BOOTCAMP EXPLOITATION DE VULNÉRABILITÉS APPLICATIVES

Maîtrisez l'ensemble des techniques d'exploitation applicatives

Ce bootcamp fait le tour des vulnérabilités applicatives et des techniques d'exploitation sur Windows et Linux, de la conception de shellcodes sur mesure pour architectures 32 et 64 bits à l'exploitation de vulnérabilités de type «use after free», combinée à du «Return Oriented Programming» (ROP).
Il s'agit d'une formation pratique avec des exploitations sur des applications d'apprentissage et des programmes réels.

Code : BEVA

PROGRAMME

Méthodes mobilisées : Cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : Les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur.

JOUR 1

Shellcoding Linux, première partie (32 bits)
- Environnement de conception de shellcodes
- Shellcode standard
- Reverse shell TCP
- Bind shell TCP

Buffer overflow sous Linux (IA-32)
- Exploitation sans protection
- Exploitation avec ASLR
- Exploitation avec NX
- Exploitation avec ASLR et NX (ROP)
- Exploitation sur IA-64 (64 bits)

JOUR 2

Shellcoding Linux, deuxième partie
- Shellcoding multi-staged
- Shellcoding 64 bits
- Shellcode standard 64 bits
- Reverse shell 64 bits

Shellcoding sous Windows
- Environnement de conception de shellcodes
- Technique de shellcoding générique

JOUR 3

Shellcoding sous Windows (suite)
- Shellcode MessageBox
- Shellcode Execute

Buffer overflow sous Windows
- Exploitation sans protection
- Contournement du stack canary (/GS)
- Contournement de la protection SafeSEH
- Contournement du DEP

JOUR 4

Format String
- Présentation
- Exploitation sous Windows
- Exploitation sous Linux
- Contre-mesures actuelles

JOUR 5

Vulnérabilités liées à la mémoire dynamique
- Présentation
- Débordement mémoire dans le tas
- Heap Spray
- Use After Free

PROCHAINES DATES

30 janvier 2023,
27 mars 2023,
5 juin 2023,
16 octobre 2023,
27 novembre 2023

OBJECTIFS

- Apprendre à écrire des shellcodes sur architecture IA 32
- Présenter et exploiter des débordements de tampon (buffer overflow) sous Linux sur architecture IA 32
- Présenter et exploiter des débordements de tampon (buffer overflow) sous Linux sur architecture IA 64
- Apprendre à écrire des shellcodes sous Linux sur architecture IA 64
- Apprendre à écrire des shellcodes sous Windows sur architecture IA 32
- Présenter et exploiter des débordements de tampon (buffer overflow) sous Windows sur architecture IA 32 sans protections
- Présenter et exploiter des débordements de tampon (buffer overflow) sur Windows sous architecture IA 32 avec protection SafeSEH
- Présenter et exploiter des débordements de tampon (buffer overflow) sur Windows sous architecture IA 32 avec protection DEP
- Présenter et exploiter des débordements de tampon (buffer overflow) sur Windows sous architecture IA 32 avec toutes les protections
- Comprendre et exploiter des vulnérabilités de type format string
- Comprendre le fonctionnement de la heap
- Comprendre et exploiter les heap overflows avec la protection NX

INFORMATIONS GÉNÉRALES

Code : BEVA
Durée : 5 jours
Prix : 3 610 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)

PUBLIC VISÉ

- Pentesters

PRÉ-REQUIS

- Avoir des notions de sécurité informatique
- Maîtriser des systèmes Windows et Linux
- Avoir des connaissances en architectures IA 32 et IA 64
- Avoir des bonnes connaissances en C, en Python et assembleur

RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne / Internet