DAWAN

Plan de la formation

www.dawan.fr

Formation Hacking et sécurité : Les fondamentaux

Durée :	4 jours (28 heures)
Tarifs inter-entreprise :	3 175,00 CHF HT (standard) 2 540,00 CHF HT (remisé)
Public :	Consultants en sécurité Ingénieurs / techniciens Administrateurs systèmes / réseaux - Toute personne intéressée par la pratique de la sécurité informatique dans une optique de défense et de durcissement des systèmes
Pré-requis :	Bonnes bases en administration système (Linux et/ou Windows) et en réseaux TCP/IP (adressage, routage, ports, services).
Objectifs :	Comprendre comment il est possible de s'introduire frauduleusement sur un système distant afin de mieux s'en protéger - Savoir quels sont les mécanismes en jeu dans le cas d'attaques réseaux et systèmes - Acquérir les compétences nécessaires pour mettre en place un dispositif global garantissant la sécurité des systèmes
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 :	CYB102746-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

Poser les bases : comprendre les réseaux et la surface d'attaque

Revoir les fondamentaux des réseaux : modèles de référence, couches, protocoles principaux (IP, TCP, UDP, HTTP, DNS, etc.)
Identifier la notion de surface d'attaque : services exposés, ports ouverts, applications publiées, accès distants
Comprendre les grandes familles d'attaques réseau : interception, manipulation, déni de service, détournement de sessions
Relier les vulnérabilités réseau aux erreurs de configuration et aux choix d'architecture
Atelier fil rouge : cartographier de manière simplifiée un réseau type (LAN, DMZ, accès internet) et repérer les points d'exposition

Analyser les attaques à distance et les phases d'un test d'intrusion

Comprendre les grandes étapes d'une intrusion : collecte d'informations, découverte, analyse, exploitation, rebond, effacement de traces
Découvrir les techniques de reconnaissance et de scan dans une optique de test de sécurité (sans entrer dans les détails opérationnels)
Identifier les vulnérabilités classiques des services exposés (mauvaises configurations, versions obsolètes, mots de passe faibles)
Relier ces techniques au cadre légal et éthique des tests d'intrusion et des audits de sécurité
Atelier fil rouge : analyser un scénario d'attaque à distance à partir de journaux et de schémas réseau et en reconstituer les grandes étapes

Comprendre les attaques systèmes : du compte utilisateur aux privilèges élevés

Distinguer attaque réseau, attaque système et exploitation applicative
Comprendre les mécanismes d'authentification et de gestion des privilèges sur un système d'exploitation
Identifier les vecteurs d'attaque systèmes fréquents : failles de configuration, services inutiles, droits trop étendus, défauts de mise à jour
Découvrir les concepts d'escalade de privilèges et de persistance dans une optique défensive (identifier, détecter, corriger)
Atelier fil rouge : partir d'un exemple de machine mal configurée et lister les faiblesses qui faciliteraient une compromission

Observer et interpréter les traces d'attaques

Comprendre le rôle des journaux (logs) systèmes, applicatifs et réseau dans la détection d'attaques
Repérer des signes de comportements anormaux : connexions inhabituelles, tentatives répétées, élévations de privilèges, modifications suspectes
Articuler les journaux locaux avec une supervision centrale (SIEM, SOC) pour la détection avancée
Relier l'analyse de traces aux processus de gestion d'incidents et de réponse aux attaques
Atelier fil rouge : analyser un extrait de journaux (simplifiés) et identifier les indices d'une tentative d'intrusion

Sécuriser les systèmes : principes de durcissement et bonnes pratiques

Appliquer les principes de durcissement des systèmes : réduction de la surface d'attaque, principe du moindre privilège, segmentation
Mettre en œuvre des mesures techniques simples et efficaces : mises à jour, désactivation des services inutiles, configuration des pare-feux locaux
Renforcer l'authentification et la gestion des comptes : mots de passe robustes, MFA, comptes de service, gestion du cycle de vie des comptes
Intégrer la sauvegarde, la restauration et la résilience dans le dispositif de sécurité global
Atelier fil rouge : établir une checklist de durcissement pour une machine type (serveur ou poste de travail) à partir d'un état initial simplifié

Construire un dispositif global de sécurité des systèmes

Relier les protections réseaux, systèmes et applicatives dans une approche de défense en profondeur
Intégrer la sécurité dans le cycle de vie des systèmes : conception, déploiement,

exploitation, décommissionnement
Articuler sécurité technique, procédures organisationnelles et sensibilisation des utilisateurs
Définir les priorités de sécurité en fonction des risques, des contraintes métiers et des ressources disponibles
Atelier fil rouge : élaborer, à partir d'un SI simplifié, un mini-plan de sécurisation progressif (actions rapides, actions structurantes, suivi)

Introduire les tests d'intrusion dans une démarche de sécurité maîtrisée

Comprendre le rôle des tests d'intrusion (pentests) dans l'évaluation de la sécurité
Distinguer audit, scan de vulnérabilités, test d'intrusion et bug bounty
Identifier les précautions à prendre : cadre légal, périmètre, autorisations, clauses contractuelles, gestion des résultats
Savoir exploiter les rapports de tests d'intrusion pour alimenter les plans de remédiation et de durcissement
Atelier fil rouge : analyser un exemple de rapport de test d'intrusion et prioriser les actions correctives à engager

Consolider ses acquis et définir un plan de progression

Synthétiser les principaux mécanismes d'attaque réseau et système abordés pendant la formation
Relier ces mécanismes aux bonnes pratiques de durcissement et de surveillance
Identifier les compétences complémentaires à développer (analyse de logs, tests d'intrusion avancés, SOC, forensic, etc.)
Définir un plan de progression personnel ou d'équipe pour renforcer la sécurité des systèmes au sein de son organisation
Atelier fil rouge final : formaliser un plan d'actions et de montée en compétences à 3-6 mois autour du hacking éthique et de la sécurité des systèmes