RANDORISEC

iOS Mobile Application Hacking

Descriptif :

L'objectif de cette formation est de transmettre les méthodes d'attaques visant les applications iOS ainsi que les recommandations permettant de contrer ou tout du moins ralentir ces attaques.
Elle s'appuie sur la méthodologie MSTG (Mobile Security Testing Guide) de l'OWASP (Open Web Application Security Project) et l'outil open-source Needle.
Comme nous pensons que le moyen le plus efficace d'apprendre passe principalement par la pratique la majeure partie de la formation repose sur des LABS (exercices pratiques) et des épreuves qui permettent aux élèves de réaliser eux-mêmes les attaques et ainsi de mieux comprendre les techniques.
A l'issue de cette formation vous serez capables d'identifier les vulnérabilités du Top10 de l'OWASP, de réaliser vous-mêmes des attaques pour récupérer des informations sensibles stockées par les applications iOS et de modifier le comportement de ces applications pour contrer des fonctions simples de sécurité (verrouillage par code PIN, détection de jailbreak, chiffrement des communications, etc…). Vous serez également en mesure d'intégrer dans vos développements des fonctions de sécurité plus efficaces.

Durée :

2 jours (environ 14h)

Public visé :

Auditeurs ou consultants en sécurité
Développeurs iOS
Ingénieurs, techniciens, administrateurs systèmes / réseaux
Responsables ou architectes sécurité

Prérequis:

Une bonne connaissance des protocoles TCP/IP, des langages de script et du développement sont un plus mais ne sont pas indispensables.

Un environnement complet sous la forme d'une machine virtuelle personnelle sera mis à disposition par le formateur pour les LABS.
Pour installer la VM chaque participant doit apporter sa propre machine avec les prérequis suivants :

- Droits d'administration ou « root » pour pouvoir modifier la configuration réseau et installer VM Player / VirtualBox
- Environ 30Go d'espace disque libre

RANDORISEC

Programme :

1. Architecture et sécurité iOS
2. Outillage et méthodologie
3. Analyse statique
    - Revue du code source
    - Ingénierie inverse
4. Sécurité des données
    - Stockage non sécurisé
    - Sources de données
    - Fichiers de cache
5. Analyse à l'exécution
    - Instrumentation de l'application (avec Cycript et Frida)
    - Contournement de fonction de sécurité (détection de jailbreak, code PIN, etc…)
    - "Patchage" du binaire (avec Hopper)
6. Sécurité des communications
    - Interception du trafic
    - Contournement du TLS pinning