Encadrement d'un test d'intrusion

2 jours - 14 heures | Code formation : ADHSYS0725

adhara

adhara.fr

Objectifs

Développer les compétences nécessaires pour mener un test d'intrusion.

Participants

Tout administrateur systèmes, ingénieur systèmes et réseaux, chef de projet en sécurité.

Prérequis

Disposer des connaissances de base en réseau TCP/IP ainsi que sur Windows et Linux.

Ouverture vers l'Intelligence Artificielle

Le formateur proposera, lorsque pertinent, un éclairage sur les usages complémentaires de l'intelligence artificielle en lien avec le programme : automatisation de tâches, assistance à l'analyse et à la création de contenus, optimisation des processus ou encore support à la prise de décision. Ces apports permettront d'illustrer de nouvelles pratiques tout en sensibilisant aux bonnes règles d'utilisation responsable (sécurité, fiabilité des résultats, respect des données).

Programme

Présentation et préparation d'un test d'intrusion

Définition d'un test d'intrusion (boîte noire, grise, blanche)
Les différentes phases d'un test d'intrusion
Les méthodes reconnues : PTES "Penetration Testing Execution Standard", OWASP "Open Web Application Security Project" Testing Guide, OSSTMM "Open Source Security Testing Methodology Manual"
Les aspects réglementaires, juridiques
Les contrats et leurs subtilités
Créer des règles de pré-engagement
Utilisation de la méthode Threat Modeling
Installation de Kali, Metasploitable et différents GIT nécessaires
Collecte d'informations avec les OSINT : Maltego, Google Hacking, Réseaux sociaux
Sniffing avec Wireshark, Dsniff
Recherche des services systèmes Banner Grabbing avec Nmap

Phase de reconnaissance et recherche de vulnérabilité

Création d'un arbre d'attaque
Analyse des vulnérabilités et ses différentes phases en respectant le périmètre : active, passive, validation, recherche
Lancer un scanner de vulnérabilités avec Nmap, OpenVAS et Nikto pour le Web
Rédiger et documenter les scores avec CVSS (Common Vulnerability Scoring System), recherche des CVE (Common Vulnerabilities and Exposures) sur exploit-db
Recherche d'installation et mot de passe par défaut
Création de dictionnaires avec cupp.py et crunch
Lancement de Responder, obtention de hash, crack des NTLM ARP poisoning, DNS poisoning avec Ettercap, Driftnet, SSLStrip
Recherche des vulnérabilités Web / mobile avec Burp

Exploitation des vulnérabilités

Exploitation des vulnérabilités, création d'un gabarit et d'une documentation
Utilisation de Metasploit et Empire (listener, stage, exploit) pour l'intrusion système
Pivoting avec Metasploit
Création d'un payload personnalisé avec MSFvenom
Utilisation des outils Nishang pour Active Directory, privilege escalation, Web Shell
Mise en pratique d'une campagne de Spear Phishing avec Gophish
Attaques Wi-Fi avec Aircrack-ng
Attaques physiques avec USB Rubber Ducky et création d'un payload
Utilisation de SQLMap, Beef pour le Web
Bypass d'IDS, reconnaissance d'Honeypot

Encadrement d'un test d'intrusion

2 jours - 14 heures | Code formation : ADHSYS0725

adhara

adhara.fr

Phase d'extinction et de nettoyage du test d'intrusion

Déterminer la valeur des machines compromises et maintenir le contrôle pour une utilisation ultérieure
Identifier et documenter les données sensibles, les paramètres de configuration, les canaux de communication
Maintenir les accès (backdoor, keylogger)
Documenter les preuves (capture d'écran, capture des credentials...)
Détruire les traces (logs)
Nettoyer les actions entreprises (supprimer les scripts, valeurs d'origine, backdoor, comptes système créés)
Terminer le rapport avec : méthodologie utilisée, objectifs, périmètre, notes générales, l'impact business potentiel
Présenter son rapport

Remarques

Pédagogie

La pédagogie est basée sur le principe de la dynamique de groupe avec alternance d'apports théoriques, de phases de réflexion collectives et individuelles, d'exercices, d'études de cas et de mises en situations observées. Formation / Action participative et interactive : les participants sont acteurs de leur formation notamment lors des mises en situation car ils s'appuient sur leurs connaissances, les expériences et mettront en œuvre les nouveaux outils présentés au cours de la session.

Public Visé

Collaborateurs - Développer ses compétences, s'affirmer comme expert dans son domaine, sécuriser son parcours professionnel ;
Entreprises ou organisations - Accélérer les évolutions de carrière des collaborateurs, augmenter l'efficacité et l'employabilité des équipes… ;
Demandeur d'emploi - Développer son employabilité, favoriser sa transition professionnelle...

Profil de l'intervenant

Consultant-formateur expert. Suivi des compétences techniques et pédagogiques assuré par nos services.

Moyens techniques

Encadrement complet des stagiaires durant la formation. Espace d'accueil, configuration technique des salles et matériel pédagogique dédié pour les formations en centre. Remise d'une documentation pédagogique papier ou numérique à échéance de la formation.

Méthodes d'évaluation des acquis

Un contact téléphonique est systématiquement établi avec le stagiaire ou la personne chargée de son inscription afin de définir le positionnement. Si besoin, un questionnaire est adressé pour valider les prérequis en correspondance et obtenir toute précision nécessaire permettant l'adaptation de l'action. Durant la formation, des exercices individuels et collectifs sont proposés pour évaluer et valider les acquis du stagiaire. La feuille d'émargement signée par demi-journée ainsi que l'évaluation des acquis sont adressées avec la facture.