+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 OSEE™ (EXP-401)

ALL-IN-ONE : EXAMEN INCLUS AU TARIF AVEC LE COURS EXP-401

5 jours (35 heures)

PRÉSENTATION

La certification Offensive Security Exploitation Expert (OSEE) est un jalon crucial pour démontrer votre expertise en matière d'exploitation offensive et de sécurité des systèmes.

Elle témoigne de votre capacité à identifier, exploiter et sécuriser les vulnérabilités dans les systèmes informatiques, ainsi qu'à développer des exploits efficaces pour les failles découvertes.

L'examen OSEE™ comporte plusieurs modules couvrant un large éventail de sujets, y compris :

- La création de shellcode personnalisé
- L'évasion d'hôte-à-invité VMware Workstation
- L'exploitation avancée des systèmes Windows
- L'analyse des cas de confusion de type dans les navigateurs
- L'écrasement de rappels de pilotes

Chaque module met à l'épreuve vos connaissances et compétences dans des domaines spécifiques de l'exploitation offensive et de la sécurité des systèmes.

Notre formation OSEE™ offre une préparation exhaustive à l'examen, en fournissant un contenu pédagogique approfondi et des exercices pratiques pour renforcer votre compréhension des concepts.

Nous couvrons chaque aspect du programme de certification, en mettant l'accent sur les compétences pratiques et les meilleures pratiques de l'industrie.

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

OBJECTIFS

- Maîtriser la création de shellcode personnalisé pour diverses architectures
- Acquérir les compétences nécessaires pour échapper aux mécanismes de sécurité de VMware Workstation
- Développer des techniques avancées d'exploitation des systèmes Windows
- Comprendre et exploiter les vulnérabilités de confusion de type dans les navigateurs
- Pratiquer l'écrasement de rappels de pilotes pour l'escalade de privilèges

PUBLIC VISÉ

- Pentesters
- Chercheurs en sécurité
- Analysts SOC

Pré-requis

- Expérience préalable dans le domaine de l'exploitation offensive ou de la sécurité des systèmes
- Connaissances avancées des systèmes d'exploitation Windows et Linux
- Familiarité avec les outils de sécurité informatique courants
- Compréhension des concepts de base de la rétro-ingénierie et de l'analyse de logiciels malveillants

Pré-requis techniques

- **Kali Linux** --> Téléchargeable ici
- Un ordinateur capable de faire fonctionner trois machines virtuelles avec facilité
- VMware Workstation 15 ou supérieur
- Processeur 64 bits avec un minimum de 4 cœurs et prise en charge de NX, SMEP, VT-d/IOMMU et VT-x/EPT
- Au moins 160 Go de disque dur disponible
- Au moins 16 Go de RAM
- Le seul système d'exploitation hôte pris en charge est Windows 10

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

PROGRAMME DE NOTRE FORMATION CERTIFICATION OSEE™

Introduction

- Introduction générale au cours
- Contexte et importance de la création de shellcode personnalisé
- Aperçu des techniques d'exploitation et des vulnérabilités abordées
- Résumé des compétences préalables nécessaires
- Présentation du programme de la formation
- Objectifs d'apprentissage
- Méthodologie de la formation

Custom Shellcode Creation

- Architecture 64 bits et ses améliorations en matière de mémoire
- Conventions d'appel et utilisation des APIs Win32
- Écriture de code d'exploitation avancé
- Techniques de création de shellcode indépendant de la position
- Utilisation de Visual Studio pour le développement d'exploits
- Création d'un framework de shellcode
- Étude de cas : Reverse Shell

VMware Workstation Guest-To-Host Escape

- Classes de vulnérabilités et introduction à la prévention de l'exécution des données (DEP)
- Techniques avancées d'exploitation :
  - Ret2Lib
  - ROP
  - Localisation des Gadgets
- Stratégies de randomisation de l'espace d'adressage (ASLR)
- Compréhension des mécanismes internes de VMware Workstation
- Cas d'étude : Vulnérabilité UaF dans VMware Workstation
- Analyse des cas d'étude de la vulnérabilité UaF
- Contournement des protections de sécurité avancées

Advanced Windows Exploitation

- Fonctionnement interne du gestionnaire de mémoire du tas de Windows
- Cas d'étude : Déclenchement et analyse approfondie des vulnérabilités UaF
- Techniques avancées d'exploitation : Contournement de l'ASLR et du DEP
- Analyse des cas d'étude de la vulnérabilité UaF
- Stratégies pour restaurer le flux d'exécution après une exploitation réussie
- Utilisation et exécution de shellcode dans des environnements Windows
- Évaluation des protections de sécurité avancées fournies par Windows Defender Exploit Guard (WDEG)

Microsoft Edge Type Confusion

- Analyse des mécanismes internes du navigateur Microsoft Edge
- Cas d'étude : Exploitation de la confusion de types
- Techniques avancées d'exploitation : Contournement de CFG et ACG

- Analyse des cas d'étude de la vulnérabilité de type Confusion
- Exploitation des appels de procédure distante (RPC) et des analyses de tampons
- Contournement des protections de sécurité dans un environnement de navigateur sandboxé
- Révision des techniques pour rendre les exploits indépendants de la version

Driver Callback Overwrite

- Introduction au noyau Windows et aux niveaux de privilège
- Techniques de débogage en mode noyau sur Windows
- Interaction avec le noyau Windows à travers les appels système natifs et les pilotes de périphérique
- Analyse des vulnérabilités et techniques d'exploitation en mode noyau
- Exploitation des callbacks de pilote et contrôle du flux d'exécution
- Méthodes pour atteindre l'indépendance par rapport à la version du système d'exploitation
- Conclusion et révision des compétences acquises

Unsanitized User-mode Callback

- Création d'applications Windows de bureau et gestion de la mémoire du pool noyau
- Analyse des objets TagWND et des callbacks en mode utilisateur
- Techniques d'exploitation avancées : Écrasement de mémoire arbitraire et escalade des privilèges
- Analyse des cas d'étude de l'exploitation des callbacks en mode utilisateur
- Exploitation des primitives de lecture et d'écriture dans le noyau
- Techniques pour restaurer le flux d'exécution après une exploitation réussie
- Méthodes pour rendre les exploits indépendants de la version

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.