M2-DNR2I TP2-1:
Surveillance de la machine et du réseau

Gaétan Richard

17 octobre 2011

1 Machine

1.1 Utilisation processeur

Il existe de nombreux logiciels qui permettent d'observer l'état de la machine et des processus qui la compose.

Regarder les pages de **man** des programmes **top**, **uptime**, **htop** et **free**

À l'aide de ces commandes, trouver :

- Le temps depuis lequel la machine est allumée ;
- L'utilisation moyenne du CPU ;
- La quantité de RAM disponible ;
- L'utilisation du swap ;
- Combien de cpu consomme le programme **top**.

Lancer alors un navigateur firefox et trouver son utilisation de CPU ainsi que la mémoire qu'il consomme.

Les événements importants arrivant à l'ordinateur sont logués dans des fichiers situés dans le répertoire `/var/log/`.

En regardant la page **man** du programme **logrotate**, expliquer la présence de fichiers `.gz`.

Regarder certains logs auxquels vous avez accès et à l'aide de **dmesg**, essayer de trouver quand une clef USB a été insérée dans la machine.

1.2 Utilisateurs

À l'aide des commandes **who**, **last** et **w**, déterminer :

- Combien de personnes sont actuellement sur la machine ;
- Quelles sont les commandes utilisées ;
- Quand vous êtes-vous connecté ce mois-ci sur la machine.

1.3 Processus

À l'aide des commandes **ps** et **netstat**, déterminer :

- le nombre de vos processus en cours d'exécution ;

– le nombre total de processus en cours d'exécution sur la machine ;
– le nombre de threads que vous possédez ;
– les services à l'écoute sur votre machine.

Trouver le numéro de processus n de votre shell et regarder le contenu du dossier `/proc/n`. À l'aide la commande **man proc**, analyser ce contenu. Trouver quelles sont les limitations imposées sur votre shell.

2 Trafic réseau

Pour ce TP, les administrateurs vous ont exceptionnellement autorisé à capturer les paquets par l'intermédiaire de la commande **sudo netdump-tp**. Cette commande crée un fichier dans le dossier `/tmp` qui s'ouvre ensuite avec le logiciel **wireshark**.

Question 1 *Faire une première capture et observer le résultat. Identifier :*
– *Un paquet* TCP *;*
– *Un paquet* UDP *;*
– *Un paquet* IPv6 *;*
– *Un paquet* IPV4 *;*
– *Un paquet* ARP.

Question 2 *À l'aide de cette même capture, regardez les adresses MAC et IP entrant en jeu. Identifier-les.*

Relancer une capture et effectuer les actions suivantes :
– Consultation d'une page web en http
– Consultation d'une page web en https
– Lancer la commande **ping mike**
– ...

(si vous n'avez pas le temps de tout faire en une fois, vous pouvez faire plusieurs captures successives).

Question 3 *Identifier dans la capture les traces des échanges précédent.*

Question 4 *Essayer de comprendre le plus de paquets possibles.*