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

Mis à jour le 11/04/2024

S'inscrire

Formation Certification OSWE™

ALL-IN-ONE : EXAMEN INCLUS AU TARIF AVEC LE COURS WEB-300

CERTIFICATIONS OFFSEC - ACHETER VOS CERTIFICATIONS

4 jours (28 heures)

PRÉSENTATION

Vous voulez être un hacker éthique expert ? La certification OSWE™ prouvera votre expertise en évaluation et en piratage d'applications web.

Après avoir suivi cette formation, vous serez capable d'examiner en profondeur le code source des applications web, savoir comment identifier les failles de sécurité et les exploiter.

Cette formation OSWE™ couvrira tous les éléments présents lors de l'examen comme les injections SQL, les injections JavaScript, le contournement d'authentification ou la déserialisation.

Après avoir suivi notre préparation, vous pourrez passer la certification OSWE™ incluse au tarif.

LE PACK PREMIUM

- 90 jours d'accès aux Labs en autoformation
- 8 accompagnements d'expert : 8 x lundi matin (de 9h à 12h30) par semaine (28 heures)
- 1 Passage de la certification

OBJECTIFS

- Être capable d'analyser en profondeur le code source d'une application web
- Identifier les vulnérabilités que de nombreux scanners d'entreprise sont incapables de détecter

- Mettre en œuvre de manière méthodique des attaques en chaîne en utilisant des vulnérabilités différentes
- Développer des compétences en résolution de problème et pensée divergente

PUBLIC VISÉ

- Hackers éthiques
- Expert en sécurité informatique
- Développeurs
- Architectes techniques
- Administrateurs
- Chefs de projet

Pré-requis

- Une solide compréhension des réseaux TCP-IP
- Avoir une expérience en administration Windows et Linux
- Une bonne connaissance de Linux
- Pouvoir écrire des scripts simples en Python / PHP / Perl / Bash
- Bonne connaissance d'au moins un langage de codage (Java, .NET, Python, etc...)
- Connaissance des proxies web
- Connaissance générale en pentesting, l'obtention de la certification OSCP™ est recommandée, mais pas obligatoire

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

PROGRAMME DE NOTRE FORMATION CERTIFICATION OSWE™

MAITRISE DES OUTILS ET ANALYSE DU CODE SOURCE

- Configurer le lab
- Bien maîtriser la suite Burp Suite (Burp Proxy, Scope, Decoder...)
- Récupération du code source
- Analyse du code source

DU XSS AU RCE

- AtMail Email Server Appliance
- Utiliser le XSS et le CSRF pour obtenir le RCE
- Session Hijacking
- Session Riding
- Les différentes vulnérabilités (atmail, addattachmentAction, globalsaveAction)

CONTOURNEMENT DES RESTRICTIONS D'ENVOI DE FICHIERS

- Shell the web
- Envoi illimité de fichiers
- Atlassian Crowd Pre-auth RCE

CONTOURNEMENT DE L'AUTHENTIFICATION ET RCE

- Présentation des vulnérabilités
- Présentation d'Atutor
- Contournement de l'authentification avec Atutor
- Présentation d'ERPNext
- Contournement de l'authentification avec ERPNext
- Présentation d'openCRX
- Contournement de l'authentification avec openCRX

VULNÉRABILITÉ DE LA RÉINITIALISATION DE MOT DE PASSE

- Tester les fonctionnalités de réinitialisation des mots de passe
- RCE avec injection SQL
- Injection SQL au LFI au RCE
- Reprise des boutiques en ligne d'OXID avant l'annonce de la décision
- Utiliser PostgreSQL
- Exploiter l'injection de H2 SQL dans le RCE

PHP TYPE JUGGLING

- OWASP - PHPMagicTricks TypeJuggling
- Les différentes vulnérabilités
- Type Juggling, PHP Object Injection, SQLi
- Exploits pour PHP Type Juggling
- PHP Magic Hashes

INJECTION JAVASCRIPT

- Présentation de Bassmaster
- Les différentes vulnérabilités
- Utiliser un Reverse Shell
- Server Side JS Injection
- Remote Code Execution in math.js
- Arbitrary code execution in fast-redact
- SetTimeout and SetInterval use eval therefore are evil
- Pentesting Node.js

LA DESERIALISATION

- La déserialisation avec Java

- La déserialisation avec .NET
- La déserialisation avec PHP
- La déserialisation avec Nodejs

ATTAQUE DE L'ENTITÉ EXTERNE XML (XXE)

- Présentation de l'injection XXE
- Du XXE au RCE
- Vulnérabilité Apache Flex BlazeDS XXE
- WebLogic EJBTaglibDescriptor XXE

WEBSOCKETS INSECURITY

- Introduction à WebSockets
- Prise de contrôle de matériel à distance par détournement
- Le détournement de sites Web
- Audit du code source
- Rédactions d'analyses de codes statiques
- TrendMicro
- Shopify Remote Code Execution
- Trouver des vulnérabilités dans le code source (APS.NET)
- Une plongée en profondeur dans la désérialisation ASP.NET

FAQ – QUESTIONS / RÉPONSES

QUEL CONTENU VAIS-JE RECEVOIR POUR LA FORMATION OSWE™ ?

En plus de la préparation que nous proposons. La formation OSWE™ comprend tous les supports de formation délivrés par OffSec :

- 10 heures de formation vidéos
- Un livre de formation en format pdf de plus de 410 pages
- Accès au forum des apprenants
- Accès au lab pendant 90 jours

QUEL EST LE PRIX DU PASSAGE DE LA CERTIFICATION OSWE™ ?

Le passage de la certification coûte 1 649€.

DANS QUELLE LANGUE LA FORMATION OSWE™ VOUS EST ENSEIGNÉE ?

Le coaching sera en français. Cependant, les contenus supplémentaires proposés par OffSec sont en anglais.

L’EXAMEN POUR LA CERTIFICATION OSWE™ EST-IL COMPRIS DANS LE PRIX DE LA

FORMATION ?

Oui, vous pourrez passer l’examen après avoir suivi la formation.

POUR QUELLE DURÉE LE LAB EST-IL ACCESSIBLE ?

Vous avez accès au lab pendant 90 jours

COMMENT SE DÉROULE L’EXAMEN POUR LA CERTIFICATION OSWE™ ?

Vous devez absolument lire le guide officiel avant de passer votre examen.

La phase pratique de l’examen dure 47 heures et 45 minutes, cette phase consiste à hacker le maximum de machines. Après cette phase, vous aurez à nouveau 24 heures pour compléter et envoyer le rapport de pentesting où vous expliquerez votre démarche.

EN QUELLE LANGUE SE DÉROULE L’EXAMEN ?

L’examen se déroule en anglais.

DOIS-JE AVOIR UNE BONNE CONNEXION INTERNET ?

Oui, car votre ordinateur doit supporter pendant 24h un flux TeamViewer tout en attaquant en permanence des machines.

DOIS-JE POSSÉDER UNE WEBCAM ?

Oui, votre webcam doit être active durant la totalité de votre examen, elle doit pouvoir filmer toute votre pièce.

Quelle est la différence entre Offensive Security et OffSec ?

Depuis mars 2023, l'entité Offensive Security s'est renommée en OffSec. Il s'agit du même organisme.

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.