FORMATION HACKING ETHIQUE PENTESTEUR N1

Ref. ***CEHP1-10***
Durée : 5.0 jour(s) / 35.0 heures

Les systèmes d'information sont omiprésents dans notre quotidien et prennent une place stratégique pour les entreprises. Une mise à mal de ces systèmes peut engendrer de lourdes conséquences et mettre en péril la pérénité d'une entreprise. Pour pouvoir se prémunir des menaces il faut maitriser la connaissance de son système et de ses vulnérabilités. Un des moyens est de réaliser des audits techniques.
Cette certification assure la maitrise des fondamentaux qu'un auditeur technique doit acquérir.

Elle s'inscrit dans un shéma de certifications visant à valider les fiches métiers de l'ANSSI suivantes : Consultant en cybersécurité, Formateur en cybersécurité, Évaluateur de la sécurité des technologies de l'information.

Pré-requis :

Connaissances en réseaux et systèmes Windows et Linux
CISR1

Personnes concernées :

Techniciens et administrateurs systèmes et réseaux
Architectes sécurité
Intégrateur sécurité
Personne étudiant la cyber-sécurité
Responsable sécurité
Auditeur sécurité

ECSF METIERS ASSOCIE :
Cybersecurity auditor, Penetration tester, Cybersecurity implementer, Cybersecurity architect, Chief information security officer

Objectifs :

Acquérir la méthodologie du pentester
Reproduire les bonnes pratiques d'audit technique
Établir un plan d'audit associé au contexte
Appliquer une méthodologie d'audit
Identifier des vulnérabilités
Évaluer la robustesse d'un système
Construire des chemins d'attaques
Ecrire un rapport d'audit

Programme :

JOUR 1

Principe du Hacking
Définition
Typologie des attaquants
Vocabulaire
Méthodologie Hacking
PTES
OWASP
OSSTMM
Red Team / Blue Team
Kill Chain uniffied
Préparation audit + rapport
Contrat
Contexte et périmètre
lois
La trousse à outil d'un pentester
Mise en place dans le cloud
Comment s'organise un rapport
OutilsVirus / ver / cheval de troie
Backdoor
Logiciel espion / Keylogger
Exploit
Rootkit
ransomware
Pourriel / Hameçonnage / canular informatique
Spearphishing
Botnet
Scanner de réseaux et de failles

QUIZZ: méthodologie, vocabulaire, outils

JOUR 2

OSINT
Présentation OSINT
Méthodologie OSINT
Exemple : Google dorks / recherche d'emails /• recherche de sous-domaine
Reconnaissance active
Principe
Méthodologie
Pratique : Nmap, metasploit, scapy
Vulnérabilités
MITRE ATT&CK
Scanner de vulnérabilités
Social ingénierie
CVE
Défaut de configuration

TD : mise en pratique méthodologie OSINT, utilisation NMAP Métasploit pour reconnaissance. Interprétation des résultats

JOUR 3

Typologie des attaques
Exploitation réseau (MITM)
Social ingénierie / Phishing / deepfaked
Server side (Exploit CVE, Cracking + Bruteforce)
Hacking Web et Application Web
Principe
Méthodologie
Typologie d'attaque : Client side, Back side,
Front side
TOP10 OWASP
Exploitation de failles
Attaque avancée

Création de Payload
Customiser ses exploits
Mise en œuvre du Pivoting
Exploitation Browser

TD : mise en œuvre attaque web, SE, Exploitation et payload.

JOUR 4

Post-exploitation
Mise en œuvre de technique d'exfiltration
Les élévations de privilège
Effectuer une énumération locale
Effacer ses traces
Rapport
Exemple de rapport
Etude d'un rapport
Communication et résultats
Mise en situation
Pentest d'un lab
Rédaction du rapport
Focus sur des technologies spécifiques
Hack Wifi
Hack Cloud
Hack IoT
Hack Mobile

TD : audit sur un environnement dédié, réalisation de chemins d'attaques, recueil des vulnérabilités et rédaction du rapport d'audit

JOUR 5

Examen blanc : Sur un lab dédié, réalisation d'une mission d'audit et radaction du rapport.
Quizz sur fondamentaux, méthodologies, technologies spécifiques

Examen : QCM sur la méthodologie d'audit, les techniques de rapports, les technologies spécifiques, les vecteurs d'attaques.
Mise en situations spécifiques sur techniques de reconnaissances, d'exploitation de post exploitation.

Démarche pédagogique :

Formation orientée sur la pratique.
70% de pratique et 30% de théorie
Cybersecurity Educator ECSF

Evaluation et validation :

A l'issue de la formation le stagiaire pourra se présenter à l'examen de certification.
Le temps destiné au passage de la certification est de 3H.
L'examen est composé de 3 parties : QCM, mise en situation sur points spécifiques, mise en situation sur cas concrets.
Il peut se dérouler à distance.

Bureau Veritas Certification assure l'examen final de ce programme de formation.

L'examen valide des domaines de compétences en relation avec les profils métiers identifiés par l'Europpean union agency for cybersecurity via l'European Cybersecurity Skills Framework

Le + :

Formation orientée sur la pratique

70% de pratique et 30% de théorie