Exploitation Avancée avec Metasploit

Formation Informatique / Réseaux et Sécurité /

Cette formation va vous plonger au cœur de Metasploit et de ses différents composants. Vous apprendrez à utiliser toutes les fonctionnalités avancées offertes par ce framework, des outils fournis par la bibliothèque Rex aux outils comme Meterpreter ou Railgun. Vous apprendrez aussi à créer une extension Meterpreter, automatiser des actions via des scripts pour Railgun, comprendre les différents modes de communication supportés par Metasploit. Vous découvrirez aussi les possibilités offertes par Metasploit pour la production d'encodeurs et de payloads polymorphiques. Cette formation est principalement destinée aux auditeurs techniques souhaitant approfondir leurs connaissances sur Metasploit et ses composants, afin d'utiliser pleinement tous les rouages internes de ce formidable outil.

OBJECTIFS

- Exploiter toutes les capacités du framework Metasploit
- Créer différentes sortes de modules pour Metasploit (encodeurs, exploits, auxiliaires...)
- Comprendre le fonctionnement de Rex
- Concevoir des extensions Meterpreter

PUBLIC

- Auditeurs techniques expérimentés

PRE-REQUIS

- Maîtrise du langage assembleur
- Maîtrise des langages C et C++
- Bonne connaissance des environnements Linux et Windows
- Maîtrise de l'utilisation conventionnelle de Metasploit
- Notions de développement de shellcode

PROGRAMME

Jour 1

Présentation du cadriciel Metasploit

Personnalisation

Metasploit et Docker

Utilisation avancée de Metasploit

- Utilisation des options avancées des modules et de meterpreter
- Contournement d'anti-virus

SEtoolkit et Metasploit

Jour 2

Reconnaissance avec Metasploit

- Utilisation des scanners
- Création d'un module de scan

Techniques d'exploitation

- Exploitation d'un poste utilisateur
- Exploitation d'un service
- Prise de contrôle d'un domaine
- Techniques de pivoting

Développement de module

- Développement d'un module d'exploitation
- Développement d'un module de fuzzing

Jour 3

Bibliothèque Rex

A retenir

Durée : **4 jours** soit 28h.
Réf. **EAM**

01 42 93 52 72

Dates des sessions

Paris
11/07/2018
26/11/2018

Cette formation est également proposée en formule INTRA-ENTREPRISE.

Inclus dans cette formation

Coaching Après-COURS

Pendant 30 jours, votre formateur sera disponible pour vous aider. CERTyou s'engage dans la réalisation de vos objectifs.

100% SATISFACTION GARANTIE

Votre garantie 100% SATISFACTION

Notre engagement 100% satisfaction vous garantit la plus grande qualité de formation.

- Présentation, Fonctionnalités
- Assemblage dynamique
- Encodage
- Logging
- Support de protocoles variés
- Développement avec Rex : exploit, payload, auxiliary

Développement de script meterpreter

- Architecture logicielle meterpreter
- Interaction avec Metasploit
- Railgun
- Développement de plugins (ruby)

Jour 4

Développement de payloads

- Rappel assembleur
- Structure d'un module de payload
- Création d'un shellcode sur mesure
- Intégration dans un module Metasploit

Créer son propre encodeur

Développement et intégration d'un nouvel encodeur

Horaires, Planning et Déroulement de cette formation

Horaires

• Formation de 9h00 (9h30 le premier jour) à 17h30.
• Deux pauses de 15 minutes le matin et l'après-midi.
• 1 heure de pause déjeuner

DEROULEMENT

• Les horaires de fin de journée sont adaptés en fonction des horaires des trains ou des avions des différents participants.
• Une attestation de suivi de formation vous sera remise en fin de formation.
• Cette formation est organisée pour un maximum de 14 participants.

PROCHAINES FORMATIONS

Réussir la Certification Gestion de Projet PMP du PMI
Réussir la Certification PRINCE2 Foundation
Réussir les Certifications PRINCE2 Foundation et PRINCE2 Practitioner
Réussir la Certification ITIL Foundation
Réussir la Certification Agile certifié SCRUM Master
Réussir les Certifications TOGAF Certified et TOGAF Foundation

Retrouvez cette formation sur notre site :
Exploitation Avancée avec Metasploit