AVANCÉ

FAISABLE À DISTANCE

EN
RÉALISABLE EN ANGLAIS

SÉCURITÉ DES RÉSEAUX

FFCNCERCERXCS05 | PRIX : 2 990 € | DURÉE : 4 JOURS

Pauses et déjeuners offerts

PRÉSENTATION

La formation identifie les problèmes de sécurité dans les réseaux, puis présente des exemples d'attaques et des solutions envisageables ainsi que leurs principes de fonctionnement. Elle apporte notamment les connaissances nécessaires à une maîtrise des protocoles de sécurité tout en mettant l'accent sur la compréhension des enjeux des accès distants et la mise en œuvre de solutions de VPN. De nombreuses démonstrations illustreront les principes d'attaques de protection exposés.

OBJECTIFS

- Présenter une vision globale des problèmes de sécurité liés aux réseaux actuels
- Expliquer les concepts sous-jacents aux solutions applicables
- Exposer l'ensemble des aspects sécurité liés à la problématique d'interconnexion des réseaux

PROGRAMME

Introduction

Concepts fondamentaux de la cybersécurité
- Problèmes de sécurité sur Internet, origine des failles, risques
- Évolutions des menaces et modes d'attaques, écosystème
- Logiciels malveillants, malwares
- Sécurité des antivirus

Attaques réseaux
- Sécurité des réseaux LAN (Ethernet, VLAN, etc.)
- Attaques réseau classiques : usurpation, Man-in-the-Middle, déni de service, etc.
- Techniques de reconnaissance et de prise d'empreinte à distance
- Attaques par déni de service (DoS, DDoS) : taxonomie, moyens de protection

Analyse de risques et audits de sécurité
- Les principales méthodes : ISO 27005, EBIOS RM
- Audit de vulnérabilités : les principes et différentes étapes
- Audit de la politique de sécurité
- Catégories, principes, outils d'audits (Nmap, Nessus, Arachni, Burp, etc.)

Supervision et gestion des événements de sécurité
- Logiciels de détection et de prévention d'intrusion, IDS/IPS
- Security information and Event Management SIEM

Protocoles de sécurité réseau
- Contextes IPv4 et IPv6
- Protocoles cryptographiques, gestion des clés, certificats X509
- Protocole SSL/TLS - IPsec
- Réseaux privés virtuels (VPN)
- Exemples et démonstrations

Architectures de sécurité
- Problématique et exemples des architectures de sécurité
- Pare-feux réseaux
- Serveurs mandataires
- Zone démilitarisée DMZ
- Place des VLAN pour la sécurité

Sécurité des réseaux sans-fil
- Problématiques de sécurité et architectures WiFi sécurisées
- Principes de sécurisation
- Architectures WiFi sécurisées en contexte Hot-Spot, résidentiel et entreprise

Synthèse et conclusion

PUBLIC/PRÉREQUIS

Toute personne désirant acquérir une vision globale de la sécurité des réseaux, impliquée dans la sécurité des systèmes d'information (SI) ou du réseau de l'entreprise, ou chargée de projets en lien avec des experts sécurité réseaux ou SI.

Une connaissance générale en réseaux IP est un prérequis. Une connaissance des bases de la sécurité sont souhaitables afin de tirer pleinement profit de cette formation.

RESPONSABLE(S)

Maya Badr
Enseignante et responsable pédagogique en cybersécurité et technologies du numérique à Télécom Paris Executive Education. Elle a obtenu son diplôme de doctorat en communications numériques de Télécom Paris.

MODALITÉS PÉDAGOGIQUES

Des exemples et des démonstrations illustrent les concepts théoriques.