**Proftpd 1.3.5**

**Cài đặt những thư viện cần thiết**

sudo apt update

sudo apt install build-essential

sudo apt-get install libssl-dev

sudo apt-get install libz-dev

sudo apt-get install daemon

**Cấu hình tường lửa**

sudo ufw allow 21

**Cài đặt proftpd phiên bản 1.3.5**

cd /opt/download

wget ftp://ftp.proftpd.org/distrib/source/proftpd-1.3.5.tar.gz

tar -xf proftpd-1.3.5.tar.gz

**Cấu hình và thiết lập proftp trên máy chủ**

./configure --with-modules=mod\_copy

./configure --enable-dso --with-shared=mod\_copy

make && make install

whereis proftpd

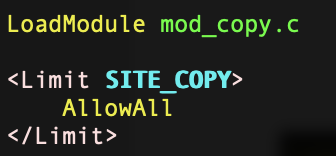
* Tập tin thực thi: /usr/local/sbin/proftpd
* Tập tin cấu hình: /usr/local/etc/proftpd.conf

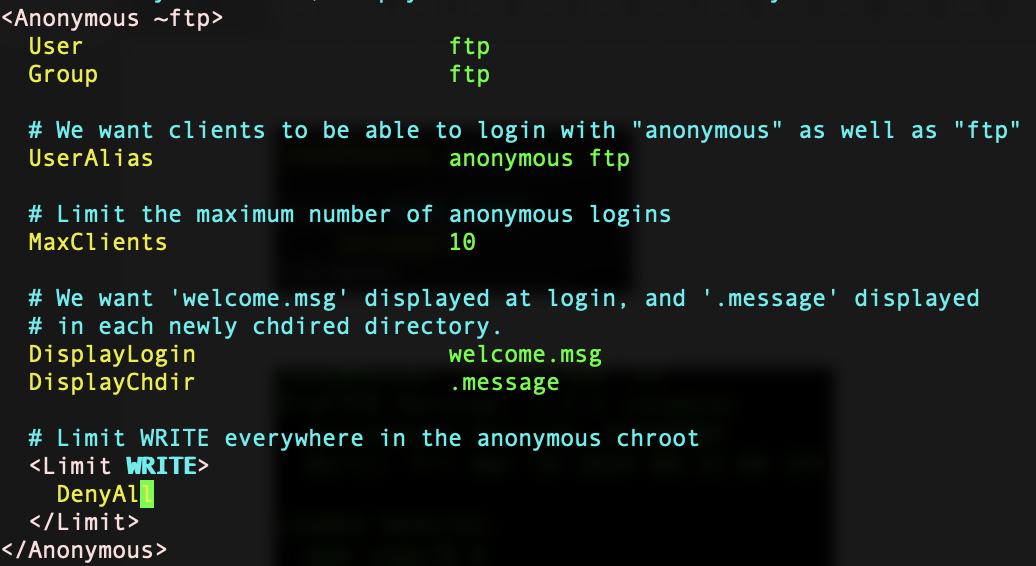


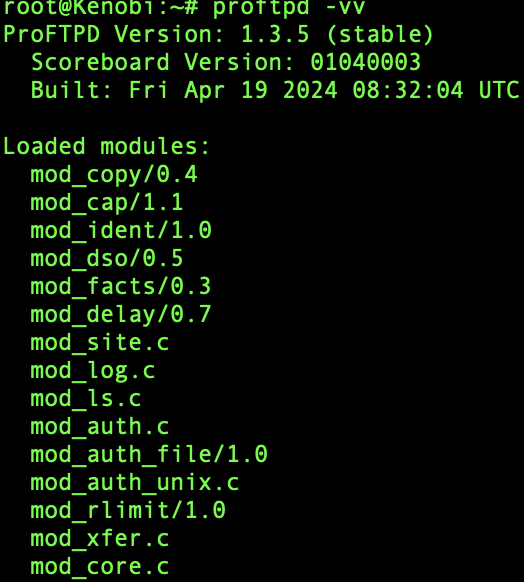
proftpd -vv: liệt kê các module của proftpd

Để khai thác lỗ hổng proftpd 1.3.5, proftpd phải tải được thư viện mod\_copy

Chỉnh sửa tập cấu hình của proftpd:







**Tạo người dùng ftp**

cd /home

sudo mkdir FTP-shared

sudo useradd ftp -p your\_password -d /home/FTP-shared

sudo passwd ftp

Trong thư mục FTP-shared, tạo thư mục download và upload:

cd /home/FTP-shared/

sudo mkdir download

sudo mkdir upload

Cấp quyền cho thư mục:

cd /home

sudo chmod 755 FTP-shared

cd FTP-shared

sudo chmod 755 download

sudo chmod 777 upload

**How to Start, Stop, and Restart the ProFTPD Service**

cp /opt/download/proftpd-1.3.5/contrib/dist/rpm/proftpd.init.d /etc/init.d/proftpd (tập tin chạy dịch vụ proftpd)

cd /etc/init.d

chmod 0755 proftpd

Proftpd bạn tải dành cho distro linux: rpm.

Bạn phải cấu hình lại proftpd để cho phù hợp với ubuntu 20.04

sudo apt-get install daemon

sudo sed -i 's/^\.\ \/etc\/rc.d\/init.d\/functions$/\.\ \/lib\/lsb\/init-functions/g' /etc/init.d/proftpd

sudo sed -i 's/status\ /status\_of\_proc\ /g' /etc/init.d/proftpd

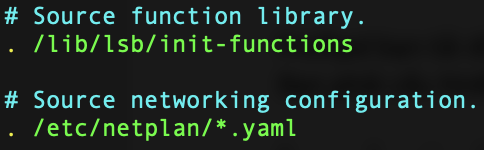
sudo sed -i 's/daemon\ --user=\$user\ \$exec\ -ud\ \$config/daemon\ --user=\$user\ --\ \$exec\ -d\ \$config/g' /etc/init.d/proftpd

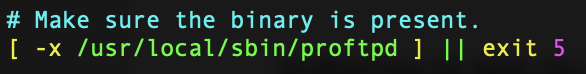
sudo sed -i 's/\/var\/lock\/subsys\/\$prog/\/var\/lock\/\$prog/g' /etc/init.d/proftpd

Source function library: /lib/lsb/init-functions

Source networking configuration: /etc/netplan/\*.yaml

Proftpd binary: /usr/local/sbin/proftpd





/etc/init.d/proftpd start

/etc/init.d/proftpd stop

/etc/init.d/proftpd status

**References:**

https://actsupport.com/how-to-install-and-configure-proftpd-on-linux-server/

https://macosx.com/threads/ftp-passive-mode-problem.234517/

https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu

http://www.proftpd.org/docs/contrib/mod\_copy.html#Installation

https://unix.stackexchange.com/questions/9314/no-such-file-or-directory-etc-init-d-functions

network configuration file: /etc/netplan/\*.yaml

https://delightlylinux.wordpress.com/2017/06/10/how-to-set-up-anonymous-ftp-with-proftp/

http://www.proftpd.org/docs/howto/DSO.html

http://proftpd.org/docs/contrib/mod\_copy.html

https://ubuntuforums.org/showthread.php?t=79588

https://stackoverflow.com/questions/19606049/nagios-4-can-t-open-etc-rc-d-init-d-functions

**VSFTPD**

Module mod\_copy của Proftpd 1.3.5 cho phép kẻ tấn công đọc và ghi các tập tin bất kỳ bằng lệnh site cpfr và site cpto. Bất kỳ người dùng nào không xác thực cũng có thể lợi dụng những lệnh này để sao chép tập tin đến vị trí họ mong muốn. Lệnh sao chép được thực thi dưới đặc quyền của dịch vụ proftpd, mặc định là đặc quyền của người dùng nobody

Để tránh bị kẻ tấn công khai thác, mình phải cập nhật phần mềm thường xuyên. Ở đây, mình sẽ tải file server mới nhất bằng vsftpd

**Install**

apt install vsftpd

service vsftpd status

**Configure Firewall**

ufw allow 21

ufw enable

**Create FTP user**

sudo useradd ftpuser

sudo passwd ftpuser

sudo mkdir /home/ftpuser/ftp

sudo chown nobody:nogroup /home/ftpuser/ftp

sudo chmod a-w /home/ftpuser/ftp

sudo mkdir /home/ftpuser/ftp/files

sudo chown ftpuser:ftpuser /home/ftpuser/ftp/files

**VSFTPD Server Configuration**

sudo mv /etc/vsftpd.conf /etc/vsftpd.conf.origin

sudo vi /etc/vsftpd.conf

listen=NO

listen\_ipv6=YES

anonymous\_enable=NO

local\_enable=YES

write\_enable=YES

local\_umask=022

dirmessage\_enable=YES

use\_localtime=YES

xferlog\_enable=YES

connect\_from\_port\_20=YES

chroot\_local\_user=YES

secure\_chroot\_dir=/var/run/vsftpd/empty

pam\_service\_name=vsftpd

force\_dot\_files=YES

pasv\_min\_port=40000

pasv\_max\_port=50000

user\_sub\_token=$USER

local\_root=/home/$USER/ftp

sudo systemctl restart vsftpd.service

**Test FTP Connection**

ftp file\_server\_ip

🡺Vì vsftpf không có mod copy nên bạn không thể khai thác lỗ hổng trên

**Secure FTP Server with TLS**

FTP vận chuyển dữ liệu ở dạng bản rõ, nó dễ bị tấn công MITM, trong khi kẻ tấn công chặn liên lạc giữa máy khách và máy chủ và có thể giả mạo dữ liệu được truyền.

FTP Server: ip 48.216.216.38

FTP Client: ip 192.168.1.6

Kết nối đến dịch vụ ftp

Lấy tài khoản người dùng bằng Ettercap

Để chống lại các cuộc tấn công mitm, mình sẽ bảo mật máy chủ file với TLS

**Tạo 1 chứng chỉ SSL:**

sudo openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem

**Secure FTP with TLS**

sudo vi /etc/vsftpd.conf

ssl\_enable=YES

rsa\_cert\_file=/etc/ssl/private/vsftpd.pem

rsa\_private\_key\_file=/etc/ssl/private/vsftpd.pem

allow\_anon\_ssl=NO

force\_local\_data\_ssl=YES

force\_local\_logins\_ssl=YES

ssl\_tlsv1=YES

ssl\_sslv2=NO

ssl\_sslv3=NO

require\_ssl\_reuse=NO

ssl\_ciphers=HIGH

systemctl restart vsftpd.service

**Testing FTP with TLS**

Mã hóa dữ liệu truyền đi bằng SSL/TLS, kẻ tấn công không thể tấn công MITM.

🡪Phòng thủ thành công

**Disable Shell Access**

sudo vi /etc/ssh/sshd\_config

DenyUsers ftpuser

sudo service sshd restart

**NFS Server**

**Installing and Configure NFS Server**

apt update

apt -y install nfs-kernel-server

systemctl status nfs-server

mkdir /exports

mkdir /exports/backups

vi /etc/exports

/exports/backups \*(rw,sync,no\_subtree\_check)

exportfs -ar

exportfs -v

ufw allow to any port nfs

**Open NFS ports on Ubuntu**

**/etc/default/nfs-kernel-server for MOUNTD:**

Original:

RPCMOUNTDOPTS="--manage-gids"

New:

RPCMOUNTDOPTS="--manage-gids --port 9024"

systemctl restart nfs-mountd.service

Xem dịch vụ mountd đang chạy trên cổng nào:

rpcinfo -p | grep 'tcp.\*mountd'

100005 1 tcp 9024 mountd

100005 2 tcp 9024 mountd

100005 3 tcp 9024 mountd

**/etc/default/nfs-common for STATD:**

Original:

STATDOPTS=

New:

STATDOPTS="--port 662"

**/etc/sysctl.conf for LOCKD:**

Add:

fs.nfs.nlm\_tcpport = 32803

fs.nfs.nlm\_udpport = 32769

Then just run:

sysctl -p

systemctl restart nfs-kernel-server

**References**

https://bgstack15.wordpress.com/2019/05/30/nfs-export-works-but-showmount-e-does-not/

https://docs.portworx.com/portworx-enterprise/operations/operate-kubernetes/storage-operations/create-pvcs/open-nfs-ports

https://askubuntu.com/questions/1313682/set-static-ports-for-nfs-v3-on-ubuntu-20-x-server

**SMB Server**

**Installing and Configuring Samba**

apt install samba

cd /etc/samba/

vim smb.conf

security=user

map to guest=bad user

[anonymous]

path=/home/anonymous

available=yes

read only=no

brosable=yes

public=yes

writable=yes

guest ok=yes

mkdir /home/anonymous

cd /home/anonymous

echo "cyberninja was here" > note.txt

service smbd restart

ufw allow samba

**Attacking Anonymous SMB**

smbclient -L //48.216.216.38

smbclient //48.216.216.38/anonymous -p 139

cat note.txt