Noyau / Modules

- Un module est un morceau de code permettant d'ajouter des fonctionnalités au noyau
  - Pilote de périphériques matériels, protocoles réseau ...
- Peut être chargé dynamiquement
  - Sans avoir à recompiler le noyau ou redémarrer le système

- Les modules sont exécutés dans l'espace mémoire du noyau
  - Ils possèdent le contrôle total de la mémoire
  - Ils peuvent détourner ou créer un appel système
- Les modules possèdent le contrôle total de la machine et peuvent :
  - Améliorer la sécurité du système (anti-virus)
  - Affaiblir la sécurité du système (rootkits…)
- Les modules ne rentrent pas en jeu dans la sécurité d'un système

Surface d’attaque

- Lorsqu’un attaquant possède un accès local non-privilégié à une machine :
  - Beaucoup de programmes s’exécutant avec les droits root ;
  - Beaucoup de fichiers intéressants en lecture pour tous les utilisateurs ;
  - Peu de restrictions sur les programmes exécutables par les utilisateurs.

⇒ plein de possibilités pour augmenter ses privilèges