DAWAN

Plan de la formation

www.dawan.fr

Formation Pentesting : réaliser des tests d’intrusion

Durée :	5 jours (35 heures)
Tarifs inter-entreprise :	3 775,00 CHF HT (standard) 3 020,00 CHF HT (remisé)
Public :	RSSI, techniciens, auditeurs amenés à faire du pentest, administrateurs systèmes et réseaux
Pré-requis :	Bonnes notions en informatique, réseaux et sécurité des systèmes d’information
Objectifs :	Comprendre les fondamentaux, le cadre juridique et les enjeux des tests d’intrusion - Connaître les différentes phases d’un test d’intrusion structuré - Utiliser les principaux outils et techniques de pentest réseaux et systèmes - Simuler des attaques et post-exploitations dans un environnement contrôlé - Rédiger un rapport d’audit professionnel et communiquer les résultats
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 :	CYB102771-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

Comprendre les fondamentaux et le cadre du pentesting

Définir le pentesting et le distinguer des autres types d'audit de sécurité
Comprendre le cadre juridique, contractuel et déontologique des tests d'intrusion
Situer les tests d'intrusion dans une démarche globale de sécurité (gestion des vulnérabilités, conformité, assurance)
Découvrir les méthodologies usuelles (OSSTMM, NIST, PTES, etc.)
Atelier fil rouge : analyser un exemple de mission de pentest et identifier les clauses et contraintes essentielles

Appliquer la méthodologie de pentest : de la reconnaissance au scan

Mettre en œuvre la reconnaissance passive (OSINT) sur une cible donnée
Conduire la reconnaissance active et la cartographie du réseau (scan de ports, services, bannières)
Utiliser des outils de scan de vulnérabilités pour identifier des failles potentielles
Structurer les résultats de la phase de reconnaissance pour préparer l'exploitation
Atelier fil rouge : réaliser une phase de reconnaissance complète sur un environnement de labo et documenter les résultats

Exploiter les vulnérabilités et mener des attaques ciblées

Utiliser Metasploit et d'autres outils pour exploiter des services vulnérables
Mener des attaques sur des services et applications courants (serveurs web, bases de données, services systèmes)
Mettre en œuvre des techniques d'élévation de privilèges et de pivot sur le réseau interne
Comprendre les risques liés aux vulnérabilités exploitées et les scénarios d'attaque associés

Atelier fil rouge : exploiter une ou plusieurs vulnérabilités dans le labo et tracer la chaîne d’attaque de bout en bout

Réaliser la post-exploitation et maintenir l’accès

Comprendre les objectifs de la post-exploitation (collecte de preuves, reconnaissance interne, mouvement latéral)
Mettre en place des mécanismes de maintien d’accès dans un cadre de test contrôlé
Identifier les données sensibles et les chemins d’attaque vers les actifs critiques
Évaluer les impacts potentiels business d’une compromission réussie
Atelier fil rouge : documenter un scénario de post-exploitation et en extraire des recommandations techniques et organisationnelles

Rédiger un rapport de pentest professionnel et restituer les résultats

Structurer un rapport de test d’intrusion : contexte, méthodologie, résultats, preuves, recommandations
Adapter le niveau de détail au public : équipes techniques, RSSI, direction
Prioriser les recommandations et proposer un plan de remédiation réaliste
Gérer la communication sur les failles découvertes et leur correction
Atelier fil rouge final : produire un rapport synthétique de pentest basé sur les exercices réalisés en laboratoire