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

Mis à jour le 19/04/2024

S'inscrire

Formation Certification OSED™

ALL-IN-ONE : EXAMEN INCLUS AU TARIF AVEC LE COURS EXP-301

3 jours (21 heures)

PRÉSENTATION

Apprendre le développement d'exploits en mode utilisateur Windows est possible avec notre formation à la préparation OSED™ pour vous enseigner les bases du développement d'exploits moderne.

Pendant notre formation OSED™, vous effectuerez des attaques basiques par débordement de mémoire tampon pour contourner les mesures d'atténuation de sécurité critiques qui protège les entreprises. Un excellent moyen pour prévenir des failles présentes dans un système informatique.

Vous serez mis à l'épreuve pour écrire un shellcode Windows à la main. De plus, vous devrez également concevoir des exploits personnalisés.

Vous devrez apprendre l'ensemble des fondamentaux de la rétro-ingénierie pour que vous soyez en capacité d'adapter les anciennes techniques aux versions plus modernes de Windows.

Après avoir effectué notre préparation, vous pourrez prétendre au passage de la certification OSED™.

OBJECTIFS

- Développer les compétences nécessaires pour savoir contourner les mesures d'atténuation de sécurité
- Écrire votre propre shellcode
- Savoir utiliser WinDbg
- Apprendre les fondamentaux de la rétro-ingénierie
- Obtenir la certification OffSec Exploit Developer (OSED)

PUBLIC VISÉ

- Testeurs d'intrusion Web
- Chercheurs en sécurité
- Développeurs
- Analystes

Pré-requis

- Familiarité avec les débogueurs (ImmunityDBG, OllyDBG)
- Familiarité avec les concepts d'exploitation de base sur 32 bits
- Familiarité avec l'écriture de code Python 3
- Capacité à lire et à comprendre le code C à un niveau de base
- Capacité à lire et à comprendre le code Assembly 32 bits à un niveau de base

Pré-requis logiciels

- **Kali Linux** --> Téléchargeable ici

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

PROGRAMME DE NOTRE FORMATION CERTIFICATION OSED™

Développement d'exploit en mode utilisateur

- À propos du cours EXP-301
- Découvrir les stratégies générales pour aborder EXP-301
- Définition des détails de l'examen
- Récapitulation

WinDbg et l'architecture x86

- Introduction à l'architecture x86
- Introduction au débogueur Windows
- Accéder à la mémoire et la manipuler à partir de WinDbg
- Contrôler l'exécution du programme dans WinDbg
- Fonctionnalités supplémentaires

Exploitation des débordements de pile

- Introduction aux débordements de pile
- Installation de l'application Sync Breeze Crash
- Plantage de l'application Sync Breeze Crash
- Exploitation d'un débordement de tampon Win32

Exploitation des débordements SEH

- Plantage du Sync Breeze
- Analyse du plantage dans WinDbg
- Introduction à la gestion des exceptionns structurées
- Débordements de gestionnaire d'exceptions structurées

Introduction à IDA Pro

- IDA Pro 101
- Travailler avec IDA Pro Wrapp

Surmonter les restrictions d'espaces : Egghunters

- Plantage du serveur web
- Analyser le plantage dans WinDbg
- Détecter les mauvais caractères
- Obtenir l'exécution du code
- Stocker de grands tampons
- Trouver votre tampon : Approche Egghunters
- Améliorer la portabilité d'Egghunter
- Améliorer SEH

Créer un Shellcode personnalisé

- Conventions d'appel sur x86
- Problème de l'appel système
- Trouver kernel32.dll
- Résoudre les symboles
- NULLFree Position-Independent Shellcode (PIC)
- Reverse Shell

Rétro-ingénierie des bogues

- Installation et énumération
- Interaction avec Tivoli Storage Manager
- Rétro-ingénierie du protocole
- Trouver davantage de bogues

Dépassements de pile et contournement de la DEP

- Prévention de l'exécution des données
- Programmation orientée retour
- Sélection de gadgets
- Contournement de la DEP

Dépassements de pile et contournement de l'ASLR

- Introduction à l'ASLR
- Recherche de joyaux cachés
- Développement de notre exploit
- Contournement de l'ASLR
- Contournement de DEP avec WriteProcessMemory

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.