Sécurité Technique

Préparation Offensive Security Exploit Developer (OSED)

Vous allez apprendre à

La préparation à la certification Offensive Security Exploit Developer (OSED) vous permettra de développer des compétences avancées en création et développement d'exploits ciblés sur des vulnérabilités système et logiciels. Vous apprendrez à analyser en profondeur des programmes vulnérables, comprendre les mécanismes de protection modernes (comme l'ASLR, DEP, et les sandboxing), et contourner ces défenses pour écrire des exploits fiables et efficaces. Cette formation vous enseignera aussi les techniques d'ingénierie inverse, le débogage avancé et la manipulation de la mémoire, vous préparant à concevoir des attaques sophistiquées et à renforcer vos capacités en sécurité offensive à un niveau expert.

Public visé

- Professionnels de la cybersécurité souhaitant approfondir leurs compétences en développement d'exploits.
- Pentesters expérimentés désirant se spécialiser dans l'exploitation de vulnérabilités binaires.
- Chercheurs en sécurité et analystes de logiciels malveillants.
- Développeurs souhaitant comprendre les techniques d'exploitation pour renforcer la sécurité de leurs applications.

Les objectifs de la formation

- Maîtriser le développement d'exploits Windows en mode utilisateur sur architecture x86.
- Contourner les mécanismes de sécurité modernes tels que DEP et ASLR.
- Développer des chaînes ROP personnalisées et écrire du shellcode sur mesure.
- Appliquer des techniques avancées de reverse engineering pour identifier des vulnérabilités.
- Préparer et réussir l'examen de certification OSED.

Les prérequis de la formation

- Familiarité avec les débogueurs tels que WinDbg, ImmunityDBG ou OllyDBG.
- Connaissances de base en exploitation sur architecture 32 bits.
- Compétences en programmation, notamment en Python 3.

Programme de la formation

- **Introduction à WinDbg**
  - Présentation de l'interface et des commandes essentielles.
  - Techniques de débogage avancées.
- **Débordements de tampon (Stack Buffer Overflows)**
  - Compréhension des vulnérabilités de débordement de tampon.
  - Techniques d'exploitation et de contournement des protections.
- **Exploitation des SEH Overflows**
  - Mécanismes de gestion des exceptions structurées sous Windows.
  - Méthodes d'exploitation des vulnérabilités SEH.
- **Introduction à IDA Pro (version gratuite)**
  - Utilisation d'IDA Free pour l'analyse statique de binaires.
  - Techniques de reverse engineering pour identifier des vulnérabilités.
- **Contournement des restrictions d'espace : Egghunters**
  - Création et utilisation d'egghunters pour localiser du shellcode en mémoire.
  - Techniques d'injection dans des espaces mémoire restreints.
- **Création de shellcode personnalisé**
  - Écriture de shellcode en assembleur.
  - Encodage et obfuscation pour échapper aux mécanismes de détection.
- **Reverse engineering de bugs**
  - Identification de vulnérabilités via l'analyse statique et dynamique.
  - Utilisation combinée de WinDbg et IDA Free pour l'analyse approfondie.
- **Bypass des protections DEP/ASLR avec des chaînes ROP**
  - Création de chaînes ROP pour contourner les protections mémoire.
  - Techniques avancées de manipulation de la pile.
- **Attaques de type format string**
  - Compréhension des vulnérabilités liées aux spécificateurs de format.
  - Méthodes d'exploitation pour lecture et écriture arbitraires en mémoire.