VUGT

**/etc/vsftp/vsftp.conf -- vsftpd is the default ftp server in RHEL7**

- /var/ftp (root directory for server, enabled by default)

- /var/ftp is owned by user/group root. Anon users are given read/execute permissions. Is also the home folder of the user "ftp" (which has nologin set in passwd)

- find that with **grep ftp /etc/passwd** listing the user 'ftp'

systemctl enable vsftp

/etc/vsftpd/vsftpd.conf    --config file has it's own man page

/usr/sbin/vsftpd

/etc/vsftpd/ftpusers  --list users who should NOT be able to log on through the system

/etc/vsftpd/user\_list --similar list of users who should NOT be able to log on through the system

/etc/vsftpd/vsftp\_conf\_migrate.sh

/var/ftp/

/var/ftp/pub  -- for anonymous users

various config file options:

anonymous\_enable=YES/NO  (enabled by default- allows anon login)

local\_enable= YES can be a security hole! - allows local users to log in - SELinux boolean ftp\_home\_user=on needed to work

write\_enable=YES/NO  (enable/disable write commands on those authenticated users)

local\_umask=022 --default permissions are 755 (directories) and 644 for files

dirmessage\_enable=YES  (messages displayed when certain directories are opened)

xferlog\_enable=YES (log transfers) /var/log/xfrlog

connect\_from\_port\_20=YES (ensure transfers are on only port 20)

chown\_uploads=YES (allows anon uploads to be owned by a specific user)

anon\_upload\_enable- self explanatory- you generally don't want anon users writing anything

anon\_mkdir\_write\_enable

Remember that wget requires you know the exact file to download.

Vugt uses lftp for client.

OLDER STUFF

#################################

TFTPD - Trivial File Transfer Protocol Daemon

#################################

Fast connectionless (UDP)

Often used with network devices (VOIP phones, PXE, router/firewall/switch)

Use for LAN only

client= tftp-\*rpm, server=tftp-server\*rpm

Server installs xinetd dependency

configure tftp via /etc/xinetd.d/tftp before starting

change 'disable' to 'no'

server is identified here as /usr/sbin/in.tftpd

server\_args specifies source folder with -s /tftpboot

service xinetd start

TFTPD listens on UDP:69 piped through xinetd (shown in netstat)

created router1.config file with touch in tftpboot/

copy cisco router "running-config" to the server tftp://192.168.75.199/router1.config

FAILED - tail var/log/messages reveals SELinux is blocking

-- SELinux says in message to run sealert -l 2asgfdagh9q-weqtr3y5

--- running this returns a detailed description specific to this instance of the error

--- says to run setsebool -P tftpd\_disable\_trans=1 and then service xinetd restart to restart tftpd as well… disables SELinux from blocking tftp

-retry tpftp:// transfer and it works

chmod 666 router1.config to make it world writable-

Use tftp client to get file from router - this downloads to current directory

tftp 192.168.75.199 -c get router1.config

-c is for command

tftp without options puts you in interactive mode

when done, he re-disabled server in xinetd.d/tftp and restarted xinet service

#################################

VSFTPD -  Very Secure File Transfer Protocol Daemon

#################################

**Still cleartext!**

- uses standard FTPD in conjunction with selinux and PAM

- chroot jail

- anon and local user authorization

- rate limiting (restrict non-anonymous users with local\_max\_rate=1000 for 1000 bytes per sec)

- no xinetd needed-but CAN be enabled - see xinetd instructions in TFTP (identical from CBTNuggets videos.

- for IPv6 two separate instances have to be running with separate cfg files (one for 4 and one for IPv6)

CBTNuggets note: vsftpd.conf and vsftp.user\_list are sometimes used in the /etc dir- not /etc/vsftp.  Says that config directive userlist\_deny=YES or NO determines if these are allowed or prohibited from logging in

yum -y install vsftpd -install it

service vsftpd start -start it

netstat -ntlp | grep 21 -make sure it's running

chkconfig vsftpd on -starts for all multiuser runlevels

- logged in as anonymous, attempted to put file but had to turn on anon\_upload\_enable

- logged in as existing user and got an error about opening users home dir.

tail /var/log/messages   -shows SELinux preventing, gives sealert -l code

sealert -l a765d6874e96…   -tells us the command to run to allow user access to home dir

setsebool -P ftp\_home\_dir=1   -this is the fix

service vsftpd restart   --run to set changes into effect

- logs in and meets file.

- notes that we need to chroot jail local users and disable anon access

- in vsftpd.conf, removes anon access.  chroot options include listing users specifically

chroot\_local\_user=YES   jails all users to their home dir.  For exceptions, chroot\_users\_list should have usernames of those users

#################################

LFTPD -  Lightweight FTP Client-shell

#################################

- Connects to FTP, HTTP, HTTPS, SFTP

- Interactive or non-interactive modes

- Supports scripting (use -f scriptname)

- behaves like BASH, command history, background cmd execution(CTRL-Z), tab completion, cat

- reconnect/retransmit/download/upload continuation (from previous session with mget and mput -c option)

- supports bookmarks

/usr/bin/lftp

/etc/lftp.conf --system-wide config

~/.lftprc --user-specific config file (also read- over-rides global conf file)

lftp  --interactive mode.  Entering 'set -a' in this mode lists all the variables that can be set

lftp username@server.name.tld  OR  lftp username:password@server.name.tld

lftp -u username,password sftp://server.name.tld

lftp.conf

- aliases set for commands (i.e., dir for ls)

- maximum redirections, proxies, passive mode on/off,

jobs --lists jobs currently running in background

mirror -v mirror/   ---mirrors a remote directory to the local system

help  ---lists commands

help command  ----lists command options

!command -- !bash  --gives a BASH shell

~/.lftp/   ---hidden directory

~/.lftp/cwd\_history  --lists transfer server history

~/.lftp/rl\_history  -- lists command history

==============================

FTP client commands

==============================

gftp for Gnome client

open ftp.server.com

cd, ls

ascii or binary to switch modes

get and put

!command runs the command on the machine you are "sitting at" rather than server.