TP AISE — Environnement Noyau

Exercice : Mise en place Virtualisation

Pour ne pas endommager votre machine, mettez en place un machine virtuelle (Virtualbox, Qemu) avec le système d'exploitation de votre choix. Un ISO pourra être fourni au début de la session. Vous penserez à installer les composants nécessaires à la compilation d'un noyau et au développement d'un module noyau.

Exercice: Mon premier noyau

Compilez votre propre noyau, en partant de la dernière distribution du Noyau Linux, disponible ici: https://www.kernel.org/. Remplacez ensuite le noyau actuel par celui que vous venez de compiler. **Il est fortement recommandé de travailler dans une machine virtuelle pour réaliser cet exercice (et les suivants)**. Vous pouvez réaliser la compilation dans l'émulateur ou sur votre machine. On pourra par exemple chercher à activer le "temps-réel" en intégrant une préemption complète du noyau (probablement dans `General Setup > Preemption Mode > Full`...)

Exercice : Un module noyau

Implémentez votre premier module noyau, qui devra disposer du squelette nécessaire pour afficher un message lorsqu'il est chargé et déchargé par le noyau. Ceci va permettre de préparer l'exercice suivant. N'hésitez pas à jeter un oeil au code du noyau que vous venez de compiler afin de comprendre comment le noyau "range" les différents composants/modules. Chaque "*.ko" représente un module noyau. Regardez le code source de certains de ces modules pour démarrer votre implémentation.

Exercice: Recompilation dynamique

Mettez en place un support DKMS pour votre module. Afin de valider son fonctionnement, on pourra tenter de réinstaller une autre version du noyau dans la VM et vérifier que notre module noyau est bien recompilé automatiquement lors du reboot.

Exercice : Un Keylogger

La definition d'un keylogger est disponible sur Wikipedia ici: https://fr.wikipedia.org/wiki/Enregistreur_de_frappe. Il s'agit d'un programme enregistrant toute la saisie faite au clavier. Dans certains cas, il peut s'agit d'un dispositif matériel, branché entre la machine et le clavier, capable ensuite de communiquer avec une ressource tierces ses données. Dans d'autres cas, cela concerne une implémentation logicielle, dissimulé dans un processus système ou dans tous les cas capables d'infecter tous les processus afin de récupérer leur entrée standards. Pour cet exercice, l'objectif sera simplement, au travers de votre module noyau précédemment écrit, de "logger" tout ce qui est entré sur le clavier et de l'écrire sur la sortie standard du module. On vérifiera son contenu en affichant /var/log/kern.log ou en exécutant dmesg.

Exercice: export des logs

L'exercice précédent n'a d'intérêt que si les données tapées peuvent être exportées à l'extérieur, vers un tiers. Dans ce dernier exercice, vous avez pour objectif de sauvegarder les entrés du claviers dans:

- un fichier (par exemple dans /root/).
- un terminal déporté (dans une seconde fenêtre par exemple)
- Via un socket, connecté à une autre machine (par exemple celle de votre binôme). Pour aller plus loin, vous pourrez implémenter un mini-serveur Web rapidement déployé dans un conteneur et disposé sur une autre machine qui se chargera de récupérer les logs de plusieurs clients (i.e. plusieurs modules noyau, celui de chaque membre de votre binôme par exemple).

Il est important de bien comprendre la portée d'un tel module noyau, enregistrant toute entrée clavier **en clair** dans un fichier. **Attention donc si, durant la session, vous accédez à un compte nécessitant une authentification !!** (Email, ssh, Facebook ?) Étant root sur vos machines, il est de votre responsabilité de vous assurer de votre propre sécurité.

Have fun :)