

SIO 1

# UN SERVEUR FTP

#### **1** – Introduction

Aujourd'hui, dans les entreprises, des centaines de fichiers sont échangés via un serveur. Mais beaucoup d'échanges ne sont pas sécurisés, ce qui facilite le piratage.

Pour contrer cette attaque, on utilise des logiciels tels que FileZilla avec lesquels ont créés des certificats qui permettront de sécuriser l'échange.

#### 2 – FTP (sous windows)

Nous allons donc mettre en place un serveur FTP (File Transfert Protocol)

L'utilisation de FileZilla se fait en deux parties : l'installation de FileZilla <u>Serveur</u> sur un poste et FileZilla <u>Client</u> sur un second poste. Une fois les deux logiciels installés, nous pouvons commencer.

Connexion au serveur	×
Adresse du Serveur:	Port : 14147
Mot de passe admin :	
Toujours se connecter à ce s	nuler

Premièrement, il faut se connecter au serveur, avec une adresse IP en 127.0.0.1 et un port 14147, nous avons mis le serveur et le client dans le même réseau. L'adresse du serveur sera alors 10.0.1.4 et le client en 10.0.1.3.

#### Différents moyens de se connecter sur son serveur FTP

- Par ligne de commande en tapant ftp puis en tapant « open 10.0.0.3 ». Il demande par la suite le nom d'utilisateur et son mot de passe à renseigner. Grâce à la commande « dir », nous pouvons avoir accès aux fichiers de l'utilisateur.

G CL	летр	mpace	1 GIRGING	
close	lcd	open	rmdir	
ftp> open 10	0.0.3			
Connecté à 1	10.0.0.3.			
220 Bon.jours	s les nuls =)			
Utilisateur	(10.0.0.3:(none))	: melina		
331 Password	d required for mel	ina		
Mot de passe				
230 Logged a	on			
ftp> ?				
Les commande	es peuvent être ab	régées. Ces con	mandes sont :	
t	delete	literal	prompt	send
?	debug	<b>l</b> s	put	status
append	dir	mdelete	pwd	trace
ascii	disconnect	mdir	quit	type
bell	get	mget	quote	user
binary	glob	mkdir	recy	verbose
bye	hash	mls	remotehelp	
cd	help	mput	rename	
close	lcd	open	rmdir	
ftp> dir				
200 Port con	nmand successful			
150 Opening	data channel for	directory listi	ing of "/"	
drwxr-xr-x 1	l ftp ftp	0 Mar 25 1	.7:14 commun	
drwxr-xr-x 1	l ftp ftp	0 Mar 25 1	.6:44 perso1	
226 Successi	fully transferred	0/0		
ftp : 114 oc	ctets reçus en 0,0	0 secondes à 11	.4,00 Ko/s.	
ftp> cd com	านก	1014 (M) 18214-		
250 CWD suce	cessful. "/commun"	is current dim	ectory.	
ftp>_dir				
200 Port con	nmand successful			
150 Opening	data channel for	directory listi	ng_of_"/commun"	
-rw-rr 1	l ftp ftp	34357 Mar 25 0	99:54 Economie.doc>	C
226 Successi	fully transferred	"/commun"	<u>1999</u>	
ftp : 64 oct	tets reçus en 0,00	secondes à 64,	WU Ko/s.	
ftp>				

Par votre navigateur web, en renseignant dans la barre d'adresse « ftp://10.0.0.3 ». Il vous demande par la suite de renseigner le nom d'utilisateur et son mot de passe.
 Vous avez par la suite accès aux différents fichiers de l'utilisateur.

( Nouvel onglet	×			
← → X 前 ☐ ft	o://10.0.0.2			☆ =
Applications Accédez	Authentification requise Le serveur ftp://10.0.0.2:21 red un mot de passe. Nom d'utilisateur : me Mot de passe : ***	e quiert un nom d'util ehdi Se connecter	Annuler	<u>ter mes favoris mainten</u>
🕒 Index de /	×			
← → C fi 🗋 ft	p://10.0.0.2			52

# Index de /

Nom	Taille	Date de modification
Commun/		28/03/14 10:48:00
inehdi/		28/03/14 10:49:00

Ensuite depuis le poste client se connecter en indiquant son mot de passe, son identifiant, l'hôte du serveur et ne pas mentionné de numéro de port.



Lors de la connexion depuis le poste client nous avons la liste d'interactions entre le poste

#### serveur et le client.

🔁 FileZilla Se	erver (127.0.0.1)				- 0 ×
File Server	Edit ?				
78	s 🖸 🗳 💡 /c/ c:\ 🚦				
FileZilla Server	version 0.9.43 beta				
Copyright 2001-	-2014 by Tim Kosse (tim.kosse@	filezilla-project.org)			
nttps://filezilla-p	project.org/				
Connected wai	ting for authentication				
Longed on	ung for douter la cauori				
Retrieving acco	ount settings, please wait				
Done retrieving	account settings				
Retrieving settin	ngs, please wait				
Done retrieving	settings				
Sending setting	s, please wait				
Done sending s	ettings.				
Retrieving settin	ngs, please wait				
Done retrieving	settings				
Retneving acco	ount settings, please wait				
Sending accourt	account settings of eattings, plages wait				
Done sending a	account settings				
Retrieving acco	ount settings, please wait				
Done retrieving	account settings				
Sending accourt	nt settings, please wait				
Done sending a	account settings.				
(000001)25/03/	/2014 17:11:23 - (not logged in) (	(10.0.1.3)> Connected, sending welcome messag	e		
(000001)25/03/	/2014 17:11:23 - (not logged in) (	(10.0.1.3)> 220 Bonjours les nuls =)			
(000001)25/03/	/2014 17:11:23 - (not logged in) (	(10.0.1.3)> USER mélina			
(000001)25/03/	/2014 17:11:23 - (not logged in) (	(10.0.1.3)> 331 Password required for melina			
(000001)25/03/	/2014 17:11:23 - (not logged in) ( /2014 17:11:22 mólina /10.0.1.1	(10.0.1.3)> PASS			
(000001)25/03/	/2014 17:11:23 - melina (10.0.1.3 /2014 17:11:22 - mélina (10.0.1.3	3)> 230 Logged on 3)> even			
(000001)25/03/	/2014 17:11:23 - mélina (10.0.1.3 /2014 17:11:23 - mélina (10.0.1.3	3) > 215   INIX emulated by File 7illa			
(000001)25/03/	/2014 17:11:24 - mélina (10.0.1.)	R)> FFAT			
(000001)25/03/	/2014 17:11:24 - mélina (10.0.1.3	3)> 211-Features:			
(000001)25/03/	/2014 17:11:24 - mélina (10.0.1.3	3)> MDTM			
(000001)25/03/	/2014 17:11:24 - mélina (10.0.1.3	3)> REST STREAM			
(000001)25/03/	/2014 17:11:24 - mélina (10.0.1.3	3)> SIZE			
(000001)25/03/	/2014 17:11:24 - mélina (10.0.1.3	3)> MLST type*;size*;modify*;			
(000001)25/03/	/2014 1/:11:24 - mélina (10.0.1.3	3)> MLSD			
(000001)25/03/	/2014 17:11:24 - melina (10.0.1.) (2014 17:11:24 - melina (10.0.1.)	3)> UTF8			
(000001)25/03/	/2014 17:11:24 - melina (10.0.1.) /2014 17:11:24 - mélina (10.0.1.)	3)> CLNT 2)> MEMT			
	2009-021029-005004100012	172 (m) m (			
ID 🛆	Account	IP Transfer		Progress Speed	
<b>-œ-</b> 000003	mélina	10.0.1.3			
1					

#### Création d'utilisateurs

1. Rendez-vous dans le menu « Edit » et choisissez « Users ».

**2. Cliquez** sur le bouton « Add » pour ajouter un utilisateur autorisé à se connecter à votre serveur. Notez qu'il devra alors respecter la casse de l'identifiant et du mot de passe, c'est-àdire qu'il devra veiller à saisir de façon différenciée les majuscules et les minuscules.

**3.** N'hésitez pas à choisir des **mots de passe** suffisamment complexes afin qu'ils ne puissent être trouvés facilement par des apprentis pirates.

Tage	Account settings	Users
- General Shared folders Speed Linits IP Filter	Grane accurate     Grane accurate     Grane accurate     Grane accurate     Grane accurate     Compose accurate	
	Maginum connection count: 0 Connection jimit per IP: 0 Eprose SSR. for user logel	( Add ) (Berrow (Regare) Copy
	Description	
OK.	1	-

Page:	Shared folders		Disa	Users
General Shared folders Speed Limits IP Filter	Directories C:\Users\PC-1 H C:\Users\PC-1 <	Aliases 0\ 0\ Remove Renam so appear at the spec e aliases for one director avoid cyclic director		mehdi melina Add Remove Rename Copy st contain the full local ter (1) nfuse FTP clients.
OK Cancel				

Gérer les accès aux différents fichiers (commun et perso)

Une fois l'utilisateur crée, se rendre dans l'onglet « Shared Folders » afin de choisir le ou les dossiers auxquels il aura accès.

Nous lui avons créé un fichier commun et un fichier personnel au nom de l'utilisateur.

On peut également choisir les droits que l'utilisateur à sur ce dossier (voir uniquement le dossier, pouvoir y ajouter des fichiers, en supprimer ...), ce qui permet, dans le cas de plusieurs compte, de voir les dossiers des autres, mais pas de pouvoir agir dessus.

Rechercher un dossier		1		52
Please select a folder that should be added to the folders list of account.	he selected user	Shared folders		
<new directory=""></new>		Directories Aliases	Files Read	mehdi
🧮 Bureau	A	<new directory=""></new>	Write	
Réseau		C:\Users\PC-10\	Delete	
Bibliothèques		H C:\Users\PC-10\	Append	
▶ <u>8</u> PC-10	E		Directories	
▲ I Ordinateur			Create	
Windows/_OS (C:)			Delete	
S Lenovo_Recovery (D:)			V List	
Lecteur BD-POM (G:)		4	V + Subdirs	Add Remove
b bureau	-			
		Add Remove Rename	Set as home dir	Rename Copy
ОК	Annuler	A directory alias will also appear at the specified path. Separate multiple aliases for one directory	d location. Aliases mus with the pipe charact	st contain the full local ter (   )
on		If using aliases, please avoid cyclic directory str	ructures, it will only co	nfuse FTP clients.
nulated by FileZilla				
с — — — — — — — — — — — — — — — — — — —	ОК	]		
EAM		-		
:size*;modify*;	Cancel			

Nous avons donc accès aux différents fichiers autorisés selon l'utilisateur. Ici l'utilisateur « Mélina » a donc seulement accès au fichier commun et à son fichier personnel.

🔁 melina@10.0.0.3 - F	ileZilla	-									- I X
Fichier Édition Affi	ichage Trans	sfert Serveur Fa	voris ?								
🛛 -   🖊 🗆 🥐	<b>F</b> # #	P3 🗽 🛷 🗐	.श 👎 <b>n</b>								
Hôte : 10.0.0.3	Identifi	iant : melina	Mot de passe :	•••••	Port :	Connexion ra	apide 💌				
Réponse : 22 Commande : P, Réponse : 22 Commande : M Réponse : 1 Pérense : 2	00 Type set to I ASV 27 Entering Pas ILSD 50 Opening dat	I sive Mode (10,0,0,3, a channel for director	192,67) ry listing of "/"								•
Statut : C	ontenu du dossi	ier affiché avec suco	ès								*
Site local : C:\Users\sjd	1\Desktop\						Site distant : /				•
	Desktop Documents Downloads Favorites Links Local Settin	s Igs				• 					
Nom de fichier	Taille de fi	Type de fichier	Dernière modificat			^	Nom de fic Taille	de fi Type de fic Derniè	re modif Droits d'ac	Propriétair	
don't starve     don't starve     BBC News - Revi     Gesco Packet Tra     desktop.ini     Microsoft Office     Microsoft Office     Microsoft Office     Microsoft Visual	9 636 032 1 261 282 2 711 2 693 2 753 1 366	Dossier de fich Vidéo MP4 Raccourci Paramètres de Raccourci Raccourci Raccourci	19/12/2013 09:13:22 09/04/2013 12:26:00 06/09/2013 08:39:35 12/09/2013 15:26:31 06/09/2013 08:55:17 19/09/2013 08:11:36 06/09/2013 08:55:18 06/09/2013 08:55:18			E	🦉 " Dommun Di melina	Dossier de 28/03/ Dossier de 28/03/	2014 10: 2014 10:		
11 fichiers et 1 dossier.	Taille totale : 8	318 527 191 octets					2 dossiers				
Serveur / Fichier local	Di	irection Fichier di	stant	Taille	Priorité Sta	atut					
Fichiers en file d'att	ente Transfe	erts échqués 🔡 Te	ansferts réussis								

De même pour l'utilisateur « Mehdi » :

Fz mehdi@10.0.0.3 - I	FileZilla	10 C			1 B B								X
Fichier Édition Af	fichage Transf	ert Serveur Fa	voris ?										
	3 2 *	P3 🙀 🛷 🔳	R 7 W										
Hôte : 10.0.0.3	Identifia	nt: mehdi	Mot de passe :	Port :	Connexion ra	apide							
Réponse : : : Commande : : : : Réponse : : : : Commande : : !	200 Type set to I PASV 227 Entering Pass MLSD	we Mode (10,0,0,3,	192,68)										
Réponse : Réponse :	150 Opening data 226 Successfully t Contenu du dossie	channel for director ransferred "/" er affiché avec suco	y listing of "/"										0
melina@10.0.0.3 ×	mehdi@10.0.0	3 ×											
Site local : C:\Users\s	io1\Desktop\				Ŧ	Site distant :	1						
	Cisco Packe Contacts Cookies Desktop Documents Downloads	t Tracer 5.3.3			^ 	••- <b>)</b>							
Nom de fichier	Taille de fi	Type de fichier	Dernière modificat			Nom de fic	Taille de fi	Type de fic	Dernière modif	Droits d'ac	. Propriétair		
don't starve     BBC News - Revi     Cisco Packet Tra     desktop.ini     desktop.ini     Microsoft Office     Microsoft Office     Microsoft Office	9 636 032 1 261 282 2 711 2 693 2 753	Dossier de fich Vidéo MP4 Raccourci Paramètres de Raccourci Raccourci Raccourci	19/12/2013 09:13:22 09/04/2013 12:26:00 06/09/2013 08:39:35 12/09/2013 08:56:17 19/09/2013 08:55:17 19/09/2013 08:11:36 06/09/2013 08:55:18		E	🅌 <table-of-contents> Commun 🏓 mehdi</table-of-contents>		Dossier de Dossier de	28/03/2014 10: 28/03/2014 10:				
11 fichiers et 1 dossier	. Taille totale : 81	18 527 191 octets				2 dossiers							
Serveur / Fichier local	Din	ection Fichier di	itant	Taille Priorité	Statut								
The second s													

#### Vérifiez le caractère non sécurisé du serveur FTP grâce à Wireshark

Nous constatons que les trames Wireshark indiquent le mot de passe et le nom de l'utilisateur et donc prouve que le serveur FTP n'est pas sécurisé.

793 218.882481 HonHaiPr_ce:ta:a6	Broadcast	ARP	60 who has 10.0.2.31? Tell 10.0.2.30
794 218.895394 10.0.3.191	10.0.3.190	TCP	66 ftp > 59695 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
795 218.895566 10.0.3.190	10.0.3.191	TCP	54 59695 > ftp [ACK] Seq=1 Ack=1 win=17408 Len=0
796 218.918570 10.0.3.191	10.0.3.190	FTP	96 Response: 220-FileZilla Server version 0.9.43 beta
797 218.927110 10.0.3.191	10.0.3.190	FTP	114 Response: 220-written by Tim Kosse (tim.kosse@filezilla-project.org)
798 218.927243 10.0.3.190	10.0.3.191	TCP	54 59695 > ftp [ACK] seq=1 Ack=103 win=17408 Len=0
799 218.927394 10.0.3.191	10.0.3.190	FTP	115 Response: 220 Please visit http://sourceforge.net/projects/filezilla/
800 218.929717 10.0.3.190	10.0.3.191	FTP	66 Request: USER simon
801 218.967219 10.0.3.191	10.0.3.190	FTP	87 Response: 331 Password required for simon
802 218.967608 10.0.3.190	10.0.3.191	FTP	66 Request: PASS simon
803 219.001384 10.0.3.191	10.0.3.190	FTP	69 Response: 230 Logged on
804 219.004707 10.0.3.190	10.0.3.191	FTP	59 Request: PWD
805 219.010394 10.0.3.191	10.0.3.190	FTP	85 Response: 257 "/" is current directory.
806 219.219291 10.0.3.190	10.0.3.191	TCP	54 59695 > ftp [ACK] Seq=30 ACk=243 Win=17152 Len=0

#### Mise en place d'un certificat FTPS

Pour mettre en place un certificat FTPS, allez dans l'onglet « option » de votre serveur et dans l'onglet « SSL/TLS settings ». Cochez la case « Enable FTP » et cliquez sur « generate new certificate ».

General settings	SSL/TLS settings	FileZilla Server
Welcome message IP bindings	Enable FTP over SSL/TLS support (FTPS)	)
····· IP Filter ···· Passive mode settings	Private key file:	Browse
···· Security settings ···· Miscellaneous	Certificate file:	Browse
···· Admin Interface setting: ···· Logging ···· Speed Limits	Key password:	Password will be stored in plaintext.
Filetransfer compression SSL/TLS settings Autoban	Allow explicit FTP over TLS	
	Force PROT P to encrypt file transfers in	n SSL/TLS mode
	Listen for implicit SSL/TLS connections on th	e following ports (default: 990):
	990	
OK	Note: Explicit FTP over TLS shares the norm	nal FTP port!
Cancel		Generate new certificate

Ensuite renseignez le code département, la ville et l'organisation pour créer le certificat et cliquez sur « browser » pour choisir le fichier où enregistrer la clé du certificat.

(			Σ3	D		
R r				1 2		
r	This dialog will self-signed cer SSL/TLS conne	Iilla Serv				
	Please fill out the require confuse clients.					
e	Key size: 💿 1280 bit	2048 bit 4096 bit		Browse		
ir J	2-Digit country code:	76		Browse		
9	Full state or province:			assword will be		
	Locality (City):	.ocality (City): le havre				
¢ H	Organization:					
	Organization unit:					
	Contact E-Mail:			000).		
	Common name (Server address):			990):		
	Save key and certificate to this file:	Brows	e			
	Generating the certificate may take some time depending on the key size.					
	Generate					
ΗL						
	1					

Zilla Server Or	X						
□ · General settir ··· Welcome ··· IP binding ··· IP Filter ··· Passive mode	This dialog will help you to create a new private key and a self-signed certificate, needed by FileZilla Server to accept SSL/TLS connections. Please fill out the required information. Wrong or missing information may confuse clients. Key size:  1280 bit  2048 bit  4096 bit	Cilla Server					
Security settir	2-Digit File7illa server						
···· Admin Interfa ···· Logging	assword will be tored in						
Speed Limits Locality     Filetransfer co     SSL/TLS and Urganit							
Autoban	Orenei						
	Contac	000)					
OK	Common name (Server address):	990):					
	Save key and certificate to this file: C:\Users\PC-10\Desktop\home\C Browse						
Cancel	Cancel Generating the certificate may take some time depending on the key size.						
	Generate certificate Cancel						

Nous constatons son fonctionnement lorsque nous nous reconnectons sur le client FTP. Nous renseignons l'hôte, le nom d'utilisateur, le mot de passe mais également le port « 990 » qui a changé dû au certificat FTPS mis en place.

faire confiance au serveu	st inconnu. Examinez le r.	certificat avec attention avant de					
Détails							
Valable du :	28/03/2014						
Valable jusqu'à :	28/03/2015						
Numéro de série :	00						
Algorithme de la dé pub	Algorithme de la dé publique : RSA avec 1280 bits						
Signature de l'algorithm	e: RSA-SHA1						
Empreinte (MD5) :	e3:c4:fd:a5:57:	fd:3a:84:aa:8c:c9:87:15:0f:bb:57					
Empreinte (SHA-1) :	Empreinte (SHA-1) : e9:56:4e:c8:1b:b1:cb:0e:b1:b4:e8:1a:cd:93:d9:c9:ef:d7:2e:1						
Objet du certificat		Émetteur du certificat					
Organisation : stiosup		Organisation : stiosup					
Pays: 76		Pays: 76					
Localité : le havre		Localité : le havre					
Détails de session Hôte : 10.0.0.2:990							
Protocole : TLS1.2 Échange de clé : RSA Chiffrement : AES-256-CBC							
				MAC : SHA2	56		
				Approuver ce certificat e	Approuver ce certificat et l'associer à la connexion ?		
	Toujours faire confiance à ce certificat lors des prochaines sessions.						

Nous testons une seconde fois la connexion avec WireShark. On s'aperçoit cette fois ci que la connexion est bien sécurisée, et que le nom et le mot de passe ne sont plus visibles.

19 6.967308000 10.0.1.1	10.0.1.2	TCP	54 63668 + ftps [EIN, ACK] Seg=1 Ack=1 win=63 Len=0
			and a state of the first state and a state of a state o
20 6 067425000 10 0 1 2	10 0 1 1	TCD	54 ftps , 62669 [ACV] spa-1 Ack-3 wip-66 Lpp-0
20 0.907453000 10.0.1.2	10.0.1.1	ICP	14 TCPS + 05008 [ACK] SEQ=I ACK=2 WIN=00 LEN=0
24 6 6 6 7 7 6 6 6 6 6 7 2			
21 6.967766000 10.0.1.2	10.0.1.1	TCP	54 TTPS + 63668 [FIN, ACK] SEG=1 ACK=2 WIN=66 LEN=0
22 6 978752000 10 0 1 1	10 0 1 2	TCD	54 63668 + ftns [ACK] seg-2 Ack-2 Win-63 Len-0
55 0.0/0/02000 TO'O'T'T	TA: A: T: C	I C P	54 65666 4 LCbs [McK] Sed-s McK-s Will-65 Fell-6

#### **3–** Conclusion

Un serveur FTP est un donc très utile et peut être un avantage énorme pour un site Web ou pour l'informatique collaborative dans lequel les fichiers doivent être partagés entre les partenaires commerciaux. Malgré l'insécurité, il est universellement accessible, parce que les clients FTP sont une partie de tous les systèmes d'exploitation et des navigateurs Web.