DAWAN

Plan de la formation

www.dawan.fr

Formation Hacking et sécurité : Niveau avancé

Durée :	5 jours (35 heures)
Tarifs inter-entreprise :	3 675,00 € HT (standard) 2 940,00 € HT (remisé)
Public :	Consultants en sécurité - Ingénieurs / techniciens Administrateurs systèmes / réseaux - Développeurs
Pré-requis :	Première expérience du hacking éthique (tests d'intrusion, audits) et de bonnes connaissances de TCP/IP ; la maîtrise de Linux en ligne de commande est un plus recommandé
Objectifs :	Comprendre comment organiser une veille sur la sécurité et savoir où rechercher des informations fiables - Identifier les faiblesses des éléments constitutifs du SI par des prises d'empreintes avancées - Disposer des compétences techniques nécessaires pour réaliser différentes attaques en environnement contrôlé afin d'en comprendre les subtilités - Être en mesure de protéger le SI par un système de contre-mesures adapté
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 :	CYB102747-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 le cadre du hacking éthique et des tests d'intrusion avancés

Repositionner le hacking éthique comme outil d'évaluation et d'amélioration de la sécurité
Rappeler le cadre légal, contractuel et déontologique des tests d'intrusion avancés
Clarifier les limites à ne pas franchir et les responsabilités du pentester et de l'organisation
Structurer un engagement de test d'intrusion : périmètre, objectifs, contraintes, livrables, gestion des risques
Atelier fil rouge : analyser un exemple de mission de test d'intrusion avancé et identifier les points de vigilance juridiques et techniques

Organiser une veille sécurité offensive et défensive

Définir les objectifs de la veille : vulnérabilités, exploits, nouvelles techniques d'attaque, contre-mesures, guides de durcissement
Identifier les sources d'information fiables : CERT, éditeurs, communautés de recherche, publications officielles, bulletins de sécurité
Structurer sa veille : sélection de sources, automatisation, priorisation, diffusion aux équipes concernées
Intégrer la veille dans le cycle de vie de la sécurité : mise à jour des mesures de protection, des scénarios d'attaque et des tests récurrents
Atelier fil rouge : construire un mini-plan de veille sécurité adapté à son contexte (sources, fréquence, format de restitution)

Collecter des informations : prises d'informations et cartographie des cibles

Approfondir les techniques de collecte d’informations dans un cadre autorisé : recherche ouverte, informations publiques, cartographie logique
Distinguer collecte passive et collecte active dans une optique de réduction du risque pour le SI testé
Consolider les informations recueillies pour construire une vue d’ensemble du périmètre à tester (services, technologies, versions, exposition)
Préparer les étapes suivantes du test (scan, prise d’empreintes, scénarios d’attaque) à partir de cette cartographie
Atelier fil rouge : à partir d’un périmètre donné, réaliser une cartographie conceptuelle des systèmes potentiellement exposés

Réaliser des scans et prises d’empreintes avancés

Approfondir les techniques de scan réseau et applicatif dans un environnement de laboratoire sécurisé
Comprendre ce que révèlent les prises d’empreintes : systèmes, services, versions, configurations, topologies probables
Adapter la stratégie de scan en fonction du contexte : contraintes de temps, impact acceptable, règles de bon usage
Interpréter les résultats pour identifier les zones de fragilité et orienter les analyses de vulnérabilités
Atelier fil rouge : analyser des résultats de scans (anonymisés) et prioriser les cibles et vecteurs d’attaque à explorer

Analyser les vulnérabilités informatiques et comprendre les techniques d’attaque

Approfondir la notion de vulnérabilité : classification, scoring, exploitabilité, impact, contexte
Comprendre les grandes familles d’attaques exploitées en pratique : défauts de configuration, vulnérabilités logicielles, injections, élévations de privilège
Relier ces vulnérabilités aux faiblesses observées lors des scans et prises d’empreintes
Comprendre, dans un environnement de test encadré, comment une vulnérabilité peut être exploitée pour démontrer un risque
Atelier fil rouge : étudier plusieurs exemples de vulnérabilités réelles, décrypter les scénarios d’exploitation et les contre-mesures possibles

Mettre en œuvre des scénarios d’attaque en laboratoire

Construire un environnement de laboratoire isolé pour l’expérimentation et la démonstration de scénarios d’attaque/défense

Mettre en place des scénarios réalistes basés sur des combinaisons de vulnérabilités (accès initial, rebond, élévation, persistance)
Observer les effets des attaques sur les systèmes et les journaux afin de mieux comprendre les traces laissées
Utiliser ces scénarios pour sensibiliser les équipes techniques et orienter les plans de remédiation
Atelier fil rouge : dérouler un scénario d'attaque complet en laboratoire et documenter les étapes et les indices observables côté défense

Définir et mettre en œuvre des contre-mesures adaptées

Relier chaque type d'attaque et de vulnérabilité à un ensemble de contre-mesures techniques et organisationnelles
Mettre en perspective durcissement, segmentation, gestion des identités, supervision et détection, corrections applicatives
Prioriser les corrections à mettre en œuvre en fonction de la criticité métier et du niveau de risque
Intégrer les enseignements des tests d'intrusion dans les politiques de sécurité et les guides de configuration
Atelier fil rouge : élaborer un plan de durcissement priorisé à partir des résultats d'un test d'intrusion avancé

Exploiter les résultats des tests d'attaque pour améliorer le SI

Structurer le reporting d'un test avancé : description des scénarios, preuves, analyse des causes, recommandations
Adapter le niveau de détail des rapports aux différents publics : direction, DSI, équipes techniques, métiers
Mettre en place un suivi des recommandations : responsables, échéances, contrôles de remise en conformité
Articuler les rapports de tests avec la gestion des risques, les audits et les plans de continuité
Atelier fil rouge : concevoir un modèle de synthèse de rapport accessible au management à partir de résultats techniques complexes

Construire une démarche continue de tests, de veille et de renforcement

Intégrer les tests d'intrusion avancés dans une démarche de sécurité globale et continue
Définir une stratégie de tests : périmètres réguliers, tests ponctuels ciblés, revues après changements majeurs
Articuler veille, tests, correctifs, durcissement et sensibilisation des équipes

Définir son propre plan de progression en hacking éthique et en défense des systèmes

Atelier fil rouge final : formaliser une feuille de route annuelle combinant veille, tests d’intrusion avancés et renforcement de la sécurité