TUTORIAL BRUTUS

Introduction :

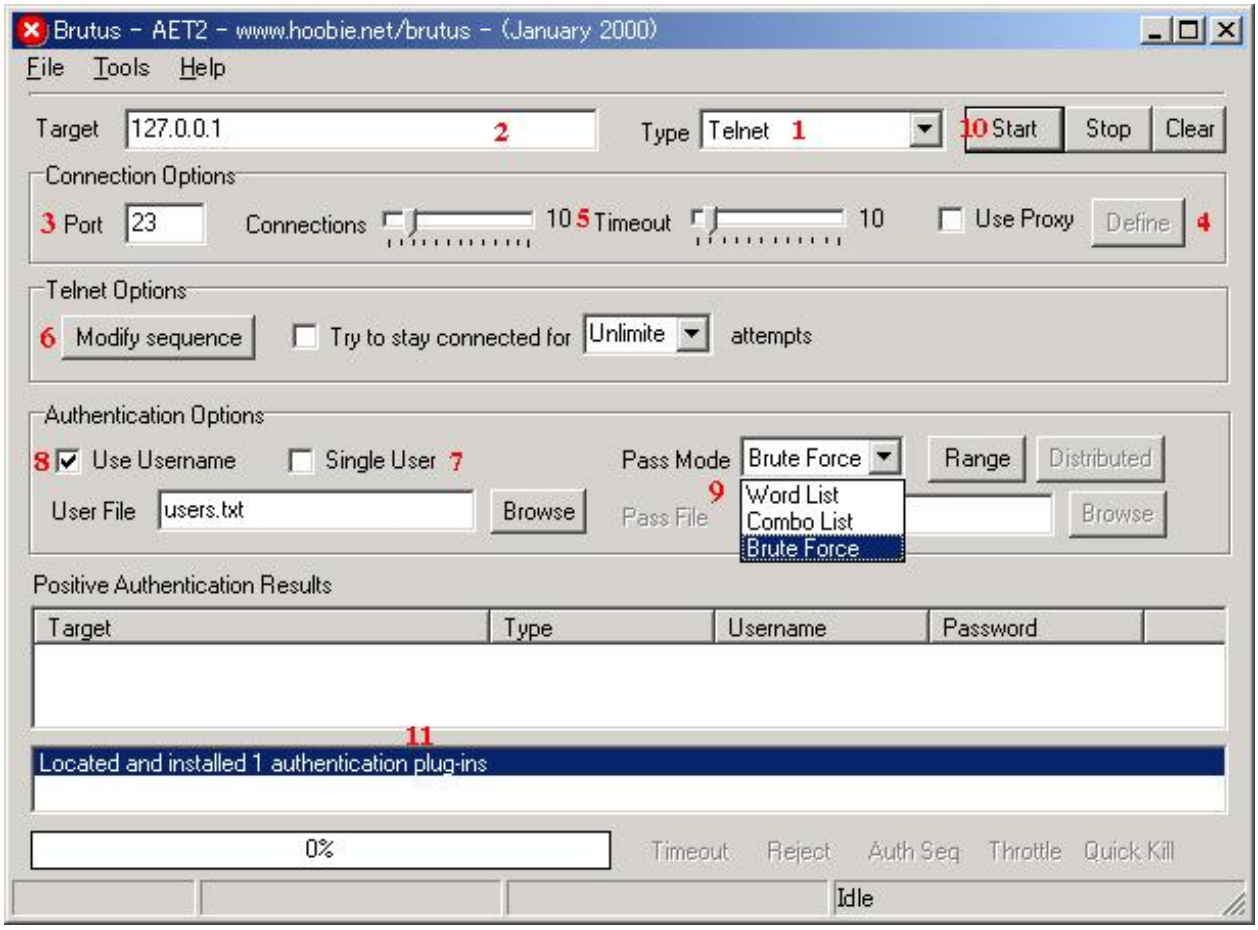
Bonjour et bien voila dans ce tutorial vous allez apprendre a brute-forcer un blog mais le principe marche aussi pour tous ce qui contient des mots de passe !!!!

Fonctionnement de brutus :

Brutus est un logiciel de brute force c'est-à-dire qui peut trouver les mots de passe de différents sites ou logiciels. Il utilise la méthode du brute force c'est-à-dire soit utiliser un dictionnaire soit utiliser la méthode d'incrémentation des caractères c'est-à-dire la suite de caractères.

Exemple : AA AB AC AD ……et ensuite …. AAA AAB AAC ….

TUTORIAL :



1 = Ici vous choisissez le type de "boite" que vous allez cracker
http (basic auth) : si le site utilise un system d'authentification basique (sans cgi).
http (from) : si le site utilise un system d'authentification avec cgi
FTP : pour cracker un password d'un FTP
POP 3 : pour cracker un compte mail (comme votre compte outlook par exemple)
TELNET : si le site est accessible par Telnet (donc le port 23)
SMD (Netbios) : Cracker la faille tellement connue du netbios (clique ici)
CUSTOM : pour personaliser l'ordre

2 = La c'est une étape tres importante, vous devez indiquer l'adresse de la cible, vous pouvez indiquer une IP ou une url de site (pas de redirections !...). Par exemple, si vous voulezšcracker un site multimania par ftp, vous devez placer dans target ftp.membre.lycos.fr. Si le site que vous voulez pirater est un site pro (donc pas d'adresse indicant l'hébergeur), vous devez tapper ftp.cible.com (ca peut varier mais je vais pas tout expliquer, à vous de réfléchir...)

3 = Connexion Option sert à définir le port que vous allez exploiter pour cracker le site. (21 pour ftp par exemple). Le reste c'est se qui va indiquer au programme le nombre d'essais qu'il va faire en cas de non réussite de la connexion. Laissez les valeurs qui sont indiquez, cette partie du programme n'est pas essentielle.

4 =Cochez use proxie sie vous utilisez un proxie, ensuite vous devez configurer ca en ouvrant "Define", indiquez l'ip du server proxy dans proxy address et le nœ du port dans proxy port. Les proxie vous permettent de brute forcer un compte de magnière un peu plus anonyme, toute fois il est préférable de prendre toutes ces précotions en spoffant correctement son ip (clique ici)

5 = ne changez rien à ces options tout se qui y est est tres bien.

6 =cette partie sert à configurer les options d'identification, il va falloir indiquer le pseudo du gars que vous allez cracker. (L'identifiant quoi !), Par exemple, si vous hacker un compte multmania avec une adresse http://membres.lycos.fr/gogo, l'identifiant sera "gogo". Ou pour un compte mail : gogo@domaine.com, l'identifiant sera "gogo".

7 =Cochez ici la case Single User, puis tappez en dessous l'identifiant. que vous venez de trouver

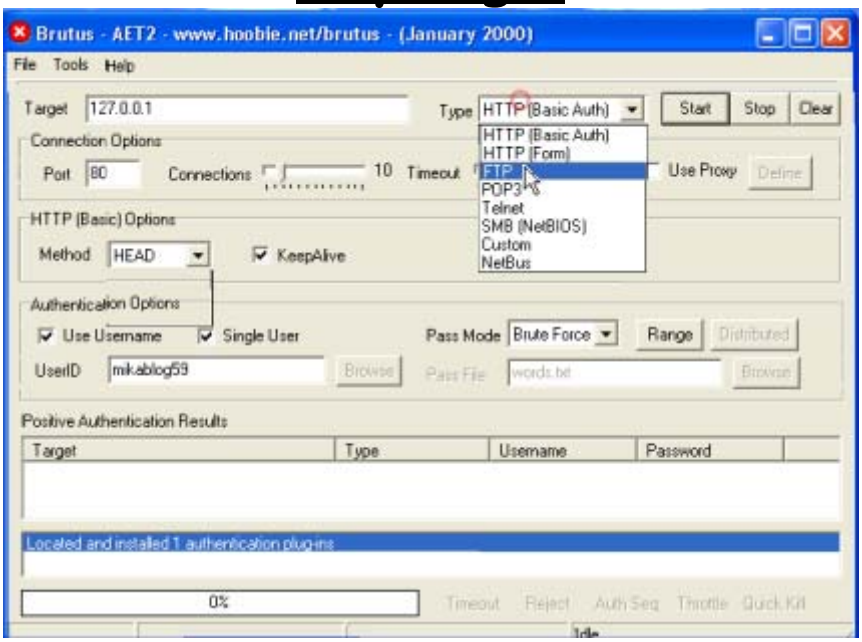
8 =Use username sert à... rien ! du moin je sais pas quoi ca sert donc laissez le comme ca et cochez la case sigle user comme cité ci-dessus.

9 = Maintenant il faut choisir le mode de cracking ! (très important !)
Word list : sélectionné cette option si vous voulez utiliser un dico, une liste de mots déjà préparé quoi ! (vous pouvez en télécharger sur les pages de download sur site)
Brute force : c'est la technique la plus utilisée, la plus bourinne aussi. Le principe est simple : le logiciel essaie des centaines de combinaisons, jusqu'à se qu'il trouve la bonne (comme cité plus haut, AA, puis AB, ... etc). Cette fonction est paramétrable (cliquez sur *range*), c'est à dire que vous pouvez sélectionner le nombre de lettre et de chiffres qu'il doit y avoir dans le mot. Essayez d'être le plus possible précis sur ces informations, car évidement plus vous laissez un large choix de combinaisons plus c'est long !...

10 = Cliquez sur start pour commencer...

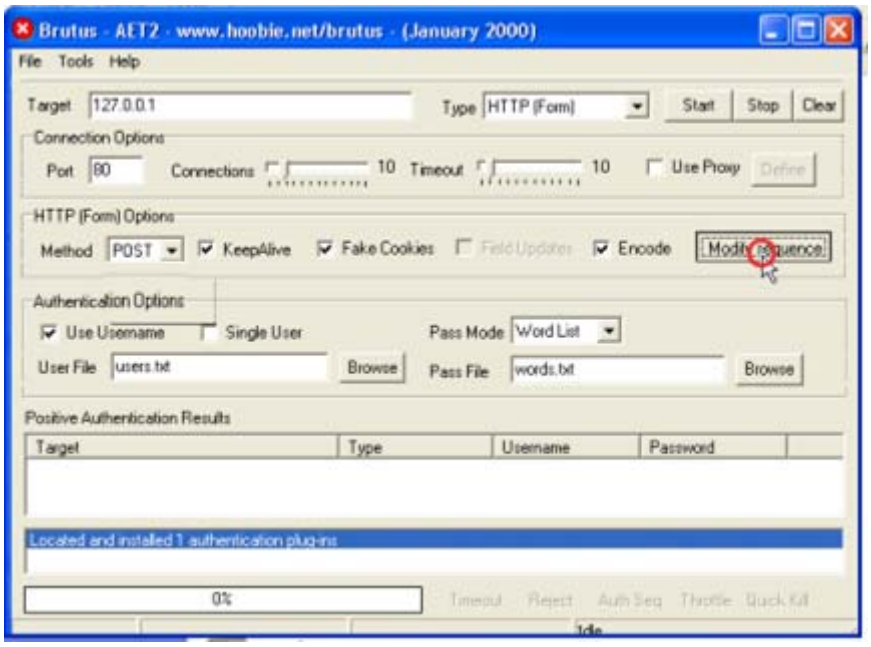
11 = Ici seront détaillés toutes les opérations que Brutus va mener !

Prenons l'exemple de brute forcé un Skyblog :

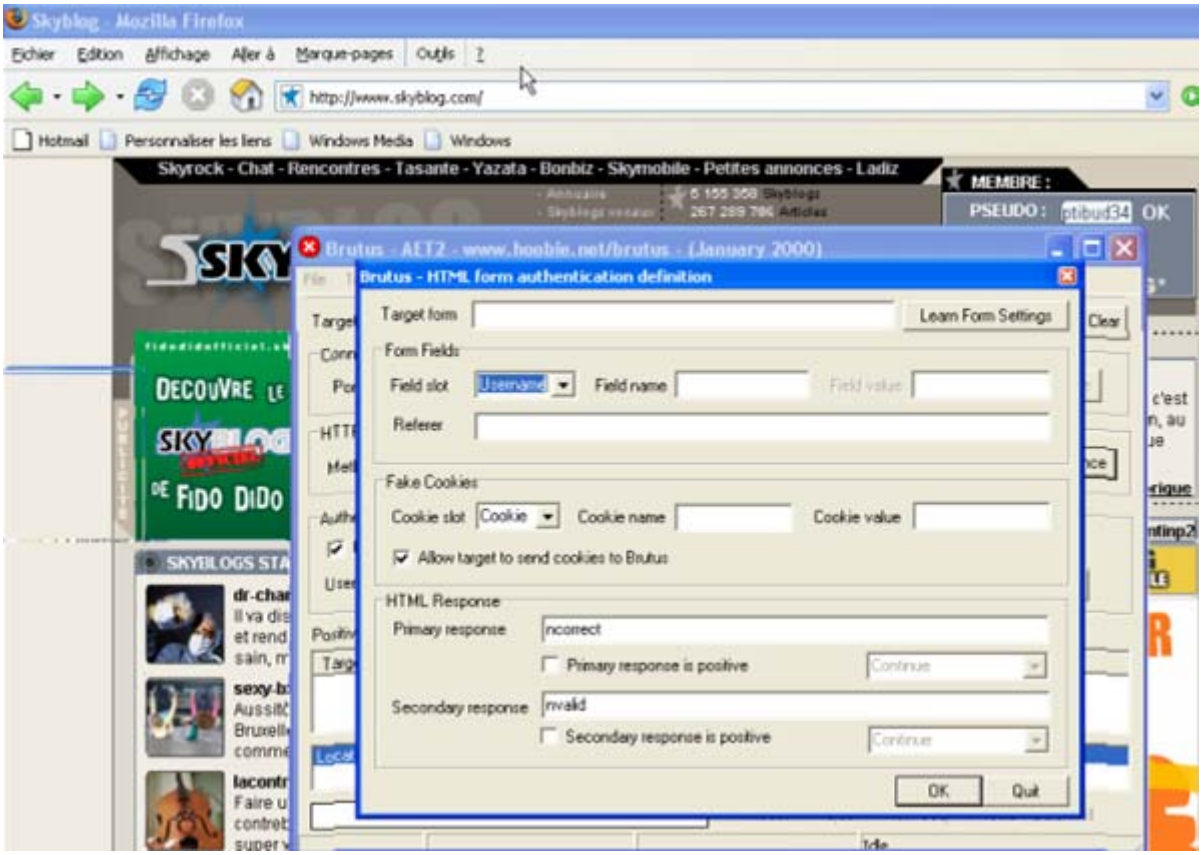


Pour Brute-Forcer un skyblog il faut cocher la case http(From)

Le Port utilisé est le port 80 pour les pages HTML et le http (form) option Méthode est POST puis cocher les cases KeepAlive et fake cookies mais pour les skyblog il n'y a pas besoin des cookies car on peut essayer son passe autant de fois que l'on souhaite tandis que MSN par exemple a besoin des cookies pour brute forcer un passe MSN.



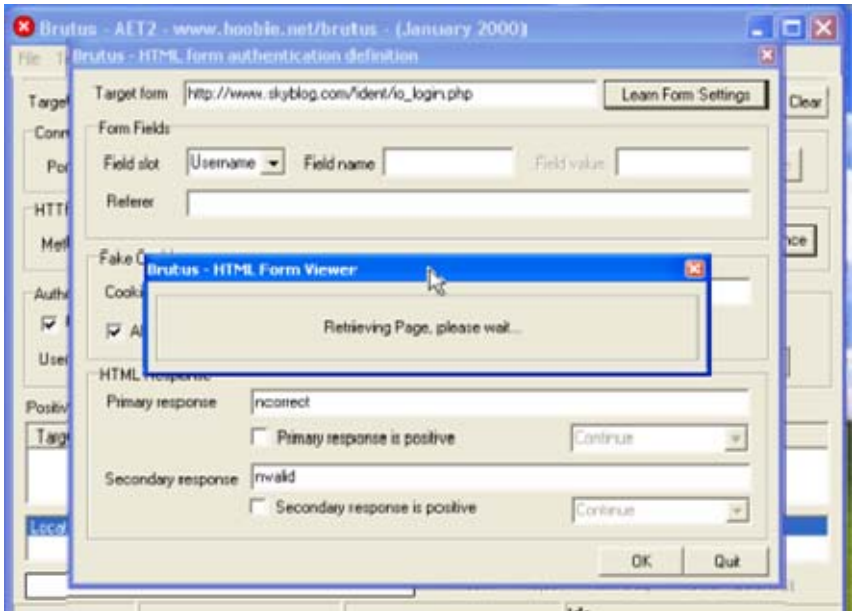
Puis ensuite faire Modify sequence



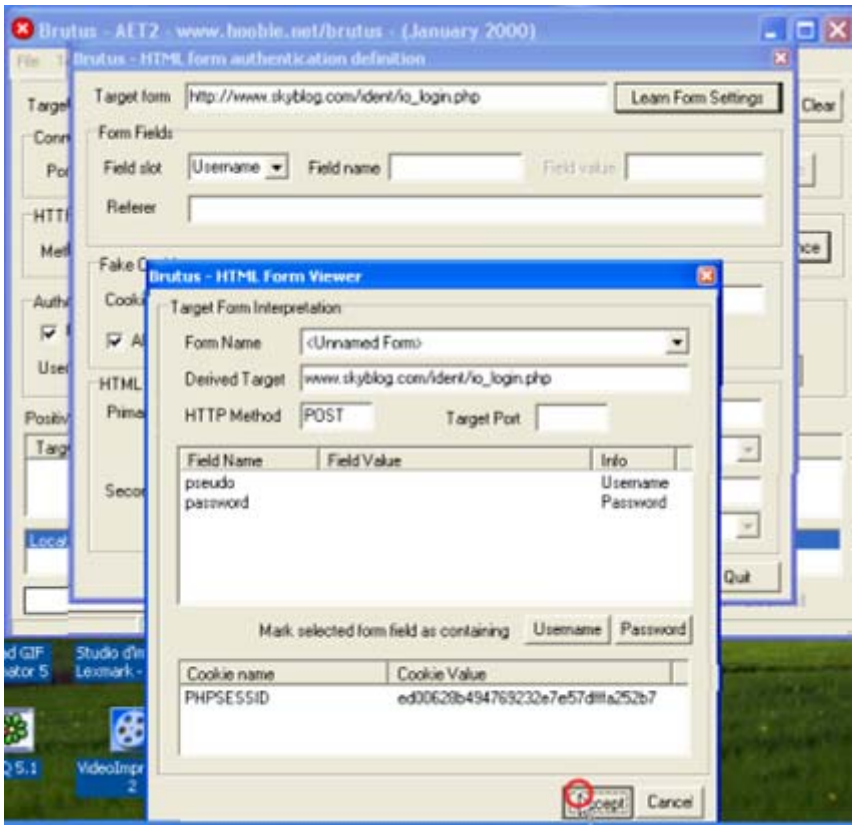
Allez sur la page http://skyblog.com et afficher le code source et rechercher le code :

`/ident/io_login.php`

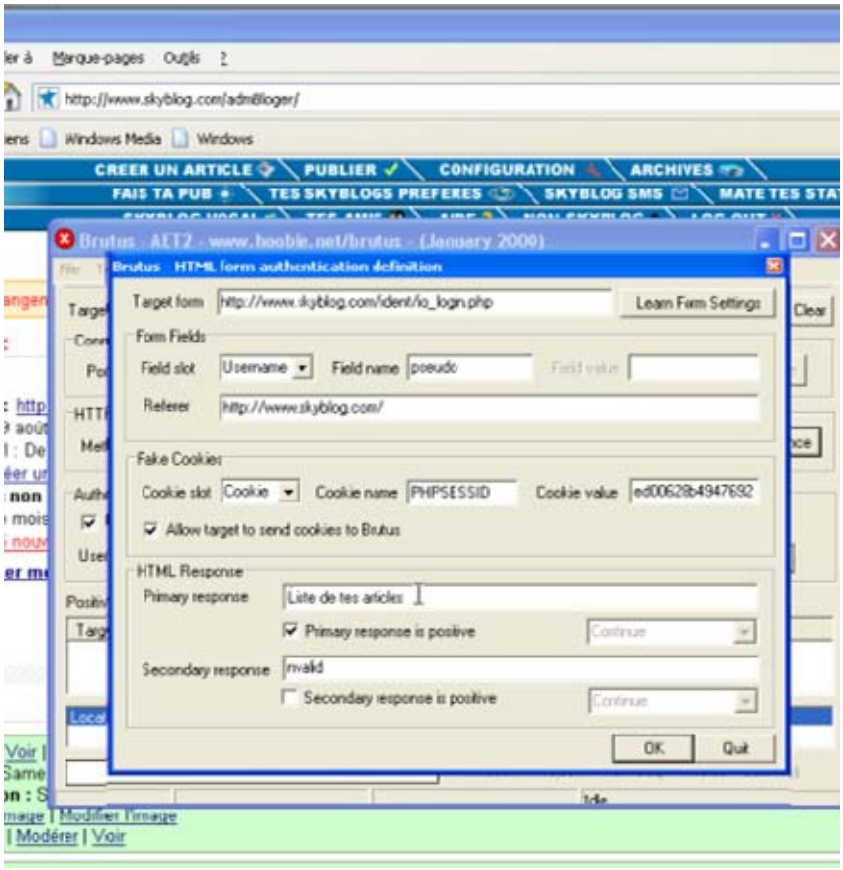
Et copier le code avec devant http://www.skyblog.com/ident/io_login.php



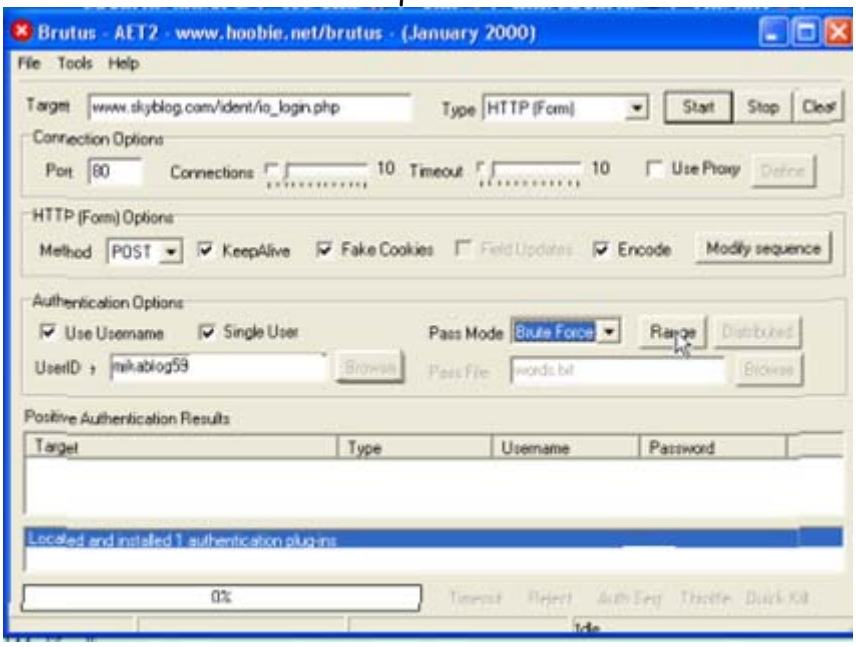
Cliquer sur Learn From Settings



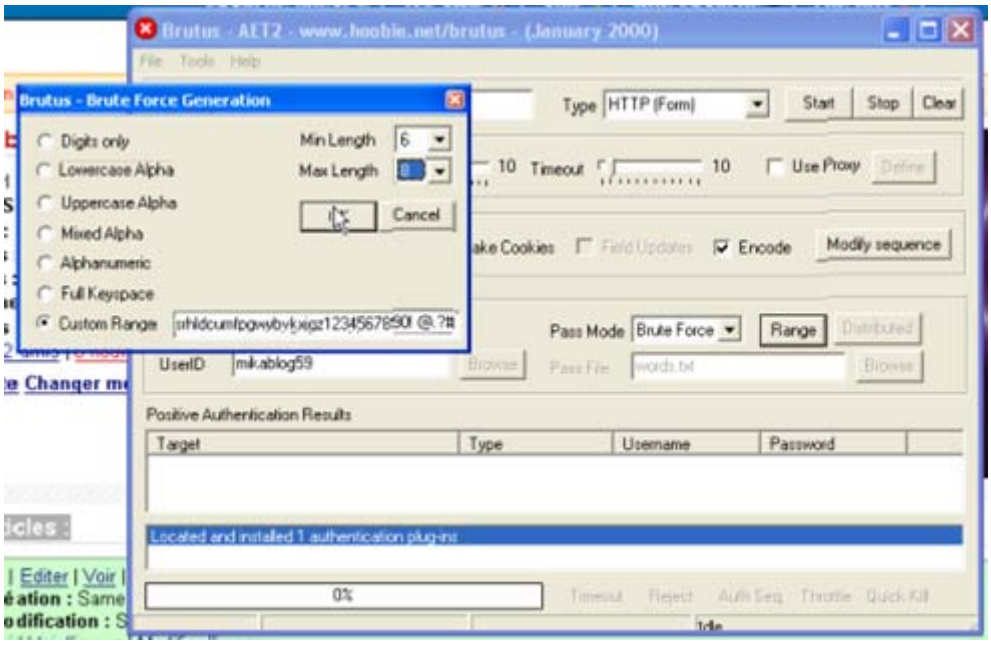
Cliquer sur le pseudo et cliquer sur USERNAME
Cliquer sur password et cliquer sur PASSWORD
Puis faire ACCEPT.



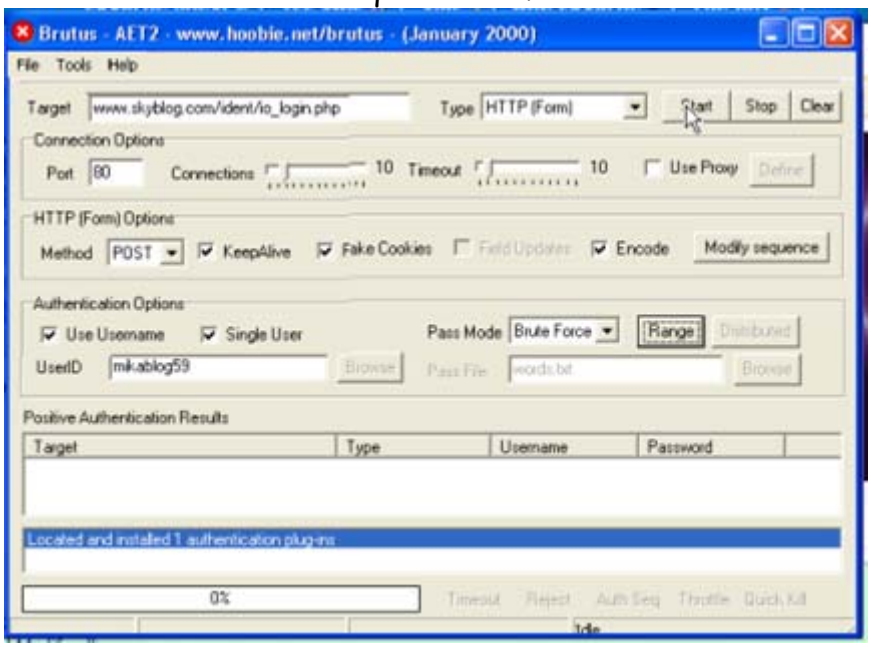
Ensuite dans Primary reponse écrire « Liste de tes article »
Cela pas arrêter la recherche de mots de passe sitôt qu'il va arriver a cette phrase.
Puis cliquer sur OK



Cocher les cases Use Username et Single User
Entrer le UserID qui est le pseudo du type qui a le skyblog
Puis choisir la méthode brute Force er cliquer sur RANGE.



Ensuite cliquer sur Custom Range comme sa il effectura une recherche avec tous les caracteres puis en MIN Length mettre 6 et en MAX Length 8
Ce qui permet de régler le nombre de caractere MINI ET MAXI
Cliquer sur OK



Ensuite cliquer sur START et hop la recherche est lancée voila il ne manque plus qu'a attendre des fois cela peut être très long mais c'est le moyen encore le plus fiable vous pouvez aussi régler les fonctions connections et Timeout pour que le logiciel cherche les mots de passe plus rapidement !!!!

Autres options

Cracker un Htaccess :

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

2- Dans la case "Target", inscrire le site de votre cible sous la forme suivante: www.nomdusiteacraker.com/nomdudossier/
*pensez à scanner l'arborescence avec intellitamper ou un autre scanner
3- Dans la partie "Connexion Options", remplir le case ainsi: dans"Port", inscrire le port du serveur http :80

mot de passe E-mail (POP) :

1- Dans "Type", sélectionner POP3
2- Dans "Target" mettre le serveur POP , pense à vérifier qu'il existe

Cracker un pass Telnet :

1- Dans "Type" sélectionner "Telnet"
3- Dans les options de connexion, laisser le port part défaut (23)

Cracker un pass NetBios :

1- Dans "Type" on sélectionne 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
4- Dans les options, 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 crack.

Voila tutorial terminer si vous avez des questions n'hésiter pas à m'envoyer un EMAIL à

Hack71@hotmail.fr