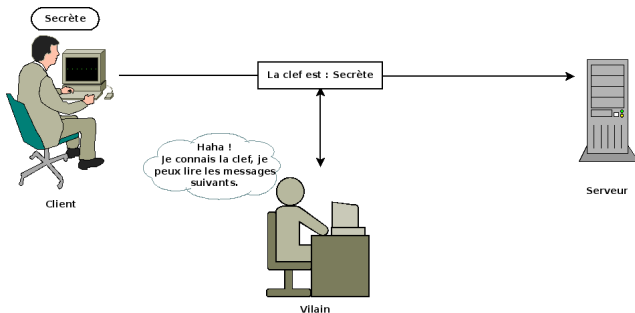
La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

Chiffrement symétrique (2/2)



- nécessité de transmettre *discrètement* la clef
- difficilement faisable en pratique

Le shell

Les différents shell
Présentation du terminal
Comment ça marche ?

ssh

Sécurité et chiffrement
La connexion

TD1

Connexion ssh à zamok
Création d'un couple de clefs

Commandes

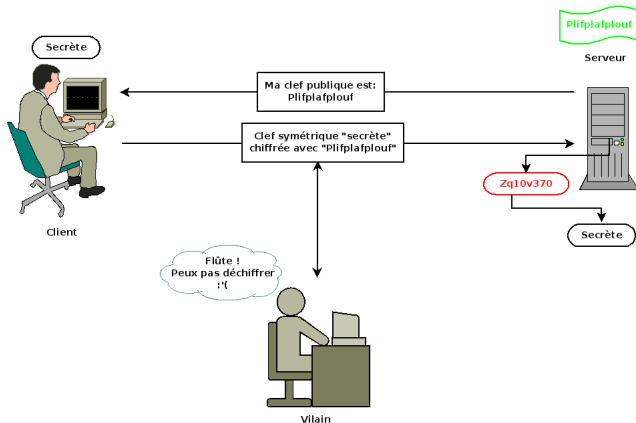
La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de configuration
wget, screen et IRC

Chiffrement asymétrique (1/2)



→ parfait !

Le shell

Les différents shell
Présentation du terminal
Comment ça marche ?

ssh

Sécurité et chiffrement
La connexion

TD1

Connexion ssh à zamok
Création d'un couple de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de configuration
wget, screen et IRC

Chiffrement asymétrique (2/2)

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clés

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Pour le chiffrement asymétrique, il faut :

- une clef **publique** qui sert à chiffrer,
- une clef **privée** qui sert à déchiffrer.

Le chiffrement asymétrique consomme plus de ressources, aussi il n'est utilisé qu'au *début de la communication* pour permettre l'échange sécurisé d'une clef symétrique.

(R)appels : définitions

Le shell

Les différents shell
Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

- Le *serveur*, ou hôte (*host*), est la machine sur laquelle on se connecte.
- Le *client* est la machine à partir de laquelle on se connecte.

Les fingerprint ssh

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

- une version courte de la clef publique du serveur
- permet de *vérifier* que c'est la vraie clef du serveur
- permet de se prémunir d'une attaque *man in the middle*
- nécessité de **vérifier** la *fingerprint*

Établissement d'une connexion `ssh`

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion `ssh` à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigation

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

`wget`, `screen` et
IRC

- 1 Le serveur envoie sa clef publique au client. Celui-ci vérifie que c'est la clef du serveur (si déjà reçue).
- 2 Le client génère une clef secrète et l'envoie au serveur en la chiffrant avec la clef publique reçue. (*chiffrement asymétrique*)
- 3 Le serveur chiffre un message standard avec la clef secrète et l'envoie au client qui le déchiffre. (*prouve que le serveur est bien le vrai serveur*)
- 4 Établissement d'un canal sécurisé grâce à la clef secrète commune. (*chiffrement symétrique*)
- 5 Le client peut alors envoyer le login et son mot de passe de l'utilisateur pour vérification.

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Plan

- 1 Présentation générale du shell
- 2 Présentation du protocole ssh
- 3 Et donc, en pratique ?
Connexion ssh à zamok
Création d'un couple de clefs
- 4 Commandes de base
- 5 Conclusion
- 6 Amusons-nous un peu

Première connexion à zamok

Pour se connecter en ssh sur zamok :

```
user@host: $ ssh loginCrans@zamok.crans.org
```

damn it !

```
The authenticity of host 'zamok.crans.org (138.231.136.1)' can't be established.  
ECDSA key fingerprint is SHA256:NuNyHJiEHVpKWWygwzx6JP1sn9hcn3iHHmSR+N3JltQ.
```

```
+---[ECDSA 521]---+
```

```
|   o=+   |  
| + o.*o. . . |  
|. O +.o . o . E|  
| + = . o . o + o |  
|. . + o S + . * |  
| . . = * O o . |  
| . * = * . |  
|   o o o   |  
|           |
```

```
+-----[SHA256]-----+
```

```
Are you sure you want to continue connecting (yes/no)?
```

Si vous tapez `yes` comme ça pouf, vous risquez de m'énervier très fort.

Le shell

Les différents shell
Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

Vérification de la fingerprint

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clés

Commandes

La base

Navigaison

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Pour avoir la fingerprint du serveur affichée en hexadécimal, on utilise la commande suivante :

```
taleroir@loire $ ssh -o FingerprintHash=md5 host@server
```

Pour avoir la fingerprint du serveur hashée en sha256, on utilise la commande suivante :

```
taleroir@loire $ ssh -o FingerprintHash=sha256 host@server
```

Quand on est sur le serveur, pour vérifier les clés, on utilise :

```
taleroir@zamok $ for file in /etc/ssh/*sa_key.pub; do ssh-keygen -lf $file; done
1024 50:f5:72:cd:2d:2b:be:e3:5c:a7:17:28:4c:6d:6c:70
    /etc/ssh/ssh_host_dsa_key.pub (DSA)
521 63:e0:64:78:56:ff:e3:4b:15:17:a8:2f:43:6c:d2:cf
    /etc/ssh/ssh_host_ecdsa_key.pub (ECDSA)
4096 b4:85:bc:47:dd:ee:d0:80:3c:20:ee:f0:de:d3:8e:3a
    /etc/ssh/ssh_host_rsa_key.pub (RSA)
```

Quand doit-on vérifier la fingerprint `ssh` ?

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion `ssh` à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

`wget`, `screen` et
`IRC`

- à chaque première connexion
- à chaque fois que la commande `ssh` prévient que la fingerprint a changé : ça peut être totalement légitime ou une attaque

Authentification par clefs

Au lieu de s'authentifier par mot de passe, il est possible de s'authentifier par un couple de clef privée/publique, c'est-à-dire par chiffrement asymétrique.

- + plus sûr puisqu'il faut que l'attaquant se procure et la clef privée et la passphrase pour pouvoir s'authentifier
- + l'utilisateur a de meilleures garanties que le serveur auquel il se connecte est bien celui auquel il souhaite se connecter
- + possibilité de « déverrouiller » la clef pour une période de temps donné et de pouvoir accéder sans taper de mot de passe aux serveurs (confort)
- *si la clef n'est pas protégée par une passphrase, cela retire une couche de sécurité*

Le shell

Les différents shell

Présentation du terminal

Comment ça marche ?

ssh

Sécurité et chiffrement

La connexion

TD1

Connexion ssh à zamok

Création d'un couple de clefs

Commandes

La base

Navigation

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de configuration

wget, screen et IRC

Génération de clefs

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Pour générer un couple de clef RSA, il faut exécuter :

```
user@host $ ssh-keygen
```

Les clefs sont stockées :

- dans `~/ .ssh/id_rsa` pour la clef privée (permission 600)
- dans `~/ .ssh/id_rsa.pub` pour la clef privée (permission 644)

Passphrase

Le shell

Les différents shell
Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

Lors de la création de la clef privée, OpenSSH demande l'entrée d'une *passphrase* qui servira à chiffrer la clef privée. Il *faut* en mettre une.

La *passphrase* sera demandée à chaque utilisation de la clef privée.

Ajouter temporairement la clef au `ssh-agent` (programme qui conserve en mémoire les clefs privées)

```
user@host $ ssh-add -t 7200 ~/.ssh/id_rsa
```

Changer la *passphrase*

```
user@host: $ ssh-keygen -p
```

Autoriser la clef publique

Le shell

Les différents shell
Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

- copier la clef *publique* sur le serveur distant auquel on souhaite pouvoir s'authentifier par clef
- l'ajouter à son `~/.ssh/authorized_keys`

```
user@host: $ ssh-copy-id -i ~/.ssh/id_rsa.pub  
loginCrans@zamok.crans.org
```

Le shell

Les différents shell
Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

Plan

- 1 Présentation générale du shell
- 2 Présentation du protocole ssh
- 3 Et donc, en pratique ?
- 4 **Commandes de base**
 - La base
 - Naviguer dans les fichiers
 - Manipulation
 - Lecture et écriture
 - Caractères de contrôle clavier
- 5 Conclusion
- 6 Amusons-nous un peu

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Commande

`echo` est une commande qui affiche une ligne de texte.

```
user@host $ echo "Hello world!"
```

On peut s'en servir pour retrouver le *shell* dans lequel on habite :

```
user@host $ echo $SHELL
```

Le shell

Les différents shell
Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

Commande

`man` permet d'afficher l'aide d'une commande (on dit "RTFM")

```
user@host $ man echo
```

Les fichiers sont rangés dans une arborescence

Le shell

Les différents shell
Présentation du terminal
Comment ça marche ?

ssh

Sécurité et chiffrement
La connexion

TD1

Connexion ssh à zamok
Création d'un couple de clés

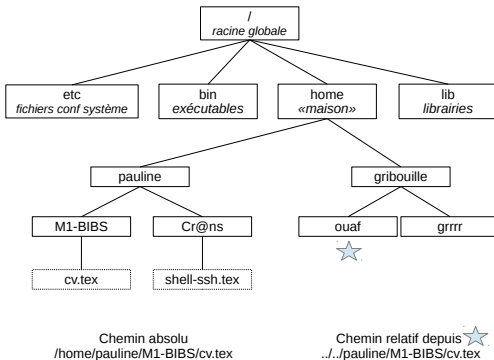
Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de configuration
wget, screen et IRC



Chemin relatif et chemin absolu

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigation

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Le chemin absolu est la succession des répertoires à parcourir depuis la **racine** pour accéder au fichier spécifié.

Le chemin relatif est la succession des répertoires à parcourir depuis le **répertoire courant** pour accéder au fichier spécifié.

On désigne par `.. /` le répertoire parent et par `.` / le répertoire courant.

cd, *change directory*

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigation

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Commande

cd est une commande qui permet de naviguer dans l'arborescence des fichiers, connaissant l'emplacement du dossier que l'on cherche.

```
user@host: $ cd fichiers_configuration
```

Que ce soit pour le chemin absolu ou pour le chemin relatif, il faut connaître l'arborescence des fichiers. Il ne faut surtout pas oublier d'utiliser la *tab-complétion*, ça fait gagner beaucoup de temps.

`pwd`, *print working directory*

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigation

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Commande

`pwd` est une commande qui permet d'afficher le dossier courant, d'afficher où l'on est.

```
user@host $ pwd
```

Cette commande est très pratique lorsque l'on ne dispose pas de `.bashrc` ou `.zshrc` *user-friendly* qui renouvelle l'affichage de la localisation à chaque retour de prompt.

ls, *list segments*

Le shell

Les différents shell
Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

Commande

`ls` est une commande qui permet d'afficher le contenu d'un répertoire.

```
user@host $ ls
```

les options utiles

- `ls -a` affiche tous les fichiers et dossiers du répertoires (même les cachés)
- `ls -l` affiche la liste des fichiers et des dossiers, avec leurs dates de dernière modification, leurs tailles, les utilisateurs propriétaires, groupe propriétaire et les droits.
- `ls -lh` même chose que précédemment, avec les tailles en format *human readable*.

mv, *move*

Le shell

Les différents shell
Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

Commande

`mv` sert à déplacer ou renommer des fichiers.

```
user@host $ mv .umaskrc ../what_is_that_file
user@host $ mv fichiers_configuration myconfig
```

les options

- `mv -i` *interactive* demande pour chaque fichier/répertoire s'il peut déplacer le fichier/répertoire
- `mv -u` *update* demande à `mv` de ne pas supprimer le fichier si la date de modification est la même ou plus récente que son remplaçant

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigation

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Commande

`cp` permet de copier un fichier ou un répertoire.

Copier un fichier dans un autre fichier :

```
user$host $ cp what_is_that_file .umaskrc
```

Copier un fichier dans un autre dossier :

```
user@host $ cp .umaskrc myconfig/
```

les options

- `cp -i` avertit de l'existence d'un fichier du même nom et demande s'il peut remplacer son contenu.
- `cp -r` permet de copier de manière récursive l'ensemble d'un répertoire et de ses sous-répertoires.
- `cp -p` préserve toutes les informations comme le propriétaire, le groupe et la date de création.

mkdir, *make directory*

Le shell

Les différents shell
Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clés

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

Commande

`mkdir` permet de créer un répertoire.

```
user@host: $ mkdir Playground
```

les options

- `mkdir -p` permet de créer une suite de répertoires :

```
user@host $ mkdir -p Playground/Crans/Seminaires/Shell-ssh/2015
```

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Commande

`touch` sert à modifier le *timestamp* d'un fichier.

```
user@host $ touch test
```

va créer le fichier `test` dans le dossier courant, s'il n'existe pas encore.

les options

- `touch -t STAMP` utilise STAMP au lieu du temps présent.
- `touch -r plop -B 5 test` fait paraître le fichier test 5 secondes plus vieux que le fichier plop.
- `touch -r plop -F 5 test` fait paraître le fichier test 5 secondes plus jeune que le fichier plop.
- `touch -m` modifie la date de dernière modification.

rm, *remove*

Le shell

Les différents shell
Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

Commande

rm permet de supprimer un fichier.

```
user@host: $ rm test
```

les options

- **rm -i** permet de demander à l'utilisateur s'il veut vraiment effacer le fichier.
- **rm -d** permet de supprimer un répertoire qu'il soit plein ou nous (dangereux).
- **rm -r** permet de supprimer un répertoire et ses sous-répertoires (très dangereux).
- **rm -f** permet de supprimer les fichiers protégés en écriture et les répertoires sans demander de confirmation (vraiment très dangereux)

cat, *concatenate*

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaison

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Commande

cat permet de concatener des fichiers ou de lire un fichier.

```
user@host $ cat ~/myconfig/.ssh/config
```

Permet d'afficher sur la sortie standard le contenu du fichier de configuration pour ssh.

```
user@host $ cat <file_1> <file_2>
```

Permet de concaténer les 2 fichiers.

les options

- `cat -n` permet de numéroter les lignes dans la sortie standard.

less, *less*

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigation

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Commande

`less` lit au fur et à mesure le fichier qu'on lui donne et permet la navigation en amont et en aval.

```
user@host $ less ~/myconfig/.ssh/config
```

les options

- `less <entrée> /pattern <entrée>` permet de rechercher le *pattern* dans le fichier, en ayant son contexte.
- `less <entrée> /!pattern <entrée>` permet de rechercher les lignes ne contenant pas *pattern*.
- `^D` permet d'avancer de N lignes (par défaut, la moitié de la taille de l'écran).
- `^B` permet de reculer de N lignes (par défaut, la moitié de la taille de l'écran).

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamor

Création d'un couple
de clés

Commandes

La base

Navigation

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Commande

`nano` est un éditeur de texte, natif sur Ubuntu et Debian.

```
user@host: $ nano <nom du fichier>
```

Permet d'éditer le fichier en question.

les raccourcis

- `^O` permet d'écrire le fichier *i.e.* de sauvegarder.
- `^X` permet de fermer le fichier.
- `^K` permet de couper les lignes.
- `^U` permet de coller les lignes.

Ce qui est pratique avec `nano`, c'est qu'il y a toujours une anti-sèche...

Il existe d'autres éditeurs de texte comme `vim` que l'on peut apprendre à dompter grâce à `vimtutor`.

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Commande

`ln` sert à faire des liens entre des fichiers *représentés par leur chemin absolu* !!

les options

- `ln -s` *symbolic* permet de créer un lien symbolique, comme un « raccourci »

```
user@host $ ln -s file1 file2
```

Permet de faire un lien depuis le fichier existant `file1` vers le fichier `file2`.

```
user@host $ ln -s ~/myconfig/.umaskrc ~
```

Permet de faire un lien depuis le fichier `.umaskrc` rangé dans `~/myconfig` vers `~`.

Caractères de contrôle clavier essentiels

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

<tab>

<tab> permet de faire de la « tab-complétion » c'est-à-dire de compléter par exemple les noms de commandes, de fichiers, les chemins. SUPER UTILE !!

^C

^C interrompt un processus attaché au terminal (SIGINT, signal 11)

^D

^D renvoie un caractère de fin de fichier (caractère ASCII 026), si le shell lit, il termine

Plan

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

1 Présentation générale du shell

2 Présentation du protocole ssh

3 Et donc, en pratique ?

4 Commandes de base

5 Conclusion

6 Amusons-nous un peu

Pourquoi il faut que vous veniez à la partie suivante

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Parce que quand y'en a plus, y'en a encore :

- plein de nouvelles commandes à découvrir
- on peut faire fonctionner les commandes les unes avec les autres
- on peut écrire des scripts trop cool
- vous pouvez interdire au voisin de lire vos fichiers (système de permissions)
- le `ssh` peut se prendre dans les deux sens, et ça peut devenir intéressant

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

Plan

- 1 Présentation générale du shell
- 2 Présentation du protocole ssh
- 3 Et donc, en pratique ?
- 4 Commandes de base
- 5 Conclusion
- 6 Amusons-nous un peu
Les fichiers de configuration
wget, screen et IRC

Récupérer un fichier de customisation déjà écrit

Le shell

Les différents shell
Présentation du terminal
Comment ça marche ?

ssh

Sécurité et chiffrement
La connexion

TD1

Connexion ssh à zamok
Création d'un couple de clés

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de configuration
wget, screen et IRC

Des gentils cranseux ont publié des fichiers de configuration pour vous éviter de les écrire à la main :

```
user@host $ git clone  
git@gitlab.crans.org:membres-actifs/fichiers_configuration.git
```

Sinon, consulter la page wiki.crans.org/VieCrans/FichiersConfiguration.

Obtenir un fichier de configuration pour son shell

Le shell

Les différents shell
Présentation du terminal
Comment ça marche ?

ssh

Sécurité et chiffrement
La connexion

TD1

Connexion ssh à zamok
Création d'un couple de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de configuration
wget, screen et IRC

- 1 Trouver quel genre de *shell* on utilise
- 2 Trouver un fichier rc correspondant au nom de son *shell*
- 3 Établir un lien symbolique entre ce fichier rc et son `$HOME`
- 4 Exécuter
`source <chemin vers le fichier rc>`

Obtenir un fichier d'alias de commande

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok

Création d'un couple
de clefs

Commandes

La base

Navigaton

Manipulation

Lecture et écriture

Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

- 1 Lire les 2 fichiers `_aliases`
- 2 Écrire un fichier `all_aliases` contenant les alias des 2 fichiers
- 3 Renommer le fichier avec le nom correspondant au *shell* utilisé
- 4 Établir un lien symbolique entre ce fichier et son `$HOME`

Configuration ssh

Le shell

Les différents shell
Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration

wget, screen et
IRC

- 1 Se balader dans `myconfig/.ssh`
- 2 Lire le contenu du fichier `myconfig/.ssh/config`
- 3 Obéir aux instructions
- 4 Établir un lien symbolique entre ce fichier et son `$HOME`

Le shell

Les différents shell
Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

Commande

wget permet de télécharger des fichiers en ligne pour les déposer dans le fichier courant.

.procmailrc

Le shell

Les différents shell
Présentation du
terminal
Comment ça
marche ?

ssh

Sécurité et
chiffrement
La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

procmail est un programme qui permet de trier ses mails dans différents dossiers dès leur arrivée dans la boîte mail. Le fichier de configuration à écrire peut être long et douloureux à écrire mais il y en a un tout prêt qui permet de trier tous les mails Crans, l'immense majorité des mailing-lists Crans ainsi que de trier automatiquement dans des dossiers les mails reçus sur une mailing-list (même si elle n'est pas Crans).

Pour le mettre en place, consulter <https://wiki.crans.org/VieCrans/FichiersConfiguration#procmail>.

Écrire "`| exec /usr/bin/procmail`" dans son
`$HOME/.forward`

Le shell

Les différents shell

Présentation du
terminal

Comment ça
marche ?

ssh

Sécurité et
chiffrement

La connexion

TD1

Connexion ssh à
zamok
Création d'un couple
de clefs

Commandes

La base
Navigation
Manipulation
Lecture et écriture
Contrôle clavier

Conclusion

TD2

Les fichiers de
configuration
wget, screen et
IRC

Commande

`screen` est un programme qui permet d'ouvrir plusieurs terminaux dans la console courante et de les récupérer après avoir quitté la console.

```
user@zamok $ screen -S NomDuScreen
```

```
user@zamok $ weechat
```

Pour détacher : `^A ^D`.

Pour rattacher :

```
user@zamok $ screen -rd
```