



# Hamster : Outils de BackTrack

Réalisé Par :

**M. Sofiane BERABEZ** 

Master II RIP Décembre 2011

### 1. Sidejacking avec Hamster et Ferret :

*Sidejacking* est une méthode passive de reniflement (sniffing) des cookies, puis de les rejouer contre les sites Web pour cloner une session (Gmail, Facebook ou autre) d'une victime. On utilise le terme «sidejacking» pour distinguer cette technique de l'attaque de *type man-in-the-middle*.

L'avantage de cette méthode est que la victime ne sera pas en mesure de constater si leurs cookies ont été volés.

Pour l'utilisation de hamster avec succès il faut d'abord respecter certaines conditions :

- La première c'est que la victime utilise une connexion ouverte, (exemple : connexion sans fil dans un café), on peut donc écouter passivement les cookies dans ce réseau.
- La seconde est que les cookies utilisés pour identifier la session de la victime ne sont pas crypté par le serveur web.

### 2. Outils Utilisés :

**Comment Sidejacking avec Hamster et Ferret** : dans ce qui suit on va faire un tutoriel sur l'utilisation d'un outil dans *BackTrack 4* qui est le *Hamster* pour accéder à un compte d'une victime qui est sur le même réseau sans connaitre son nom d'utilisateur et mot de passe par un simple vol de cookies en ouvrant les deux paramètres du **Hamster** qui sont *Ferret & hamster* tout en les localisant.

- Hamster agit donc comme un serveur proxy qui remplace vos cookies avec les cookies de la session de la victime c-à-d réécrire les cookies pour le compte de l'attaquant, hamster manipule toutes les données qui ont été récupérées par Ferret.
- Ferret (sniffer) analyse les paquets HTTP. Cet outil utilisé pour récupérer des cookies d'une session, il s'exécute au background d'un processus pour la capture des cookies de session qui transitent via un réseau.

**Backtrack :** Dans cette démonstration nous utilisons Backtrack 4 qui est une distribution linux tournant sur un Live CD qui permet de faire des tests de sécurité sur son réseau.

### 3. Lancer Hamster:

On ouvre le Shell, D'abord on localise Hamster dans pentest/sniffers/hamster/

On lance la commande **./hamster** comme le montre la figure suivante et on remarque bien que navigateur doit être configurer avec un proxy sous l'adresse **1270.0.1** et le port **1234** 

## Projet Sécurité Informatique

### Hamster



Fig 1: Exécution de Hamster

### Configuration de Firefox : Dans Firefox :

Aller dans le menu Edit -----Preferences

- 1. Puis sélectionnez le bouton Advanced et ensuite Network
  - Sélectionner Configuration Manuelle du proxy
  - Saisir ce HTTP Proxy: 127.0.0.1 et le Port: 1234
  - > Cocher Utiliser ce proxy pour tous les protocoles cliquer sur ok.

On doit avoir un écran comme ci-dessous :

0	Welcome	To Backtrack 4 - Con	nmercial -	Mozilla F	irefox	_	
<u>F</u> ile <u>E</u> dit ⊻iew <mark>100</mark> [6	1	Firefox Pref	erences			×	2 <sup>4</sup> 4 0 10 0 10
🔶 🔶 🖉 🦳	¢10		F		Ö	pogle	0
BackTrack Linux	Main Tabs	Content Applications	Privacy	Security	Advanced	pit Project	**
Ge	eneral Network		Conne	ction Set	tinas		~
Welcom	Connection	Configure Proxies	to Access	the inte	rnet		
	Configure how	O No proxy					
	Offline Storage	O Auto-detect pro	xy settings	for this ne	t <u>w</u> ork		
	Use up to	O Use system pro	xy settings				
		<ul> <li>Manual proxy co</li> </ul>	nfiguration	:			
	The following w	<u>H</u> TTP Proxy:	127.0.0.1		Port:	1234	
			Use this	s pro <u>x</u> y ser	ver for all protoco	ls	
		<u>S</u> SL Proxy:	127.0.0.1		P <u>o</u> rt:	1234 🗧	
		ETP Proxy:	127.0.0.1	£	Port:	1234	
	1	<u>G</u> opher Proxy:	127.0.0.1		Port:	1234 -	
OF		SO <u>C</u> KS Host:	127.0.0.1	S	Por <u>t</u> :	1234 🗧	
"Of	⊙ socks v4 ⊚ socks vs						
Ba(	Bai <u>N</u> o Proxy for: localhost, 127.0.0.1						
hov	Help		Example: .	mozilla.or	g, .net.nz, 192.168	3.1.0/24	+
Done —		O <u>A</u> utomatic prox	/ configurat	ion URL:			8
ैद 🞘 🔤 🥹 🗃 ।	🖛 💥 📃	👻 🥹 Welcom 🌗	Firefox	🗃 root@l	ot 🛛 🗖 💽 🖓	1 2 <b>21:</b>	11 >

Fig 2 : Configuration de proxy de Mozilla

2. Dans **Main**, dans le champ de la page d'accueil (home page), changer la page d'accueil pour **http://hamster**/ afin qu'il s'ouvre automatiquement lorsque vous lancez le navigateur.



Et pour faire fonctionner Hamster on ouvre notre navigateur (qui est sur <u>http://hamster</u>) et l'interface web de Hamster nous apparait :



Fig 4 : interface web de Hamster

Puis on clique sur adapters pour choisir notre **adapter** (**interface**) qui lance lui-même **ferret** en background pour commencer le sniffing et pour cela on doit d'abord connaitre les noms des *adapters* (*interfaces*) qui sont présents en lançant la commande *ifconfig* 

Hamster - Mozilia Firefox		
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp		144 144 144 144
🔶 🗼 🔻 😂 🚳 🏠 🔀 http://hamster/	☆▼ <b>C</b> ▼ Google	0
BackTrack Linux II Offensive-Security Cerix IT II Exploit Database Aircrack-ng	The Metasoloit Pro	iect »
Session Edit View Bookmarks Settings Help		
<pre>noo clc tal </pre> root@bt:~# ifconfig th0 Link encap:Ethernet HWaddr 08:00:27:00:c9:f8 inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255 inet6 addr: fe80::a00:27ff:fe00:c9f8/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:104 errors:0 dropped:0 overruns:0 frame:0 TX packets:116 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:69208 (69.2 KB) TX bytes:17899 (17.8 KB)	5.0	n the re k on ser sure
No targe has been selec yet	ame [ pwnsauce ]	nd
scri		•ns 🗶
🔧 🍓 🔤 🥹 🜌 🚋 💥 📃 💽 🧕 Hamster - Moz 🜌 root@bt [3]-	1 2	23:54 >

Fig 5 : Adapters (interfaces)

On va choisir notre adapter eth0 et on clique *sur submit query* et on aura la figure suivante et en background on aura ferret activé

20	Hamster - Mozilla Firefox		×
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hig	li <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp		4 <sup>4</sup> 4 4 4 4 4
🔶 🏟 🝷 🔁 (	🚳 🏠 📓 http://hamster/	G ▼ Google @	2
NackTrack Linux	戻 Offensive-Security 😫 Gerix.IT 🚺 Exploit Database 🐚 Aircrack-r	ng 📑 The Metasploit Project	>>
no cloned	To start monitoring, type in the adapter name and This adapter must support 'promiscuous' mode m to first configure the adapter on the command line adapters	d hit the [Submit] button. nonitoring. You may have ne, especially for wifi	
target 	etho Submit Query		
No target has been selected yet			
Done	🖉 🛶 💥 💽 🖌 🕑 Firefox [2] 🔺 🜌 root@bt [2] 🔺	■■ 🖓 1 2 <b>2 1:2</b> ]	3

Fig 6 : choix de l'adapters (de l'interface)

Et la figure suivante nous montre l'exécution de ferret en background et début du sniffing sur l'interface **eth0** 

📧 💿 root@bt: /pentest/sniffers/hamster - Shell - Konsole 📰 🗃 🕅	
Session Edit View Bookmarks Settings Help	
hiOkd9z6McxY0jU-hwdaJsE3ykrB0z1KY0Xf4s0ngigZiCpeTXNMJ5sFZsXLr4X0BFyUh4_B950RKns9	Google 🔍
starting adapter eth0 [0] ferret [1] -i [2] eth0 [3]hamster	əloit Project 🛛 🕺
<ul> <li> FERRET 1.2.0 - 2008 (c) Errata Security</li> <li> build = Mar 11 2009 17:41:22 (32-bits)</li> <li> libpcap version 0.9.8</li> <li>1 eth0 (No description available)</li> <li>2 any (Pseudo-device that captures on all interfaces)</li> <li>3 lo (No description available)</li> </ul>	lick on the ake sure 'H, click on c browser just
Sniffing on interface "eth0" SNIFFING: eth0 LINKTYPE: 1 Ethernet GET /safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc2hhdmFyEAEYgccDIMDJAzItgeMAAP8A	i make sure vser and
Traffic seen GET /safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc2hhdmFyEAEYgccDIMDJAzItgeMAAP 8A HTTP/1.1 Host: safebrowsing-cache.google.com User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.15) Gecko/200910281	e
Shell	
Done	2 10 • 17

Fig 7 : Exécution en background de Ferret et le début de sniffing

Maintenant après avoir lancé Hamster et Ferret et après configuration de notre navigateur on va se connecter sur un compte on s'authentifier et récupérer ces cookies, pour les rejouer après. J'ai choisi de me connecter au site de POF.com pour faire mes tests, je lance <a href="http://www.pof.com/">http://www.pof.com/</a> et je m'authentifie avec un login *Sofiane\_Hmaster* et un mot de passe, après avoir ouvert mon compte sur POF je réactualise <a href="http://hamster/">http://hamster/</a>



Fig 8 : Ouverture d'une session Compte POF

Sur la figure suivante qui est l'interface web de l'outil Hamster on remarque que l'interface sur laquelle on est en train d'écouter est affichée ainsi que le nombre de paquet et le nombre qui transitent sur notre réseau.



Fig 9 : Interface web du Hamster avec l'interface écouté et le nombre de paquet transitant

0	Free Online Dating at POF.com''' - Mozilla Firefox 📃 🗐 🕱
<u>F</u> ile <u>E</u> dit ⊻iew H	Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp
🔶 🔶 👻	🔞 🏠 http://www.pof.com/ 🔗 🕇 Google 🔍
BackTrack Linux	Session Edit View Bookmarks Settings Help
Hamster	Referer: http://www.google.fr/search?sclient=psy-ab&hl=fr&site=&source=hp&q=plen▲ ty+of+fish&btnG=Rechercher Cookie: ft=Saturday, December 10, 2011 12:37:41 PM; usernameb=Sofiane_Hamster; t mp_track=31903547; t_user_id=37526434; alogin=s4rbykpkx2mhxoqxkyg10kp2; username =Sofiane_Hamster; user_idb=37526434
ore Relationships igned and built POF tes and more relatic an it was for me to	<pre>POST /inbox.aspx POST /inbox.aspx HTTP/1.1 Host: www.pof.com User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.15) Gecko/200910281 4 Ubuntu/8.10 (intrepid) Firefox/3.0.15 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-us,en;q=0.5 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 300 Referer: http://www.pof.com/ Cookie: ft=Saturday, December 10, 2011 12:37:41 PM; usernameb=Sofiane_Hamster; t</pre>
Scripts Current Waiting for www.po	<pre>mp_track=31903547; t_user_id=37526434; alogin=s4rbykpkx2mhxoqxkyg10kp2; username =Sofiane_Hamster; user_idb=37526434; ASP.NET_SessionId=l5f0eu1bmdox55tafpsxz4j1; POFIMSession=634591836790894587</pre>
ेद 👰 📰 🥹 ।	🜌 🖙 💥 💽 🗸 🥑 Free Online D. 🜌 root@bt [2]- 🚺 🔊 🏹 1 2 🎁 🛄 >

Fig 10: les paquets sniffés et les cookies récupérés

La figure ci-dessus montre les paquets sniffés et tous les cookies récupérés par **Ferret** et qu'on pourra utiliser pour accéder mon compte POF sans s'authentifier à nouveau. Et c'est le but de l'outil **Hamster**.

### Comment peut-on rejouer ces cookies via l'interface web et accéder à un compte ?

Si notre pc est équipé d'une carte réseaux qui permet le mode promescous on pourra rejouer les cookies directement via l'interface web de Hamster sans avoir à les remplacer manuellement de la manière suivante :

Après avoir s'authentifier à un compte on réactualise <u>http://hamster/</u> et cette page doit nous apparaitre (Image prise dans le livre : BackTrack 4: Assuring Security by Penetration Testing des auteurs Shakeel Ali Tedi Heriyanto)



Après une petite attente, on verra l'apparition d'adresses IP. On clique sur l'adresse IP de la victime afin de cloner ses sessions. Dans la fenêtre de gauche, on voit les sites que la victime est en train de visiter.

🖳 🗧 Hamster - Konqueror	
Location Edit View Go Bookmarks Tools Settings Window Help Hamster Konqueror	
000208=%=%	-55
Ex Location: 18 http://127.0.0.1:1234/	10. 1.
192.168.1.97	
[cookies]	
http://ocsp.verisian.com:80/	
<ul> <li>http://mail.vimg.com/d/combo?/mg/11 4 9/css/folders.css</li> </ul>	
•	
http://l.yimg.com/he/combo?js/v4/yui2/ycw.utii_2.1_1282245542.9814-min.j	
<ul> <li>http://mail.yimg.com/d/combo7/mg/11_4_9/css/compose.css</li> </ul>	
http://l.yimg.com/he/combo?js/v4/yui2/ycw.util_2.1_1282245542.9814-min.j	
<ul> <li>http://l.vimg.com/he/combo?css/v4/ycw.base_2.1_1282245542.9814-min.cs;</li> </ul>	
http://ycw.updates.yahoo.com/getVersions.php	
<ul> <li>http://mail.yimg.com/d/combo?/mg/11_4_9/js/showmessage.js</li> </ul>	
<ul> <li>http://mail.yimg.com/d/combo?/mg/11_4_9/css/showmessage.css</li> </ul>	
•	
http://us.mc1144.mail.yahoo.com/mc/showMessagerview=getMessages&tik	
<ul> <li>http://l.yimg.com/a/lib/uh/15/js/uh_utils_mail_rsa-1.0.0.js</li> </ul>	
bttp://content vieldmananer edgesuite net/at	100000000000000000000000000000000000000
28 Images of 34 loaded.	86%

Et pour accéder au compte Yahoo de la victime on n'a qu' cliquer sur le line approprié et on aura accès à sa messagerie comme suit :



### **Conclusion : Protégeons-nous**

La leçon à tirer de cette étude est que les utilisateurs ne peuvent vraiment pas se permettre d'être laxiste sur le cryptage des données envoyées sur les réseaux ouverts sans fil et aussi de se déconnecté a chaque fin d'utilisation d'une session sur le net.