

Rhibi hamza, Fras Hammami, Rebhi Adel

Partie 1 : TELNET

1) Sudo su
Gedit etc/hosts
Ajouter www.firasars2015.com

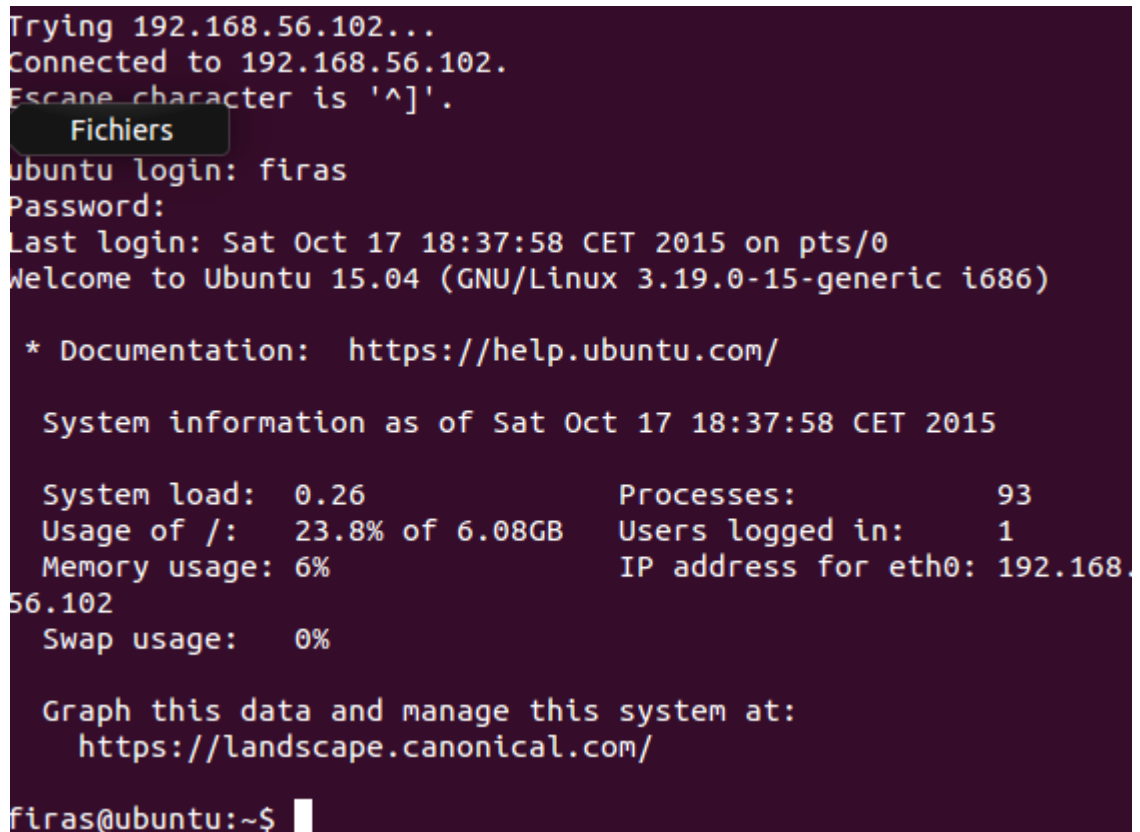
2) dans le serveur tapez dans le terminal :

/etc/init.d/networking restart

Après avoir connaître l'adresse ip de l'interface eth0 par la commande
ifconfig

Puis tapez /etc/init.d/openbsd-inetd restart

3) tapez dans le terminal telnet 192.168.56.102



```
Trying 192.168.56.102...
Connected to 192.168.56.102.
Escape character is '^]'.
Fichiers
ubuntu login: firas
Password:
Last login: Sat Oct 17 18:37:58 CET 2015 on pts/0
Welcome to Ubuntu 15.04 (GNU/Linux 3.19.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

System information as of Sat Oct 17 18:37:58 CET 2015

System load:  0.26           Processes:            93
Usage of /:   23.8% of 6.08GB Users logged in:        1
Memory usage: 6%           IP address for eth0: 192.168.
56.102
Swap usage:   0%

Graph this data and manage this system at:
https://landscape.canonical.com/

firas@ubuntu:~$
```

5) les 3 premiers paquets hanshak :

14	70.8134920	192.168.56.101	192.168.56.102	TCP	66 54540→23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
15	70.8146780	192.168.56.102	192.168.56.101	TCP	66 23→54540 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
16	70.8148920	192.168.56.101	192.168.56.102	TCP	54 54540→23 [ACK] Seq=1 Ack=1 Win=65700 Len=0

6) on remarque que telnet utilise par défaut le port 23 , on remarque aussi que le login et le mot de passe n'ont pas chiffrer

```

0.....XTERM.....!#.....!#.....P.....38400,3840
ubuntu login: fffirraass
Password: firas
Last login: Sat Oct 17 18:52:42 CET 2015 on pts/0
welcome to ubuntu 15.04 (GNU/Linux 3.19.0-15-generic i686)
* Documentation: https://help.ubuntu.com/
System information as of Sat Oct 17 18:52:43 CET 2015
System load: 0.0      Processes: 89
Usage of /: 23.8% of 6.08GB   Users logged in: 1
Memory usage: 6%      IP address for eth0: 192.168.56.102
Swap usage: 0%
Graph this data and manage this system at:
https://landscape.canonical.com/
.]0;firas@ubuntu: ~.firas@ubuntu:~$

```

telnet donc n'est pas sécurisé

7) cd /home/firas
Mkadir hammami

```

firas@ubuntu:~$ cd ..
firas@ubuntu:/home$ ls
firas
firas@ubuntu:/home$ cd firas
firas@ubuntu:~$ mkdir hammami
firas@ubuntu:~$

```

Et par wireshark

```

mkkdd1rrr hhaammmaamm1111
.]0;firas@ubuntu: ~.firas@ubuntu:~$ |

```

Partie 2 : SSH

8) pour lancer ssh ,il faut tapez dans le terminal du serveur ssh
firas@192.168.56.102

9) ~/.ssh/known_hosts : Ce fichier contient la clé publique de tous les serveurs ssh sur laquelle ce compte c'est connecté. Il est vide après la première connexion

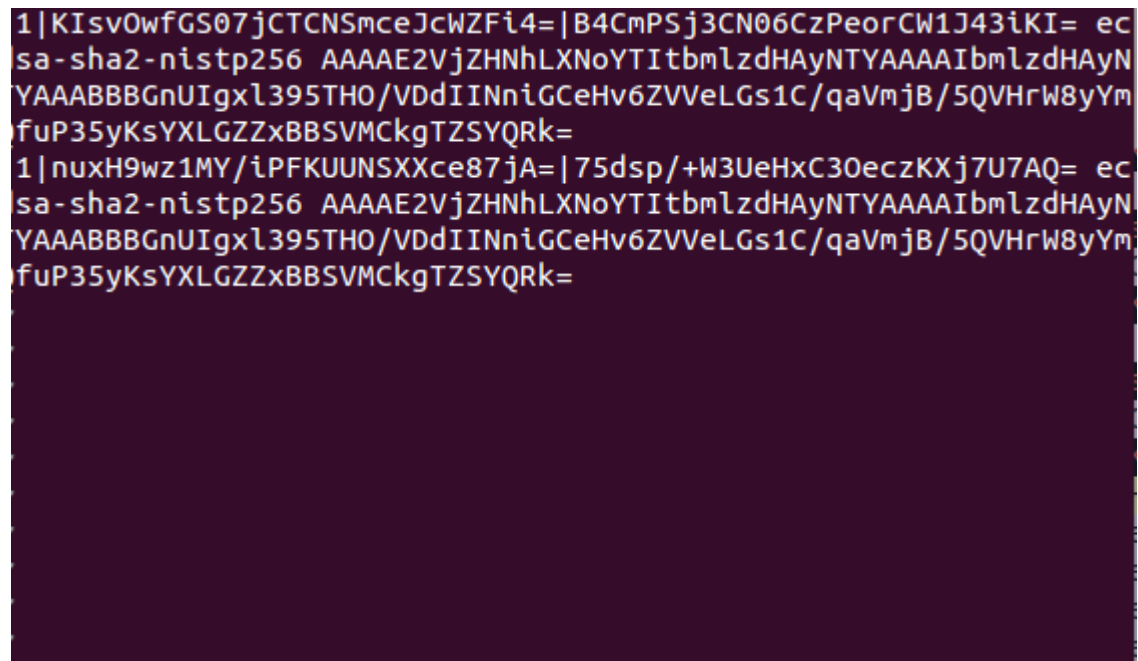
10) lancez wireshark

11) tapez `ssh firmas@192.168.56.102` puis « yes »

12) il vous demande si la clef publique présentée par le serveur est bien le bon. Pour être sûr que vous vous connectez au bon serveur, vous devez connaître de façon certaine d sa clef publique et la comparer à celle qu'il vous affiche

13) Authentification par clef

14) la fichier `known_hosts` contient le clé publique du serveur



15) tapez `mkdir firmas`

16) si on veut connecter une deuxième fois , il'y 'a pas de confirmation pour l'échange du clé public , parce que il'est déjà enregistré dans `knowns_hosts`

17)

1) l'établissement de la connexion

Seq	Port	IP	Protocol	Details
11	20.7318220	192.168.56.101	192.168.56.102	TCP 80 57844->22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
12	26.7367710	192.168.56.102	192.168.56.101	TCP 66 22->57844 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
13	26.7370360	192.168.56.101	192.168.56.102	TCP 54 57844->22 [ACK] Seq=1 Ack=1 Win=65700 Len=0

2) le port ssh est le 22 par défaut

Echange de version `sshv2`

Seq	Port	IP	Protocol	Details
63	107.895114	192.168.56.101	192.168.56.102	SSHv2 134 client: Encrypted packet (len=80)

Seq	Port	IP	Protocol	Details
64	107.907084	192.168.56.102	192.168.56.101	SSHv2 134 Server: Encrypted packet (len=80)

Négociation avec le protocole arp
 6/ 112.914224 Cadmusco_ec:83:47 Cadmusco_00:3c:86 ARP

60 Who has 192.168.56.101? Tell 192.168.56.102

68 112.914277 Cadmusco_00:3c:86 Cadmusco_ec:83:47 ARP

42 192.168.56.101 is at 08:00:27:00:3c:86

Donné crypté

75	116.350161	192.168.56.102	192.168.56.101	SSHv2	118 Server: Encrypted packet (len=64)
76	116.350644	192.168.56.101	192.168.56.102	SSHv2	166 Client: Encrypted packet (len=112)
77	116.350868	192.168.56.101	192.168.56.102	SSHv2	118 Client: Encrypted packet (len=64)

18) ouvrir le fichier /etc/ssh/sshd_config. Avec vi

Password authentication no et enregistrer

19) on remarque que il y'a encore authentication par mot de passe

20) avec la commande ssh-keygen. On peut générer deux clés .

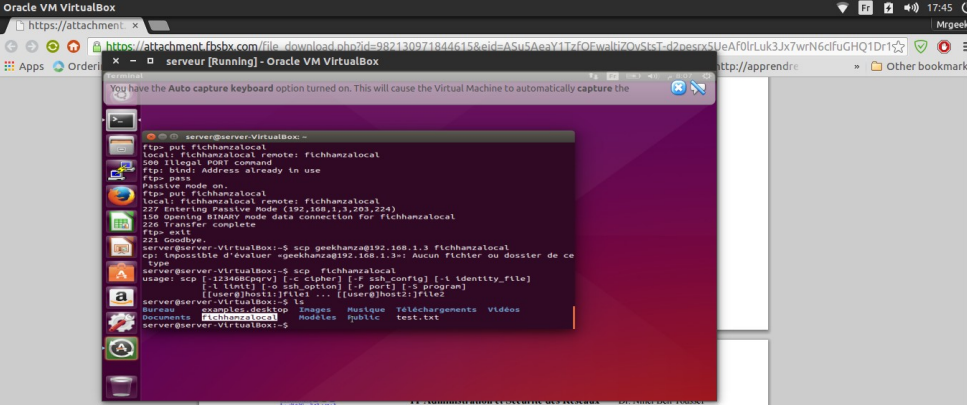
```
root@ubuntu:/etc/ssh# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
a6:85:40:9c:44:03:1d:c0:cd:a4:fe:2b:21:4d:5c:28 root@ubuntu
The key's randomart image is:
+---[RSA 2048]---+
| .o%Bo          |
| E ooB.         |
|  o...          |
| .o  . .        |
| o.   . S       |
| . o.   +       |
| . . . .        |
| . . .          |
| ..            |
+-----+
root@ubuntu:/etc/ssh#
```

23) on remarque qu'il y'a un échange de clé

II.2 Activité 2 : Transfert de fichiers FTP vs SCP

1) service proftpd start

2) touch fichhamzalocal

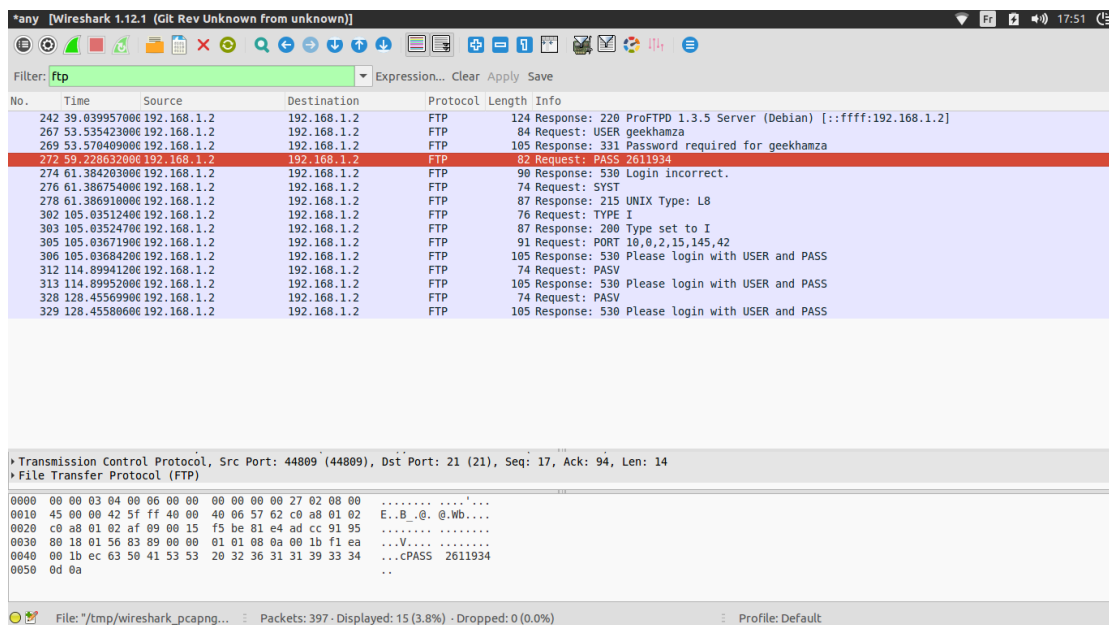


```
server@server-VirtualBox:~$ ftp put fichhamzalocal
local: fichhamzalocal remote: fichhamzalocal
500 Illegal PORT command
ftp: bind: Address already in use
ftp: pass
Passive mode on.
ftp: put fichhamzalocal
local: fichhamzalocal remote: fichhamzalocal
227 Entering Passive Mode (192,168,1,3,203,224)
150 Opening BINARY mode data connection for fichhamzalocal
226 Transfer complete
ftp: exit
221 Goodbye.
server@server-VirtualBox:~$ scp geekhanza@192.168.1.3 fichhamzalocal
cp: impossible d'évaluer «geekhanza@192.168.1.3»: Aucun fichier ou dossier de ce type
server@server-VirtualBox:~$ scp fichhamzalocal
usage: scp [-rsSP] [-c cipher] [-P ssh_config] [-i identity_file]
[-l link] [-o ssh_option] [-P port] [-S program]
[user@host1:]file1... [user@host2:]file2
server@server-VirtualBox:~$ ls
Bureau  documents  desktop  images  Musique  Téléchargements  Vidéos
server@server-VirtualBox:~$
```

4. Lancez Wireshark pour la capture de trafic.
5. Au niveau du client, transférez le fichier **fichlocal** avec la commande **ftp** vers le répertoire personnel ~ du compte <votre prénom> dans le serveur en lui donnant un nom différent <votre prénom>-ftp (Exemple : **finatftp**).
6. Vérifiez que le fichier a été transféré.
7. Sous Wireshark, montrez que le mot de passe est transféré en clair.
8. Enregistrez et fermez la capture de trafic. Relancez à nouveau.
9. Au niveau du client, transférez cette fois le fichier **fichlocal** avec la commande **scp** vers le répertoire personnel ~ du compte <votre prénom> dans le serveur en lui donnant un nom

5)ftp fichhamza local /home/geekhamza/hamzaftp

7) le mot de passe est transférer en claire



The image shows a Wireshark capture of an FTP session. The packet list on the left shows several FTP packets. Packet 272 is highlighted, showing a request for the password '2611934'. The packet details pane on the right shows the 'File Transfer Protocol (FTP)' section, which includes the 'cPASS' command and the password '2611934' in the 'data' field. The packet bytes pane at the bottom shows the raw data of the packet, including the password in plaintext.

No.	Time	Source	Destination	Protocol	Length	Info
242	39.039957000	192.168.1.2	192.168.1.2	FTP	124	Response: 220 ProFTPD 1.3.5 Server (Debian) [::ffff:192.168.1.2]
267	53.535423000	192.168.1.2	192.168.1.2	FTP	84	Request: USER geekhamza
269	53.570409000	192.168.1.2	192.168.1.2	FTP	105	Response: 331 Password required for geekhamza
272	59.228632000	192.168.1.2	192.168.1.2	FTP	82	Request: PASS 2611934
274	61.384203000	192.168.1.2	192.168.1.2	FTP	90	Response: 530 Login incorrect.
276	61.386754000	192.168.1.2	192.168.1.2	FTP	74	Request: SYST
278	61.386910000	192.168.1.2	192.168.1.2	FTP	87	Response: 215 UNIX Type: L8
302	105.035124000	192.168.1.2	192.168.1.2	FTP	76	Request: TYPE I
303	105.035247000	192.168.1.2	192.168.1.2	FTP	87	Response: 200 Type set to I
305	105.036719000	192.168.1.2	192.168.1.2	FTP	91	Request: PORT 18,0,2,15,145,42
306	105.036842000	192.168.1.2	192.168.1.2	FTP	105	Response: 530 Please login with USER and PASS
312	114.899412000	192.168.1.2	192.168.1.2	FTP	74	Request: PASV
313	114.899520000	192.168.1.2	192.168.1.2	FTP	105	Response: 530 Please login with USER and PASS
328	128.455699000	192.168.1.2	192.168.1.2	FTP	74	Request: PASV
329	128.455800000	192.168.1.2	192.168.1.2	FTP	105	Response: 530 Please login with USER and PASS

9)

tapez scp fichhamzalocal geekhamza@192.168.1.2:/home/geekhamza/hamzascp

10) on remarque que le fichier est crypté

11) conclusion :

FTP est un protocole pour le transfert des fichier du serveur vers client ou inverse avec des données transférés en claire ,, de meme scp mais il est sécurisé

TELNET est un protocole pour contrôler a distance des machine ,mais il n'est pas sécurisé , de meme ssh mais avec un niveau du sécurité évolué