
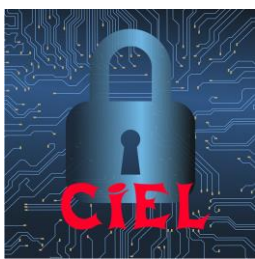







2 nd e BAC Pro CIEL	<p>Identifier les attaques courantes</p> <p>Mot de passe</p>	 <p>Année 2025/2026</p>
		

Nom		
Prénom		
Date		
<u>Matériel</u> <u>Outillage</u> 	⇒ Script Python	<u>Durée : 3H</u> 
<u>Travaux à réaliser</u> 	⇒ Analyse de mot de passe ⇒ Analyse de deux techniques de forcebrute	
<u>Pôle d'activité :</u> Valorisation de la donnée et cybersécurité		
<u>Activités :</u> ⇒ D2 : Développement et validation de solutions logicielles		
<u>Taches :</u> ⇒ T2 : Développement, utilisation ou adaptation de composants logiciels ⇒ T3 : Tests et validation		
<u>Compétences :</u> ⇒ C06 : Valider la conformité d'une installation ⇒ C08 : Coder		
		
Lorsque le logo  apparaît, il est indispensable d'appeler l'enseignant pour vérification.		

A. Mise en contexte

Vous êtes technicien(ne) informatique junior au sein du service informatique d'une PME de services numériques.

L'entreprise a récemment été confrontée à plusieurs incidents de sécurité :

- ⇒ réception de courriels frauduleux (phishing)
- ⇒ tentatives d'accès non autorisées à des comptes utilisateurs
- ⇒ utilisation de mots de passe jugés trop simples par l'administrateur réseau

À la suite de ces incidents, le responsable informatique souhaite sensibiliser les utilisateurs aux risques liés aux mots de passe faibles, même lorsque ceux-ci semblent complexes (présence de majuscules, chiffres ou caractères spéciaux).

Afin de mieux comprendre ces risques, il vous est demandé d'utiliser des outils de simulation permettant d'estimer le temps nécessaire pour retrouver un mot de passe selon différentes méthodes d'attaque (brute force naïf et attaque par dictionnaire).

L'objectif n'est pas de pirater des comptes, mais de comprendre les mécanismes utilisés par les attaquants afin d'adopter de meilleures pratiques de sécurité.

B. Problématique

Un mot de passe contenant des majuscules, des chiffres et des caractères spéciaux est-il toujours suffisamment sécurisé ?

En quoi les différentes méthodes d'attaque (brute force naïf et attaque par dictionnaire) influencent-elles le niveau de risque associé à un mot de passe ?



C. Compétences

C01 COMMUNIQUER EN SITUATION PROFESSIONNELLE (ANGLAIS/FRANÇAIS)	
La présentation (typographie, orthographe, illustration, lisibilité) est soignée et soutient le discours avec des enchaînements cohérents	
La présentation orale (support et expression) est de qualité et claire	
L'argumentation développée lors de la présentation et de l'échange est de qualité	
L'argumentation tient compte des éventuelles situations de handicap des personnes avec lesquelles il interagit	
C03 PARTICIPER A UN PROJET	
Les rôles et tâches de chacun sont identifiés ; le cas échéant, les besoins spécifiques des personnes en situation de handicap sont pris en compte	
Le planning prévisionnel est compris	
Le suivi du projet est respecté	
L'espace collaboratif est correctement utilisé	
C04 ANALYSER UNE STRUCTURE MATÉRIELLE ET LOGICIELLE	
Le besoin est identifié ainsi que les ressources matérielles, logicielles et humaines	
Les logiciels d'analyse et de tests sont utilisés selon les procédures de traitement d'incidents	
Les informations nécessaires sont extraites des documents réglementaires et/ou constructeurs	
Les indicateurs de fonctionnement sont interprétés	
Les fiches de test ou d'intervention sont renseignées	
C06 VALIDER LA CONFORMITÉ D'UNE INSTALLATION	
Les exigences du cahier des charges sont respectées	
Les tests sont effectués	X
Les résultats attendus sont vérifiés	X
La procédure de test est respectée	X
C07 RÉALISER DES MAQUETTES ET PROTOTYPES	
Le placement et routage sont conformes au cahier des charges	
La génération des fichiers de fabrication du PCB est conforme aux attentes	
Le PCB est réalisé, contrôlé et conforme aux IPC (tolérances mécaniques, finition de surface, propreté, ESD etc.)	
Les composants sont conformes à la nomenclature (marquage, étiquetage)	
La nomenclature des composants est respectée	
Le brasage de la carte est conforme à la nomenclature et aux IPC	
Les contraintes liées aux impacts environnementaux sont intégrées	
Le contrôle visuel de la carte assemblée est conforme au dossier de fabrication	
Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	
C08 CODER	
Les environnements de développement et de test sont mis en oeuvre en tenant compte des contraintes de fonctionnalités et de sécurité	X
Le module logiciel est débogué et syntaxiquement correct	
Les composants logiciels individuels sont développés et testés conformément aux spécifications du cahier des charges et des bonnes pratiques	
La solution (logicielle et matérielle) est intégrée et testée conformément aux spécifications du cahier des charges et des bonnes pratiques	X
Le code est commenté et le logiciel est documenté	

C09 INSTALLER LES ÉLÉMENTS D'UN SYSTÈME ÉLECTRONIQUE OU INFORMATIQUE	
L'ensemble des éléments pour l'installation du système est complet et vérifié par rapport au cahier des charges	
Les éléments du système sont installés et raccordés selon une procédure	
La configuration est réalisée	
La mise en service est réalisée	
L'état de l'installation est renseigné de manière écrite ou orale	
Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	
C10 EXPLOITER UN RÉSEAU INFORMATIQUE	
Les alertes et problèmes rencontrés sont renseignés	
Les différents éléments d'un réseau ou d'un système à partir d'un schéma fourni sont identifiés	
La mise à jour des équipements (iOS, OS, logiciel, firmware) est effectuée	
Les optimisations nécessaires sont effectuées	
C11 MAINTENIR UN SYSTÈME ÉLECTRONIQUE OU RÉSEAU INFORMATIQUE	
L'intervention est préparée	
Le dysfonctionnement est constaté	
La maintenance ou la réparation est réalisée	
La fiche d'intervention est correctement renseignée	
Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	

Nature de complexité de l'activité :

Découverte	X
Intermédiaire	
Bac Pro	

D. Les attaques par mot de passe

Le mot de passe est souvent la clé d'accès principale aux services numériques et qu'il peut être volé par phishing, deviné ou retrouvé par des attaques automatisées.

Lorsqu'un attaquant parvient à obtenir ou à deviner un mot de passe, il peut :

- ⇒ Accéder à des données personnelles ou professionnelles
- ⇒ Se faire passer pour un utilisateur légitime
- ⇒ Compromettre un système informatique

Il existe plusieurs méthodes pour retrouver un mot de passe. Dans cette activité, vous allez vous intéresser à deux types d'attaques automatisées :

- ⇒ L'attaque par force brute naïve
- ⇒ L'attaque par dictionnaire

L'objectif n'est pas d'apprendre à pirater, mais de comprendre les risques afin de mieux s'en protéger.

1) Attaque par force brute naïve

L'attaque par force brute naïve consiste à tester toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe.

L'attaquant définit un jeu de caractère (minuscule, majuscules, chiffres, caractères spéciaux) et une longueur maximale du mot de passe.

Le programme test ensuite les combinaisons une par une, sans aucune intelligence particulière.

Par exemple, si le mot de passe est composé uniquement de chiffres (0 à 9) et comporte 4 caractères, il existe $10 \times 10 \times 10 \times 10 = 10\,000$ combinaisons possibles.

Donc, plus le mot de passe est long et varié plus le nombre de combinaisons à tester augmente, et plus le temps nécessaire devient important.

Cette méthode finira toujours par trouver le mot de passe si on dispose suffisamment de temps. Mais elle devient très longue lorsque le mot de passe est long et complexe, et souvent inefficace contre des mots de passe bien construits.

2) Attaque par dictionnaire

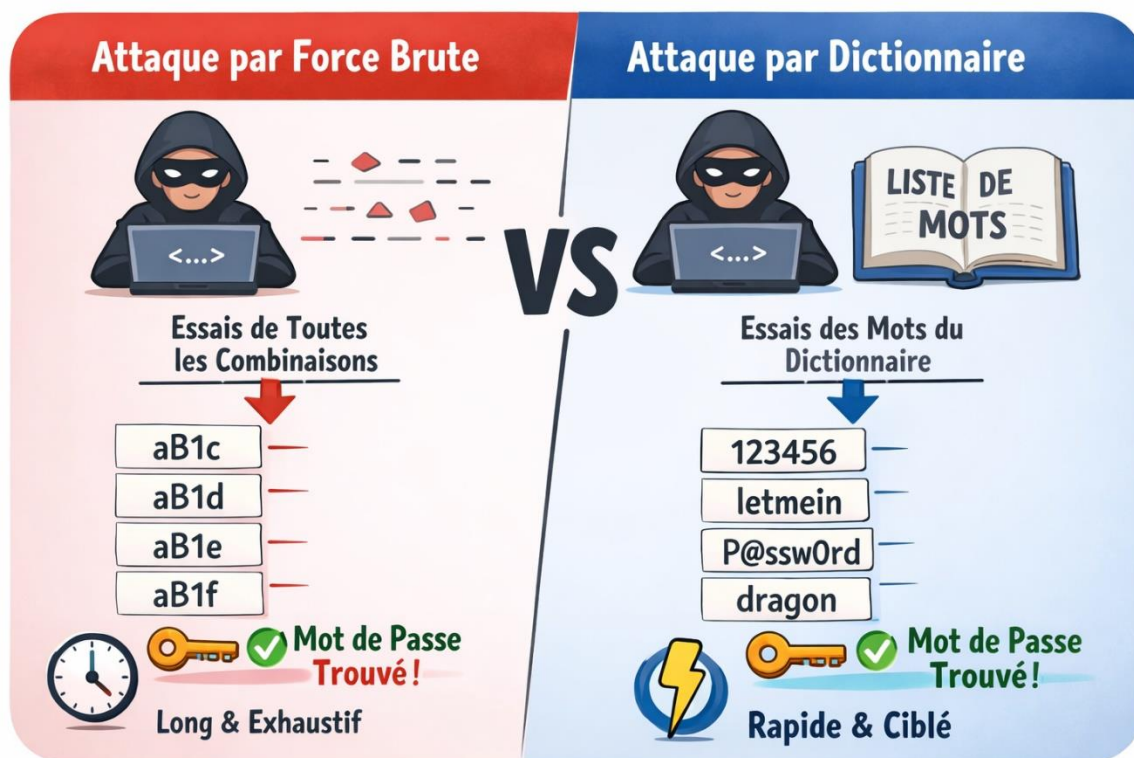
L'attaque par dictionnaire repose sur une idée simple : beaucoup d'utilisateurs choisissent des mots de passe courants ou prévisibles.

Au lieu de tester toutes les combinaisons possibles, l'attaquant utilise un fichier dictionnaire contenant :

- ⇒ Des mots courants
- ⇒ Des prénoms
- ⇒ Des suites de caractères fréquemment utilisées
- ⇒ Des variantes connues (password, Password, P@ssw0rd,...)

Le programme teste les mots du dictionnaire les uns après les autres.

Cette méthode est très rapide si le mot de passe se trouve dans le dictionnaire et redoutablement efficace contre les mots de passe courants. Néanmoins, il reste inefficace si le mot de passe n'apparaît pas dans le dictionnaire et dépend entièrement de la qualité et la taille du dictionnaire.



E. Attaque par Force Brute et Dictionnaire

Créer un nouveau document Word intitulé « *NOM*-MotDePasse.docx » avec *NOM* votre nom de famille.

Créer un titre de niveau 1 intitulé « Test de robustesse de mot de passe ».

Créer un nouveau document Excel.

En vous aidant du script Python fourni « TestMotDePasse.py », **tester** les mots de passe présents en annexe 1. **Préparer** un tableau sous Excel tels que :

Mot de passe	10k-most-common-passwords	500-worst-passwords	french_passwords_top10000	darkweb2017_top-10000	probable-v2_top-12000	mitworm-dictionary	normal	rockyou
1234								

Vous appliquerez une couleur sur les cellules « Force Brute » en fonction des résultats du script :

- ⇒ Rouge pour une durée inférieure ou égale à l'ordre de l'heure
- ⇒ Orange pour une durée inférieure ou égale à l'ordre de la semaine
- ⇒ Vert clair pour une durée inférieure ou égale à l'ordre de l'année
- ⇒ Vert foncé pour une durée supérieure à l'année

Dans la cellule dictionnaire, vous détaillerez dans quel(s) dictionnaire(s) sont présent les mots de passe s'ils sont présents. (Voir document ressource « Mise en forme conditionnel sur Excel »).

S'ils sont présents dans au moins un dictionnaire la cellule sera rouge

S'ils sont présents dans aucun dictionnaire, la cellule sera verte.

Tester votre date de naissance au format DDMMYY (jour-mois-année) et **ajouter** là dans le tableau.

Proposer 5 mots de passe très complexe, **tester** le script et **reporter** le résultat dans le tableau.

Tester un mot de passe que vous avez l'habitude d'utiliser, **reporter** le résultat dans le tableau (**ATTENTION : Ne reporter pas votre mot de passe ! remplacer par « ***** »**).

Sélectionner et **copier-coller** votre tableau dans « Paint » pour convertir votre tableau en image.

Copier-coller l'image de Paint dans votre compte-rendu sur Word.

Créer un titre de niveau 1 intitulé « Synthèse ».

En vous aidant du script et des résultats de vos tests, **expliquer** les principales caractéristiques de complexité d'un mot de passe lors d'une attaque par force brute naïve. **Donner** votre avis sur la complexité de votre mot de passe personnel. **Conclure** sur l'efficacité des deux différentes attaques.

Annexe 1 : Mot de passe à tester

1234	azerty	passwordcomplique
MotDePasse	cest1s3cr3t	12345678901234567890
P@ssw0rd	ordinateur	MaisonBlanche1989
zyv-tr	7j8k91	gT5p9Wq
Tr0ubadour!	JadoreLeChocolat!	LesElephantsDansent@Minuit
P@\$s\$word123	Az3rty!	Admin@123
Welcome@1	M0tDeP@ss3	Iloveyou!
BULL\$EY	Minecraft123	fortnight
Johnny!1€	won2008100%	w0LVes22%%