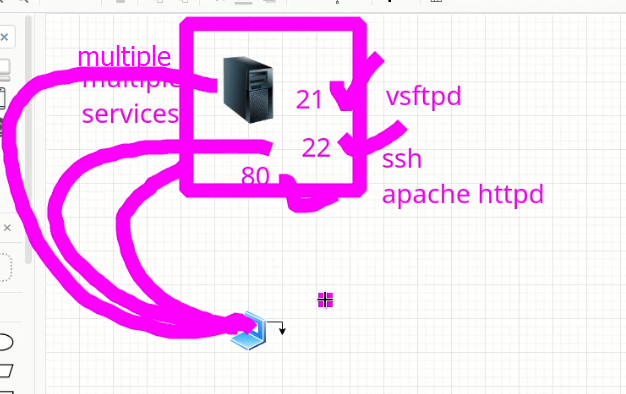
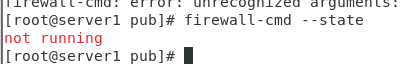
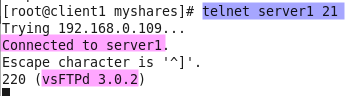
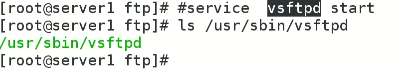
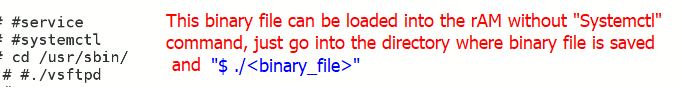
Lecture 10

**ServicecConcepts-Securing-vSFTP**

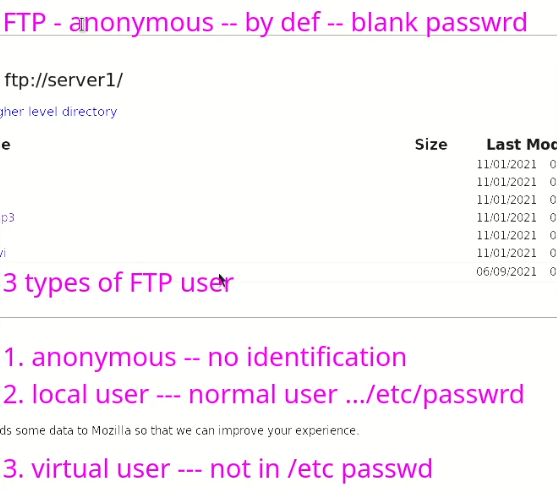
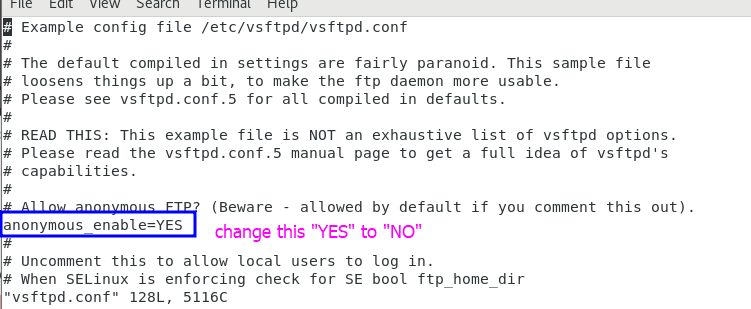
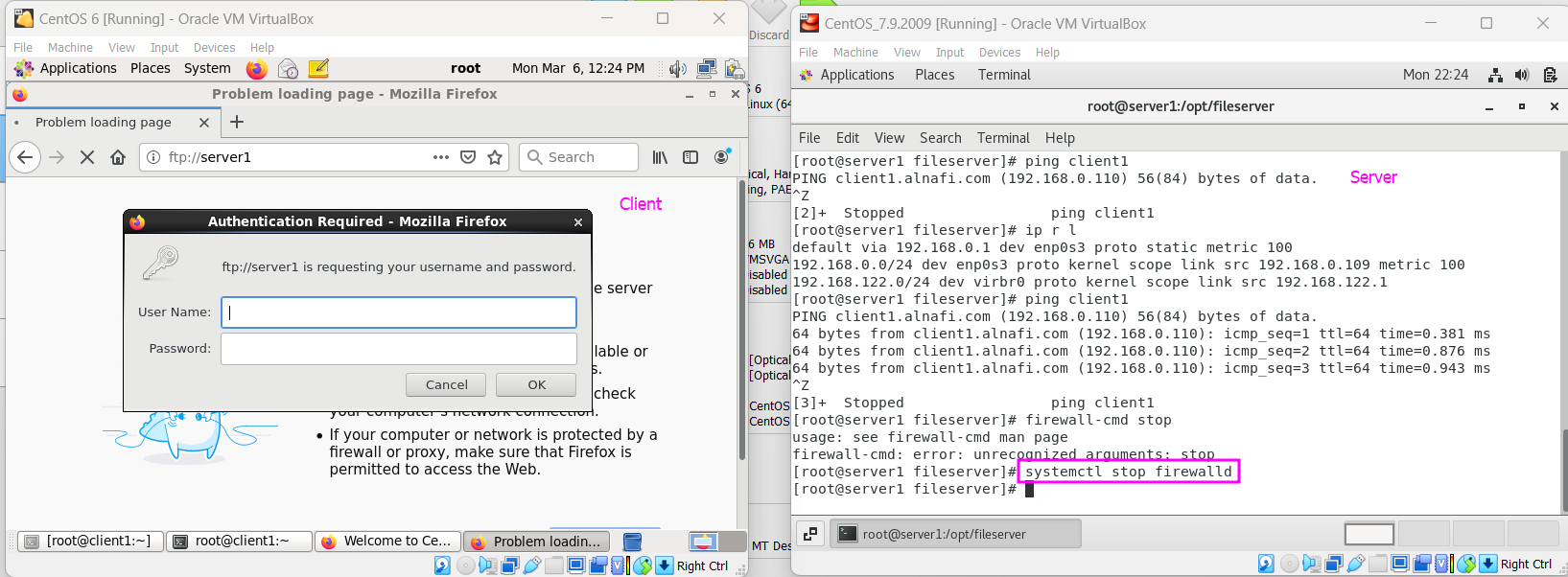
**Services**



* Multiple services can be configured on a single machine but it is not a -professional way because in production environment this practice is avoided.
* vsftbd package is already installed in our machine (during last lacture)
* in RHEL 8 or CentsOS 8
  + **systemctl -list-units**
  + this is detail of all services.
  + **$ list-uint-files** 🡪 also lists details of services
  + **Same thing in CentOS 6 🡪 $ chkconfig --list**
* **$ systemctl list-unit-files | grep -i vsftpd**
* A picture containing text

  Description automatically generated
* That’s why a newly installed package
  + **$ systemctl enable <package>** 🡪 the package will start while booting. 🡪 remember it is not start of a package
  + To start that package 🡪 **$ systemctl start <package>**
  + To check status **$ systemctl status <package>**
  + To check opened port **$ ss -tulnp | grep -I <package>**
  + Default path of **“ftp”** is **“/var/ftp/**
    - There is a directory called **“pub”**
    - The **"pub"** directory in **"/var/ftp/"** is a commonly used directory in FTP servers. "pub" stands for "public", and it is often used to store files that can be accessed by anyone who has access to the FTP server.
    - In many FTP servers, the "pub" directory is created by default as a subdirectory of "/var/ftp/". It may contain subdirectories for different types of files, such as "documents", "images", "music", and so on. These subdirectories may be further organized by file type, date, or other criteria.
    - The contents of the "pub" directory are often publicly accessible and may be downloaded or uploaded by anyone who has access to the FTP server. However, it is also possible to restrict access to certain files or directories within the "pub" directory by setting appropriate permissions and user groups.
    - It is important to note that the "pub" directory may not be secure for sensitive or confidential information, as it is accessible to anyone who has access to the FTP server. In such cases, it may be necessary to use more secure methods of file transfer, such as SFTP or SCP.
  + How to check “firewall” status on server
  + $ firewall-cmd - -state
  + 
  + telnet on client to check port no 21 is open or not
  + 
* **Important** **🡪 to check which corresponding files are copied by a specific package in system.**
  + $ rpm -ql **<package\_name>**
  + $ rpm -qc **<package\_name>** 🡪 filters and displays “configuration files”.
  + $ rpm -qd **<package\_name>** 🡪 shows “documents” copied during installation of a specific package.
  + Every package has most important file (binary\_file) 🡪 it is program of a specific package.
  + **Whenever we start a package or service by $ systemctl start vsfptd 🡪 its binary file is loaded into the RAM**
  + 
  + This binary file (mostly in /sbin/ directory) can be loaded into RAM with “systemctl start” 🡪
  + To locate binary file $ which <package\_name> e.g $ which vsftpd
  + 
  + 
  + To take it our of memory or RAM 🡪 $ pidof <binary\_file> and then $ pkill <PID>

**FTP (securing vsFTPd)**

* 
* *We can download content from internet because we access that content as “anonymous” user type.*
* For security reasons this anonymous user type must be disabled.
* The anonymous user type is enabled because it is written in binary (file) of FTP.
* To disable it,
  + - One way is to get source code of FTP server and then change it there.
    - 2nd option is change it in **configuration,**
    - There is a config file 🡪 of the package (vsftpd)
    - *Configuration file* ***(every service has a config file)*** *can change running binary parameters.*
    - $ rpm -qc <package\_name>
    - <package\_name>.**conf**
    - Here for “vsftpd”
      * $ /etc/vsftpd/vsftpd.conf
    - **Professional way** to do it is to take backup of that “conf” file.
    - 
    - $ vi /etc/vsftpd/vsftpd.conf 🡪 to edit.
    - 
    - Then **restart** the service to load it again into the RAM with changes.
    - $ systemctl restart vsftpd
    - I did it successful on VMs
    - 
    - But I must disable the firewall always after reboot.
    - I restarted both VMs too
    - After disabling the anonymous user in “vsftpd” and setting it value to “No” the client cant access the files available in /var/ftp and a popup requires username and password.