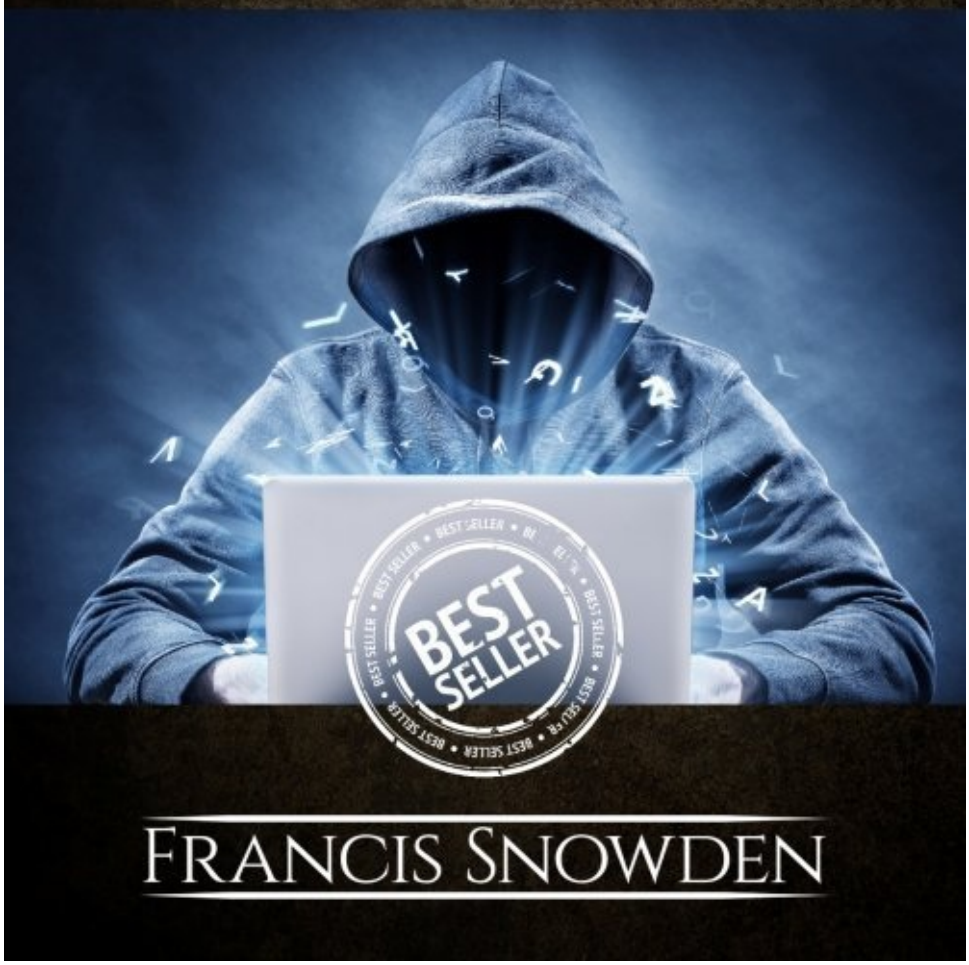
PIRATAGE INFORMATIQUE

LE PIRATAGE INFORMATIQUE POUR LES DÉBUTANTS

FRANCIS SNOWDEN

PIRATAGE INFORMATIQUE

LE PIRATAGE INFORMATIQUE POUR LES DÉBUTANTS



FRANCIS SNOWDEN

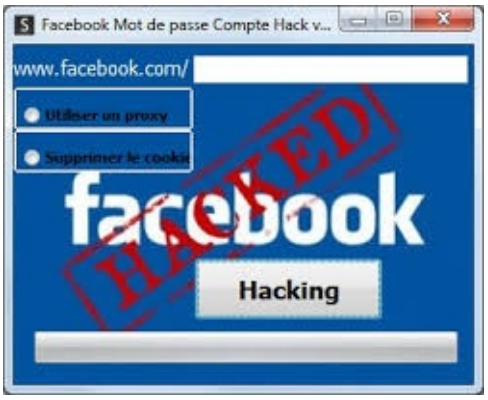
Introduction

Je veux vous remercier et vous féliciter d’avoir télécharger ce livre!

Tout ce que vous devez savoir sur le piratage informatique est dans ce livre.

Francis Snowden

Technique #1 : ***Hacker les mots de passe***



Les mots de passe sont les portes d'un système d'information. Y entrer par effraction est le b.a.-ba du piratage informatique.

Un mot de passe robuste est composé de lettres en majuscule et en minuscule, de chiffres et de caractères spéciaux. Il doit avoir au minimum 8 caractères. Mémorisez-le au lieu de le noter. Changez-le régulièrement. Malgré ces conseils, la majorité des utilisateurs ne respectent pas cette structure. Ils mettent ainsi leur système informatique à la portée des pirates.

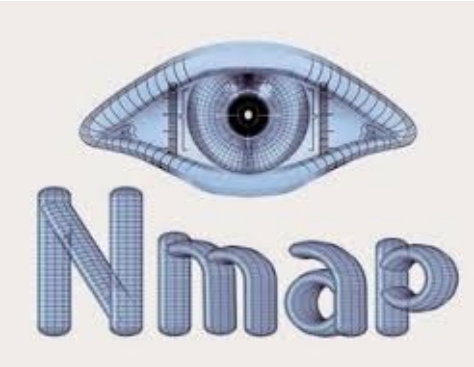
Pour ce faire, les pirates utilisent un logiciel spécial. « L0phtCrack », « John the ripper » font partie des plus connus dans la matière. L'application va tenter de découvrir LA combinaison identifiant et mot de passe. Ces programmes utilisent 3 méthodes. L'attaque brute-force essaie toutes les combinaisons possibles. L'attaque à partir d'un dictionnaire ou d'une liste est restreinte aux mots usuels : prénoms, ville… L'attaque hybride se focalise sur les combinaisons à priori renforcées.

Hacker une connexion Wi-Fi revient à trouver sa clé de protection. Le processus est similaire que pour les comptes utilisateurs. Les manipulations sont accessibles pour les curieux non débutants. Des mots clés pertinents dans le moteur de recherche Google permettent d'avoir un tutoriel complet sur le sujet.

Au sein d'une entreprise, les administrateurs techniques s'en servent pour tester

« l’étanchéité » des comptes des employés.

Technique #2 : ***Scanner les ports ouverts***

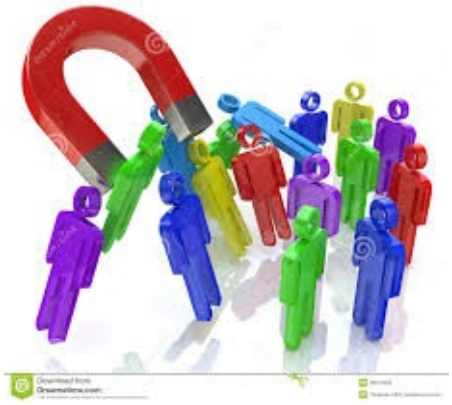


Les ordinateurs d'un réseau informatique communiquent entre eux à l'aide des ports. Les connexions internet circulent aussi par ces mêmes ports. Un réseau est protégé par un pare-feu. Cette barrière limite le fonctionnement de certains programmes. Certains ports sont laissés ouverts.

Les pirates traquent ces passages à l'aide d'outils. Ils sont communément connus sous l'appellation « scanner ». L'objectif est d'identifier le système d'exploitation. Une fois découvert, le hacker y entre et exploite ses failles. Tel un fantôme, un expert ne laissera aucune trace. Il créera une porte dérobée sur votre réseau pour y revenir sans encombre.

Pour vous prémunir de ce genre d'attaque, vous devez surveiller régulièrement vos ports ouverts. Fermez ceux qui sont inutiles. Mettez à jour votre système d'exploitation périodiquement. Pour vous faciliter la vie, utiliser un progiciel détecteur ou prévention d'intrusion. Automatisez le processus.

Technique # 3 : ***Ruser avec l'ingénierie sociale***



Cette méthode exploite les faiblesses humaines pour extraire des informations confidentielles d'une société. Il ne faut pas être un spécialiste pour parvenir à ses fins. Ci-après quelques techniques :

Le pirate usurpe l'identité d'un manager d'une entreprise. Il appelle ensuite la réception et use de son autorité pour obtenir des informations importantes. Dans la même optique, il vole le nom d'un personnel du département informatique pour recevoir votre identifiant et votre mot de passe.

Les malins enverront un mail accompagné d'une pièce jointe ou d'un lien infecté. Ouvrir le document ou cliquer le lien donne la voie au hacker.

Les spécialistes dupliquent des sites internet. S'ils ne font pas attention, les internautes tombent dans le panneau.

En être informé est la première arme contre cette escroquerie.

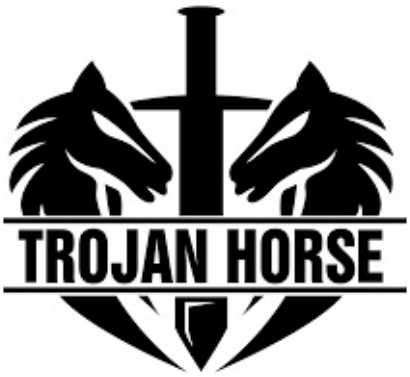
Technique # 4 : ***Exploiter la vulnérabilité des systèmes et des logiciels***

Les programmes et les systèmes d’exploitation ne sont pas parfaits. Les mises à jour existent pour améliorer leur protection.

Metasploit fait partie des progiciels qui détectent ces faiblesses. Il a la capacité de s’immiscer dans des programmes célèbres installés sur votre ordinateur : Adobe Reader, Java…

Maintenez à jour votre panoplie de logiciels et votre système d’exploitation pour s’en protéger. Assurez-vous que vous êtes bien sur le site officiel.

Technique # 5 : ***Pénétrer à l’aide d’un troyen***

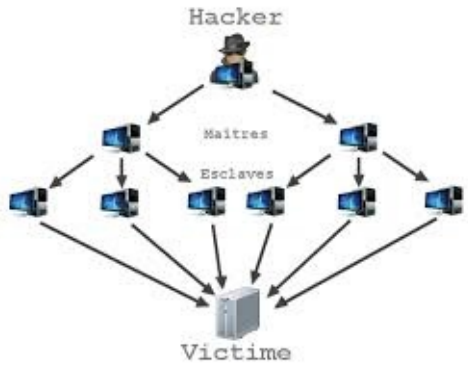


Un troyen (trojan) est un programme malicieux. Il a une apparence attrayante, mais s’avère destructif une fois exécuté. Ses actions se prolifèrent en silence dans votre système.

Les trojans sont véhiculés par des pièces jointes de mails, des plug-ins de navigateurs, des progiciels illégaux… Une fois activé, le pirate peut manipuler vos données à sa guise.

Pour s’en prémunir, privilégiez le téléchargement des programmes légaux. Vaut mieux débourser de l’argent pour se protéger. Vérifiez le contenu des mails des inconnus suspects avant d’accéder aux pièces jointes.

Technique # 6 : ***Bloquer les serveurs***



La technique du « Déni de Service » a pour objectif d’obstruer les serveurs cibles.

Le pirate envoie des requêtes en quantité et de manière continue au serveur, jusqu’à ce que celui-ci sature. La cible finit par ne pas fonctionner.

Pour prévenir ce genre d’invasion, renforcez le paramétrage des serveurs.

Conclusion

Cliquez ICI pour recevoir tout le contenue sur ce sujet dont vous avez toujours rêvé, et ce, gratuitement.

Merci d’avoir téléchargé ce livre!