+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 24/01/2024

S'inscrire

Formation Pentest Mobile

5 jours (35 heures)

Présentation

La sécurité mobile a parcouru un long chemin au cours des dernières années. Il est passé de "devrait-il être fait ?" à "ça doit être fait !" Parallèlement au nombre croissant d'appareils et d'applications, il y a également une augmentation du volume d'informations personnelles identifiables (PII), de données financières et bien plus encore. Ces données doivent être sécurisées.

C'est pourquoi le Pentesting est si important pour les développeurs d'applications modernes. Vous devez savoir comment identifier les faiblesses d'une application mobile, et comment les corriger d'une façon optimale pour assurer la sécurité des données de l'utilisateur.

Cette formation en cybersécurité vous donne les compétences nécessaires pour tester vos applications mobiles en tant que débutant, développeur ou professionnel de la sécurité. Vous commencerez par découvrir les composants internes d'une application Android et iOS.

En allant de l'avant, vous comprendrez le fonctionnement inter-processus de ces applications. Ensuite, vous allez configurer un environnement de test pour cette application en utilisant divers outils pour identifier les failles et les vulnérabilités dans la structure des applications. En particulier, les participants auront l'occasion de dérouler une serie d'exercice qui couvrent les domaines majeurs de la sécurité mobile, à savoir :

- L'analyse statique
- Sécurité des mécanismes de stockage des données
- L'analyse dynamique
- Sécurité de la couche transport

L'ensemble des exercices est inspiré des scénarios d'exploitation et des vulnérabilités déjà retrouvées sur des applications réelles. Après avoir recueilli toutes les informations sur ces failles de sécurité, nous commencerons à sécuriser nos applications contre les différentes menaces identifiées.

Objectifs

- Connaître l’architecture des systèmes Android et iOS
- Mise en place d’un environnement de test
- Savoir rejouer et simuler des attaques visant les applications Android et iOS
- Comprendre et mettre en œuvre les mesures permettant de développer des applications mobiles nativement sécurisées

Public visé

- Développeurs
- Chefs de projets
- Techniciens SSI
- Auditeurs
- Pentesteurs
- RSSI

Pré-requis

- Connaissances sur Linux
- Avoir une bonne connaissance des réseaux, des systèmes, de la sécurité est un plus

Pré-requis techniques

- Avoir une machine avec Ubuntu Linux 22.04 à nu

Programme de la formation Pentesting Mobile

Généralités sur la sécurité des applications mobiles

- La part de marché des smartphones
- Différents types d'applications mobiles (Native, Mobile web, Hybrid)
- Vulnérabilités publiques Android et iOS
- Les principaux défis de la sécurité des applications mobiles
- La méthodologie des tests de pénétration des applications mobiles (Découverte, Analyse / évaluation, Exploitation, Reporting)
- Le projet de sécurité mobile OWASP (MSTG et MASVS)

Fouiner dans l'architecture

- L'importance de l'architecture
- L'architecture Android
- L'architecture iOS

Préparation de l'environnement et des outils de test

- Mobexler : la machine virtuelle de pentesting des applications mobiles
- Android Studio et SDK : configuration d’un émulateur ou branchement à un périphérique réel
- Apktool : utilitaire de modification des programmes d’installation
- JADX : utilitaire de décompilation des applications
- Ghidra : outil avancé pour le reverse des applications
- Frida : outil d’analyse dynamique
- Objection : outil complémentaire d’analyse dynamique
- Configuration des outils spécifiques à la plateforme iOS

Modélisation des menaces d'une application

- Assets
- Threats (Menaces)
- Vulnérabilités
- Risque
- Approche des threat models
- Threat modeling d'une application mobile

Attaques sur les applications Android

- Prise en main de l’environnement et réalisation de tests basiques
- Modification et patching de binaires
- Analyse et exploitation des mécanismes de stockage local des données
- Identification des mécanismes de chiffrement non sécurisés
- Analyse des composantes Android (activités, receivers etc.)
- Interception et analyse du trafic réseau
- Évaluation des mécanismes de défense anti-reverse
- Contournement des mécanismes de détection d’un environnement rooté
- Analyse et exploitation des mécanismes de backup
- Analyse et évaluation des paramètres de build
- Analyse et exploitation des mécanismes de communication inter- processus (IPC)
- Analyse statique de code source

Attaques sur les applications iOS

- Prise en main de l’environnement et réalisation des tests basiques
- Modification et patching de binaires
- Analyse statique du code source
- Analyse et exploitation des mécanismes de stockage local des données
- Identification des mécanismes de chiffrement non sécurisés
- Utilisation de Frida
- Interception et analyse du trafic réseau
- Évaluation des mécanismes de défense anti-reverse
- Contournement des mécanismes de détection d’un environnement jailbreaké
- Analyse et exploitation des mécanismes de backup
- Analyse et évaluation des paramétrages de build
- Analyse et exploitation des mécanismes de communication inter- processus (IPC)

Sécuriser vos applications Android et iOs

- Concevoir des applications mobiles nativement sécurisées
- Carte mentale de sécurité pour les développeurs (iOS et Android) sur les Top 10 des risques visant les applications mobiles
- Checklist OWASP des bonnes pratiques de développement mobile sécurisé
- Automatisation des recettes de sécurité dans une chaine CI/CD
- Mécanismes anti-reverse pour la protection des binaires

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.