Cycle Techniques de Hacking et Contre-Mesures

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

DURÉE
10 jours (70h)

RÉFÉRENCE
SEC41

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

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Connaitre les différentes cibles d'un piratage
- Etre capable de lutter contre le hacking
- Assimiler le mécanisme des principales attaques
- Comprendre et expérimenter des techniques de hacking avancées
- 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

Programme détaillé

1 / Evolution de la cybersécurité

- Nouveaux acteurs et nouvelles portées de la cybersécurité
- Sécurité et juridique
- CNIL ANSSI
- ENISA
- Les normes

2 / Principes généraux de la sécurité informatique

- Pourquoi la sécurité informatique ?
- Les piliers de la sécurité informatique : confidentialité, intégrité, disponibilité...
- Les composants de la cybersécurité : Que veut-on protéger ? Pourquoi ?
- Défense en profondeur et politique de sécurité
- Méthodes et normes pour l'analyse des risques

3 / Introduction à la cybercriminalité

- L'évolution de la cybercriminalité. Son impact
- Les types d'attaquants (White hat...)
- Qu'est-ce que le hacking ?
- Les principaux groupes de hackers
- Les types d'attaques (Malware, MITM, SE...)
- Les différentes phases d'une attaque (Cyber Kill Chain)
- Sophistication des techniques d'attaques
- Les différentes lois et référentiels

4 / Reconnaissance passive et active

Innov Systems

- Utiliser les outils publics pour obtenir des informations sur une cible
- Les outils de reconnaissance active (Nmap, Hping3) et leur signature (Wireshark)
- Banner grabbing : description des services d'une cible
- Les outils d'analyse (NmapSE et Metasploit)
- Analyse de vulnérabilités

5 / Bien comprendre les protocoles réseaux

- D’autres aspects des protocoles IP, TCP et UDP
- Focus sur ARP et ICMP
- Le routage forcé de paquets IP
- Problèmes de sécurité de TCP/IP
- Filtrage sérieux : l'utilité
- Sécurisation des serveurs : un impératif
- Routeur filtrant au firewall stateful inspection
- Bref présentation des solutions et des produits

6 / Connaitre les attaques sur réseau

- Liste des protocoles les plus vulnérables
- Compréhension et utilisation des techniques de "l'homme du milieu" (MITM)
- Attaques sur les protocoles réseaux
- IDLE Scan
- LLMNR (Link-Local Multicast Name Resolution)
- WPAD (Web Proxy Auto Discovery)
- DoS
- ARP (Address Resolution Protocol)
- Usurpation d'IP et MAC
- DHCP (Dynamic Host Configuration Protocol)
- DNS (Domain Name System)
- Description des Protocoles 802.11 et attaques associées

Innov Systems

7 / Les vulnérabilités des applications web

- Top 10 OWASP
- Comprendre les attaquse par injection
- Les failles XSS (Cross-Site Scripting)
- Les mauvaises configurations de sécurité
- Reconnaissance et utilisation des références directes non sécurisées à un objet
- Cross-Site Resquest Forgery (CSRF)
- Cookie poisonning, session hijacking...
- Exploitation de vulnérabilités connues

8 / Exploitation

- Les frameworks offensifs (Metasploit, Empire)
- Recherche et obtention d'accès via une vulnérabilité identifiée

9 / Post-exploitation

- Objectifs de la phase de post-exploitation
- Identification des modules de post-exploitation

10 / Exploitation Web avancée

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

11 / Cryptanalyse

- Rappels sur la cryptographie
- Identification des algorithmes

Inov Systems

- Attaque sur le chiffrement par flux
- Attaques sur les modes ECB et CBC
- Le padding oracle

12 / **Préparation et initialisation des phases à l'exploitation**

- Terminologie
- 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

13 / **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)

14 / **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

Inov Systems

15 / 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

16 / Escalade de privilèges et mouvements latéraux

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

17 / 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

Inov Systems

Prochaines dates programmées

04 au 15 Jan. 2027	Présentiel - Casablanca
01 au 12 Mars 2027	Présentiel - Casablanca
26 Avr. au 07 Mai 2027	Présentiel - Casablanca
21 Juin au 02 Juil. 2027	Présentiel - Casablanca
16 au 27 Août 2027	Présentiel - Casablanca

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

Innov Systems — Tous droits réservés

Innov Systems