Programmation Noyau

EXERCICE 1 – Linux Kernel Module

1) Expliquez ce qu'est un module noyau sous Linux et comment en programmer un.
2) Faites un petit module noyau qui écris "*Hello World !*" lorsqu'il est chargé.
3) Créez un makefile pour compiler ce module à l'extérieur des sources du noyau.

EXERCICE 2 – Linux Security Module

1) Décrivez et expliquez comment marchent les Linux Security Modules (LSM).
2) Implémentez un module pour le noyau Linux qui empêche le lancement de tous les exécutables pour un utilisateur ayant l'UID 1000.
3) Créez un makefile pour compiler ce module à l'extérieur des sources du noyau.

EXERCICE 3 – Linux Kernel Rootkit

1) Expliquez le principe d'un kernel rootkit et de la technique dite du "*system call hooking*".
2) Implémentez un module qui masque les fichiers qui appartiennent à l'utilisateur ayant l'UID 1000 et qui commencent par un '$' via la technique du '*system call hooking*".
3) Rendez le module en question invisible lors d'un `lsmod` et expliquez votre technique.
4) Créez un makefile pour compiler ce module à l'extérieur des sources du noyau.