

Mis à jour le 28/05/2024

S'inscrire

# Formation Android Sécurité et Pentest

3 jours (21 heures)

## Présentation

En 2019, le nombre de [cyberattaques ciblant les entreprises a augmenté de 67%](#) en France. Seulement 10% des entreprises étaient aptes à y faire face.

Malheureusement, le nombre d'attaques cybercriminelles est en forte croissance chaque année que ce soit pour les attaques ciblant les sites internet ou les applications.

Notre formation Android Sécurité et Pentest vous permettra de répondre grâce une approche pratique, à l'un des enjeux les plus importants du 21e siècle qui est la sécurisation des applications sous Android.

À l'issue de cette formation, vous pourrez pratiquer et comprendre les techniques utilisées par la Red Team pour mieux défendre en tant que Blue Team. Vous saurez comment analyser les spécificités d'un système informatique sur mobile, identifier les failles de sécurité ainsi que réaliser des tests de pénétration adaptés et efficaces pour s'introduire dans un système Android. Avec une approche offensive et en mettant en place des tests d'intrusion poussés, vous pourrez ainsi assurer et prévenir la sécurité de vos applications smartphone.

Notre formation Android Sécurité et Pentest se basera sur la dernière version d'Android, à savoir [Android 11](#).

## Objectifs

- Connaître l'architecture des systèmes Android
- Mise en place d'un environnement de test
- Attaque sur les applications Android
- Analyser et identifier les failles de sécurité Android

## Public visé

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

## Pré-requis

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

## Programme de la formation Android Sécurité et Pentest

Android Application Fundamentals

ADB (Android Debug Bridge)

Modify Code (Smali)

Other interesting tricks / Spoofing Location

Static Analysis

Dynamic Analysis

Automatic Analysis

Obfuscating/Deobfuscating code

Lab

## 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.