Programme de formation

Sécurité informatique - Hacking Ethique Niveau 2 Technique d'audit et de pentesting avancée

5 jours - 35 heures	Code formation : ADHSYS0796

Objectifs

Faire l'état des lieux des menaces récentes et des faiblesses d'infrastructure courantes. Comprendre et expérimenter des techniques de hacking. avancées. Appréhender des méthodes offensives dans la pratique. Développer les compétences nécessaires pour mener un test d'intrusion

Participants

Décideurs, responsables DSI, responsables sécurité du SI, chefs de projets IT.

Prérequis

Avoir des connaissances générales en système, réseau, développement et test d'intrusion. Avoir suivi la formation Hacking Ethique Niveau 1

Pédagogie

La pédagogie est basée sur le principe de la dynamique de groupe avec alternance d'apports théoriques, de phases de réflexion collectives et individuelles, d'exercices, d'études de cas et de mises en situations observées. Formation / Action participative et interactive : les participants sont acteurs de leur formation notamment lors des mises en situation car ils s'appuient sur leurs connaissances, les expériences et mettront en œuvre les nouveaux outils présentés au cours de la session.

Remarques

Ateliers pratiques proposés pour chaque thématique abordées afin d'appliquer les concepts enseignés dans une démarche éthique.

Certification

Profil de l'intervenant

Consultant-formateur expert. Suivi des compétences techniques et pédagogiques assuré par nos services.

Moyens techniques

Encadrement complet des stagiaires durant la formation. Espace d'accueil, configuration technique des salles et matériel pédagogique dédié pour les formations en centre. Remise d'une documentation pédagogique papier ou numérique à échéance de la formation.

Méthodes d'évaluation des acquis

Exercices individuels et collectifs durant la formation. La feuille d'émargement signée par demi-journée ainsi que l'évaluation des acquis de fin de stage sont adressées avec la facture.

Programme

Programme de formation

Sécurité informatique - Hacking Ethique Niveau 2 Technique d'audit et de pentesting avancée

5 jours - 35 heures	Code formation : ADHSYS0796

Menaces sur les SI

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

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 (Transmission Control Protocol)
- SSH (Secure SHell)
- DNS (Domain Name System)
- HTTP (Hypertext Transfer Protocol)
- HTTPS (Hypertext Transfer Protocol Secure)

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)

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 (NT LAN Manager)
- Kerberos
- Digest SSP
- TSPKG
- LiveSSP
Credential Guard
Présentation de l'outil "Mimikatz"

Sécurité informatique - Hacking Ethique Niveau 2 Technique d'audit et de pentesting avancée

5 jours - 35 heures | Code formation : ADHSYS0796

Phases de post-exploitation

Énumération post-exploitation
- GPP
- Listing des permissions ACL / AD
- Recherche des délégations de droits
- Extraction des profils Wi-Fi
- Récupération de certificats
- Identification de fichiers intéressants par classification inversée

Présentation d'un outil de base de données relationnelle (BloodHound)
Obtention d'identifiants supplémentaires
- Extraction des identifiants en cache
- Extraction des hashes de la base SAM
- Extraction des identifiants stockés dans les logiciels
- Etude des droits associés aux comptes de services

Pivoting
- Accès aux ressources internes
- Accès aux réseaux restreints type "SCADA"
- Exfiltration des données via le montage d'un proxy socks4a