HACKING & SÉCURITÉ : EXPERT

Une analyse poussée de l'attaque pour mieux vous défendre

Ce cours vous permettra d'acquérir un niveau d'expertise élevé dans le domaine de la sécurité des systèmes d'information en réalisant différents scénarios complexes d'attaques.

Cette formation porte également sur une analyse poussée des vulnérabilités.

Code : HSE

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (TP, cas pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Réseau
- Options avancées de Nmap et développement d'un script NSE
- Scapy
- IPv6 - mitm6
- HSRP / VRRP
- Introduction à la sécurité des protocoles de routage (OSPF, BGP, etc.)

JOUR 2

Système
- Exploitation avancée et mise en place d'un pivot avec Metasploit
- Attaque d'une infrastructure Microsoft (Responder / Pass-The-Hash / CME / ntlmrelayx)
- Élévation de privilèges
- Techniques de contournement

JOUR 3

Applicatif
- Introduction aux Buffer Overflows 32-bits
- Exploitations basiques de débordement de tampon en 32-bits
- Exploitation via Ret2PLT (32-bits et 64-bits)
- Contournement de l'ASLR (32 bits)
- Introduction et exploitation via ROP
- Exploitation de débordement de tampon sous Windows
- Protections contre les Buffer Overflows

JOUR 4

Web
- Injections de commandes
- Attaques contre des JWT vulnérables
- Injections SQL avancées
- XXE
- SSRF / CSRF
- Injection d'objets / Dé-sérialisation
- Liens symboliques ZIP
- IDOR

JOUR 5

CTF final
- CTF sur la plateforme MALICE

PROCHAINES DATES

19 février 2024
27 mai 2024
30 septembre 2024
4 novembre 2024

OBJECTIFS

- Comprendre et effectuer des attaques réseau avancées
- Comprendre et effectuer des attaques système avancées
- Apprendre les différentes méthodes d'élévation de privilèges sur un système Windows ou sur un réseau interne
- Comprendre et effectuer des attaques Web avancées
- Apprendre le concept des dépassements de tampon (buffer overflows) et le mettre en pratique
- Appliquer l'ensemble des attaques abordées durant les précédents jours via un CTF

INFORMATIONS GÉNÉRALES

Code : HSE
Durée : 5 jours
Prix : 4 650 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel

PUBLIC VISÉ

- Consultants en sécurité
- Ingénieurs / Techniciens
- Administrateurs systèmes / réseaux
- Développeurs

PRÉ-REQUIS

- Avoir suivi la formation HSA ou une formation équivalente
- Maîtriser des protocoles réseaux
- Maîtriser des systèmes Windows et Linux
- Savoir développer des scripts
- Avoir des connaissances sur le développement Web et le fonctionnement des applications Web

RESSOURCES

- Support de cours
- 1 PC par personne
- Environnement Windows de démonstration et Linux
- Metasploit