Techniques de Hacking et Contre-mesures : niveau 2

Lien : https://innov-systems.com/formation/techniques-de-hacking-et-contre-mesures-niveau-2

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC43

CATÉGORIE
Test d'Intrusions, Techniques de Hacking, Contre Mesures et Audit

OBJECTIFS DE LA FORMATION

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

- Acquérir un niveau d’expertise élevé dans le domaine de la sécurité en réalisant différents scénarios complexes d’attaques
- Appréhender des méthodes offensives dans la pratique

POUR QUI ?

- Administrateurs de systèmes
- Techniciens chargés du support
- Toutes personnes impliquées dans la sécurité du système d’information

Innov Systems

Programme détaillé

1 / Les modèles SI (questions, Cloud privé, C2 : Command et Control)

- Statistiques
- Blocage des malwares par type de contenu
- Domaines les plus difficiles à défendre
- Vulnérabilités / attaques
- Motivations
- Failles connues et 0day (exploit.in)
- Etude des séquences d'exploitation

2 / Exploitation Web avancée

- Injection SQL avancée
- Cross-Site Scripting avancé
- Oracle utilisateur
- Race condition LFI et phpinfo
- Désérialisation et exécution de code

3 / Cryptanalyse

- Rappels sur la cryptographie
- Identification des algorithmes
- Attaque sur le chiffrement par flux
- Attaques sur les modes ECB et CBC
- Le padding oracle

4 / Préparation et initialisation des phases à l'exploitation

- Terminologie

Innov Systems

- Présentation de différents framework et outils offensifs (Metasploit, Empire et Powershell)
- Création de différents types de charges pour l'exploitation
- Intégrer de nouveaux Exploits dans Metasploit
- Différents types de connexions (Bind et Reverse)
- Focus sur les stagers : TCP, SSH, DNS, HTTP, HTTPS

5 / Positionnement et attaquant externe

- Social Engineering : Techniques de "Phishing", Clone de page d'authentification, SPF
- Fichier malicieux : Macros Office, PDF, HTML, APK
- Etude et exploitation réseaux Wi-Fi environnant
- Recherche d'identifiants sur les bases de "Leak"
- Les attaques Cloud (Office 365, Azure, AWS)

6 / Positionnement et attaquant interne

- Analyse et compréhension des vulnérabilités protocolaires (DHCP, DNS, NTP...)
- Etude des différents processus d'authentification Microsoft (Kerberos, LAN Manager et Smart card)
- Gestion des identifiants en mémoire au travers des SSP et SSPI : NTLM, Kerberos, Digest SSP, TSPKG, LiveSSP
- Credential Guard
- Présentation de l'outil "Mimikatz"
- Obtention d'un accès avec identifiants
- Obtention d'un accès sans identifiants

7 / Phases de post-exploitation

- Enumération post-exploitation
- Présentation d'un outil de base de données relationnelle (BloodHound)
- Obtention d'identifiants supplémentaires dans les logiciels
- Etude des droits associés aux comptes de services proxy socks4a

Innov Systems

8 / Escalade de privilèges et mouvements latéraux

- Tentative d'escalade des privilèges verticale
- Tentative d'escalade des privilèges horizontale

9 / Autres techniques

- Evasion des systèmes de défense
- Persistance : Registre, Tâches planifiées, DLL Hijacking, Hidden process
- Exfiltration de données via canaux cachés : DNS, BSSID
- Pentester tips

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

04 au 08 Jan. 2027	Présentiel - Casablanca
01 au 05 Mars 2027	Présentiel - Casablanca
26 au 30 Avr. 2027	Présentiel - Casablanca
21 au 25 Juin 2027	Présentiel - Casablanca
16 au 20 Août 2027	Présentiel - Casablanca

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

Inov Systems

Réservation & Renseignements

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

Innov Systems — Tous droits réservés

Innov Systems