Introduction

Imaginez que dans quelque temps, dans un futur pas si lointain, un attaquant décide d'attaquer les biens digitaux d'une multinationale, ciblant des droits de propriété intellectuelle de plusieurs centaines de milliers de dollars, enfouis dans une infrastructure de plusieurs millions de dollars. Naturellement, l'attaquant commence par lancer la dernière version de Metasploit. Après avoir exploré le périmètre de la cible, il trouve un point faible et commence une série méthodique d'attaques, mais même après avoir compromis près de tous les aspects du réseau, le jeu ne fait que commencer. Il manoeuvre à travers les systèmes, identifiant les composants centraux et cruciaux de l'entreprise qui lui permettent de vivre. Avec une seule touche, il peut s'emparer de millions de dollars de l'entreprise, et compromettre toutes leurs données sensibles. Bienvenue dans le monde des pentests et le futur de la sécurité.

Pourquoi faire un pentest ?

Les entreprises investissent des millions de dollars dans des programmes de sécurité pour protéger des infrastructures critiques, identifier les fentes dans l'armure et prévenir d'importantes fuites de données. Un pentest est un des moyens les plus efficaces pour identifier les faiblesses systémiques et les déficiences dans ces programmes. En tentant de contourner les contrôles de sécurité et d'esquiver les mécanismes de sécurité, un pentesteur est capable d'identifier les voies par lesquelles un pirate pourrait compromettre la sécurité d'une entreprise et l'endommager dans son ensemble.

En lisant ce livre, souvenez-vous que vous ne ciblez pas nécessairement un ou plusieurs systèmes. Votre but est de montrer, de manière sûre et contrôlée, comment un attaquant pourrait causer de sérieux dégâts dans l'entreprise et impacter sa capacité, entre autres choses, à générer des revenus, maintenir sa réputation et protéger ses clients.

Pourquoi Metasploit ?

Metasploit n'est pas qu'un outil. C'est tout un cadre qui fournit l'infrastructure nécessaire pour automatiser les tâches mondaines, routinières ou complexes. Cela vous permet de vous concentrer sur les aspects uniques ou spéciaux d'un pentest, et d'identifier les failles dans vos programmes de sécurité.

En progressant dans les chapitres de ce livre, grâce à une méthodologie bien huilée, vous commencerez à voir les nombreuses façons dont Metasploit peut être utilisé

lors de vos pentests. Metasploit vous permet de bâtir facilement des vecteurs d'attaques pour améliorer ses exploits, payloads, encodeurs et bien plus afin de créer et exécuter des attaques plus avancées. Dans ce livre, nous présentons des outils tiers – dont certains ont été écrits pas les auteurs de ce livre – qui se servent de Metasploit comme base. Notre but est de vous rendre accessible le framework, vous montrer des attaques avancées et s'assurer que vous pouvez appliquer ces techniques de façon responsable. Nous espérons que vous prendrez plaisir à lire ce livre autant que nous avons eu plaisir de le créer. Que les jeux et la joie commencent !

Un bref historique de Metasploit.

Metasploit a d'abord été conçu et développé par HD Moore alors qu'il travaillait pour une entreprise de sécurité. Quand HD a réalisé qu'il passait le plus clair de son temps à valider et assainir des codes d'exploits publics, il a commencé à créer un cadre flexible et facile de maintien pour la création et le développement d'exploits. Il publia sa première version de Metasploit écrite en Perl en octobre 2003, avec un total de 11 exploits.

Avec l'aide de Spoonm, HD a publié un projet totalement réécrit, Metasploit 2.0, en avril 2004. Cette version incluait 19 exploits et plus de 27 payloads. Peu après cette publication, Matt Miller (Skape) a rejoint l'équipe de développement de Metasploit, et alors que le projet gagnait en popularité, Metasploit Framework a reçu un fort soutien de la communauté de la sécurité de l'information et est vite devenu un outil nécessaire pour le pentest et l'exploitation.

Suivant une réécriture complète en langage Ruby, l'équipe Metasploit publia Metasploit 3.0 en 2007. La migration de Perl vers Ruby prit 18 mois et ajouta plus de 150 000 lignes de nouveau code. Avec la sortie de 3.0, Metasploit a été massivement adopté par la communauté de la sécurité, et a vu grandir le nombre de ses contributions utilisateur.

À l'automne 2009, Metasploit a été racheté par Rapid7, un leader dans le domaine du scan de vulnérabilité, ce qui a permis à HD de créer une équipe pour se concentrer uniquement sur le développement de Metasploit Framework. Depuis l'acquisition, les mises à jour sont faites plus rapidement que quiconque n'aurait pu l'imaginer. Rapid7 a publié deux produits commerciaux basés sur Metasploit Framework : Metasploit Express et Metasploit Pro. Metasploit Express est une version plus légère de Metasploit Framework, avec une GUI et des fonctionnalités supplémentaires, incluant notamment la rédaction de rapports, entre autres fonctions utiles. Metasploit Pro est une version élargie de Metasploit Express, qui peut se vanter de faire de la collaboration, de l'intrusion en groupe et d'encore bien d'autres fonctionnalités, quelque chose d'aussi simple qu'un clic grâce, entre autres, à un tunnel VPN (réseau privé virtuel).