Formation
« Audit sécurité d'applications mobiles Android et iOS »

Réf : SECUMOBILE

Vous souhaitez acquérir des compétences dans l'audit des applications mobiles Android et iOS ? Ou vous voulez approfondir vos connaissances sur les vulnérabilités propres à ces plateformes ? Ou bien vous souhaitez connaitre la démarche à adopter pour auditer une application mobile ? Cette formation vous permettra de passer en revue les techniques nécessaires pour auditer une application mobile, ainsi que les vulnérabilités les plus courantes sur ce type d'applications.

Objectifs

- Appréhender les problématiques sécurité des applications mobiles
- Savoir effectuer une analyse statique
- Utiliser Frida pour réaliser une analyse dynamique
- Intercepter le trafic d'une application mobile

Durée & horaires

- 3 jours soit 21 heures
- De 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 20 participants

Public visé

- Administrateurs système ou réseau
- Développeurs
- Consultant en sécurité souhaitant acquérir des compétences en audit d'applications mobiles

Pré-requis

- Bonne connaissance en informatique
- Connaissances en réseau (TCP/IP et HTTP) et Linux (savoir utiliser le terminal)
- Connaissances de base en sécurité

Méthode pédagogique

- Cours magistral
- Travaux pratiques

Supports

- Support de cours au format papier en français pour les sessions en présentiel
- Ordinateur portable mis à disposition du stagiaire

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUMOBILE par HS2.**

Programme

Jour 1

iOS

Présentation de l'écosystème iOS

- Architecture iOS et fonctionnalités de sécurité
- OWASP MSTG et MASVS
- Techniques utilisées pour auditer une application
- Jailbreak : histoire, types et évolution
- Mise en place d'un environnement de test
- Signature d'applications
- Présentation de Corellium

Analyse statique d'applications iOS

- Analyse des méta-données liées aux applications
- Déchiffrement d'une application
- Décompilation avec Hopper
  - Travaux Pratiques
    - Automatisation de l'analyse statique avec MobSF
    - Déchiffrement d'une application récupérée de l'AppStore
    - Décompilation et retro-ingénierie d'une application

Android

Présentation de l'écosystème Android

- Architecture d'Android (Composants et Sandboxing)
- Structure et contenu d'un APK
- Présentation de l'Android Manifest
- Mise en place d'un environnement de test
  - Travaux Pratiques : Développement d'une application Android

Analyse statique et modification d'applications Android

- Décompilation d'une application avec JADX
- Analyse statique avec apktool
- Modification d'une application Android avec apktool
- Signature d'une application Android
  - Travaux Pratiques
    - Recherche et identification de secrets au sein d'une application
    - Modification d'une application Android

Jour 2

iOS

Analyse des données d'applications iOS

- Les données sauvegardées par iTunes
  - Travaux Pratiques : Récupération d'informations sensibles à partir d'une sauvegarde
- Les données stockées sur le terminal
  - Travaux Pratiques : Récupération d'informations sensibles / via les journaux

Analyse dynamique d'applications iOS

- Interfaces et implémentations en Objective-C
- Rétro-ingénierie d'une application pour contourner des fonctions de sécurité
  - Travaux Pratiques : Décompilation, retro-ingénierie puis modification en mémoire d'une application avec Frida pour contourner une fonction de sécurité

Android

Analyse dynamique d'applications Android

- Revue des différentes méthodes de stockage de données
  - Shared Preferences
  - Bases de données (SQLite)
  - Stockage interne et externe
  - Travaux Pratiques : Exploitation des faiblesses de chaque méthode
- Comparaison de l'utilisation d'un émulateur ou d'un terminal physique
- Techniques de détection d'un émulateur ou d'un équipement "rooté"
- Revue des contrôles d'accès des composants Android
  - Activities
  - Content Providers
  - Travaux Pratiques : Exploitation des faiblesses de contrôle d'accès
  - Travaux Pratiques : Décompilation, rétro-ingénierie puis modification en mémoire d'une application avec Objection pour contourner une fonction de sécurité

Jour 3

iOS

Sécurité des communications des applications iOS

- Interception du trafic réseau
- Fonctionnement et implémentation du Certificate Pinning
- Techniques de contournement du Certificate Pinning
  - Travaux Pratiques
    - Interception de trafic non chiffré
    - Interception de trafic chiffré
    - Contournement du Certificate Pinning

Que faire sans terminal iOS jailbreaké ?

- Analyse des sauvegardes et des journaux
- Interception du trafic réseau
- Side-loading d'application pour embarquer un framework d'analyse (Frida/Cycript/Objection)

Android

Sécurité des communications des applications

- Revue des faiblesses courantes
- Interception du trafic réseau
- Fonctionnement et implémentation du Certificate Pinning
- Techniques de contournement du Certificate Pinning
  - Travaux Pratiques : Inteception de trafic chiffré et contournement du Certificate Pinning

Instrumentation d'applications Android avec Frida

- Présentation de Frida
- Création de scripts Frida pour instrumenter du code Java
- Utilisation de Frida pour instrumenter du code natif
  - Travaux Pratiques : Utilisation de Frida pour contourner des routines de détection de "root"