

SÉCURITÉ SYSTÈMES ET RÉSEAUX

CODE2UTF('8211',0) LES FONDAMENTAUX

CODE STAGE : S-SRF

OBJECTIFS

Pouvoir évaluer les risques internes et externes liés à l'utilisation d'Internet
Comprendre quels sont les mécanismes qui permettent de garantir la fiabilité et la confidentialité des données grâce aux différentes solutions sécurisantes
Disposer d'une première approche des concepts techniques, pour comprendre la sécurité des systèmes d'information

DURÉE

4 jours

PUBLIC

Responsables informatique
Administrateurs réseaux
Techniciens
Webmasters
Responsables de la sécurité informatique

PRÉ-REQUIS

Il est nécessaire d'avoir une bonne connaissance générale des réseaux et des systèmes d'exploitation courants
Les participants intéressés par une mise en pratique opérationnelle de la sécurité préféreront la formation Sécurité systèmes et réseaux Mise en oeuvre (S-RES)

PROGRAMME

ENVIRONNEMENT

Le périmètre (réseaux, systèmes d'exploitation, applications)
Les acteurs (hackers, responsables sécurité, auditeurs, vendeurs et éditeurs)
La veille technologique

Les organismes officiels

LES MÉTHODES DES ATTAQUANTS

Les scénarios d'attaques intrusion, DDOS,

Les attaques sur les protocoles réseaux

Les faiblesses des services : Web, VoIP, Messagerie

Le code vandale : virus, vers et chevaux de Troie

LA SÉCURITÉ DES ACCÈS, FIREWALL, WAF, PROXY, NAC

accès des stations aux réseaux entreprise, 802.1X, NAC

Les différents types de firewalls

Les règles de filtrage

Les règles de la translation d'adresse (NAT)

La mise en oeuvre d'une zone démilitarisée (DMZ)

La détection et surveillance avec les IDS

intégration d'un firewall dans le réseau entreprise

La gestion et l'analyse des fichiers log

LA SÉCURITÉ DES SYSTÈMES D'EXPLOITATION

Le Hardening de Windows

Le Hardening d'Unix/Linux

Le Hardening des nomades : IOS / Android

LA SÉCURITÉ DES APPLICATIONS AVEC EXEMPLE D'ARCHITECTURES

Les serveurs et clients Web

La messagerie électronique

La VoIP IPbx et téléphones

LA SÉCURITÉ DES ÉCHANGES, LA CRYPTOGRAPHIE

objectif du cryptage et fonctions de base

Les algorithmes symétriques

Les algorithmes asymétriques

Les algorithmes de hashing

Les méthodes d'authentification (pap, chap, Kerberos)

Le HMAC et la signature électronique

Les certificats et la PKI



Les protocoles SSL IPSEC S/MIME

Les VPN réseau privé virtuel site à site et nomade

