Attaques de mots de passe

1. **Objectifs**

- Connaitre les attaques de mots de passe

- **Présentation**



- La plupart des systèmes sont configurés de manière à bloquer temporairement le compte d’un utilisateur après un certain nombre de tentatives de connexion infructueuses. Ainsi, un pirate peut difficilement s’infiltrer sur un système de cette façon.
- En contrepartie, un pirate peut se servir de ce mécanisme d’autodéfense pour bloquer l’ensemble des comptes utilisateurs afin de provoquer un déni de service.
- Sur la plupart des systèmes les mots de passe sont stockés de manière chiffrée (cryptée) dans un fichier ou une base de données. Néanmoins, lorsqu’un pirate obtient un accès au système et obtient ce fichier, il lui est possible de tenter de casser le mot de passe d’un utilisateur en particulier ou bien de l’ensemble des comptes utilisateurs.
- L'usurpation d'adresse IP (en anglais : **IP spoofing**) est une technique de hacking consistant à utiliser l'adresse IP d'une machine, ou d'un équipement, afin d'en usurper l'identité. Elle permet de récupérer l'accès à des informations en se faisant passer pour la machine dont on spoofe l'adresse IP. De manière plus précise, cette technique permet la création de paquets IP avec une adresse IP source appartenant à quelqu'un d'autre.

- ## Attaque par dictionnaire



- Une **attaque par dictionnaire** est une technique ou une méthode utilisée pour violer la sécurité informatique d'une machine ou d'un serveur protégé par mot de passe. Une attaque par dictionnaire tente de déjouer un mécanisme d'authentification en saisissant systématiquement chaque mot d'un dictionnaire comme mot de passe ou en essayant de déterminer la clé de déchiffrement d'un message ou d'un document chiffré.
- C'est une attaque qui profite du fait que les utilisateurs ont tendance à employer des mots communs et des mots de passe courts. Le pirate utilise une liste de mots communs, le dictionnaire, et les essaye, bien souvent avec des chiffres avant et/ou après les mots, à l'encontre des comptes d'une entreprise pour chaque nom d'utilisateur. (Les noms d'utilisateur sont généralement très simples à identifier car ils sont presque toujours basés sur le nom des employés.)
- Les outils d’attaque par force brute peuvent demander des heures, voire des jours, de calcul même avec des machines équipées de processeurs puissants. Ainsi, une alternative consiste à effectuer une attaque par dictionnaire.
- La plupart du temps les utilisateurs choisissent des mots de passe ayant une signification réelle. Avec ce type d’attaques, un tel mot de passe peut être craqué en quelques minutes.

- ## Force brute

apcpedagogie.com

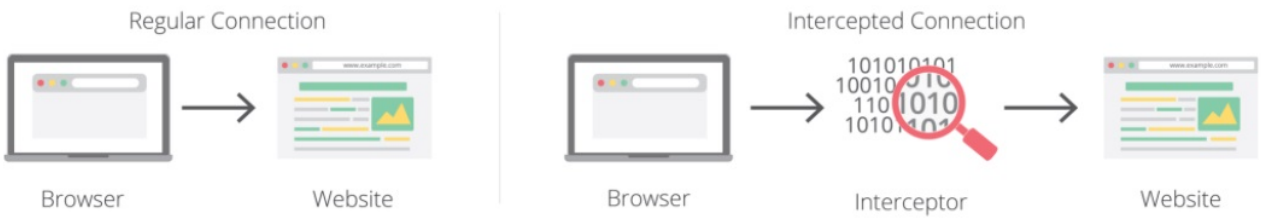


- Une attaque par force brute (brute force attack) consiste à tester, l'une après l'autre, chaque combinaison possible d'un mot de passe ou d'une clé pour un identifiant donné afin se connecter au service ciblé.
- Il s’agit d’une méthode ancienne et répandue chez les pirates. Le temps nécessaire à celle-ci dépend du nombre de possibilités, de la vitesse que met l’attaquant pour tester chaque combinaison et des défenses qui lui sont opposées.
- Utilisation d'un programme pour générer des mots de passe potentiels ou même des ensembles de caractères aléatoires. Ces attaques commencent par les mots de passe faibles et couramment utilisés, comme Motdepasse123 puis évoluent. Les programmes qui exécutent ces attaques essayent habituellement des variantes avec des majuscules et minuscules.

Interception de trafic

- Au cours de cette attaque, le cyber-escroc utilise un logiciel comme les renifleurs de paquet pour surveiller le trafic réseau et enregistrer les mots de passe lorsqu'ils sont transmis. De la même manière que l'écoute clandestine ou l'interception d'une ligne téléphonique, le logiciel surveille et enregistre les informations cruciales. Bien évidemment, si cette information (comme les mots de passe) n'est pas chiffrée, la tâche est plus simple. Cependant, même les informations chiffrées peuvent être déchiffrées, selon le niveau de sécurité de la méthode de chiffrement utilisée.

Attaque de l'intercepteur



- Les attaques d'interception permettent aux utilisateurs non autorisés d'accéder à nos données, applications ou environnements, et constituent principalement une attaque contre la

confidentialité.

- L'interception peut prendre la forme d'une visualisation ou d'une copie non autorisée de fichiers, d'une écoute clandestine de conversations téléphoniques ou de la lecture d'e-mails, et peut être effectuée sur des données au repos ou en mouvement. Correctement exécutées, les attaques d'interception peuvent être très difficiles à détecter.
- Au cours de cette attaque, le programme du pirate ne surveille pas seulement les informations qui sont transmises mais s'introduit lui-même activement au milieu de l'interaction, en empruntant généralement l'identité d'un site Web ou d'une application.
- Cela permet au programme d'enregistrer les identifiants de l'utilisateur ainsi que d'autres informations sensibles comme les numéros de compte et de sécurité sociale.
- Les attaques de l'intercepteur sont souvent facilitées par les attaques d'ingénierie sociale qui attirent l'utilisateur vers un site factice.
- Il existe deux manières principales d'intercepter les connexions : localement et à distance .
    - **Interception locale** :
        - Lorsque l'intercepteur s'exécute directement sur l'ordinateur d'un utilisateur, la pile réseau du système d'exploitation est modifiée pour intercepter et rediriger les connexions vers le logiciel d'interception.
        - Cette technique est souvent utilisée par les logiciels antivirus pour surveiller les connexions réseau afin d'identifier les téléchargements malveillants et par certaines souches de logiciels malveillants pour voler des informations d'identification ou injecter des publicités.
    - **Interception à distance** :
        - L'interception à distance est réalisée en insérant la surveillance le long du chemin réseau reliant l'ordinateur de l'utilisateur au site qu'il parcourt. Par exemple, cela peut être réalisé en redirigeant le trafic réseau vers l'intercepteur à l'aide de règles de pare-feu.
        - L'interception du réseau est généralement effectuée par un "boîtier de sécurité" qui tente de détecter les attaques ou de surveiller l'exfiltration de données d'entreprise pour tous les ordinateurs d'un réseau.
        - Ces boîtes sont souvent également utilisées pour intercepter et analyser les e-mails.

- ## Attaque de l'enregistreur de frappe

apcpedagogie.com



- Un enregistreur de frappes est un logiciel ou un composant matériel qui a la capacité d'intercepter et d'enregistrer les informations rentrées avec le clavier dans l'ordinateur infecté.
- Cet outil a souvent l'habilité de se positionner entre le clavier et le système d'exploitation afin d'en intercepter toutes les communications sans que l'utilisateur ne s'en aperçoive. Un keylogger peut soit stocker les données localement sur la machine infectée, soit les envoyer sur un PC à distance contrôlé par le pirate, s'il fait partie d'un outil d'attaque plus élaboré qui a la possibilité de communiquer avec l'extérieur.
- Bien que le terme "enregistreur de frappes" soit habituellement utilisé en relation avec des outils malveillants, certains outils de surveillance légitimes utilisés par les agences d'application de la loi, sont également dotés d'enregistreurs de frappes.
- Un cyber-escroc parvient à installer un logiciel qui enregistre les touches saisies sur le clavier par l'utilisateur, lui permettant ainsi de connaître non seulement le nom d'utilisateur et le mot de passe d'un compte, mais également le site Web ou l'application exacte sur laquelle l'utilisateur s'est connecté avec les identifiants. Ce type d'attaque survient généralement après une autre attaque au cours de laquelle le logiciel malveillant enregistreur de frappe est installé sur son ordinateur.

Attaques d'ingénierie sociale

- Les attaques d'ingénierie sociale font référence à une vaste gamme de méthodes pour obtenir des informations de la part des utilisateurs. Voici certaines des techniques utilisées :
  - **Hameçonnage** : e-mails, SMS, etc. envoyés pour amener l'utilisateur à fournir ses identifiants, à cliquer sur un lien qui installe un logiciel malveillant ou à accéder à un site Web factice.
  - **Harponnage** : similaire au hameçonnage mais avec des e-mails/SMS plus élaborés et personnalisés, basés sur des informations déjà recueillies auprès des utilisateurs. Par

exemple, il est possible que le pirate sache que l'utilisateur possède un type particulier d'assurance et y fasse référence dans l'e-mail ou utilise le logo et la mise en page de l'entreprise pour rendre l'e-mail authentique.

- **Appâtage** :



  - Qu’est-ce que le **baiting** ou **appâtage** ? L’appâtage ou baiting, tel un véritable Cheval de Troie, utilise les médias physiques et exploite la curiosité de la cible.
  - Il s’agit d’une escroquerie qui, sur bien des plans, est semblable à une attaque de phishing. Toutefois, ce qui distingue le baiting d’autres attaques d’ingénieries sociales, c’est la promesse d’un élément ou d’un bien utilisé par les pirates pour attirer leurs victimes.
  - Les "baiters" peuvent offrir gratuitement aux utilisateurs des téléchargements de musique ou de films en échange de leurs identifiants de connexion à un site.
  - Les pirates laissent des clés USB ou autres appareils infectés dans des lieux publics ou professionnels, en espérant qu'ils soient récupérés et utilisés par les employés.

  Exemple :

  - Dans le but final d'infiltrer le réseau d'une entreprise. L'ingénieur social distribue aux employés des appareils infectés par des logiciels malveillants. En conséquence, ils espèrent que ce matériel sera inséré dans des ordinateurs connectés au réseau.
  - Par conséquent, cela donnera l'occasion de diffuser du code malveillant. Les clés USB infectées sont présentées aux employés en guise de récompense pour leur participation à une enquête. Par exemple, les appareils d'apparence innocente se trouvent dans un panier de cadeaux placé dans le hall de l'entreprise pour que les employés puissent simplement les saisir sur le chemin du retour vers leur zone de travail.

- **Quid pro quo** :

apcpedagogie.com

- Le cyber-escroc usurpe l'identité de quelqu'un, comme un employé de l'assistance technique, et interagit avec un utilisateur pour lui soutirer des informations.
- Attaque utilisant un échange d'information ou de service pour convaincre la victime d'agir.
- Lors des attaques en quiproquo, le pirate promet un avantage en échange de l'information. Cet avantage prend généralement la forme d'un service, tandis que dans le cas de l'appâtage, il prend la forme d'un bien.

- **Maliciel** :
  - Un **logiciel malveillant** ou **maliciel**, aussi dénommé **logiciel nuisible** ou **programme malveillant** ou **pourriciel** (de l'anglais **malware**, **maliciel** est un logiciel malveillant conçu pour infiltrer ou endommager un système informatique. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires.
  - Parmi ses conséquences :
    - Les programmes malveillants vous intimident avec des logiciels de sécurité non autorisés aussi appelés épouvanticiels. Il s'agit habituellement d'un message d'avertissement qui s'affiche précisément pour vous avertir que votre ordinateur rencontre un problème de sécurité ou pour vous donner d'autres renseignements erronés.
    - Ils reformatent le disque dur de l'ordinateur touché entraînant ainsi la perte de toutes informations qui s'y trouvaient.
    - Ils modifier ou suppriment les fichiers.
    - Ils volent de l'information de nature délicate.
    - Ils envoient des courriels à votre nom.
    - Ils prennent le contrôle de votre ordinateur et de tous les logiciels qui sont en marche.
- **Faux-semblant** :



apcpedagogie.com

- La technique du faux-semblant ("pretexting") est une autre forme d’ingénierie sociale dans laquelle les pirates se basent sur un faux-semblant ou un subterfuge qu’ils ont imaginé et qu’ils soumettent à leur victime pour lui soutirer ses données personnelles.
- Fausse identité pour tromper les victimes et soutirer de l'information.
- Souvent, dans les attaques de ce genre, un escroc prétend qu’il a besoin de certaines informations concernant sa cible pour confirmer son identité.
- La technique du faux-semblant peut aussi être employée en se faisant passer pour un collègue, la police, la banque, les autorités fiscales, le clergé, des experts de compagnies d’assurance – ou de tout autre individu investi d’une autorité ou d’un droit de savoir dans l’esprit de la victime ciblée.
- Le pirate qui utilise ce subterfuge doit simplement préparer les réponses aux questions que la victime serait susceptible de lui poser.
- Dans certains cas, il n’a besoin que d’adopter une voix autoritaire, un ton impérieux, et de disposer d’une capacité à réagir rapidement pour élaborer un scénario de circonstance.
- Les attaques basées sur la technique du faux-semblant sont utilisées couramment pour obtenir des renseignements sensibles ou non. Par exemple, en octobre, un groupe d’escrocs s’est fait passer pour les représentants d’agences de mannequins et de services d’escorte, s’inventant des références et des questions d’entretien pour pousser des femmes et des adolescentes à leur adresser des photos d'elles nues – qu’ils ont par la suite transférées à des entreprises pornographiques contre de grosses sommes d’argent.

L’utilisation du calcul distribué

- L’arrivée du calcul distribué dans la sphère du cybercrime marque un nouveau tournant pour les attaques de mots de passe.
- Le calcul distribué consiste à répartir le traitement mathématique de données sur plusieurs ordinateurs. Jusqu’ici, cette manière d’utiliser les ordinateurs en réseau était réservée au monde scientifique qui a parfois besoin de capacités de calcul très importantes.
- Depuis 2009, les pirates se sont approprié cette technologie car le décodage de mots de passe fait justement parti des opérations qui demandent un très grand nombre de calculs.
- Aujourd’hui, pour quelques centaines de dollars, il est possible d’acquérir des solutions tout en un de recherche de mots de passe. Les méthodes utilisées restent les mêmes qu’auparavant : brut force, recherche avec dictionnaires ou en exploitant des faiblesses dans la méthode de chiffrement.

apcpedagogie.com

- Les logiciels se chargent de partager les calculs entre les ordinateurs en réseau et utilisent la puissance des cartes graphiques pour accélérer les opérations. En effet, grâce à leurs puces spécialisées dans le traitement des nombres, ces éléments sont souvent plus puissants que les processeurs centraux.
- Les vitesses atteintes sont de l'ordre de 1 000 000 000 mots de passe traités par seconde pour un système distribué de moyenne ou de grande ampleur (c'est ce que l'on peut obtenir avec un supercalculateur d'une université par exemple).
- Les systèmes de cloud computing (ex : Amazon EC2) qui proposent des solutions de calculs distribués peuvent tout à fait servir de base pour ce genre d'opération.
- La conclusion d'une étude sur le coût d'une recherche de mot de passe via les possibilités offertes par les services de cloud computing porte à 10 le nombre de caractères qu'un mot de passe doit aujourd'hui comporter pour que le coût de sa recherche devienne vraiment un frein. Il est donc conseillé d'obliger les utilisateurs à créer des mots de passe d'au moins cette longueur.

Choix des mots de passe

- Il est aisément compréhensible que plus un mot de passe est long, plus il est difficile à casser. D'autre part, un mot de passe constitué uniquement de chiffres sera beaucoup plus simple à casser qu'un mot de passe contenant des lettres :
- Un mot de passe de quatre chiffres correspond à 10 000 possibilités (104). Si ce chiffre paraît élevé, un ordinateur doté d'une configuration modeste est capable de le casser en quelques minutes.
- On lui préférera un mot de passe de quatre lettres, pour lequel il existe 456 972 possibilités (264). Dans le même ordre d'idée, un mot de passe mêlant chiffres et lettres, voire également des majuscules et des caractères spéciaux sera encore plus difficile à casser.
- Mots de passe à éviter :
  - Votre identifiant ;
  - Votre nom, votre prénom ou celui d'un proche ;
  - Un mot du dictionnaire ;
  - Un mot à l'envers (les outils de cassage de mots de passe prennent en compte cette possibilité) ;
  - un mot suivi d'un chiffre, de l'année en cours ou d'une année de naissance (par exemple « password1999 »).

Exercices d'application

[h5p id="55"]

Sommaire du cours Administration et sécurité des sites web

Source : https://apcpedagogie.com/attaques-de-mots-de-passe · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com

apcpedagogie.com