" Grow your business safely
"

"Nous avons un service d'excellente qualité : une équipe disponible et extrêmement compétente." **AMERSPORTS**

+33 1 58 56 60 80

Rechercher

CERBERHOST : LES ATTAQUES PAR « BRUTEFORCE » OU « FORCE BRUTE »

avril 2nd

philippe

Blog, CerberHost, Featured, Sécurité

aucun commentaire

Dans le cadre de la sécurisation d'infrastructures et d'accès, on ne soulignera jamais assez l'intérêt de l'usage de mots de passes solides. Toute la logique de ce conseil devient évidente une fois que l'on connaît l'existence de cette menace qu'est l'attaque par « bruteforce », et que l'on comprend son fonctionnement.

Le but est toujours le même : deviner le bon mot de passe en multipliant les tentatives.

Pour un résultat plus rapide, la technique est bien évidemment automatisée par des outils comme THC Hydra ou, pour le cas des vols d'authentifiant sur Icloud que nous avons pu voir récemment, par des outils comme iDict.

Il est possible de bruteforcer de très nombreux types d'authentifications :

- WiFi
- Compte utilisateurs sur des sites
- Login / password de boites email en POP3/IMAP

- Accès Shell ou FTP/SFTP
- Accès VPN
- etc…

L'attaque par dictionnaire

La principale méthode reste l'approche par dictionnaire.

En pratique, il est très simple de se procurer un dictionnaire de mot de passe potentiels. Il s'agit en réalité d'un document répertoriant des mots courants, ou des prénoms par exemple, sur lequel un pirate peut se baser pour lancer son attaque. Le dictionnaire de correction orthographique des OS comme Linux est une bonne base. Il existe un très grand nombre de dictionnaires disponibles en ligne :

- http://www.skullsecurity.org/wiki/index.php/Passwords
- http://www.insidepro.com/eng/download.shtml
- ftp://ftp.ox.ac.uk/pub/wordlists/
- etc.

Un bon dictionnaire est ciblé pour un pays et une langue, et potentiellement pour une catégorie d'utilisateurs. Beaucoup d'attaquants disposent d'ailleurs de dictionnaires ciblés pour des populations, avec les mots les plus utilisés, les prénoms d'enfants, les noms d'animaux domestiques, les combinaisons de dates de naissances, numéros de CB, de téléphone, de plaque d'immatriculations, etc…

Certains outils, comme ceux évoqués plus haut, vont d'ailleurs effectuer des attaques hybrides en combinant les possibilités, par exemple le prénom kevin et un numéro de date de naissance par exemple.

XKCD a parfaitement résumé le problème dans ce petit comic : http://xkcd.com/936/

Limiter les tentatives

Si le système attaqué n'impose pas une limitation sur les tentatives d'authentification, l'attaque par bruteforce peut prendre beaucoup de temps, mais elle a des chances non négligeables d'aboutir. Une défense pertinente consiste à mettre en place un nombre de tentatives maximum avant de désactiver le compte ou d'augmenter le temps minimum entre deux tentatives.

Bien que simple, cette approche de sécurisation permet de considérablement ralentir, voire de stopper l'attaquant dans ses tentatives. La longueur potentielle de l'attaque le découragera souvent et l'incitera à changer de cible.

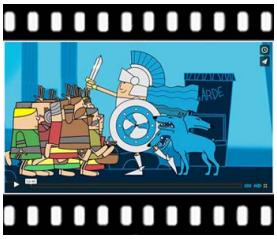
Dispositifs au sein de Cerberhost contre les bruteforce

L'un des outils que Cerberhost utilise pour se prémunir contre ces attaques est « Fail2ban » qui est un composant opensource qui va justement limiter les tentatives en trop grand nombre. D'autres mécanismes reportent à notre pare-feu, NAXSI. Ce dernier effectue un filtrage par réputation d'IP ; ainsi, les IP à l'origine de trop de tentative infructueuses seront bloquées.

Il est également conseillé de mettre en place une limitation du nombre de tentatives directement dans le framework ou l'outil utilisé.

Découvrir CerberHost

CerberHost protège contre toutes les failles du TOP 10 Owasp, les bruteforce, les overflows et bien plus.



Pour découvrir CerberHost en images, venez visionner sa vidéo de présentation : ICI

DÉCOUVREZ NBS SYSTEM

Notre société, fondée en 1999, est spécialisée dans la sécurité informatique, les audits de sécurité, l'hébergement de serveurs et de sites E-commerce (voir notre blog www.Ecommerce-Squad.com)

SOCIÉTÉ

- Nous contacter
- Qui sommes-nous ?
- Références client
- Recrutement