



SÉCURISATION DES RÉSEAUX

Protégez votre réseau des attaques informatiques

Code : SR

Cette formation a pour but de passer en revue les différentes attaques visant les protocoles et équipements réseau. Une démonstration et mise en pratique des attaques sera faite ainsi que l'explication des contre-mesures à apporter.

Nous étudierons dans un premier temps les attaques visant ou utilisant les protocoles de couche 2 qui profitent de problèmes de configuration des commutateurs (switchs). Suivront les attaques ciblant les routeurs et les systèmes VPN.

Enfin, nous nous intéresserons aux équipements permettant de renforcer la sécurité d'un réseau informatique (Pare-feu, IDS/IPS, Proxy, etc.)

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Présentation des enjeux de la sécurité des réseaux

Démonstration des attaques ciblant les équipements de niveau 2 et leurs contre-mesures

- ARP
- VLAN
- CDP
- Spanning Tree
- Etc.

JOUR 2

Attaque et protection des équipements et protocoles de niveau 3

- Ipv4 et Ipv6
- RIP
- OSPF
- EIGRP
- BGP

JOUR 3

Attaques et contre-mesures sur les passerelles virtuelles

- VRRP
- HSRP
- GLBP

Attaques et contre-mesures sur les VPN

Chiffrement des communications : utilisations et bonnes pratiques

Les outils de protection réseau

- Pare-feu
- IDS/IPS
- Serveur mandataire



PROCHAINES DATES

7 février 2024
 24 avril 2024
 16 septembre 2024
 16 décembre 2024



OBJECTIFS

- Comprendre et savoir réaliser des attaques et s'en prémunir sur les protocoles réseau de base (CDP, STP, ARP, DHCP et DNS)
- Comprendre et savoir réaliser des attaques et s'en prémunir sur les VLAN (Double Tagging, Virtual Trunking Protocol, Dynamic Trunking Protocol)
- Comprendre et savoir réaliser des attaques et s'en prémunir sur le protocole NDP
- Comprendre et savoir réaliser des attaques et s'en prémunir sur l'auto-configuration IPv6
- Comprendre et savoir réaliser des attaques et s'en prémunir sur les protocoles de routage (RIP, OSPF, HSRP, IPSec IKE)
- Comprendre et savoir réaliser des attaques et s'en prémunir sur les protocoles SSL/TLS
- Comprendre et savoir configurer un pare-feu réseau
- Comprendre et savoir configurer un serveur mandataire
- Comprendre et savoir configurer un IDS



INFORMATIONS GÉNÉRALES

Code : SR

Durée : 3 jours

Prix : 2 300 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92)



PUBLIC VISÉ

- Administrateurs réseau / système
- Techniciens réseau / système
- Ingénieurs réseau / système



PRÉ-REQUIS

- Notions de sécurité informatique
- Maîtriser les protocoles réseaux
- Maîtriser les modèles OSI et TCP/IP
- Avoir des connaissances en architecture des réseaux



RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne
- Environnement de démonstration