Ingénierie Offensive et Développement d’Exploit en Cybersécurité Avancée

Lien : https://innov-systems.com/formation/ingenierie-offensive-et-developpement-dexploit-en-cybersecurite-avancee

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SEC300**	**Cybersécurité technique**

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les mécanismes internes des systèmes Windows et Linux pour identifier des failles exploitables
- Concevoir et personnaliser des charges utiles (payloads) adaptées à différents contextes d’attaque
- Maîtriser les techniques modernes d’exploitation et de contournement des protections
- Automatiser des attaques via le développement d’outils offensifs
- Appliquer une approche méthodique de test d’intrusion sur des environnements complexes

POUR QUI ?

- Pentesters confirmés souhaitant monter en expertise
- Ingénieurs sécurité ou responsables Red Team
- Développeurs sécurité spécialisés en exploitation et reverse engineering

Programme détaillé

1 / PRÉPARATION DE L'ENVIRONNEMENT D'EXPLOITATION

- Configuration d'un lab Windows/Linux pour la recherche de vulnérabilités
- Automatisation de la collecte et de l'analyse via scripts personnalisés
- Création d'un environnement de débogage et d'observation mémoire

2 / MÉTHODOLOGIE D'ATTAQUE AVANCÉE

- Analyse de surface d'attaque et cartographie interne
- Identification de vecteurs d'exploitation potentiels
- Techniques de persistance et de pivoting

3 / UTILISATION AVANCÉE DES OUTILS D'ATTAQUE

- Mimikatz, CrackMapExec, Impacket - exploitation et extension
- Scripts PowerShell et Python pour automatiser les phases d'intrusion
- Techniques furtives d'énumération réseau et d'exploitation ciblée

4 / ATTAQUES SUR L'INFRASTRUCTURE WINDOWS

- Abus de Kerberos : constrained et unconstrained delegation
- Exploitation des ACLs et GPOs pour l'escalade de privilèges
- Persistence via Scheduled Tasks et WMI

5 / TECHNIQUES DE MOUVEMENT LATÉRAL

- Relais NTLM avancé et abus du protocole SMB
- Attaques sur les environnements Active Directory distribués
- Techniques d'évasion des contrôles de domaine

6 / EXPLOITATION ET BYPASS DES CONTRÔLES DE SÉCURITÉ

- Bypass d’UAC, AMSI et AppLocker
- Injection de code dans les processus système
- Techniques d’évasion EDR avec obfuscation et sandbox evasion

7 / DÉVELOPPEMENT DE PAYLOADS PERSONNALISÉS

- Construction d’un shellcode compatible multi-architecture
- Utilisation des API Windows pour la création dynamique de charges
- Intégration de chiffrement et de communication réseau chiffrée

8 / TECHNIQUES D’INJECTION ET DE MASQUAGE

- Process hollowing et thread hijacking
- Injection DLL et PE dans différents contextes de mémoire
- Techniques d’anti-forensics et camouflage dans les processus légitimes

9 / EXPLOITATION BINAIRE ET FUZZING

- Introduction à l’analyse statique et dynamique de binaires
- Fuzzing d’applications avec AFL, WinAFL et libFuzzer
- Construction d’un exploit : de la faille au contrôle du flux d’exécution

10 / MÉCANISMES DE PROTECTION ET LEURS LIMITES

- ASLR, DEP, SEHOP, CFG : comprendre et contourner
- Analyse des protections mémoire et détournement d’exécution
- Étude des techniques de mitigation modernes

11 / EXPLOITATION AVANCÉE

- Ret2libc, ROP et JOP
- Techniques hybrides et chainage multi-vulnérabilités

- Création d’exploits stables dans des environnements protégés

12 / CAS PRATIQUE : DU VULNÉRABLE AU SHELLCODE

- Identification d’un binaire vulnérable
- Écriture pas à pas d’un exploit opérationnel
- Vérification et ajustement contre les protections système

13 / AUTOMATISATION D’ATTAQUES OFFENSIVES

- Utilisation de Python pour créer des frameworks d’attaque
- Développement d’outils internes pour la Red Team
- Création d’un pipeline de test d’exploitation automatisé

14 / POST-EXPLOITATION ET PERSISTANCE AVANCÉE

- Techniques de maintien d’accès à long terme
- Exfiltration furtive et communication sécurisée
- Escalade de privilèges et pivoting avancé

15 / SCÉNARIO FINAL : CAMP D’ENTRAÎNEMENT OFFENSIF

- Simulation d’une intrusion complète sur environnement d’entreprise
- Analyse forensique inversée pour évaluer la discrétion de l’attaque
- Débriefing technique et consolidation des acquis

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

20 au 24 Juil. 2026	Présentiel - Casablanca
14 au 18 Sep. 2026	Distanciel
09 au 13 Nov. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com