FTP Server configuration with security

Table of Contents

1. Objective of the Activity

The main objective of this activity is for students to acquire practical skills in configuring FTP servers, addressing two different scenarios: one anonymous and another with local user authentication. Additionally, students are expected to implement security measures through encryption.

This activity will provide students with valuable hands-on experience in configuring and securing FTP servers, preparing them for real-world challenges in the field of system and network administration.

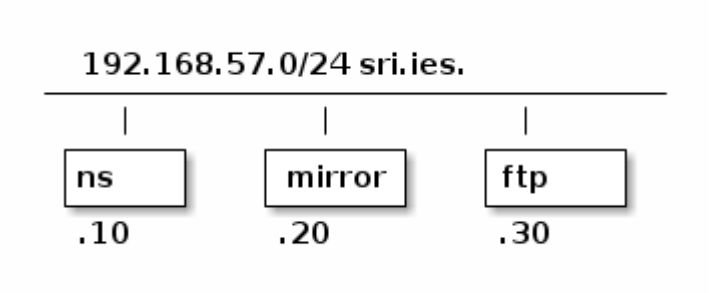

Figure 1. Network diagram

2. Requirements

Prerequisite knowledge

1. Familiarity with the operating system used for the activity (Linux Debian 12).
2. Basic knowledge of network protocols and services.
3. Basic knowledge of DNS protocol and configuration.

Necessary resources

1. Virtual machines with compatible operating systems for FTP server installation.
2. FTP server software (`vsftpd`), FTP clients (command line like ftp and GUI clients like FileZilla Client or CrossFTP).
3. Encryption tools, such as SSL/TLS (included in Debian).
4. Documentation and reference manuals on FTP server configuration and security measures implementation, availables in Moodle as PDF files or the reference in Internet.

3. Agrupation

This activity is better done with a team of two "good" system administrators.

4. Steps to Follow

4.1. Configuration of the Anonymous FTP Server

Document and explain how the configuration was achieved.

1. Install FTP server software on the assigned machine.
2. Configure the FTP server to allow anonymous connections.
3. Set secure access permissions for shared directories.
4. Local users are not allowed.
5. Anonymous users has NO write permissions.
6. Anonymous users are not asked for an anonymous password.
7. Data connection timeout will be 30 secs.
8. Limit max data transfer bandwidth to 5KB/s
9. The server shows a banner "*Welcome to SRI FTP anonymous server*"
10. The server shows an ascii art file in the land directory.
11. Test the configuration with two clients. Test passive and active connection mode (`pftp` for passive connection).

4.2. Configuration of the FTP Server with local users

Document and explain how the configuration was achieved.

1. Install FTP server software on a second machine or in the same server with virtual FTP servers and a second network adapter.
2. Configure the FTP server to authenticate users using operating system accounts. It has two accounts `charles` and `laura`. Their passwords are `1234`.
3. The user `charles` is chrooted and `laura` is not.
4. Anonymous users are forbidden.
5. The server shows a banner "*Welcome to SRI FTP server*"
6. Set access permissions for shared directories for authenticated users.
7. Test the configuration with two clients.

4.3. Implementation of Encryption (SSL/TLS)

Document and explain how the configuration was achieved.

1. Configure the SSL/TLS security layer on second FTP server.
2. Demonstrate the encryption capability during data transfer.
3. Verify correct configuration using testing tools and certificate checks.
4. Local users are forced to connect with a secure connection.
5. Document on the importance of encryption in secure file transfer.

4.4. Configuration of DNS server

1. Install a third virtual machine with a FTP server with authority on the domain `sri.ies`. This machine is `ns.sri.ies`.
2. It has records for `mirror.sri.ies` that points to the anonymous FTP server and `ftp.sri.ies` for the local users' FTP server.
3. Redirect queries for other domains to Cloudfare's server `1.1.1.1`.
4. Both FTP servers has `ns.sri.ies` as name server.

5. Deliverables

- Detailed document describing the configuration of each FTP server.
- Screenshots illustrating the operation of the servers.
- Comments on the implemented security measures and the importance of encryption in file transfer.
- Configuration files for the servers
- Vagrant configuration to deploy the activity

5.1. Evaluation

Assessment will be based on the documentation provided by students, including screenshots, configuration files, and detailed explanations of each step.

Consideration will be given to the security of the implemented configurations, especially regarding user management and data protection through encryption.

5.1.1. Rubric

Table 1. Anonymous server rubric

Requirement	0 points	1 point	3 points
Configure anonymous connections	No	Yes, but there is a problem	It works as expected
Local users are not allowed	Local users can connect	Yes, but there is a problem	It works as expected
Anonymous users has NO write permissions	It can upload files	-	It works as expected
Anonymous users are not asked for a anonymous password.	The server ask for a password	-	It works as expected
Data connection timeout will be 30 secs	Timeout is not set	Timeout is set but it's wrong	It works as expected
Limit max data transfer bandwidth to 5KB/s	Limit is not set	Limit is set but it's wrong	It works as expected
The server shows a banner	No banner	It shows a wrong banner	It works as expected
The server shows an ascii art file in the land directory	No ascii art	Your ascii art makes my eyes bleed.	It works as expected

Table 2. FTP server with local users rubric

Requirement	0 points	1 point	3 points
You can access with users `charles` and `laura`	Access is not possible	There is some problem	Works as expected
The user `charles` is chrooted	He is not chrooted	-	Works as expected
The user `laura` can move outside its home folder	She is chrooted	-	Works as expected
Anonymous users are forbidden	Anonymous users can access	-	Works as expected
The server shows a banner	No banner	It shows a wrong banner	It works as expected

Requirement	0 points	1 point	3 points
Configure the SSL/TLS on FTP server	It does not work	-	It works as expected
Local users are forced to connect with a secure connection	Users can connect through a plain connection	-	It works as expected

Table 3. Documentation rubric

Requirement	0 points	2 point	5 points
Document the configuration of the servers	No documentation at all	The documentation consist on a dump of configuration files	Well documented and explained. The configuration files are commented.
Documentation shows the tests	No tested	Something is tested, not all	Everything is tested
Document on the importance of encryption in secure file transfer.	No documentation about it.	Explain something but it's not enough or the quality is low.	Well documented and explained.

Table 4. Deployment

Requirement	0 points	1 point	3 points
Deployment is automatized	Deployment is manual	Deployment needs some manual changes	Deployment is automatic

5.2. References

- Course notes in Moodle
- https://man.archlinux.org/man/vsftpd.conf.5
- https://www.digitalocean.com/community/tutorials/how-to-set-up-vsftpd-for-anonymous-downloads-on-ubuntu-16-04

6. Resultados de aprendizaje y criterios de evaluación

Resultados de Aprendizaje	Criterios de evaluación
RA1. Administra servicios de resolución de nombres, analizándolos y garantizando la seguridad del servicio.	d), e), g) j)
RA4. Administra servicios de transferencia de archivos ase- gurando y limitando el acceso a la información.	a), b), c), d), e), f), g), h), i)