MAJ 20/02/2023

Formation « Tests d'intrusion et développement d'exploits »

Réf : PENTEST2

Pour tester des vulnérabilités complexes, les outils et exploits grand public rencontrent parfois leurs limites. Maitrisez les concepts derrière ces outils et apprenez à concevoir des attaques vous permettant de tirer profit de toutes les situations.

Objectifs

- Maîtriser les vulnérabilités complexes
- Comprendre le fonctionnement des exploits
- Développer des outils d'attaque
- Contourner les protections système
- Élargir la surface d'attaque

Attention, cette formation ne traite pas des bases des tests d'intrusion ni de l'utilisation de Metasploit, elle va exclusivement au-delà.

Durée & horaires

- 5 jours soit 35 heures
- Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h et de 13h30 à 16h00/16h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Pentesters expérimentés
- Développeurs expérimentés

Pré-requis

- Avoir suivi avec succès la formation PENTEST1
- Ou avoir une certification reconnue similaire comme OSCP, GIAC GPEN, etc
- Ou posséder une très bonne expérience des tests d'intrusion et pouvoir le démontrer

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs
- Les concepts essentiels développés dans la formation sont illustrés au travers de mises en pratique sur PC permettant d'acquérir des compétences concrètes applicables en tests d'intrusions
- Un réseau vulnérable fidèle à la réalité sert de plateforme pour les tests
- Tous les outils utilisés sont issus du monde libre et peuvent être réutilisés lors des missions
- Les techniques et outils classiques ainsi que modernes sont utilisés tout au long de la formation

Supports

- Support de cours en Français imprimé
- Cahier d'exercices
- Cahier de corrections
- Ordinateur portable prêté pour la réalisation des exercices

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PENTEST2 par HS2.**

Programme

Environnement Windows (avec plusieurs TP)

- Attaques sur le réseau
  - Collecte sur les partages réseau
  - Relais NTLM avancé
  - Abus de IPv6
- Délégation Kerberos
- Attaques sur les GPOs
- Abus des ACLs

Exploitation Wi-Fi (avec TP)

- Exploiter la découverte réseau
- WPA2 Entreprise
- Attaques avec point d'accès malveillant
  - Vol d'identifiants
  - Relais EAP

Développement de charges malveillantes (avec plusieurs TP)

- Techniques d'injection
  - Injection PE
  - Injection de DLL
  - Process Hollowing
- Contournement d'antivirus
  - Contournement de la signature
  - Contournement d'EDR

Exploitation de binaires

- Le CPU
- Assembleur
- Organisation de la mémoire
- Fuzzing (avec TP)
- Ecrire un shellcode
  - Les bases d'un shellcode
  - Adaptation du shellcode à différentes contraintes
- Buffer Overflow (avec plusieurs TP)
  - Détournement d'exécution
  - Protections applicatives
    - ASLR
    - NX/DEP
    - Canary
  - Techniques de contournement
    - Ret2libc
    - Ret2plt
    - ROP
    - Exploitation SEH
- Format String (avec TP)
  - Lecture arbitraire
  - Ecriture arbitraire
  - Détours par .dtors
  - Ecraser la GOT