Ref. formation 202502297427

Cybersécurité Avancé : Hacking et Sécurité Réseaux

Financement

Formation professionnelle continue
Non conventionnée / sans dispositif

Organisme responsable et contact

DAWAN
GAYE Fatoumata
09.72.37.73.73
carif-aquitaine@dawan.fr

Accès à la formation

Publics visés :

Demandeur d'emploi
Jeune de moins de 26 ans
Personne handicapée
Salarié(e)
Actif(ve) non salarié(e)

Sélection :

Dossier

Niveau d'entrée requis :

Sans niveau spécifique

Conditions d'accès :

aucune

Prérequis pédagogiques :

Non renseigné

Contrat de professionnalisation possible ?

Non

Objectif de la formation

Découvrir la sécurité Réseau - Comprendre les failles et menaces - Protéger ses infrastructures

Contenu et modalités d'organisation

Maîtriser les fondamentaux de la Cybersécurité Problèmes de sécurité sur l'Internet Origine des failles, risques et menaces Fondamentaux sur la gestion des risques Organigramme typique d'une attaque Logiciels malveillants (état de l'art) Risques liés aux Malware Antivirus (fonctionnement et limites) Attaques logiques Analyse d'une APT (Advanced Persistent Threat) Authentification et gestion de mots de passe Menaces sur les applications Web (OWASP...) Identifier les attaques réseaux Sécurité des réseaux LAN (Ethernet, VLAN...) Attaques réseau classiques : usurpation, man-in-the-middle, déni de service... Techniques de reconnaissances et de prise d'empreinte à distance Attaques par déni de service : taxonomie, moyens de protection Atelier pratique : exploitation ARP, prise d'empreinte via nmap Mettre en place des pare-feux et architectures de sécurité Problématique des architectures de sécurité Exemples d'architectures sécurisées : DMZ, cloisonnements, VLANs multiples Pare-feux réseaux (filtres de paquets, relais applicatifs, stateful inspection) Acteurs majeurs du marché des pare-feux réseaux, comparaison entre produits commerciaux et produits non commerciaux Critères de choix d'un pare-feu réseau Exemple de configuration d'un pare-feu réseau Évolution des pare-feux Atelier pratique : mise en place d'un pare-feu basique et de routage de ports avec iptables Maîtriser les protocoles de sécurité réseau Contextes IPv4 et IPv6 : nature des faiblesses de chacun des protocoles Handshake, record, alert et change Faiblesses inhérentes aux protocoles : telnet vs ssh v1 / v2, encapsulation, tunnelling TLS/SSL : rôle et fonctionnement, historique des failles, appréhension de l'impact Le problème du repli (fallback) Réseaux privés virtuels (VPN) : typologie des réseaux VPN, architectures et protocoles PPTP et L2TP, solutions techniques, état de l'art. IPsec : principe de fonctionnement, mise en œuvre, architecture, modes de fonctionnement Atelier pratique : analyse de trafic SSL, mise en place d'une session IPSec, franchissement de firewall via un tunnel ssh. Détecter et gérer des événements de sécurité Détection/prévention d'intrusion (IDS/IPS) : principes, architectures,

…

Parcours de formation personnalisable ? **Oui** **Type de parcours** ***Non renseigné***

Validation(s) Visée(s)

> Attestation de fin de formation

Et après ?

Suite de parcours

Non renseigné

Calendrier des sessions

Numéro Carif	Dates de formation	Ville	Organisme de formation	Type d'entrée	CPF	Modalités
00570335	du 12/02/2025 au 31/12/2026	Bordeaux (33)	DAWAN		Non éligible	FPC