Développez vos talents
Certifiez vos compétences

Sécurité offensive

Techniques de hacking et contre-mesures - Niveau 2

5 jours (35h00) | SEC-HACK2 | Code Certif Info : 94833 | Certification M2i Sécurité Pentesting (non incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cybersécurité › Sécurité offensive

À l'issue de ce stage vous serez capable de :

- 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.

Niveau requis

Avoir des connaissances générales en système, réseau, développement et test d'intrusion.

Public concerné

Etudiants, administrateurs système, consultants en sécurité de l'information.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Programme

Jour 1

2019 : 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)

Exemples de travaux pratiques (à titre indicatif)

- *Prise en main des outils*
- *Création et intégration d'un payload*

Jour 2

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)

Exemples de travaux pratiques (à titre indicatif)

- *Clone d'une page d'authentification*
- *Compréhension de menaces et attaques physiques*
  - *Rubber Ducky*
  - *Bash Bunny*
  - *Packet Squirrel*
  - *Lan Turtle LAN et 3G*

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"

Exemples de travaux pratiques (à titre indicatif)

- *Lister différentes techniques d'utilisation de l'outil Mimikatz sans que celui-ci ne soit détecté*
- *Sélectionner la technique qui semble la plus efficace, expliquer pourquoi et la mettre en pratique*

Jour 3

- Obtention d'un accès avec identifiants
  - Tentative de propagation
  - Listing des permissions ACL / AD / SQL
  - Recherche de délégations
- Obtention d'un accès sans identifiants
  - Identification de vulnérabilités
  - Tentative d'utilisation d'exploits communs
  - Zoom sur la vulnérabilité MS17-010
  - LLMNR et NBT-NS Poisoning
  - Etude et crack des hashes
  - Attaque par "relais" SMB
  - Attaques de type "Man In The Middle"
  - SPN
  - Kerberoasting
  - Tentative de propagation

Exemple de travaux pratiques (à titre indicatif)

- *Attaque de type relais LLMNR (Link-Local Multicast Name Resolution) et NBT-NS (NetBIOS Name Service)*

Phases de post-exploitation

- Enumération 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)

Jour 4

- 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

Exemples de travaux pratiques (à titre indicatif)

- *Collecter des données pour Bloodhound*
- *Identifier le plus court chemin vers un compte à hauts privilèges*

Escalade de privilèges et mouvements latéraux

- Tentative d'escalade des privilèges verticale
  - Modification de démarrage via le BIOS
  - Exploits
  - Mauvaise configuration
- Tentative d'escalade des privilèges horizontale
  - Identification des accès locaux distants
  - Pass-the-hash
  - Pass-the-ticket
  - VSS (Volume Shadow Copy Service)
  - DCSync
  - WinRM / WMI

Exemple de travaux pratiques (à titre indicatif)

- *Atteindre le compte précédemment identifié, via les différentes techniques enseignées*

Jour 5

Autres techniques

- Evasion des systèmes de défense
  - Détection des signatures
  - Evasion des systèmes antivirus
  - Obfuscation de code avec Powershell
  - Désactivation des systèmes d'évènements
  - AMSI Bypass
  - Applocker Bypass
- Persistence
  - Registre
  - Tâches planifiées
  - DLL (Dynamic Link Libraries) Hijacking
  - Hidden process
- Exfiltration de données via canaux cachés
  - DNS (Domain Name System)
  - BSSID (Basic Service Set Identifier)
- Bonus : pentester tips

Exemple de travaux pratiques (à titre indicatif)

- *Trouver un moyen d'exécuter un script Powershell dans un environnement sécurisé*

Certification (en option)

- Prévoir l'achat de la certification en supplément
- L'examen (en français) sera passé le dernier jour, à l'issue de la formation et s'effectuera en ligne
- Il s'agit d'un QCM dont la durée moyenne est d'1h30 et dont le score obtenu attestera d'un niveau de compétence

Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)

Compétences visées

- Définir les forces et faiblesses du système de sécurité en place
- Identifier les vulnérabilités
- Mesurer les impacts des menaces de sécurité
- Définir la portée des tests de pénétration
- Réaliser les tests de pénétration
- Etablir les résultats Pentesting.