DAWAN

Plan de la formation

www.dawan.fr

Formation Tests d’intrusion sur infrastructures internes et Active Directory – Niveau expert

Durée :	5 jours (35 heures)
Tarifs inter-entreprise :	3 975,00 CHF HT (standard) 3 180,00 CHF HT (remisé)
Public :	Consultants en sécurité, pentesters - Administrateurs systèmes / réseaux Ingénieurs / techniciens sécurité - Responsables d’infrastructures Windows / AD
Pré-requis :	Bonne connaissance de TCP/IP et des architectures réseau d’entreprise - Première expérience en hacking éthique / tests d’intrusion (ou formation “Hacking et sécurité – Niveau avancé”) - Connaissances de base d’Active Directory (domaines, contrôleurs, GPO, comptes, groupes)
Objectifs :	Comprendre les spécificités de la sécurité des infrastructures internes et d’Active Directory - Identifier les faiblesses d’architecture, de configuration et de gestion des identités dans un environnement AD - Disposer des compétences nécessaires pour conduire des scénarios réalistes de tests d’intrusion internes en environnement contrôlé - Être en mesure de proposer des contre-mesures concrètes pour renforcer la sécurité d’AD et de l’infrastructure interne
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 :	CYB102749-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

Analyser l’architecture interne et le rôle d’Active Directory

Revoir les composants d’une infrastructure interne typique : LAN, serveurs, postes, contrôleurs de domaine, services d’annuaire
Comprendre le rôle d’Active Directory dans la gestion des identités, des autorisations et des postes
Identifier les principaux services liés : DNS, DHCP, services de fichiers, applications métiers intégrées à AD
Repérer les zones d’exposition internes et les surfaces d’attaque propres à un SI Windows / AD
Atelier fil rouge : cartographier une architecture interne de type entreprise et situer les composants AD clés dans le schéma

Identifier les faiblesses d’architecture et de configuration AD

Analyser les choix d’architecture : forêts, domaines, relations d’approbation, délégations d’administration
Identifier les mauvaises pratiques courantes : comptes trop privilégiés, groupes mal

gérés, GPO trop permissives
Comprendre l'impact des mauvaises configurations DNS, des partages ouverts et des droits NTFS inadaptés
Relier ces faiblesses à des scénarios d'escalade de privilèges et de compromission globale du domaine
Atelier fil rouge : à partir d'un exemple de configuration AD (schématisée), lister les failles de conception les plus critiques

Réaliser la reconnaissance et la cartographie interne en environnement contrôlé

Mettre en œuvre des techniques de découverte interne pour identifier machines, services et domaines AD dans un réseau de test
Collecter les informations exposées par les services d'annuaire et les protocoles internes (dans un cadre légal et isolé)
Construire une cartographie logique des relations entre comptes, groupes, machines et privilèges
Utiliser cette cartographie pour prioriser les cibles et scénarios d'attaque à étudier
Atelier fil rouge : construire une vue "chemin d'attaque potentiel" à partir des informations collectées dans un labo

Comprendre les scénarios d'attaque internes sur AD

Analyser des scénarios typiques de compromission : vol de mots de passe, réutilisation d'identifiants, mouvements latéraux
Comprendre les mécanismes d'authentification (Kerberos, NTLM) et les attaques permettant de les détourner dans un contexte pédagogique
Identifier les chemins d'escalade de privilèges depuis un compte standard jusqu'aux comptes à haut niveau de privilèges
Relier ces scénarios aux traces observables dans les journaux et la supervision
Atelier fil rouge : étudier des scénarios d'attaque internes documentés et en dégager les points faibles structurels d'AD

Observer les traces et indicateurs d'attaques dans un environnement AD

Comprendre les journaux clés à surveiller sur les contrôleurs de domaine et les machines membres
Identifier les comportements anormaux : connexions inhabituelles, modifications de groupes, création de comptes, changements de GPO
Articuler la collecte de logs AD avec une solution centralisée de supervision / corrélation (SIEM)

Proposer des règles d’alerte simples pour détecter des comportements suspects liés à AD
Atelier fil rouge : analyser des extraits de journaux (simplifiés) pour y déceler des indices d’activité malveillante

Définir et appliquer des contre-mesures adaptées à l’infrastructure AD

Mettre en œuvre les grands principes de durcissement d’Active Directory : comptes protégés, segmentation des privilèges, bastion d’administration
Renforcer les politiques de mots de passe, d’authentification forte et de gestion des comptes à privilèges
Limiter les possibilités de mouvement latéral : segmentation réseau, restrictions d’accès, durcissement des postes d’admin
Documenter les mesures prises et les intégrer dans les politiques et procédures internes
Atelier fil rouge : élaborer un plan de durcissement priorisé pour un domaine AD à partir d’un état initial décrit

Intégrer les tests d’intrusion AD dans une démarche globale de sécurité

Définir les périmètres et la fréquence des tests internes axés sur AD et l’infrastructure
Articuler audits, tests manuels, outils de revue de configuration et scénarios d’attaque/défense
Mettre en place un cycle d’amélioration continue : analyse, corrections, vérifications, mise à jour des scénarios
Rendre les résultats utilisables par les équipes exploitation et projet
Atelier fil rouge : construire une mini-feuille de route annuelle de tests et de durcissement AD pour une organisation type

Capitaliser sur les enseignements et formaliser les recommandations

Structurer un rapport orienté “infrastructure / AD” : constats, scénarios, risques, préconisations
Adapter la présentation des résultats aux directions, à la DSI et aux équipes techniques
Identifier les alertes urgentes et les chantiers de fond à engager
Définir un plan de progression personnel autour des tests AD et de la sécurité Windows
Atelier fil rouge final : rédiger une synthèse de recommandations AD à destination d’une direction informatique