VIVALTEK | BRUTE FORCE SECURITY

Un mot de passe craqué, c'est tout votre Système d'Information qui s'effondre !

INTRODUCTION

Beaucoup d'entreprises investissent dans des firewalls, des antivirus et des audits complexes.

Cependant, **un mot de passe insuffisamment sécurisé peut anéantir tous ces efforts.**

Les attaques par « force brute » profitent de la négligence humaine pour forcer vos accès et compromettre vos serveurs, vos postes de travail et vos applications.

Un compte administrateur compromis, ce sont souvent des semaines d'arrêt, des pénalités contractuelles et une perte de confiance durable de vos clients.

OBJECTIFS

Évaluation interne de la vulnérabilité d'un système aux attaques par « force brute ».

- **Sécuriser votre activité**
- **Protéger vos partenaires**
- **Anticiper les failles de votre système**
- **Valoriser votre image**
- **Démontrer la solidité de vos accès**

LES CHIFFRES CLÉS*

385 000
cyberattaques réussies en France en 2022.

131 000
Nombre d'attaques liées à des tentatives par force brute en 2022.

34 %
des entreprises françaises déclarent avoir été victimes d'attaques de ce type en 2023.

2,8
millions d'adresses IP utilisées pour tenter de compromettre de nouveaux équipements en 2025.

**Toutes les sources sont disponibles sur notre site internet, dans la fiche produit correspondante.*

CONTACTEZ NOTRE EXPERT 02 52 61 46 75 | contact@vivaltek.com

Mais qu'est-ce que c'est la « force brute » ?

Une attaque par « force brute » consiste à tester toutes les combinaisons possibles (par ex. de mots de passe) afin de se connecter à des services dans le but de **voler ou exploiter vos données.**

Comment fonctionne Brute Force Security ?

Le module « Brute Force Security » **évalue la robustesse des systèmes d'authentification** en testant différentes combinaisons de mots de passe et d'identifiants.

2 techniques possibles :

La « Force brute » classique qui teste plein de mots de passe sur un seul compte.

Le « Password spraying » qui teste un mot de passe sur plusieurs comptes.

Sur quoi s'appuie Brute Force Security ?

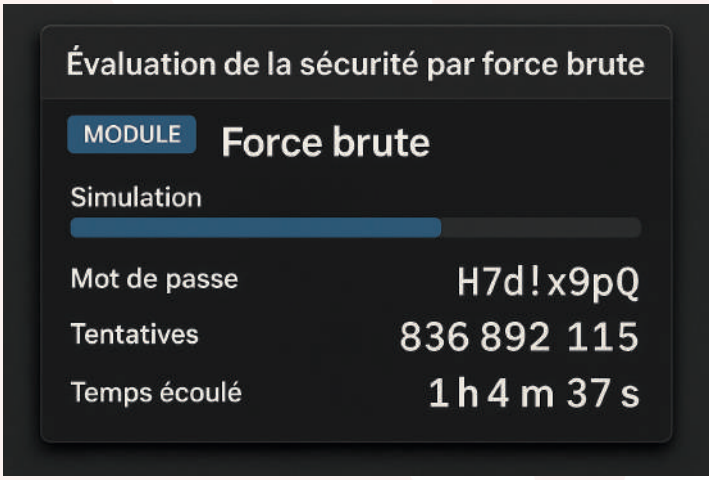
- Les dictionnaires, bases de données ou wordlists utilisés pour **tester de très nombreuses combinaisons** d'identifiants ou de mots de passe.
- Une **puissance de calcul élevée**, idéale pour accélérer le traitement des hashs locaux.
- Une **large capacité réseau** permettant de tester efficacement les services actifs tels que SSH, RDP[3], FTP, SMB ou encore HTTP Auth.

Pourquoi effectuer une simulation avec Brute Force Security ?

1. **Évaluer la solidité réelle** de vos **mécanismes d'authentification** et de vos **services exposés** (SSH, Telnet, RDP[1], portails web, Extranet, etc.).
2. **S'assurer de l'existence** et du **bon fonctionnement** des contre-mesures.
3. **Valider les contrôles de défense** mis en place et **détecter les failles types** (CAPTCHA, MFA, SIEM/SOC[2], Lockout, etc.).
4. **Évaluer la capacité de détection et de réaction** (SOC & MSSP[3]) : voir si le SOC reçoit l'alerte, et s'assurer qu'un ticket d'incident est ouvert automatiquement.
5. **Sensibiliser et former** les équipes en interne sur l'utilisation des **mots de passe faibles.**
6. **Répondre aux exigences de conformité** (ISO 27001, NIS2, ANSSI) via une **validation technique des protections** contre les attaques par « force brute » ainsi que des tests périodiques pour vérifier l'**efficacité des contrôles.**

Simulation avec Brute Force Security :

Évaluer la robustesse des accès, tester les défenses et la réactivité (SOC), former les équipes, et garantir la conformité aux normes via des tests réguliers.



Sur quelle fréquence évaluer votre système avec Brute Force Security ?

Afin de garantir un niveau de sécurité optimal et conforme aux exigences actuelles, **un audit externe de sécurité annuel constitue à minima une bonne pratique à adopter.**

Selon le niveau de sensibilité des activités de l'organisation et les exigences réglementaires spécifiques (finance, santé, assurance, etc.), cet audit externe peut être complété par des **tests de sécurité plus fréquents, réalisés de manière continue, mensuelle ou trimestrielle.** Ils permettent de maintenir une posture de sécurité active et réactive face à l'évolution constante des menaces.

Ces actions peuvent être menées sur un **large périmètre** exposé publiquement (infrastructure, applications, extranet) ou ciblées sur des comptes ou systèmes sensibles, selon les **priorités de l'organisation.**

Sécurisez votre activité, protégez vos partenaires et valorisez votre image.

Nous démontrons la solidité de vos accès face aux attaques automatisées et anticipons les failles de votre système avant qu'un cybercriminel ne les exploite.

Lexique

[1]**RDP (Remote Desktop Protocol) :** Protocole qui permet de prendre le contrôle à distance d'un ordinateur, en affichant son bureau comme si vous étiez devant, tout en transmettant les données de manière sécurisée.

[2]**SOC (Security Operations Center) :** Centre de sécurité qui surveille en temps réel l'ensemble des systèmes informatiques d'une organisation, afin de détecter, analyser et réagir rapidement aux cybermenaces.

[3]**MSSP (Managed Security Services Provider) :** Prestataire externe qui gère et surveille la cybersécurité d'une entreprise à distance, en fournissant des services comme la détection des menaces, la réponse aux incidents ou la gestion des pares-feux.

Consultez notre lexique complet à l'adresse suivante : https://vivaltek.com/lexique-complet

VIVALTEK
2, Impasse Johannes Gutenberg, Z.A Les Acacias III 85430 La Boissière des Landes
02 52 61 46 75 | contact@vivaltek.com