

## Piratage éthique et contre-mesures : Travaux Pratiques - 4 jours

### Savoir prévenir les failles réseau et système

*formation 537*

- Vous apprendrez à**
- Utiliser le piratage éthique pour mettre en évidence les faiblesses de votre entreprise et choisir les contremesures
  - Recueillir des informations grâce à la reconnaissance, aux données publiées et aux outils de scan
  - Sonder et compromettre le réseau en utilisant des outils de piratage pour tester et optimiser votre sécurité
  - Comprendre la manière dont les "hackers" malveillants exploitent les failles du réseau pour se "l'approprier"
  - Protéger votre entreprise de l'escalade de privilèges pour empêcher les intrusions
  - Déjouer des antivirus, des pare-feu et des IDS
- Objectif** Alors que la complexité des failles réseau ne cesse de croître, il devient indispensable de prendre des mesures défensives proactives pour contrer les attaques malveillantes. Lors de ce cours, vous apprendrez à identifier les faiblesses dans un réseau d'entreprise avec le même état d'esprit et les mêmes méthodes que les "hackers". Vous acquerez les compétences pour exploiter de manière systématique les défenses internes et externes. Vous apprendrez à élaborer des contre-mesures ainsi qu'à réduire et limiter les risques encourus par votre entreprise.
- À qui s'adresse cette formation** Consultants en sécurité, auditeurs en assurance de l'information, programmeurs, testeurs de la sécurité PCI, ainsi que les personnes impliquées dans la mise en œuvre et les mesures de cybersécurité. Une connaissance de la sécurité à un niveau comparable à celui de la formation 468, "Sécurité système et réseau", ainsi qu'une expérience significative en TCP/IP sont nécessaires.
- Travaux pratiques** Les exercices pratiques, inspirés de méthodes de piratage et de contre-mesures, comprennent :
- Préparation de la boîte à outils du "hacker"
  - Scan de ports avancé
  - Mise en relation des vulnérabilités et des exploits
  - Identification des vulnérabilités d'un réseau
  - Exécution d'attaques par injection
  - Prédiction et piratage de sessions Web
  - Empoisonnement DNS pour attirer des clients
  - Configuration et utilisation du Framework Metasploit
  - Mise en échec de pare-feu sans états, d'IDS et de logiciels d'antivirus
  - Cloner un site Web et dérober les mots de passe

## Piratage éthique et contre-mesures : Travaux Pratiques - 4 jours

### Savoir prévenir les failles réseau et système

*formation 537*

#### Introduction au piratage éthique

- Définition d'une méthodologie de tests de pénétration
- Création d'un plan de test de sécurité
- Respect des normes PCI
- Construction d'une "boîte à outils" de piratage

#### Prise d'empreintes et recueil d'informations

##### Acquisition d'informations sur la cible

- Localisation d'informations utiles et pertinentes
- Récupération des données publiées
- Analyse de sites d'archive

##### Scan et énumération des ressources

- Identification des méthodes d'authentification
- Analyse des pare-feu
- Recueil des informations contenues dans les courriels
- Interrogation des services réseau
- Scans avec HTML

##### Identification des vulnérabilités

##### Mise en relation des faiblesses et des exploits

- Recherche dans les bases de données
- Détermination de la configuration de la cible
- Outils d'évaluation de vulnérabilité

##### Tirer parti des possibilités d'attaque

- Découverte des sources d'exploits
- Attaques avec Metasploit

#### Attaque de serveurs et d'infrastructures pour optimiser les défenses

##### Contournement de listes de contrôle d'accès (ACL) de routeurs

- Identification de ports filtrés
- Manipulation de ports pour obtenir l'accès
- Connexion à des services bloqués

##### Compromettre des systèmes d'exploitation

- Étude des modes de protection de Windows
- Analyse des processus Linux/UNIX

##### Corruption d'applications Web

- Injection de code SQL et HTML
- Piratage de sessions Web par prédiction et fixation

- Contournement des mécanismes d'authentification

#### Manipulation de clients pour révéler les menaces internes

##### Appâter et piéger les utilisateurs internes

- Empoisonnement du DNS
- Cross-site scripting (XSS)
- Prise de contrôle des navigateurs

##### Création d'un malware personnalisé

- Recueil d'informations client
- Énumération des données internes

##### Déployer une boîte à outils d'ingénierie sociale

- Cloner un site légitime
- Détourner l'attention des clients en infectant le DNS
- Délivrer des payloads personnalisés aux utilisateurs

#### Exploitation de cibles pour accroître la sécurité

##### Introduction d'outils de prise en main à distance (remote shells)

- Connexion directe ou inversée
- Utilisation de l'outil Meterpreter de Metasploit

##### Attaque par rebonds

- Attaques de médias portables
- Routage via des clients compromis
- Transfert et redirection de ports

##### Vol d'informations cible

- Mots de passe "hachés"
- Extraction de données de routage, DNS et NETBIOS

##### Téléchargement et exécution de charges utiles

- Contrôle des processus de mémoire
- Utilisation du Remote File System (RFS)

##### Tests d'antivirus et de la sécurité IDS

##### Déguisement du trafic réseau

- Obfuscation de vecteurs et de charges utiles
- Contournement des défenses de périmètre

##### Déjouer les systèmes d'antivirus

- Falsification d'en-têtes de fichiers pour injecter un malware
- Identification des failles dans la protection antivirus

#### Atténuation des risques et mesures à prendre

- Compte rendu des résultats et création d'un plan d'action
- Gestion des correctifs et de la configuration
- Recommandation de contre-mesures de cybersécurité
- Se tenir informé sur les outils, tendances et technologies