400 FORMATIONS
POUR FAIRE LA DIFFÉRENCE

TECHNIQUES DE HACKING CODE2UTF('038',0) PENTEST CODE2UTF('8211',0) INITIATION

CODE STAGE : HS1

OBJECTIFS

L'objectif de cette formation est de détecter les fragilités dcode2utf('8217',0)un système par la connaissance des différentes cibles dcode2utf('8217',0)un piratage, appliquer des mesures et des règles basiques pour lutter contre le hacking ainsi que de comprendre le mécanisme des principales attaques Cybers.

DURÉE

5 jours

PUBLIC

Consultant en cybersécurité, administrateur système, ingénieur en informatique, développeur

PRÉ-REQUIS

Posséder des bases dans la sécurité des systèmes dcode2utf('8217',0)information. Connaître le fonctionnement dcode2utf('8217',0)un des systèmes Windows et Linux ainsi que les langages Shell.

PROGRAMME

Jour 1 matin

Histoire et chiffres
Qu'est ce que la cybersécurité ?
Histoire de la cybersécurité Impacts suite à une cyber-attaque
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

Jour 1 AM

Les différentes lois & référentiels (PTES, OWASP, Article 323, Les normes ISO 27000, MITRE : ATT&CK, Scoring CVSS)

TD / Technique d'intrusion hardware (Bypass de sessions Windows et Linux)

Jour 2 Matin

Reconnaissance passive & active Utilisation d'outils publiques pour obtenir des informations sur une cible (Google Dorks, OSINT Framework, Social Engineering, Maltego..)

TP 1 / Reconnaissance passive d'une entreprise.
TD / Création de dictionnaire (Crunch, cupp.py, Top probable)
TP 2 / Technique d'attaque par dictionnaire

Jour 2 AM

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, Metasploit)
Analyse de vulnérabilités (Nessus, OpenVas, ExploitDB, CVE, CWE, CAPEC, NVD, ...)

TP 3 / Récupération d'informations sur une infrastructure virtualisée

Jour 3 Matin

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, WPAD, DoS, ARP, usurpation d'IP & MAC, DHCP, DNS)

TP 4 / Mise en pratique des techniques MITM

Jour 3 AM

Description des Protocoles 802.11 et attaques associées TD / 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

Jour 4 M atin

TD / Démonstration Injection et XSS Cross-Site Request Forgery (CSRF)

Jour 4 AM

Exploitation de vulnérabilités connues

TP 5 / 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

TD / Utilisation de la faille "Eternalblue"

Jour 5 Matin

Création d'une charge (Payload)

TP 6 / Création d'une charge malveillante
Post-Exploitation TD / Démonstration du module Meterpreter

Jour 5 AM

Identification des modules de post-exploitation Pour aller plus loin...

TP 7 / Création d'une persistance ou d'une porte dérobée sur une machine compromise

Modalité d'évaluation des acquis : Examen pour l'obtention d'un Badge ESD Academy de Techniques de hacking Fondamentaux

Documents :

Supports Livret stagiaire : livret_stagiaire_techniquesdehackingfondamentaux.pdf Cahier dcode2utf('8217',0)exercice : cahier_exercice_techniquesdehackingfondamentaux.pdf Machines virtuelles : VM_techniquesdehackingfondamentaux.ova

SQLI INSTITUT

400 FORMATIONS
POUR FAIRE LA DIFFÉRENCE