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 ADet ensuite AAA AAB AAC

🗙 Brutus - AET2 - www.hoobie.net/brutus - (January 2000) - 🗆 × File Tools Help Target 127.0.0.1 Type Telnet 1 0 Start -Stop Clear 2 -Connection Options Connections Use Proxy 3 Port 23 Define 4 Telnet Options Try to stay connected for Unlimite - attempts 6 Modify sequence -Authentication Options 8 🔽 Use Username Single User 7 Pass Mode Brute Force 🔻 Range Distributed Word List User File users.txt Browse Browse Combo List Brute Force **Positive Authentication Results** Username Password Target Туре Located and installed 1 authentication plug-ins 0% Timeout. Reject Auth Seq Throttle Quick Kill Idle

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 <u>ici</u>)
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 <u>ftp.membre.lycos.fr</u>. 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 <u>ici</u>)

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 !

TUTO BY POLUX-01

<u>Prenons l'exemple de brute forcé un</u> <u>Skyblog :</u>

Farget 127.0.0.1 Connection Options Port Port 80 Connections HTTP (Basic) Options Method Method HEAD	Type	HTTP (Basic Auth) HTTP (Basic Auth) HTTP (Form) POP3-K Telnet SMB (NetBIOS) Custom NetBus	Use Proxy Deline
Authentication Options	Pass Mo Browse Pats File	de Brute Force 💌	Range Distributed
ositive Authentication Results Target	Туре	Usemame	Password
Localed and installed T authentication plug-ins			

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

Connection Options Port BO Connections To Timeout To Timeout To Use HTTP (Form) Options Method POST Receptore KeepAlive Fake Cookies Fake Cookies Fake Updates Fake Cookies Receptore Recep	Proxy Deline Modify sequence
HTTP (Form) Options Method POST V KeepAlive V Fake Cookies I Field Updates V Encode Authentication Options V Use Username V Single User Pass Mode Brute Force Range	Modily sequence
Authentication Options	
	Distributed
UserID [mikablog59 Browse] Pass File [words.ht	Biowne
ostive Authentication Results	
Target Username Passwo	rd

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.

Target 127.0.01	Type HTTP (Form)	• Start	Stop Charl
Port 80 Connections 7 10 Tr	meout 7	T Use Prosp	Defice
HTTP (Form) Options Method POST V IV KeepAlive IV Fake Cookie Authentication Options	a 🗖 FelóUpdates 🔽	Encode Mod	(Quence)
Use Usemanne Single User User File users tot Browse	Pass Mode Word List Pass File words.bit	<u> </u>	Browse
Positive Authentication Results			
Target Type	Usemame	Paseword	

Puis ensuite faire Modify sequence

Echler Edition Affichage Afler à Morques	ages Outle 2	
Distanal Differencesiar in terror Difference	e Maria 🗋 Werkur	
Skyrock - Chat - Renconti	es - Tasante - Yazata - Bonbiz - Skymobile - Petites annonces - Ladiz	* MEMBRE:
Conception in the second	- Skyblings verdaus 7 267 269 766 Anticlea	PSEUDO: stibud34 OK
SKA	tus - AET2 - www.hoobie.net/brutus - (January 2000) Brutus - HTML form authentication definition	
Targe	Target form	Learn Form Settings Clear
DECOUVRE LE Por	Form Fields Field slot Field name Field name Field value	c'est
	Referer	n, au Je
PE FIDO DIDO	Fake Cookies Cookie slot Cookie name Cookie slot Cookie value	rique ntinp2
dr-char	Allow target to send cookies to Brutus HTML Response	<u>i</u>
II va dis et rend Positiv sain, m Tato	Primary response Incorrect	R
Aussit Provide	Secondary response mail	
comme Locat	Secondary response is positive	
Faire u contret		

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

90	Target form http://w	www.skyblog.com/lident/io_login.php	Learn For	m Settings
nn ² of	Form Fields Field slot	me 💌 Field name	Field value	
T	Helerer			
e1	Fake C Brutus - HT	ML Form Viewer		
the	Cooki	K		
1	R A	Retrieving Page, please wait		
e	HTML			
έν.	Primary response	ncorrect		_
12		Primary response is positive	Continue	7
	Secondary response	rwald		
		The second secon		

Cliquer sur Learn From Settings

I arget ton	m http://www.skyblog.com	Vident/io_login.php Learn Form Settin
Form Field	da	
Field slot	Usemane 💌 Field n	ame Field value
Referer		
Fake	rutus - HTML Form Viewe	* 8
Cooki	Target Form Interpretation	
₩ A	Form Name CUrna	med Form>
HTML	Derived Target www.sk	kyblog.com/ident/io_login.php
Prima	HTTP Method POST	Target Port
	End Name	Oldan Linte L
Secon	pseudo Pien	Username
	paraword	Password
		-
		Qui
	Mark selected	form field as constaining Username Passaged
Studio d'in	Fran Jakons	
Lexmark -	Cookie name	Cookie Value
	PRP3E3510	egulub20043476323287e57dillb23257

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

Mindaue		per/	
	: Media 🛄 Windows		
CR	AIS TA PUB	ES SKYBLOGS PREFERES	SKYBLOG SMS
	CHARLOC HOCAL	V TER ALLE	
9 Brut	us AETZ - www.ho	obie.net/brutus - (Jenuery 200 Absolication deficition	
-	Turnet from Dame 2 to	underhand an Edited for Just also	
Targe	Target form [http://ww	ww.wyolog.com/ident/io_logn.php	Learn Ferm Settings
Core	Form Fields	-	-
Por	Field slot Useman	e · Field name preudo	Field value
HTT	Referer http://w	ww.skyblog.com/	
Met			
	Fake Cookier		· · · · · · · · · · · · · · · · · · ·
Auto	Cookie slot Cookie	Cookie name [PHPSESSID	Cookie value ed00628b4947692
R	Allow target to se	nd cookies to Brutus	
User	HTML Response		
10.000	Primary response	Liste de tes aricles 1	
Packin	1.	Primary response is positive	Contrue 2
Positiv		the state of the second se	1
Positiv		Law and the	
Positiv	Secondary response	Invald	
Positiv Targ	Secondary response	Invald C Secondary response is positive	Contrue
Positiv	Secondary response	Invald	Continue 🕑

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

and the second se		The second second second		
arget www.skyblog.com/ident/io_login.	php	Type HTTP (Form)	 Start S 	top Cle
Port 80 Connections	10 Ti	meout []	Use Progr	Defee
HTTP (Form) Options Method POST • F KeepAlive	🖙 Fake Cooki	n 🗖 FeldUpdaws 🛛	Encode Modily	sequence
Authentication Options		Pass Mode Blue Force	Barge Dire	land
UserID + mikablog59	Browns	Pass file words bit		00120
ositive Authentication Results				
Target	Туре	Usemame	Password	

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.

de Modily sequence	ield Updates 😰 Encode	ity_Cancel ake Cookie	C Uppercase Alpha C Mixed Alpha C Alphanumeric
Biolive	de Brute Force Range words.tet	ldcum/pgwsbyljxigz12345678501@.7# D. [mikablog59Browse	Full Keyspace Custom Range uhldcum/powsb UserID mikable Changer me
		e Authentication Results	Positive Authenticati
assword	Usemame Passw	Туре	Target
assword	Words bit	D [mkablog59 Browse] e Authentication Results et Type	Changer me Positive Authenticati Target

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

trant Junan skublen com/ident/in loan	oho	Tune HTTP (Form)	- Start Stor	
ager [mm.squog.com.oenno_ogr.	huh	(Mar Lance & and	-12- 1 suit	
Port 80 Connections	10 Tr	meout []	Use Proop	eñee
ITTP (Form) Options				
Method POST . KeepAlive	Fake Cookie	n 🗖 Field Opdates 🕞	Encode Modily se	quence
Authentication Options			-	
🔽 Use Usemane 🛛 🔽 Single User		Pass Mode Brute Force	Range: Dimitizu	(ed)
UserID mikablog59	Browse	Paul File [words.bd	Brot	49.0
silive Authentication Results		1000		-
and a second		1 leave ame	Parmind	1

Ensuite cliquer sur START et hop la recherche est lancée voila il ne mangue 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 !!!!

<u>Autres options</u>

<u>Cracker un Htaccess :</u>

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

2- Dans la case "Target", inscrire le site de votre cible sous la forme suivante: <u>www.nomdusiteacraker.com/nomdudossier/</u>

*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