Sécurité offensive de niveau avancé

Référence : **SECPNT2** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Avoir suivi la formation SECPNT1 - Tests d'intrusion ou posséder une bonne expérience des tests d'intrusion.

PROFIL DES STAGIAIRES

• 1-Pentesters expérimentés. • 2-Développeurs expérimentés.

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.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité offensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

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