GUIDE POUR LES DÉBUTANTS EN MATIÈRE DE PIRATAGE INFORMATIQUE

COMMENT PIRATER UN RÉSEAU SANS FIL, SÉCURITÉ DE BASE ET TEST DE PÉNÉTRATION, KALI LINUX, VOTRE PREMIER PIRATAGE

ALAN T. NORMAN

Alan T. Norman

Guide Pour Les Débutants En Matière De Piratage Informatique

Аннотация

Ce livre vous apprendra comment vous protéger contre les attaques de piratage les plus courantes en sachant comment le piratage fonctionne réellement! Après tout, afin d'éviter que votre système ne soit compromis, vous devez garder une longueur d'avance sur tout pirate informatique. Vous pouvez le faire en apprenant comment pirater et comment faire un contre-hack.

Ce livre vous apprendra comment vous protéger contre les attaques de piratage les plus courantes en sachant comment le piratage fonctionne réellement!

Après tout, afin d'éviter que votre système ne soit compromis, vous devez garder une longueur d'avance sur tout pirate informatique.

Vous pouvez le faire en apprenant comment pirater et comment faire un contre-hack.

Dans ce livre sont des techniques et des outils qui sont utilisés par les pirates informatiques et éthiques - toutes les choses que vous trouverez ici vous montreront comment la sécurité des informations peut être compromise et comment vous pouvez identifier une attaque dans un système que vous essayez de protéger .

Dans le même temps, vous apprendrez également comment minimiser tout dommage dans votre système ou arrêter une attaque en cours.

Avec Hacking: Computer Hacking Beginners Guide…, vous apprendrez tout ce que vous devez savoir pour entrer dans le monde secret du piratage informatique. Il fournit un aperçu complet du piratage, du cracking et de leurs effets sur le monde.

Vous en apprendrez plus sur les conditions préalables au piratage, les différents types de pirates et les nombreux types d'attaques de piratage:

Attaques actives
Attaques de mascarade
Rejouer les attaques
Modification des messages
Techniques d'usurpation
WiFi Hacking
Hacking Tools
Votre premier hack Passive Attack

Téléchargement Hacking: Computer Hacking Beginners Guide Comment pirater un réseau sans fil, des tests de sécurité et de pénétration de base, Kali Linux, votre premier hack tout de suite - Cette étonnante nouvelle édition met une richesse de connaissances à votre disposition.

Vous apprendrez comment pirater un mot de passe de messagerie, des techniques d'usurpation d'identité, le piratage WiFi et des conseils pour un piratage éthique.

Vous apprendrez même comment faire votre premier hack.

Faites défiler vers le haut et profitez instantanément de cette offre incroyable

Содержание

GUIDE POUR LES DÉBUTANTS EN MATIÈRE DE PIRATAGE INFORMATIQUE

COMMENT PIRATER UN RÉSEAU SANS FIL, SÉCURITÉ DE BASE ET TEST DE PÉNÉTRATION, KALI LINUX, VOTRE PREMIER PIRATAGE

ALAN T. NORMAN

Traducteur : Ilyasse Kourriche

Avis de non-responsabilité :

Veuillez noter que les informations contenues dans ce document ne sont pas destinées à des fins éducatives et de divertissement. Tout a été fait pour fournir des informations complètes, exactes, à jour et fiables. Aucune garantie de quelque nature que ce soit n'est exprimée ou implicite.

En lisant ce document, le lecteur accepte qu'en aucun cas

l'auteur ne soit responsable des pertes, directes ou indirectes, qui résultent de la diffusion des informations contenues dans ce document, y compris, mais sans s'y limiter, les erreurs, omissions ou inexactitudes.

Pourquoi Vous Devriez Lire Ce Livre

Comme tout autre progrès technologique dans l'histoire de l'humanité, les avantages que l'humanité a tirés de l'informatisation et de la numérisation de notre monde ont un prix. Plus nous pouvons stocker et transmettre d'informations, plus celles-ci deviennent vulnérables au vol ou à la destruction. Plus nos vies deviennent dépendantes de la technologie et de la communication rapide et instantanée, plus les conséquences de la perte d'accès à ces capacités sont importantes. Il est non seulement possible, mais en fait courant, que des milliards de dollars soient transférés à l'étranger en un clin d'œil. Des bibliothèques entières peuvent être stockées sur des appareils qui ne sont pas plus grands qu'un pouce humain. Il est courant de voir des enfants jouer à des jeux plutôt banals sur des smartphones ou des tablettes qui ont une puissance de calcul supérieure à celle de machines qui, il y a 50 ans à peine, auraient rempli des salles entières.

Cette concentration sans précédent de données et de richesses numériques, associée à la dépendance croissante de la société à l'égard des moyens de stockage et de communication numériques, a été une aubaine pour les opportunistes avisés et malveillants désireux de tirer parti de chaque vulnérabilité. Des individus commettant des petits vols et des fraudes aux activistes politiques, en passant par les cabales criminelles

importantes et très organisées, les groupes terroristes et les acteurs des États nationaux, le piratage informatique est devenu une industrie mondiale de plusieurs milliards de dollars, non seulement en ce qui concerne la commission des crimes eux-mêmes, mais aussi en ce qui concerne le temps, les efforts et les capitaux consacrés à la protection des informations et des ressources. Il est impossible d'exagérer les implications de la sécurité informatique à notre époque. L'infrastructure critique des villes et de nations entières est inextricablement liée aux réseaux informatiques. Les enregistrements des transactions financières quotidiennes sont stockés numériquement, dont le vol ou la suppression pourrait faire des ravages dans des économies entières. Les communications sensibles par courrier électronique peuvent influencer les élections politiques ou les procès lorsqu'elles sont rendues publiques.

Parmi les vulnérabilités potentielles, la plus préoccupante est peut-être celle du domaine militaire, où les instruments de guerre de plus en plus informatisés et mis en réseau doivent à tout prix être tenus à l'écart des mauvaises mains. Ces menaces très médiatisées s'accompagnent d'effets moins importants, mais cumulatifs, de transgressions à plus petite échelle comme le vol d'identité et les fuites d'informations personnelles qui ont des conséquences dévastatrices sur la vie des gens ordinaires.

Tous les pirates n'ont pas nécessairement des intentions malveillantes. Dans les pays où la liberté d'expression est entravée ou où les lois sont oppressives, les pirates informatiques

servent à diffuser des informations vitales au sein de la population qui pourraient normalement être supprimées ou aseptisées par un régime autoritaire. Bien que leur activité soit toujours illégale selon les lois de leur propre pays, beaucoup sont considérés comme servant un but moral. Les lignes éthiques sont donc souvent floues lorsqu'il s'agit de piratage à des fins d'activisme politique ou de diffusion d'informations qui pourraient être utiles au public ou aux populations opprimées. Afin de limiter les dommages qui peuvent être causés par des individus et des groupes aux intentions peu honorables, il est nécessaire de se tenir au courant des outils, des procédures et des mentalités des pirates informatiques. Les pirates informatiques sont très intelligents, ingénieux, adaptables et extrêmement persistants. Les meilleurs d'entre eux ont toujours eu, et continueront probablement à avoir, une longueur d'avance sur les efforts déployés pour les contrer. Ainsi, les spécialistes de la sécurité informatique s'efforcent de devenir tout aussi habiles et praticiens de l'art du piratage que leurs adversaires criminels. Dans le processus d'acquisition de ces connaissances, le "hacker éthique" est censé s'engager à ne pas utiliser les compétences acquises à des fins illégales ou immorales.

Ce livre est destiné à servir d'introduction au langage, au paysage, aux outils et aux procédures du piratage informatique. En tant que guide pour débutants, il suppose que le lecteur a peu de connaissances préalables sur le piratage informatique en soi, en dehors de ce à quoi il a été exposé dans les médias ou lors

de conversations informelles. Il suppose également que le lecteur est familiarisé avec la terminologie informatique moderne et l'Internet. Les instructions détaillées et les procédures de piratage spécifiques n'entrent pas dans le cadre de ce livre et sont laissées à la discrétion du lecteur, qui sera plus à l'aise avec le matériel.

Le livre commence au *chapitre 1 : Qu'est-ce que le piratage ?* avec quelques définitions de base afin que le lecteur puisse se familiariser avec une partie du langage et du jargon utilisés dans le domaine du piratage et de la sécurité informatique, ainsi que pour lever toute ambiguïté dans la terminologie. Le chapitre 1 distingue également les différents types de pirates informatiques en fonction de leurs intentions éthiques et juridiques et des ramifications de leurs activités.

Dans le *chapitre 2 : Vulnérabilités et exploits,* le concept central de vulnérabilité des cibles est introduit, décrivant les principales catégories de vulnérabilité et quelques exemples spécifiques. Cela conduit à une discussion sur la manière dont les pirates informatiques tirent parti des vulnérabilités par la pratique de l'exploitation.

Le chapitre 3 : Pour commencer passe en revue les nombreux sujets et compétences avec lesquels un hacker débutant doit se familiariser. Du matériel informatique et de réseau aux protocoles de communication, en passant par les langages de programmation informatique, les principaux domaines d'actualité de la base de connaissances d'un hacker sont décrits.

Le chapitre 4 : La boîte à outils du pirate informatique

examine le matériel, les logiciels, les systèmes d'exploitation et les langages de programmation courants que les pirates informatiques préfèrent généralement pour exercer leur métier.

Les procédures générales relatives à certaines attaques informatiques courantes sont examinées au *chapitre 5 : Obtenir l'accès, qui* fournit quelques exemples d'attaques qui intéressent souvent les pirates et les professionnels de la sécurité informatique.

Le chapitre 6 : Activités malveillantes et code révèle certaines des attaques et constructions les plus malveillantes des pirates informatiques qui visent à causer du tort. Les différences entre les différentes catégories de codes malveillants sont expliquées.

Le chapitre 7 : le piratage sans fil se concentre spécifiquement sur l'exploitation des vulnérabilités des protocoles de cryptage des réseaux Wi-Fi. Les outils matériels et logiciels spécifiques nécessaires pour exécuter des attaques Wi-Fi simples sont énumérés.

Le lecteur trouvera des conseils pratiques sur la mise en place et la pratique du piratage de niveau débutant au *chapitre 8 : Votre premier piratage.* Deux exercices sont sélectionnés pour aider l'aspirant hacker à se familiariser avec des outils simples et un équipement peu coûteux.

Le chapitre 9 : Sécurité défensive et éthique du hacker conclut cette introduction au hacking par quelques notes sur la manière de se protéger des hackers, et aborde certaines questions philosophiques associées à l'éthique du hacking.

Chapter 1. Qu'est-ce que le hacking ?

Il est important de jeter les bases d'une bonne introduction au piratage informatique en discutant d'abord de certains termes couramment utilisés et de lever toute ambiguïté quant à leur signification. Les professionnels de l'informatique et les amateurs sérieux ont tendance à utiliser beaucoup de jargon qui a évolué au fil des ans dans ce qui était traditionnellement une clique très fermée et exclusive. La signification de certains termes n'est pas toujours claire sans une compréhension du contexte dans lequel ils ont été développés. Bien qu'il ne s'agisse pas d'un lexique complet, ce chapitre présente certains des termes de base utilisés par les pirates et les professionnels de la sécurité informatique. D'autres termes apparaîtront dans les chapitres suivants, dans les domaines appropriés. Aucune de ces définitions n'est en aucune façon "officielle", mais représentent plutôt une compréhension de leur usage courant.

Ce chapitre tente également de clarifier ce qu'est le piratage en tant qu'activité, ce qu'il n'est pas et qui sont les pirates. Les représentations et les discussions sur le piratage informatique dans la culture populaire peuvent avoir tendance à brosser un tableau trop simpliste des pirates informatiques et du piratage informatique dans son ensemble. En effet, la traduction des mots à la mode et des idées fausses populaires fait perdre toute compréhension précise.

Hacking & Hackers

Le mot "piratage" évoque généralement l'image d'un cybercriminel solitaire, penché sur un ordinateur et transférant de l'argent à volonté depuis une banque sans méfiance, ou téléchargeant facilement des documents sensibles depuis une base de données gouvernementale. En anglais moderne, le terme "hacking" peut prendre plusieurs sens différents selon le contexte. D'une manière générale, le mot fait référence à l'acte d'exploitation

les vulnérabilités de la sécurité informatique pour obtenir un accès non autorisé à un système. Cependant, avec l'émergence de la cybersécurité comme industrie majeure, le piratage informatique n'est plus exclusivement une activité criminelle et est souvent réalisé par des professionnels certifiés qui ont été spécifiquement sollicités pour évaluer les vulnérabilités d'un système informatique (voir la section suivante sur le piratage "chapeau blanc", "chapeau noir" et "chapeau gris") en testant différentes méthodes de pénétration. En outre, le piratage informatique à des fins de sécurité nationale est également devenu une activité sanctionnée (qu'elle soit reconnue ou non) par de nombreux États-nations. Par conséquent, une compréhension plus large de ce terme devrait reconnaître que le piratage est souvent autorisé, même si l'intrus en question subvertit le processus normal d'accès au système.

L'utilisation encore plus large du mot "piratage" implique la modification, l'utilisation non conventionnelle ou l'accès subversif de tout objet, processus ou élément de technologie - et pas seulement des ordinateurs ou des réseaux. Par exemple, dans les premiers temps de la sous-culture des pirates informatiques, il était courant de "pirater"

des téléphones publics ou des distributeurs automatiques pour y accéder sans utiliser d'argent - et de partager les instructions pour ce faire avec la communauté des pirates informatiques dans son ensemble. Le simple fait de mettre des objets ménagers normalement mis au rebut à des fins nouvelles et innovantes (utilisation de canettes de soda vides comme porte-crayons, etc.) est souvent appelé "piratage". Même certains processus et raccourcis utiles pour la vie quotidienne, comme l'utilisation de listes de choses à faire ou la recherche de moyens créatifs pour économiser de l'argent sur des produits et services, sont souvent qualifiés de piratage informatique (souvent appelé "life hacking"). Il est également courant de rencontrer le terme "hacker" pour désigner toute personne particulièrement douée ou compétente dans l'utilisation des ordinateurs.

Ce livre se concentrera sur le concept de piratage informatique qui concerne spécifiquement l'activité consistant à accéder à des logiciels, des systèmes informatiques ou des réseaux par des moyens non intentionnels. Cela inclut les formes les plus simples d'ingénierie sociale utilisées pour déterminer les mots de passe jusqu'à l'utilisation de matériel et de logiciels sophistiqués

pour une pénétration avancée. Le terme " hacker" sera donc utilisé pour désigner toute personne, autorisée ou non, qui tente d'accéder subrepticement à un système ou à un réseau informatique, sans tenir compte de ses intentions éthiques. Le terme "cracker" est également couramment utilisé à la place de "hacker" - en particulier en référence à ceux qui tentent de casser des mots de passe, de contourner les restrictions logicielles ou de contourner la sécurité informatique de toute autre manière.

Les "Chapeaux" Du Piratage Informatique

Les scènes hollywoodiennes classiques de l'Ouest américain présentent souvent des représentations caricaturales d'adversaires armés - généralement un shérif ou un marshal contre un bandit ignoble ou une bande de mécréants. Il était courant de distinguer les "bons" des "méchants" par la couleur de leur chapeau de cow-boy. Le protagoniste courageux et pur portait généralement un chapeau blanc, tandis que le méchant en portait un de couleur sombre ou noir. Cette imagerie s'est étendue à d'autres aspects de la culture au fil des ans et a fini par faire son chemin dans le jargon de la sécurité informatique.

Chapeau Noir

Un pirate informatique (ou cracker) est celui qui tente sans ambiguïté de compromettre la sécurité d'un système informatique (ou d'un code logiciel fermé) ou d'un réseau d'information

sciemment contre la volonté de son propriétaire. Le but du pirate informatique est d'obtenir un accès non autorisé au système, soit pour obtenir ou détruire des informations, soit pour provoquer une perturbation dans le fonctionnement, soit pour refuser l'accès aux utilisateurs légitimes, soit pour prendre le contrôle du système pour leurs propres besoins. Certains pirates saisiront, ou menaceront de saisir, le contrôle d'un système - ou empêcheront l'accès d'autres personnes - et feront chanter le propriétaire pour qu'il paie une rançon avant de renoncer au contrôle. Un hacker est considéré comme un chapeau noir même s'il a ce qu'il qualifierait lui-même de nobles intentions. En d'autres termes, même les pirates qui piratent à des fins sociales ou politiques sont des chapeaux noirs parce qu'ils ont l'intention d'exploiter les vulnérabilités qu'ils découvrent. De même, les entités d'États-nations adverses qui piratent à des fins de guerre peuvent être considérées comme des chapeaux noirs, indépendamment de leurs justifications ou du statut international de leur nation.

Chapeau Blanc

Parce qu'il y a tant de façons créatives et imprévues d'accéder aux ordinateurs et aux réseaux, souvent la seule façon de découvrir des faiblesses exploitables est de tenter de pirater son propre système avant qu'une personne aux intentions malveillantes ne le fasse en premier et ne cause des dommages irréparables. Un hacker en chapeau blanc a été spécifiquement autorisé par le propriétaire ou le gardien d'un système cible à découvrir et à tester ses vulnérabilités. C'est ce qu'on appelle un test de pénétration. Le pirate en chapeau blanc utilise les mêmes outils et procédures qu'un pirate en chapeau noir, et possède souvent les mêmes connaissances et compétences. En fait, il n'est pas rare qu'un ancien chapeau noir trouve un emploi légitime en tant que chapeau blanc, car les chapeaux noirs ont généralement une grande expérience pratique de la pénétration des systèmes. Les agences gouvernementales et les entreprises sont connues pour employer des criminels informatiques autrefois poursuivis en justice pour tester des systèmes vitaux.

Chapeau Gris

Comme son nom l'indique, le terme "chapeau gris" (souvent orthographié comme "grey") est un peu moins concret dans sa caractérisation de l'éthique du hacker. Un hacker en chapeau gris n'a pas nécessairement l'autorisation du propriétaire ou du gardien du système, et pourrait donc être considéré comme agissant de manière non éthique lorsqu'il tente de détecter des vulnérabilités de sécurité. Cependant, un chapeau gris n'effectue pas ces actions dans l'intention d'exploiter les vulnérabilités ou d'aider les autres à le faire. Au contraire, il effectue essentiellement des tests de pénétration non autorisés dans le but d'alerter le propriétaire de toute faille potentielle. Souvent, les chapeaux gris pirateront dans le but exprès de renforcer un système qu'ils utilisent ou dont ils jouissent pour empêcher toute subversion future par des acteurs ayant des intentions plus malveillantes.

Conséquences Du Piratage Informatique

Les conséquences d'un accès non autorisé à un ordinateur vont des coûts et inconvénients mineurs de la sécurité de l'information au quotidien à des situations gravement dangereuses, voire mortelles. Bien que des sanctions pénales sévères puissent être prises à l'encontre des pirates informatiques qui sont attrapés et poursuivis, la société dans son ensemble supporte le poids des coûts financiers et humains du piratage informatique malveillant. En raison de la nature interconnectée du monde moderne, un seul individu intelligent assis dans un café avec un ordinateur portable peut causer d'énormes dommages à la vie et aux biens. Il est important de comprendre les ramifications du piratage afin de savoir où concentrer les efforts pour la prévention de certains crimes informatiques.

Criminalité

Il y a, bien sûr, des conséquences juridiques pour les pirates informatiques pris en train de s'introduire dans un système ou un réseau informatique. Les lois et les sanctions spécifiques varient selon les nations ainsi qu'entre les différents États et municipalités. L'application des lois varie également d'un pays à l'autre. Certains gouvernements n'accordent tout simplement pas la priorité à la poursuite des cybercrimes, surtout lorsque les victimes se trouvent en dehors de leur propre pays. Cela permet à de nombreux pirates informatiques d'opérer en toute impunité dans certaines régions du monde. En fait, certaines nations avancées ont des éléments au sein de leur gouvernement dans lesquels le piratage est une fonction prescrite. Certains organismes militaires et civils de sécurité et d'application de la loi disposent de divisions dont le mandat est de pirater les systèmes sensibles d'adversaires étrangers. C'est un point de discorde lorsque certains de ces organismes s'immiscent dans les fichiers et les communications privées de leurs propres citoyens, ce qui entraîne souvent des conséquences politiques.

Les sanctions pour piratage illégal dépendent largement de la nature de la transgression elle-même. Accéder aux informations privées d'une personne sans son autorisation entraînerait probablement une peine moins lourde que d'utiliser cet accès pour voler de l'argent, saboter du matériel ou

commettre une trahison. Des poursuites très médiatisées ont été engagées à la suite de vols par des pirates informatiques qui vendaient ou diffusaient des informations personnelles, sensibles ou classifiées.

Victimes

Les victimes du piratage vont des personnes qui reçoivent des blagues relativement inoffensives sur les médias sociaux, à celles qui sont publiquement gênées par la publication de photos ou d'e-mails personnels, en passant par les victimes de vol, de virus destructeurs et de chantage. Dans les cas plus graves de piratage où la sécurité nationale est menacée par la diffusion d'informations sensibles ou la destruction d'infrastructures essentielles, c'est la société dans son ensemble qui est victime.

Le vol d'identité est l'un des crimes informatiques les plus courants. Les pirates informatiques ciblent les informations personnelles de personnes peu méfiantes et utilisent les données à des fins personnelles ou les vendent à d'autres personnes.

Souvent, les victimes ne savent pas que leurs informations ont été compromises jusqu'à ce qu'elles constatent une activité non autorisée sur leur carte de crédit ou leur compte bancaire. Bien que les données personnelles soient souvent obtenues par des pirates informatiques en ciblant des victimes individuelles, certains criminels sophistiqués ont pu, ces dernières années, accéder à de vastes bases de données d'informations personnelles et financières en piratant les serveurs de détaillants et de fournisseurs de services en ligne possédant des millions de comptes clients. Ces violations de données très médiatisées

ont un coût énorme en termes monétaires, mais elles portent également atteinte à la réputation des entreprises ciblées et ébranlent la confiance du public dans la sécurité de l'information. Des violations de données similaires ont entraîné la diffusion publique de courriers électroniques et de photographies personnelles, ce qui est souvent source d'embarras, de dommages aux relations et de pertes d'emploi pour les victimes.

Coûts De La Prévention

Il y a une impasse classique en matière de prévention du piratage informatique. Pour la plupart des individus, il suffit d'un peu de bon sens, de vigilance, de bonnes pratiques de sécurité et de quelques logiciels librement disponibles pour rester protégé contre la plupart des attaques. Cependant, avec la popularité croissante de l'informatique dématérialisée, où les fichiers sont stockés sur un serveur externe en plus ou au lieu de l'être sur des appareils personnels, les individus ont moins de contrôle sur la sécurité de leurs propres données. Cefait peser une lourde charge financière sur les gardiens des serveurs en nuage pour protéger un volume de plus en plus important d'informations personnelles centralisées.

Les grandes entreprises et les entités gouvernementales se retrouvent donc régulièrement à dépenser chaque année pour la sécurité informatique des sommes égales ou supérieures à celles qu'elles pourraient perdre dans la plupart des attaques courantes. Néanmoins, ces mesures sont nécessaires car une attaque réussie, à grande échelle et sophistiquée - même si elle est peu probable - peut avoir des conséquences catastrophiques. De même, les personnes qui souhaitent se protéger des cybercriminels achètent des logiciels de sécurité ou des services de protection contre le vol d'identité. Ces coûts, ainsi que le temps et les efforts consacrés à la mise en œuvre d'une bonne sécurité de l'information, peuvent

constituer une charge indésirable.

Sécurité Nationale Et Mondiale

La dépendance croissante des systèmes de contrôle industriel à l'égard des ordinateurs et des dispositifs en réseau, ainsi que la nature rapidement interconnectée des infrastructures critiques, ont rendu les services vitaux des nations industrielles très vulnérables aux cyber-attaques. Les services municipaux d'électricité, d'eau, d'égouts, d'Internet et de télévision peuvent être perturbés par des saboteurs, que ce soit à des fins d'activisme politique, de chantage ou de terrorisme. Même une interruption de courte durée de certains de ces services peut entraîner la perte de vies humaines ou de biens. La sécurité des centrales nucléaires est particulièrement préoccupante, comme nous l'avons vu ces dernières années, les pirates informatiques peuvent implanter des virus dans les composants électroniques couramment utilisés pour perturber les machines industrielles.

Les systèmes bancaires et les réseaux d'échanges financiers sont des cibles de choix pour les pirates informatiques, qu'ils cherchent à réaliser des gains financiers ou à provoquer des perturbations économiques dans un pays rival. Certains gouvernements déploient déjà ouvertement leurs propres hackers pour la guerre électronique. Les cibles du piratage gouvernemental et militaire comprennent également les véhicules et les instruments de guerre de plus en plus interconnectés. Les composants électroniques peuvent être

compromis par des pirates sur la chaîne de production avant même qu'ils ne soient intégrés dans un char, un cuirassé, un avion de chasse, un drone aérien ou tout autre véhicule militaire - les gouvernements doivent donc faire attention à qui ils font appel dans la chaîne d'approvisionnement. Les communications sensibles par courrier électronique, téléphone ou satellite doivent également être protégées des adversaires.

Les États nations ne sont pas les seuls à menacer les systèmes militaires avancés. Les organisations terroristes deviennent de plus en plus sophistiquées et adoptent des méthodes plus technologiques.

Chapter 2. Vulnérabilité et exploitation

L'essence du piratage est l'exploitation de failles dans la sécurité d'un ordinateur, d'un appareil, d'un composant logiciel ou d'un réseau. Ces failles sont connues sous le nom de vulnérabilités. L'objectif du pirate est de découvrir les vulnérabilités d'un système qui lui donnera l'accès ou le contrôle le plus facile possible pour atteindre ses objectifs. Une fois que les vulnérabilités sont comprises, l'exploitation de ces vulnérabilités peut commencer, le pirate profitant alors des failles du système pour y accéder. En général, les pirates informatiques en chapeau noir et en chapeau blanc ont l'intention d'exploiter les vulnérabilités, bien qu'à des fins différentes, où les chapeaux gris tenteront d'avertir le propriétaire afin que des mesures puissent être prises pour protéger le système.

Vulnérabilités

Les vulnérabilités des systèmes informatiques et des réseaux ont toujours existé et existeront toujours. Aucun système ne peut être rendu étanche à 100 % car quelqu'un devra toujours pouvoir accéder aux informations ou aux services protégés. De plus, la présence d'utilisateurs humains représente une vulnérabilité en soi car les gens sont notoirement peu doués pour pratiquer une bonne sécurité. Au fur et à mesure que les vulnérabilités sont découvertes et corrigées, de nouvelles prennent presque instantanément leur place. Le va-et-vient entre l'exploitation des pirates et la mise en œuvre des mesures de sécurité représente une véritable course aux armements, chaque partie devenant plus sophistiquée en tandem.

Vulnérabilités Humaines

Une vulnérabilité rarement discutée est celle de l'utilisateur humain. La plupart des utilisateurs d'ordinateurs et de systèmes d'information ne sont pas des experts en informatique ou des professionnels de la cybersécurité. La majorité des utilisateurs savent très peu de choses sur ce qui se passe entre leurs points d'interface et les données ou les services auxquels ils accèdent. Il est difficile d'amener les gens à changer leurs habitudes à grande échelle et à utiliser les pratiques recommandées pour définir des mots de passe, examiner soigneusement les courriels, éviter les sites web malveillants et maintenir leurs logiciels à jour. Les entreprises et les organismes publics consacrent beaucoup de temps et de ressources à la formation de leurs employés pour qu'ils suivent les procédures de sécurité de l'information appropriées, mais il suffit d'un maillon faible de la chaîne pour donner aux pirates la fenêtre qu'ils recherchent pour accéder à un système ou à un réseau entier.

Les pare-feu et les dispositifs de prévention des intrusions les plus sophistiqués et les plus coûteux sont rendus inutiles lorsqu'un utilisateur interne clique sur un lien malveillant, ouvre un virus dans une pièce jointe à un courriel, branche une clé USB compromise ou donne simplement son mot de passe d'accès par téléphone ou par courriel. Même lorsqu'on leur rappelle sans cesse les meilleures pratiques de sécurité, les utilisateurs

ordinaires constituent la vulnérabilité la plus facile et la plus constante à découvrir et à exploiter. Parfois, les vulnérabilités humaines sont aussi simples que de pratiquer une mauvaise sécurité des mots de passe en laissant des mots de passe écrits sur des notes en clair, parfois même attachés au matériel utilisé. L'utilisation de mots de passe faciles à deviner est une autre erreur courante des utilisateurs. Un système d'entreprise particulier a été compromis lorsqu'un pirate informatique malin a intentionnellement laissé une clé USB dans le parking d'une entreprise. Lorsqu'un employé sans méfiance l'a trouvée, il a placé la clé dans son ordinateur de travail et a ensuite déclenché un virus. La plupart des individus ne prennent pas la sécurité informatique au sérieux avant qu'un incident ne se produise, et même alors, ils retombent souvent dans les mêmes habitudes. Les pirates informatiques le savent et en profitent aussi souvent que possible.

Vulnérabilités Des Logiciels

Tous les ordinateurs dépendent de logiciels (ou de "microprogrammes", dans certains appareils) pour traduire en action les commandes de l'utilisateur. Le logiciel gère les connexions des utilisateurs, effectue des recherches dans les bases de données, exécute les soumissions de formulaires du site web, contrôle le matériel et les périphériques, et gère d'autres aspects des fonctionnalités de l'ordinateur et du réseau qui pourraient être exploités par un pirate informatique. Outre le fait que les programmeurs font des erreurs et des oublis, il est impossible pour les développeurs de logiciels d'anticiper toutes les vulnérabilités possibles dans leur code. Le mieux que les développeurs puissent espérer est de corriger et de modifier leurs logiciels

au fur et à mesure que des vulnérabilités sont découvertes. C'est pourquoi il est si important de maintenir les logiciels à jour.

Certaines vulnérabilités des logiciels sont dues à des erreurs de programmation, mais la plupart sont simplement dues à des défauts de conception imprévus. Les logiciels sont souvent sûrs lorsqu'ils sont utilisés tels qu'ils ont été conçus, mais des combinaisons imprévues et involontaires d'entrées, de commandes et de conditions entraînent souvent des conséquences imprévues. En l'absence de contrôles stricts sur la façon dont les utilisateurs interagissent avec les logiciels,

de nombreuses vulnérabilités des logiciels sont découvertes par erreur ou au hasard. Les pirates informatiques se font un devoir de découvrir ces anomalies le plus rapidement possible.

Exploits

Trouver et exploiter les vulnérabilités pour accéder aux systèmes est à la fois un art et une science. En raison de la nature dynamique de la sécurité de l'information, il y a un jeu constant de "chat et de souris" entre les pirates et les professionnels de la sécurité, et même entre les adversaires des États nations. Afin de rester en tête (ou du moins de ne pas être trop loin derrière), il faut non seulement se tenir au courant des dernières technologies et des vulnérabilités, mais aussi être capable d'anticiper la façon dont les pirates et le personnel de sécurité réagiront aux changements dans le paysage global.

Accès

L'objectif le plus courant de l'exploitation est d'accéder à un système cible et d'en contrôler un certain niveau. Comme de nombreux systèmes ont plusieurs niveaux d'accès pour des raisons de sécurité, il arrive souvent que chaque niveau d'accès ait sa propre liste de vulnérabilités et soit généralement plus difficile à pirater car des fonctionnalités plus vitales sont disponibles. Le coup d'accès ultime pour un hacker est d'atteindre le niveau super-utilisateur ou root (un terme UNIX) - connu sous le nom de "getting root" dans le jargon des hackers. Ce niveau le plus élevé permet à l'utilisateur de contrôler tous les systèmes, fichiers, bases de données et paramètres d'un système autonome donné.

Il peut être assez difficile de percer la racine d'un système informatique sécurisé en un seul exploit. Le plus souvent, les pirates exploitent des vulnérabilités plus faciles ou profitent des utilisateurs moins expérimentés pour obtenir d'abord un accès de bas niveau. À partir de là, d'autres méthodes peuvent être employées pour atteindre les niveaux supérieurs, des administrateurs jusqu'à la racine. Grâce à l'accès à la racine, un pirate peut consulter, télécharger et écraser des informations à volonté et, dans certains cas, supprimer toute trace de sa présence dans le système. C'est pourquoi l'obtention de la racine dans un système cible est un point de fierté, car c'est la plus grande réussite des pirates informatiques, qu'ils soient en noir ou en

blanc.

Refuser L'accès

Dans de nombreux cas, l'accès à un système cible particulier est impossible, extrêmement difficile ou même non souhaité par un pirate informatique. Parfois, l'objectif d'un hacker est simplement d'empêcher des utilisateurs légitimes d'accéder à un site web ou à un réseau. Ce type d'activité est connu sous le nom de déni de service (DoS). L'objectif d'une attaque par déni de service peut varier. Comme elle est relativement simple à exécuter, il s'agit souvent d'un exercice de débutant pour un hacker inexpérimenté ("newbie", "n00b", ou "néophyte" dans le jargon) afin de gagner quelques droits de vantardise. Les hackers plus expérimentés peuvent exécuter des attaques DoS soutenues qui perturbent les serveurs commerciaux ou gouvernementaux pendant une période prolongée. Ainsi, des groupes organisés de pirates informatiques prennent souvent un site web en "otage" et exigent une rançon des propriétaires en échange de l'arrêt de l'attaque, le tout sans jamais avoir à y accéder.

Chapitre 3. Pour commencer

Les hackers ont la réputation d'être des individus très intelligents et prodigieux à bien des égards. Il peut donc sembler écrasant et difficile de partir de zéro et d'atteindre n'importe quel niveau de compétence pratique. Il faut se rappeler que chacun doit commencer quelque part lorsqu'il apprend un sujet ou une compétence. Avec du dévouement et de la persévérance, il est possible d'aller aussi loin dans le monde du piratage que votre volonté peut vous mener. Une chose qui vous aidera à devenir un hacker est de vous fixer des objectifs. Demandez-vous pourquoi vous voulez apprendre le hacking et ce que vous avez l'intention d'accomplir. Certains veulent simplement apprendre les bases afin de pouvoir comprendre comment se protéger, ainsi que leur famille ou leur entreprise, contre les attaques malveillantes. D'autres cherchent à se lancer dans une carrière de piratage informatique ou de sécurité de l'information.

Quelles que soient vos raisons, vous devez vous préparer à acquérir un certain nombre de nouvelles connaissances et compétences.

Apprendre

L'arme la plus importante dans l'arsenal d'un hacker est la connaissance. Non seulement il est important pour un hacker d'en apprendre le plus possible sur les ordinateurs, les réseaux et les logiciels, mais pour rester compétitif et efficace, il doit se tenir au courant des changements constants et rapides dans le domaine de l'informatique et de la sécurité informatique. Il n'est pas nécessaire pour un hacker d'être un ingénieur, un informaticien, ou d'avoir une connaissance intime de la conception des microprocesseurs ou du matériel informatique, mais il doit comprendre comment fonctionne un ordinateur, quels en sont les principaux composants et comment ils interagissent, comment les ordinateurs sont mis en réseau à la fois localement et via Internet, comment les utilisateurs interagissent généralement avec leurs machines, et - le plus important - comment les logiciels dictent le fonctionnement de l'ordinateur. Un excellent hacker parle couramment et pratique plusieurs langues informatiques et comprend les principaux systèmes d'exploitation. Il est également très utile pour un hacker de se familiariser avec l'histoire, les mathématiques et la pratique de la cryptographie.

Il est possible, et de plus en plus fréquent, qu'un profane ayant peu d'expérience du piratage et des connaissances faibles ou intermédiaires en programmation mène une attaque contre

un système. Les gens le font souvent en utilisant des scripts et en suivant des procédures qui ont été développées par des opérateurs plus expérimentés. Cela se produit le plus souvent avec des types d'attaques plus simples, comme le déni de service. Ces pirates informatiques inexpérimentés sont connus dans la communauté des pirates informatiques sous le nom de "script kiddies". Le problème avec ce type d'activité est que les auteurs n'ont pas une grande connaissance de ce qui se passe dans le code qu'ils exécutent et ne peuvent pas anticiper les effets secondaires ou d'autres conséquences involontaires. Il est préférable de bien comprendre ce que vous faites avant de tenter une attaque.

Ordinateurs Et Processeurs

Les ordinateurs varient en taille, forme et fonction, mais la plupart d'entre eux ont essentiellement le même design. Un bon hacker devrait étudier comment les ordinateurs ont évolué des premières machines du ^{20e} siècle aux machines beaucoup plus sophistiquées que nous utilisons aujourd'hui. Ce faisant, il devient évident que les ordinateurs ont les mêmes composants de base. Pour être un hacker efficace, vous devez connaître les différents types de processeurs qui existent sur la majorité des ordinateurs modernes. Par exemple, les trois plus grands fabricants de microprocesseurs sont Intel, American Micro Devices (AMD) et Motorola. Ces processeurs comprennent la plupart des ordinateurs personnels qu'un pirate informatique rencontrera, mais chacun a son propre jeu d'instructions. Bien que la plupart des pirates aient rarement affaire à des langages de programmation au niveau de la machine, des attaques plus sophistiquées peuvent nécessiter une compréhension des différences entre les jeux d'instructions des processeurs.

Certains processeurs sont programmables par l'utilisateur final. Ils sont connus sous le nom de Field-Programmable Gate Arrays (FPGA) et sont de plus en plus souvent utilisés pour les systèmes embarqués, notamment dans les contrôles industriels. Il est connu que des pirates informatiques accèdent à ces puces pendant leur production afin de déployer des logiciels

malveillants à la destination finale. Une compréhension de l'architecture et de la programmation des FPGA est nécessaire pour ce type d'attaques sophistiquées. Ces attaques intégrées sont particulièrement préoccupantes pour les clients militaires et industriels qui achètent des puces à grande échelle pour des systèmes critiques.

Mise En Réseau Et Protocoles

L'un des sujets les plus importants à étudier pour l'aspirant hacker est celui de l'architecture des réseaux et des protocoles. Les ordinateurs peuvent être mis en réseau dans de nombreuses configurations et tailles différentes, et avec différentes technologies qui régissent leur interconnexion. Du fil de cuivre à la fibre optique, en passant par les connexions sans fil et par satellite, ainsi que des combinaisons de tous ces médias, nous avons construit un vaste réseau d'ordinateurs à travers le monde. Ce réseau peut être compris dans son intégralité à grande échelle, mais aussi être considéré comme une connexion de réseaux autonomes plus petits.

En termes de taille, les réseaux informatiques ont traditionnellement été classés en réseaux locaux (LAN) et en réseaux étendus (WAN). Les WAN relient généralement plusieurs réseaux locaux. Il existe plusieurs autres désignations pour différentes tailles de réseaux, et la terminologie évolue constamment en fonction des nouvelles technologies et des nouvelles conductivités. Suivre ces changements est l'une des tâches permanentes d'un hacker.

Les réseaux ont également des architectures différentes. L'architecture est déterminée non seulement par la configuration des différents nœuds, mais aussi par le support qui les relie. À l'origine, les ordinateurs en réseau étaient toujours connectés par

un fil de cuivre. Les câbles de réseau en cuivre couramment utilisés, souvent appelés câbles Ethernet, sont constitués de paires de fils de cuivre torsadés. Bien que le plus courant de ces câbles soit le câble de catégorie cinq, ou CAT-5, il commence à céder la place à une nouvelle norme, CAT-6, qui a une plus grande capacité de transmission des signaux.

Pour les applications à très haut débit et sur de longues distances, on choisit généralement des câbles à fibres optiques. Les fibres optiques utilisent la lumière au lieu de l'électricité et ont une très grande capacité de transport de l'information. Elles sont utilisées pour transporter la plupart des services modernes de télévision par câble et d'internet à haut débit. La fibre optique sert de colonne vertébrale à l'internet. Dans les petites zones, les réseaux sans fil sont très courants. Grâce au protocole Wi-Fi (Wireless Fidelity), les réseaux sans fil existent dans un grand nombre de réseaux locaux personnels, privés et commerciaux. Les pirates informatiques sont souvent particulièrement intéressés par le piratage des réseaux Wi-Fi, ce qui entraîne l'évolution des normes de sécurité Wi-Fi.

Quelle que soit l'architecture ou le moyen de transmission, lorsque deux terminaux communiquent sur un réseau, ils doivent le faire en utilisant un ensemble de règles communes appelées protocole. Les protocoles de mise en réseau ont évolué depuis la création des premiers réseaux informatiques, mais ils ont conservé la même approche de base par couches. En général, un réseau est conceptualisé en termes de différentes couches qui

remplissent différentes fonctions. C'est ce qu'on appelle aussi une pile. Les protocoles de communication les plus couramment utilisés aujourd'hui sont le protocole Internet (IP) et le protocole de contrôle de transmission (TCP). Pris ensemble, ils sont communément appelés TCP/IP. Ces protocoles changent et sont parfois normalisés. Il est essentiel pour le pirate d'apprendre ces protocoles et leur relation avec la communication entre les différentes couches de la pile. C'est ainsi que les pirates peuvent obtenir des niveaux d'accès de plus en plus élevés à un système.

Langages De Programmation

Il peut sembler décourageant d'apprendre un langage de programmation en partant de zéro sans l'avoir jamais fait auparavant, mais beaucoup de gens trouvent qu'une fois qu'ils maîtrisent un langage de programmation, il est beaucoup plus facile et rapide d'en apprendre d'autres. Les pirates doivent non seulement comprendre les langages de programmation pour pouvoir exploiter les vulnérabilités des logiciels, mais beaucoup d'entre eux doivent écrire leur propre code pour pouvoir exécuter une attaque particulière. Lire, comprendre et écrire du code est fondamental pour le piratage.

Les langages de programmation vont du code machine très obscur, qui est en format binaire et hexadécimal et qui est utilisé pour communiquer directement avec un processeur, aux langages orientés objet de haut niveau qui sont utilisés pour le développement de logiciels. Les langages orientés objet de haut niveau les plus courants sont C++ et Java. Le code écrit dans des langages de haut niveau est compilé dans le code machine approprié pour un processeur particulier, ce qui rend les langages de haut niveau très portables entre différents types de machines. Une autre catégorie est celle des langages scriptés, dans lesquels les commandes sont exécutées ligne par ligne au lieu d'être compilées en code machine.

L'apprentissage des langages de programmation prend du

temps et de la pratique - il n'y a pas d'autre moyen de devenir compétent. Les longues soirées et les marathons nocturnes d'écriture, de débogage et de recompilation de code sont un rituel courant chez les hackers débutants.

Конец ознакомительного фрагмента.