Provadys Institute

Techniques d'intrusion informatique et hacking

Ces techniques permettent de s'assurer qu'un périmètre n'est pas affecté par les failles de sécurité les plus fréquentes, que pourraient exploiter des pirates opportunistes. Ces techniques sont majoritairement automatisées. Les contre-mesures à mett

Une session basée sur des ateliers techniques pratiques pour la maitrise des concepts et la prise en main des outils.

Tests d'intrusion basiques

Cartographier le périmètre visible par les agresseurs potentiels

- Collecte active ou passive d'informations techniques

Identifier les accès et vulnérabilités potentielles

- Collecte de logins valides et tests des mots de passe par défaut
- Utilisation des bases de vulnérabilités publiques

Mise en œuvre des outils d'analyse automatique

- Attaque par force brute / Dictionnaires
- Scanner de vulnérabilités & Traitement des faux positifs
- Scanner de vulnérabilités applicatives
- Tests de cryptographie (version SSL, longueur des clés, algorithmes, validité de certificat...)
- Méthode HTTP, XST,...
- Outils d'exploitation

provadys

Mise en œuvre des techniques manuelles d'attaque

- Tests pré authentification
- Techniques d'injection

Théorie des failles système les plus exploitées

- Buffer overflows
- Race conditions

Mise en oeuvre des techniques d'attaque applicatives

- Techniques d'injection diverses

Tests d'intrusion avancés

Dans un deuxième temps, les tests correspondant à des attaques ciblant particulièrement un périmètre seront abordés. Ces tests sont essentiellement manuels, et mettent en jeu des compétences techniques plus spécifiques.

Attaques des applications web

- Attaque des systèmes d'authentification
- Manipulation de champs HTTP
- Gestion de la session
- Path transversal
- Injection de commandes
- Commentaires
- Contrôles côté client
- Cross-site scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Injection SQL
- Encodage
- Messages d'erreur
- DoS applicatif
- Injection CRLF
- HRS
- Attaques de webservices
- Web 2.0 (AJAX, XMLHttpRequest, etc...)
- HTML5

provadys

Attaques des applications non web

- Attaques à froid
- Attaques à chaud: écoute mémoire, Debugging, Activité réseau,

  Activité système de fichiers, Activité CPU/mémoire, Utilisation de bibliothèques, Bases de registres, Variables d'environnement , etc.

- Attaques réseau
- Interception/modification des flux IP

INFOS PRATIQUES
Durée : 3 j.
Tarif : 1 970 € HT
OBJECTIFS
Comprendre et évaluer la menace ambiante
Maîtriser l'évaluation automatisée de la sécurité des infrastructures **PUBLIC CONCERNÉ**
Analyste sécurité des SI
Auditeurs internes
Risk Manager RSSI DSI Développeurs, etc.
PRÉREQUIS
Connaissance des principaux protocoles de l'Internet (DNS, DHCP, HTTP, etc...)
FORMATION PROPOSÉE
Eligible au DIF
Inter-entreprise : oui
Intra-entreprise: oui
CONTACT
contact@provadys.com
Provadys Paris : +33 (0)1 46 99 93 80
Provadys Sophia-Antipolis : +33 (0)4 93 00 87 50
Provadys Nantes : +33 (0)2 85 52 65 48

provadys