CyberSécurité - Techniques de hacking et contre-mesures - Fondamentaux

TECHHACK1

Qu'elles proviennent d'une erreur, d'une négligence ou de procédés illicites, les failles de sécurité représentent aujourd'hui l'une des préoccupations majeures des organismes privés ou publics. Piratage des systèmes de traitement automatisé de données, vol de données personnelles, perte d'informations confidentielles et stratégiques, les enjeux sont importants et lourds de conséquences. A l'issue de cette formation vous serez capable de : Détecter les fragilités d'un système par la connaissance des différentes cibles d'un piratage, Appliquer des mesures et des règles basiques pour lutter contre le hacking, Comprendre le mécanisme des principales attaques

Présentiel - Synchrone

Objectifs

Public Visé

Décideurs, responsables DSI, responsables sécurité du SI, chefs de projets IT.

Pré Requis

Bases en sécurité des systèmes d'information, compréhension des réseaux et de la gestion des données et de leurs flux.

Objectifs pédagogiques et d'évaluation

Définir les forces et faiblesses du système de sécurité en place
Identifier les vulnérabilités
Mesurer les impacts des menaces de sécurité
Définir la portée des tests de pénétration
Réaliser les tests de pénétration
Etablir les résultats Pentesting

Méthodes pédagogiques

Beaucoup de tests et d'exemples concrets en lien direct avec les besoins des participants
Des techniques directement mobilisables dans le cadre de leurs fonctions
Formation axée sur la mise en pratique
Méthode participative
Mise en situation professionnelle
Alternance de cours et d'exercices dirigés ou en autonomie
Travaux individuels et corrections collectives
Evaluation croisée et partage de bonnes pratiques
Quizz

Parcours pédagogique

Histoire et chiffres
Qu'est-ce que la cybersécurité ?
Histoire de la cybersécurité
Impacts suite à une cyberattaque
Les types d'attaquants (White hat...)
Qu'est-ce que le hacking ?
Les types d'attaques (Malware, MITM, SE...)
Les différentes phases d'une attaque (Cyber Kill Chain)
Les métiers de la cybersécurité
Les différentes lois et référentiels
PTES (Penetration Testing Execution Standard)
OWASP
Article 323
Les normes ISO 27000
MITRE : ATT&CK – Scoring CVSS (Common Vulnerability Scoring System)
Exemple de travaux pratiques (à titre indicatif)
Technique d'intrusion hardware (Bypass de sessions Windows et Linux)

Reconnaissance passive et active
Utilisation d'outils publics pour obtenir des informations sur une cible
Google Dorks
OSINT Framework
Social Engineering
Maltego...
Présentation des outils de reconnaissance active (Nmap, Hping3) et leur signature (Wireshark)
Banner grabbing : description des services d'une cible
Présentation des outils d'analyse (NmapSE et Metasploit)
Analyse de vulnérabilités

STRATEGIE INFORMATIQUE - Numéro de déclaration d'activité (ne vaut pas agrément de l'état) : 95970120697

Stratégie Informatique
Guadeloupe : Immeuble la Coupole, Grand-Camp 97142 ABYMES Tél : 05 90 83 06 18 Fax : 05 90 83 46 71
Martinique : Immeuble Sera n°6, Zone de Manhity 97232 LAMENTIN Tél : 05 96 57 40 20 Fax : 05 96 51 60 53
SARL AU CAPITAL DE 7775€ - SIRET 352 717 193 00044-APE 6202 A

Nessus
OpenVas
ExploitDB
CVE (Common Vulnerability Enumeration)
CWE (Common Weakness Enumeration)
CAPEC (Common Attack Pattern Enumeration and Classification)
NVD (National Vulnerability Database)...
Exemples de travaux pratiques (à titre indicatif)
Reconnaissance passive d'une entreprise
Création de dictionnaire (Crunch, cupp.py, Top probable)
Technique d'attaque par dictionnaire
Récupération d'informations sur une infrastructure virtualisée

Attaques réseau
Liste des protocoles les plus vulnérables
Compréhension et utilisation des techniques de "l'homme du milieu" (MITM)
Attaques sur les protocoles réseaux
IDLE Scan
LLMNR (Link-Local Multicast Name Resolution)
WPAD (Web Proxy Auto Discovery)
DoS – ARP (Address Resolution Protocol)
usurpation d'IP et MAC
DHCP (Dynamic Host Configuration Protocol)
DNS (Domain Name System)
Description des Protocoles 802.11 et attaques associées
Exemples de travaux pratiques (à titre indicatif)
Mise en pratique des techniques MITM
Evil-Twin, brute-force WPA2

Attaques Web
Présentation du Top 10 OWASP
Apprentissage et compréhension des injections
Exploitation de failles Cross-Site Scripting (XSS)
Exploitation des mauvaises configurations de sécurité
Reconnaissance et utilisation des références directes non sécurisées à un objet

Cross-Site Request Forgery (CSRF)
Exploitation de vulnérabilités connues
Exemples de travaux pratiques (à titre indicatif)
Démonstration Injection et XSS
Challenge Web client et serveur

Exploitation
Présentation et prise en main des frameworks offensifs (Metasploit, Empire)
Recherche et obtention d'accès via une vulnérabilité identifiée
Exemple de travaux pratiques (à titre indicatif)
Utilisation de la faille "Eternalblue"

Création d'une charge (Payload)
Exemple de travaux pratiques (à titre indicatif)
Création d'une charge malveillante

Post-exploitation
Objectifs de la phase de post-exploitation
Identification des modules de post-exploitation
Exemples de travaux pratiques (à titre indicatif)
Démonstration du module Meterpreter
Création d'une persistance ou d'une porte dérobée sur une machine compromise

Moyens pédagogiques

Stratégie Informatique
Guadeloupe : Immeuble la Coupole, Grand-Camp 97142 ABYMES Tél : 05 90 83 06 18 Fax : 05 90 83 46 71
Martinique : Immeuble Sera n°6, Zone de Manhity 97232 LAMENTIN Tél : 05 96 57 40 20 Fax : 05 96 51 60 53
SARL AU CAPITAL DE 7775€ - SIRET 352 717 193 00044-APE 6202 A

1 ordinateur par stagiaire - Salle de formation claire, climatisée et spacieuse - Tableau blanc - Vidéo projecteur - Support de cours - Logiciel d'assistance des stagiaires à distance

Qualification Intervenant·e·s

Formateur - Consultant spécialisé dans la sécurité des systèmes d'information

Méthodes et modalités d'évaluation

Evaluation diagnostique en amont : questionnaire d'auto-positionnement et recueil des attentes & besoins – Tour de table - Evaluation formative en cours de formation : exercices - Evaluation sommative en fin de formation : exercice/QCM - Bilan individuel des compétences acquises – Attestation de fin de formation - Questionnaire de satisfaction à chaud - Questionnaire de satisfaction à froid envoyé 15 jours après la formation pour assurer le suivi post formation

Modalités d'accessibilité handicap

Nos formations sont accessibles aux personnes en situation de handicap et aux besoins spécifiques. Une étude personnalisée avec notre référente handicap, permettra d'adapter les moyens pédagogiques, techniques ou organisationnels.

Durée

35.00 Heures **5** Jours

Effectif

De 3 à 8 Personnes

STRATEGIE INFORMATIQUE - Numéro de déclaration d'activité (ne vaut pas agrément de l'état) : 95970120697

Stratégie Informatique
Guadeloupe : Immeuble la Coupole, Grand-Camp 97142 ABYMES Tél : 05 90 83 06 18 Fax : 05 90 83 46 71
Martinique : Immeuble Sera n°6, Zone de Manhity 97232 LAMENTIN Tél : 05 96 57 40 20 Fax : 05 96 51 60 53
SARL AU CAPITAL DE 7775€ - SIRET 352 717 193 00044-APE 6202 A