

Formation Sécurité des systèmes d'exploitations



Objectif :

Appréhender le fonctionnement internes des systèmes, Comprendre les mécanismes de sécurité liés au système, consolider la sécurité d'un système

Prérequis :

Connaissance professionnelle de Windows server et GNU / Linux



Jour 1 :

Historique

Module 1: Introduction au fonctionnement d'un système

- ▶ Principaux éléments composant le système
- ▶ Les couches du système d'exploitation

Module 2: Architecture générale des systèmes

- ▶ Processus,
- ▶ Systèmes de fichiers

Module 3: Architecture des applications

- ▶ Executables, Bibliothèques, Frameworks.
- ▶ Design patterns

Module 4: Architecture de Sécurité Applicative

- ▶ ACLs
- ▶ Architecture des services de sécurité applicative

Jour 2 :

Module 5: Architecture et implémentation d'un système UNIX

- ▶ Implémentations propres aux systèmes UNIX
- ▶ Design et implémentation des composants d'un système UNIX

Module 6: Mécanismes de sécurité des systèmes UNIX

- ▶ Chiffrement des VFS
- ▶ SELinux, AppArmor

Module 7: Architecture et implémentation de Windows

- ▶ Implémentations propres aux systèmes Windows
- ▶ Design et implémentation des composants d'un système Windows

Module 8: Mécanismes de sécurité Windows

- ▶ ACLS, GPO...
- ▶ Registre Windows

Jour 3 :

Module 9: Mécanismes de détection et d'identification d'intrusion

- ▶ IDS, IPS

Module 10: Monitoring des couches basses d'un système

- ▶ /proc
- ▶ syslog

Module 11: Implémentation et configuration des pare-feu

- ▶ Pare feu Windows
- ▶ pf, netfilter

Module 12: Outils de sécurisation des systèmes

- ▶ Outils divers de consolidation et d'audits système.

Module 13: Sécurisation et optimisation des noyaux

- ▶ kernel stripping
- ▶ kernel hardening & optimisations

48, Avenue Bellefontaine

59250 Halluin

(+33) 03.66.72.48.44

Pour vous inscrire, merci de nous communiquer vos besoins, identités, financements et dates par courriel :

formations@serval-concept.com