Date: Lundi 04 octobre 2004 à 18:55:16
Sujet: 3 Sécurité et Hacking

Attaque par proxy avec le cracker par brute force, Brutus Aet2

Utilisez Brutus Aet2 pour cracker les mots de passe

Dans ce tutorial nous utiliserons un technique du Brute Force. Selon certaines rumeurs, quelques hébergeurs détecteraient les attaques de Brute Force et ils banniraient les personnes identifiées et en cas de récidive certains hébergeur vous dénoncerait a votre FAI. Les informations ci-dessous ne sont publiées qu'a titre purement informatif. Les tentatives d'intrusions dans un système (qu'il soit protégé ou non) sont sévèrement punies par la loi.
Le logiciel :
Nous allons utilisé Brutus Aet2. Ce logiciel est un cracker de mot de passe tout protocoles et il contient la fameuse fonction : la Brute Force.
Vous pouvez effectuer une attaque par brute force sur un de vos propres serveurs pour tester la résistance et la qualité de vos mots de passes.
Vous allez également vous rendre compte que le Brute Force est très très long, c'est pourquoi cette technique n'est pas réellement efficace.
Dans un avenir plus ou moins lointain avec les ordinateurs quantique, cette technique de crackage des passwords reviendra peut être en force mais pour l'instant elle ne peut servir qu'a casser dans des délais courts des mots de passes très simple (exemple : 535462 ou azerty)
PROXY
Voila pour vous masquez, nous allons utiliser MULTIPROXY (Telechargez le ici). Il nous faut aussi une liste de proxy. Donc apres avoir téléchargé le logiciel, dezipper-le, installez-le et executtez le. 1) installer MultiProxy Il vous faut encore télécharger une liste de proxy anonymes afin de pouvoir utiliser ceux-ci. Cliquez sur le lien ci-dessous avec le bouton droit de votre souris et choisissez "Enregistrer la cible sous...". Enregistrez le fichier "Proxy.txt" dans le répertoire où vous avez installé MultiProxy. Si vous ne savait pas ou vous l'avez installé aller dans "C:/Program Files/Multiproxy".
Téléchargez une liste de proxies anonymes (fichier .txt) 2) configurer votre logiciel de navigation

Maintenant il va falloir configurer votre navigateur pour qu'il ne se connecte plus directement au Web mais qu'il passe automatiquement par le biais de MultiProxy. Internet Explorer 5 :

Allez dans le menu Outils>Options Internet puis

choisissez l'onglet Connexions. Cliquez sur Paramètres dans "Options de numérotation" pour une connexion classique (56K) ou "Paramètres du réseau local" pour une connexion ISDN, câble ou ADSL (128, 256 ou 512K). Cochez le case "Utiliser un serveur proxy".

Dans la partie Adresse, notez : 127.0.0.1

Dans la case Port, notez : 8088

Cliquez sur le bouton "Avancés" et cochez la case "Utiliser le même serveur proxy pour tous les protocoles."

Ensuite cliquez sur OK pour valider les parametres.

Netscape 4 :

Allez dans le menu Edition/Préférences. Dans la partie gauche de la fenêtre ainsi ouverte, cliquez sur la case "Avancé". Choisissez ensuite "Proxies ", "Configuration manuelle de proxy" et cliquez sur le bouton "Voir".

Dans la partie Adresse, notez : 127.0.0.1

Dans la case Port, notez : 8088

Ensuite cliquez sur OK pour valider les parametres.

3) configurer MultiProxy

Executez MultiProxy. Vous devriez voir un écran qui ressemble à ça : Pendant quelques instants, le programme va tester automatiquement les proxies pour lesquels il est configuré par défaut. Attendez qu'il ait fini, il y a 7 proxy configurer par default donc cela devrait etre rapide. Quand l'écran devient blanc cela veut dire que c'est fini. Sur la fenetre principale il y a différentes options :

- Connection status : Cette fenêtre montre en temps réel les proxies utilisés par votre navigateur lorsque vous consultez une page Web.
- About : La version et l'auteur de MultiProxy. L'equivalant de "A propos de" en francais.
- Options : Les options de configuration. Nous allons voir ça plus bas.
- Check all proxies : En francais "Vérifier tous les proxy". Lorsque le programme est configuré par défaut il vérifit à son lancement que tous les proxy pour lequel il est configuré sont bien opérationnels, il en profite également pour les classer en fonction de leur vitesse. Si vous cliquez sur ce bouton, il effectuera une nouvelle vérification.
- Update proxy list : Lance votre navigateur et ouvre la page Web de l'auteur qui propose une liste mise à jour de proxy. Faites une mise a jour environ tout les mois car beaucoup de proxy s'arrete de fonctionner et de nouveau apparaisent.
- Close : Fermer le programme.

En pressant le bouton "Annulez" vous minimiserez seulement le programme dans la barre des tâches. Passons maintenant aux choses sérieuses. Cliquez sur "Options". Nous n'allons pas passer en revue toutes les options possibles, mais seulement les plus intéressantes...

- Dans la rubrique "Connect via", assurez-vous que la case "Anonymous proxies only" ("N'utiliser que des proxies anonymes") est bien cochée. Si elle n'est pas cochéez vous ne serait pas anonyme.
- Dans la rubrique "Test anonimity via" ("Tester l'anonymat"), assurez-vous aussi que la case " Connect back..." ("Répondre à mon ordinateur par le biais du port...") est bien cochée.
- Verifiez aussi que "Test all servers..." ("Tester les proxies au lancement du programme"), " Autosort..." ("Trier les proxies en fonction de leur vitesse") et "Next fastest..." ("Utiliser les proxies dans l'ordre de leur classement") soient également cochées.
- Notez le chiffre 20 si vous avez une connexion ADSL (256k ou 512k), sinon pour les connections 56k et 128k inscrivez 8 dans la case "Max simultaneous connections" ("Nombre maximum de connexions simultanées" susceptibles d'être gérées par le logiciel pour télécharger, par exemple, les éléments composant une page web) et 10 dans la case "Default Timeout" ("Durée limite" au-delà de laquelle un proxy qui ne répond pas sera considéré comme ne fonctionnant pas).
- L'option "Maintain fixed proxy/IP per web-site" ("N'utiliser qu'un seul proxy/IP par site web") est à cocher si vous rencontrez des difficultés à afficher certains sites. En effet, il arrive que des serveurs refusent de fonctionner si vous changez d'adresse IP de manière aléatoire comme le permet MultiProxy. Maintenant, cliquez sur l'onglet "Proxy servers list". Cliquez sur le bouton "Menu ", choisissez l'option Files/Import proxy list. Double-cliquez sur le fichier Proxy.txt que vous avez téléchargé tout à l'heure. Voilà, votre liste de proxy c'est agrandit. Maintenant, il va falloir tester et l'épurer les proxy. Cliquez à nouveau sur le bouton "Menu", choisissez l'option Proxy list/Test all proxies. Laissez le programme travailler jusqu'à ce qu'il ait fini (cela peut prendre quelques minutes). Revenez dans Options/Proxy servers list et ensuite, cliquez à nouveau sur le bouton "Menu". Sélectionnez alors, une à une et successivement, les options suivantes :

1) Proxy list/Delete non responding (a pour effet de supprimer les proxies qui n'ont pas répondu pendant la phase de test).

2) Proxy list/Delete non-anonymous (a pour effet de

supprimer les proxies qui ne se sont pas révélés "non transparents" pendant la phase de test).

3) Proxy list/Delete duplicate servers (a pour effet de supprimer les proxies "en double").

4) Proxy list/Get host names for all IPs (a pour effet d'enregistrer les "noms d'hôtes" des serveurs proxy afin d'accélérer votre connexion). Attendez quelques instants que le programme ait fini de travailler. A partir de la version 1.0, vous pouvez cliquer avec le bouton droit de votre souris sur la liste de proxy afin de faire apparaître les diverses options du bouton "Menu". Voilà, maintenant, la seule contrainte lorsque vous voudrez surfer, consistera à lancer MultiProxy avant votre logiciel de navigation. MultiProxy mettra toujours un certain temps à tester touts les proxy avant d'être opérationnel. Mais, c'est bien peu de choses pour pouvoir surfer anonymement... Quand vous voudrez surfer "normalement", il vous suffira de décocher l'option "utiliser un proxy" dans votre navigateur et vous n'aurez alors pas besoin de lancer MultiProxy. Pour ceux qui ont des firewalls ou des anti-virus ayant cette fonction :

Vos logiciels pare-feu doivent permettre à MultiProxy de communiquer librement. Ainsi, avec ZoneAlarm, vous devrez autoriser le logiciel à fonctionner en "serveur" (ne vous inquiétez pas, le risque n'est pas grand). Avec un firewall "à règles" (ex.: AtGuard, BlackIce, etc.), pensez à autoriser les connexions entrantes et sortantes de MultiProxy, sinon rien ne fonctionnera.

Si, alors que vous utilisez MultiProxy, vous vous rendez sur un site de test de sécurité (ex.: www.grc.com), l'adresse IP qui apparaîtra ne sera pas la vôtre, mais celle d'un des proxies choisi par MP. Pas de panique, donc, si le test fait apparaître de drôles de failles de sécurité... Ce n'est pas votre ordinateur qui aura été testé, mais celui d'un proxy.

Attention : Certains proxy refuseront de se connecter à des sites a contenu pornographique. En effet, ils sont configurés pour protéger les jeunes internautes et vous devrez alors "actualiser/rafraîchir" votre navigateur pour que ces sites s'affichent.

Publication de Tout sur l'informatique - Programmation C#, Sécurité, Divx, P2P:
http://www.zmaster.fr

URL de cette publication
http://www.zmaster.fr/modules.php?name=News&file=article&sid=7