

Objectifs

- ▶ Connaître les vulnérabilités dues à la programmation
- ▶ Savoir comment elles peuvent être exploitées
- ▶ Connaître l'impact de ces vulnérabilités
- ▶ Savoir comment éviter d'introduire ce type de faille dans ses développements propriétaires

Des travaux pratiques seront effectués tout au long de la formation sur des systèmes Windows.

Pré-requis

- ▶ Connaissance du fonctionnement des systèmes d'exploitation (en particulier Windows)
- ▶ Connaissance du langage C
- ▶ Connaissance du langage assembleur

Contenu

- ▶ Windows stack overflow - Basic
- ▶ Windows stack overflow - Advanced
- ▶ Windows Heap Overflow

Programme détaillé au dos.

Informations pratiques

- ▶ Participants : un maximum de 10 inscrits
- ▶ Formateur : expert sécurité/R&D
- ▶ Matériel : poste individuel, mêmes systèmes et outils que le formateur
- ▶ Locaux : 75 avenue Victor Hugo 92 500 Rueil-Malmaison
5 minutes à pieds du RER Rueil-Malmaison (sortie 5 Victor Hugo)
(Parking disponible sur simple demande)

Durée : 3 jours

Code : EVW

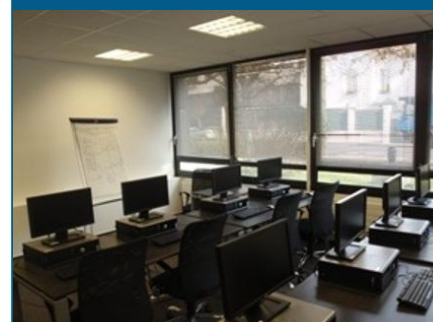
Prix : 2 400 € HT

Catalogue :

www.atlab.fr/formations.html

Inscription :

contact@atlab.fr
Tél : 01 47 08 88 00



Jour 1 : Windows stack overflow - Basic

Présentation des stack overflows	Structure de la pile Erreurs de programmation
Utilisation d'un debugger pour la création d'exploit	Présentation des processus Windows sous OllyDbg
Travaux pratiques	
Construction de stack overflows à l'aide d'un framework (metasploit)	Création du Stack Overflow Découverte automatique de l'adresse de retour Recherche de valeurs fiables
Travaux Pratiques	
Payload windows génériques	

Jour 2 : Windows Stack Overflow - Advanced

Contournement du /gs version 1 (xp sp1)	Présentation Contournement
Travaux Pratiques	
Contournement du /gs version 2 (xp sp2 - 2003 sp1)	Présentation Contournement
Travaux pratiques	
Contournement du /safeseh	Présentation Contournement sous 2003 SP0 Contournement sous 2003 SP1-SP2 à aujourd'hui
Travaux pratiques	
Contournement du hardware dep / nx	Présentation Contournement sous XP SP2 / 2003 SP1-SP2 à aujourd'hui
Travaux pratiques	

Jour 3 : Windows Heap Overflow

Exploitation des heap overflows sous Windows 2000	Présentation du Heap sous Windows Techniques d'exploitation
Travaux pratiques	
Protection du heap sous Windows xp/2003	Présentation Cas exploitables
Travaux pratiques	

Bonus : Format string sous Windows