

Tutoriel Brutus

Soumis par PasswordOne
06-11-2010
Dernière mise à jour : 06-11-2010

Formation pour Brutus

Introduction

La force brute, est une technique de hacking consistant à cracker un mot de passe en utilisant un logiciel prévu à cet effet et qui se chargera pour son utilisateur d'essayer tous les mots de passe. Le plus connu de tous est sans aucun doute Brutus, et ce tutorial a pour but d'en expliquer les différentes options. Brutus permet de trouver un grand nombre de mots de passe de types: HTTP, FTP, telnet, SMB (NetBIOS) ou encore POP3. Pour éviter les répétitions il est possible de configurer Brutus afin qu'il fasse ses recherches via un Proxy.

Configuration du Proxy

L'utilisation d'un Proxy bien qu'elle ne soit pas obligatoire au fonctionnement de Brutus, reste tout de même fortement recommandée, cependant cette option entraîne souvent un gros ralentissement de la vitesse de recherche, ce qui pose souvent la problématique suivante : sécurité ou performance? Chacun fera son choix. Pour activer l'option de recherche via un Proxy procéder de la manière suivante :

1- cocher la case "Use Proxy".

2- cliquer sur "Define" pour régler les options du Proxy.

3- entrer les informations suivantes : Proxy Type: Laisser "SOCKS (v5)", dans Proxy Address, inscrire l'adresse IP de votre serveur Proxy, puis inscrire le port de votre serveur Proxy.

4- Si l'utilisation votre serveur Proxy nécessite un login et un mot de passe, cocher "Proxy requires authentication" et entrer le login et le password dans les cases appropriées.

Configuration des logins

Lorsque vous vous identifiez deux choses sont nécessaires : un login (nom d'utilisateur) et un mot de passe, pour permettre à Brutus de travailler, il va donc falloir lui indiquer le login dont vous voulez obtenir le mot de passe.

1- Si le serveur n'utilise pas de login (quasiment impossible, mais cette option a quand même été prévue), décocher "Use Username" et la configuration du login est terminée

2- Si vous connaissez le login (le cas le plus courant), cocher "Use Username", et "Single User", et inscrivez le login dans "UserID"

3- Si vous ne connaissez pas le login (cas rare mais qui peut se présenter), cocher simplement "User UserName" puis cliquer sur "Browse" pour sélectionner un fichier.txt contenant des logins. Brutus possède de plusieurs dicos par défaut, je vous conseille de créer les votre, un dico n'est ni plus ni moins qu'un simple fichier texte contenant des mots qui seront essayés par Brutus (soit lors du processus d'authentification: login, soit lors de l'attaque par Brute Force: password).

Configuration de Pass File et de Pass Mode

Plusieurs méthodes de recherche vous sont proposées, c'est ce que vous allez configurer avec l'option Pass Mode, et pour chaque méthode de recherche vous avez besoin d'un dico, c'est ce que l'option Pass File est à même de configurer. Il y a cependant une exception à cette règle qui va s'appliquer à la méthode Brute Force et qui sera abordée plus bas.

1-Utilisation de la méthode "Word List": cette méthode est personnellement celle que je préfère, elle consiste à laisser Brutus travailler sur un dico prédéfini contenant tous les mots de passe que l'on souhaite essayer.

2- Utilisation de la méthode "Brute Force": elle consiste à tenter toutes les combinaisons possibles à partir d'une chaîne de caractères : lettres minuscules, majuscules, nombres, et caractères spéciaux. Aucun dico n'est demandé lors du choix de cette méthode, mais le bouton "Range" à côté de "Pass Mode", va s'afficher, cliquer dessus, cette fenêtre va s'afficher :

2.1- sélectionner les caractères qui serviront à constituer les mots de passe que vous voulez essayer.

2.2- l'option "Min Length" permet de choisir la longueur Minimale du mot de passe (inutile par exemple de vouloir tenter un mot de passe de moins de 6 caractères lorsque vous savez qu'à l'inscription on vous en demande un minimum de 6 caractères, pour gagner du temps ce genre d'informations est précieux)

2.3- enfin dans "Max Length" sélectionner la longueur maximum du mot de passe.

3- Utilisation de la méthode "Combo", cette méthode est utile lorsque vous ne connaissez pas le login de votre cible et elle permet de ne pas être obligé de travailler sur deux dicos en même temps, car elle vous permet de réunir dans un même fichier texte un login et un mot de passe.

Exemple de combo : admin:pass

Récupération des mots de passe

Lorsque votre recherche est terminée et que celle-ci s'est avérée payante, vous devriez obtenir le mot de passe de votre "cible" dans la partie de Brutus intitulée "Positive Authentication Results"

Obtenir un mot de passe HTTP (Htaccess)

Parfois lorsque l'on souhaite accéder à un dossier ou à une page d'un site, il est possible de rencontrer la fenêtre ci-dessous :

Pour obtenir ce type de mot de passe il faut utiliser Brutus de la manière suivante :

1- Dans Type, sélectionner "HTTP (Basic Auth)".

2- Dans la case "Target", inscrire le site de votre cible sous la forme suivante: www.onecarlos.fr/nomdudossier/

3- Dans la partie "Connection Options", remplir le case ainsi : dans "Port", inscrire le port du server http (80 par défaut), laissez "Connections" et "Timeout" comme ils sont, ne rien changer dans "HTTP (Basic) Options" et finalement dans "Authentication Options", configurer le login et le Pass Mode et enfin cliquer sur "Start".

Obtenir un mot de passe FTP (File Transfert Protocol)

Pour obtenir le mot de passe d'un utilisateur sur un serveur FTP, la marche à suivre est la suivante :

1- Dans "Type" on sélectionner FTP.

2- Dans Target, mettre l'adresse IP ou le nom du server FTP. Un bon moyen de trouver l'IP d'un serveur FTP est d'utiliser la méthode suivante : Sous Dos (Cliquer Exécuter puis cmd) tapez ftp -n puis open ftp://www.votrecible.com/, et l'IP s'affichera.

3- Dans "Connection Options" laisser le port par défaut (21), et ce qui se trouve dans "FTP Options".

4- Régler le login et la méthode de Pass Mode et cliquer sur Start.

Obtenir un mot de passe E-Mail (POP3)

Voici la partie du tutorial qui m'a le plus demandé ces derniers temps, pour cracker le mot de passe d'une adresse mail, vous allez devoir suivre ces instructions :

1- Dans "Type", sélectionner POP3

2- Dans "Target" mettre le serveur POP3, une recherche sur Google vous fournira tous les serveurs POP3 que vous voulez. ATTENTION cette méthode sera inefficace sur les comptes mail de fournisseurs comme HOTMAIL pour la bonne et simple raison qu'il ne dispose pas de serveur POP3, il faut donc se rabattre sur le type HTML pour que cela soit efficace, pensez donc à effectuer une recherche avant de lancer votre attaque.

3- Dans les Options de connexion, on laisse le port par défaut (110) et on ne touche pas à "Connections" ni à "Timeout"

4- remplir le reste des options concernant le login et le "Pass Mode" comme indiqué précédemment.

5- On clique sur "Start" pour lancer l'attaque.

Obtenir un mot de passe Telnet

Pour obtenir un mot de passe Telnet, configurer Brutus de cette manière :

1- Dans "Type" sélectionner "Telnet"

2- Dans "Target" inscrire l'IP ou le nom du server (d'ailleurs expliqué de manière plus détaillée plus haut dans ce tutorial)

3- Dans les options de connexion, laisser le port par défaut (23), et ne rien changer à "Connection" ni à "Timeout", laisser ce qui se trouve dans "Telnet Options" par défaut.

4- choisir le login et la méthode Pass Mode comme expliqué précédemment.

5- Cliquer sur "Start"

Obtenir un mot de passe NetBios (SMB)

1- Dans "Type" on sélectionne SMB (NetBIOS)

2- Dans "Target" inscrire http:// + l'adresse IP de la victime + Son lecteur. Exemple : En imaginant que l'adresse IP de la victime est 255.255.255.255, que son lecteur est C dans "Target" vous écrirez: http://255.255.255.255/C

3- Dans les options de connexion on laisse le port 139 (Port par défaut de NetBIOS).

4- Dans les options SMB, cocher "Use NT" si vous utilisez NT et inscrire le domaine.

5- Dans les options d'authentifications, inscrire le login et indiquer la méthode de Pass Mode.

Cliquer sur "Start"

Fin de ce tutorial

Cet Article est issu de <http://www.ilyas-soft.net/brutus.html>