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

Mis à jour le 26/04/2024

S'inscrire

Formation et préparation à la Certification OSMR™ (EXP-312)

ALL-IN-ONE : EXAMEN INCLUS AU TARIF AVEC LE COURS EXP-312

4 jours (28 heures)

PRÉSENTATION

La certification OSMR™ (EXP-312) offre une occasion inestimable de valider vos compétences en sécurité macOS, vous permettant de démontrer votre expertise dans un domaine en constante évolution.

Cette formation OSMR™ offre une plongée approfondie dans le paysage de la sécurité macOS, mettant l'accent sur :

- L'analyse avancée des systèmes
- L'identification des failles de sécurité
- Les techniques d'exploitation

Notre formation OSMR™ (EXP-312) fournit une préparation complète à l'examen, offrant un contenu didactique de qualité et des exercices pratiques pour renforcer votre compréhension et vos compétences dans la sécurisation des systèmes Apple.

Nous mettons régulièrement à jour notre programme pour refléter les dernières tendances et évolutions dans le domaine de la sécurité macOS, assurant ainsi des informations les plus récentes et pertinentes.

La formation OSMR™ est constamment mise à jour pour refléter les dernières tendances et évolutions dans le domaine de la sécurité informatique d'OffSec.

OBJECTIFS

- Comprendre l'architecture et les mécanismes de sécurité spécifiques à macOS

- Acquérir des compétences avancées en analyse binaire et en débogage sur macOS
- Maîtriser les techniques d'injection de code et d'exploitation des services système
- Apprendre à contourner les mécanismes de sécurité tels que TCC, GateKeeper et la sandbox macOS
- Développer des stratégies avancées d'attaque et de défense sur les systèmes macOS

PUBLIC VISÉ

- Pentesters
- Chercheurs en sécurité
- Développeurs
- Développeurs d'applications macOS
- Analysts SOC

Pré-requis

- Connaissance de la programmation en C
- Une expérience normale d'utilisateur avec macOS
- Une connaissance de base de l'assemblage 64 bits et du débogage
- Compréhension des concepts de base de l'exploitation

Note : Ambient IT n’est pas propriétaire de OSMR™, cette certification appartient à OffSec ® Services LLC.

PROGRAMME DE NOTRE FORMATION CERTIFICATION OSMR™

Introduction

- Aperçu du cours OSMR™ (EXP-312)
- Stratégies générales pour aborder le cours
- Présentation des laboratoires VPN EXP-312
- À propos de l'examen OSMR
- Installation des machines virtuelles sur Apple Silicon
- Configuration de Xcode et Homebrew
- Conclusion de l'introduction

Analyse binaire sur macOS

- Vue d'ensemble du système macOS
- Analyse statique et dynamique des binaires
- Utilisation des outils de ligne de commande
- Utilisation de Hopper pour l'analyse statique
- Débogage avec LLDB
- Débogage dynamique et tracing avec DTrace

- Cas d'étude et exemples pratiques
- Conclusion sur l'analyse binaire

Crafting Shellcodes et Injection Dylib

- Écriture de shellcodes en ASM et en C
- Création de shellcodes personnalisés
- Injection de Dylib et DYLD_INSERT_LIBRARIES
- Contournement des mécanismes de sécurité avec les Dylib
- Utilisation du micro-noyau Mach pour l'injection
- Interception de fonctions et hooking sur macOS
- Exemples de cas d'utilisation et pratiques recommandées
- Conclusion sur le crafting shellcodes et l'injection Dylib

Contournement des mécanismes de sécurité

- Compréhension des profils Sandbox macOS
- Bypassing TCC, GateKeeper et File Quarantine
- Techniques de symlink et hardlink attacks
- Obtenir l'exécution de code kernel
- Exemples de contournement réussis
- Analyse de cas d'étude
- Bonnes pratiques pour la sécurisation de macOS
- Conclusion sur le contournement des mécanismes de sécurité

Exploitation Mach IPC et Chaining Exploits

- Exploitation des communications inter-processus Mach
- Cas d'exploitation CVE-2022-22639
- Chaînage d'exploits sur macOS Ventura
- Mitigations sur macOS Ventura
- Études de cas et exemples pratiques
- Bonnes pratiques pour la détection et la prévention
- Stratégies de défense recommandées
- Conclusion sur l'exploitation Mach IPC et le chaînage d'exploits

Analyse des failles de sécurité

- Comprendre les vulnérabilités et leurs impacts
- Recherche et identification de bugs sur macOS
- Analyse de cas de failles de sécurité connues
- Méthodologies de recherche et de rapport
- Pratiques de coordination de la divulgation
- Exercices pratiques d'analyse de failles
- Retour d'expérience et leçons apprises
- Conclusion sur l'analyse des failles de sécurité

Stratégies d'attaque avancées

- Exploration des vecteurs d'attaque sophistiqués
- Développement de techniques d'exploitation avancées
- Contournement des mécanismes de détection
- Analyse de cas d'attaques ciblées
- Défense contre les menaces avancées
- Utilisation d'outils de sécurité spécialisés
- Simulation d'attaques dans des environnements contrôlés
- Conclusion sur les stratégies d'attaque avancées

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.