DAWAN

Plan de la formation

www.dawan.fr

Formation Cybersécurité Avancée : Hacking et Sécurité Réseaux

Durée :	5 jours (35 heures)
Tarifs inter-entreprise :	3 475,00 CHF HT (standard) 2 780,00 CHF HT (remisé)
Public :	Administrateurs Réseaux expérimentés
Pré-requis :	Très bonnes connaissances des réseaux
Objectifs :	Découvrir la sécurité Réseau - Comprendre les failles et menaces - Protéger ses infrastructures
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
Modalités d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB100230-F
Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73

Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Approfondir les fondamentaux de la cybersécurité réseau

Repositionner les enjeux actuels de la cybersécurité pour les réseaux d'entreprise
Analyser l'origine des failles, risques et menaces dans les infrastructures connectées
Rappeler les principes de gestion de risques appliqués aux systèmes et réseaux
Comprendre l'organigramme typique d'une attaque pour mieux structurer la défense
Étudier l'état de l'art des logiciels malveillants et des attaques logiques (ransomware, APT…)
Identifier les limites des solutions classiques (antivirus, filtrage simple, mots de passe faibles)
Sensibiliser aux menaces applicatives Web à partir des grandes familles OWASP

Identifier et analyser les attaques réseaux

Revoir les principes de sécurité des réseaux LAN (Ethernet, VLAN, routage interne)
Observer les attaques réseau classiques : usurpation, man-in-the-middle, déni de service…
Mettre en œuvre des techniques de reconnaissance et de prise d'empreinte à distance (scans, fingerprinting)
Comprendre la taxonomie des attaques par déni de service et les grandes familles de protections
Atelier pratique : analyser un trafic compromis (ARP spoofing, scan nmap) et en déduire des mesures de défense

Concevoir des architectures sécurisées et déployer des pare-feux

Identifier les enjeux d'architecture de sécurité dans un SI : zones, rôles, exposition Internet
Étudier des exemples d'architectures sécurisées : DMZ, VLAN multiples, cloisonnement des environnements
Revoir les principes des pare-feux réseau : filtrage de paquets, stateful inspection,

relais applicatifs
Comparer les grandes familles de solutions du marché (open source et commerciales) et leurs cas d'usage
Définir des critères de choix d'un pare-feu réseau selon le contexte et les contraintes de l'entreprise
Mettre en œuvre une configuration de base (règles, NAT, journalisation) et vérifier son efficacité
Atelier pratique : construire une mini-architecture segmentée et mettre en place un pare-feu basique avec iptables

Maîtriser les protocoles et mécanismes de sécurité réseau

Comprendre les enjeux de sécurité d'IPv4 et IPv6 et leurs faiblesses spécifiques
Revoir les notions de handshake, enregistrement, alerte et changement d'état dans les protocoles sécurisés
Comparer les protocoles non sécurisés et leurs alternatives chiffrées (telnet vs SSH, tunnels, encapsulation…)
Analyser le rôle de TLS/SSL dans la protection des échanges et l'impact des vulnérabilités connues
Identifier les risques liés aux mécanismes de repli (fallback) et aux anciennes versions de protocoles
Distinguer les principaux types de VPN (site à site, nomade) et leurs architectures associées
Comprendre le fonctionnement d'IPsec et ses modes de mise en œuvre dans une architecture réseau
Atelier pratique : analyser une session TLS, tester un tunnel SSH et mettre en place une connexion IPsec simple

Déployer des capacités de détection et de supervision sécurité

Situer le rôle de l'IDS/IPS dans une architecture de défense en profondeur
Comprendre les principes de détection et de prévention d'intrusion (signatures, comportement, positionnement réseau)
Découvrir les briques d'un SIEM : collecte, corrélation, tableaux de bord, alertes
Structurer une stratégie de monitoring des logs : quelles sources, quels formats, quels indicateurs suivre
Mettre en place un premier dispositif de surveillance réseau basé sur un IDS open source (ex. Suricata)
Atelier pratique : positionner un IDS sur un réseau simulé, activer la capture (port mirroring) et interpréter les premières alertes

Réaliser des audits techniques et piloter les actions de remédiation

Distinguer les grandes catégories d’audit : organisationnel, configuration, vulnérabilités, tests d’intrusion contrôlés
Comprendre le rôle des techniques de social engineering et de cassage de mots de passe dans une démarche d’audit
Découvrir l’écosystème des outils d’audit (scanners de vulnérabilités, frameworks d’exploitation, scripts maison)
Savoir lire et exploiter un rapport de scan (Nessus, OpenVAS…) pour prioriser les actions de correction
Structurer une démarche d’audit de configuration réseau (pare-feu, routeurs, équipements d’accès)
Atelier pratique : réaliser un mini-audit réseau (scan, analyse des résultats, recommandations) et formaliser un plan d’actions

Sécuriser les réseaux Wi-Fi d’entreprise

Identifier les spécificités de sécurité des réseaux 802.11 et les principales menaces associées
Revoir l’historique des mécanismes de protection Wi-Fi (WEP, WPA, WPA2, WPA3) et leurs limites
Mettre en perspective 802.11i, 802.1X et EAP dans la sécurisation des accès Wi-Fi
Différencier les architectures Wi-Fi : hot-spot, résidentiel, entreprise, invités
Comprendre les risques liés aux portails captifs et aux mécanismes d’authentification simplifiés
Atelier pratique : analyser la sécurité d’un réseau Wi-Fi simulé, illustrer une attaque simple et définir une politique Wi-Fi durcie

Consolider ses acquis par un cas pratique de bout en bout

Synthétiser les notions abordées : menaces, architectures, pare-feux, VPN, IDS/IPS, audits
Étudier le cas d’une application Web exposée via un accès Wi-Fi dédié et un réseau segmenté
Identifier les faiblesses potentielles à chaque étape : poste client, Wi-Fi, pare-feu, DMZ, application, logs
Proposer une stratégie de durcissement et de surveillance adaptée à l’environnement présenté
Atelier final : scénariser et documenter la sécurisation complète de l’architecture, depuis l’accès Wi-Fi jusqu’à l’application, avec plan d’actions priorisé