root@ubuntuWebServer:/etc# ldd $(which sshd) | grep libwrap

libwrap.so.0 => /lib/x86\_64-linux-gnu/libwrap.so.0 (0x00007f9122442000)

# /etc/hosts.deny: list of hosts that are \_not\_ allowed to access the system.

# See the manual pages hosts\_access(5) and hosts\_options(5).

#

# Example: ALL: some.host.name, .some.domain

# ALL EXCEPT in.fingerd: other.host.name, .other.domain

#

# If you're going to protect the portmapper use the name "rpcbind" for the

# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.

#

# The PARANOID wildcard matches any host whose name does not match its

# address.

#

# You may wish to enable this to ensure any programs that don't

# validate looked up hostnames still leave understandable logs. In past

# versions of Debian this has been the default.

# ALL: PARANOID

sshd,vsftpd: ALL

ALL:ALL

# /etc/hosts.allow: list of hosts that are allowed to access the system.

# See the manual pages hosts\_access(5) and hosts\_options(5).

#

# Example: ALL: LOCAL @some\_netgroup

# ALL: .foobar.edu EXCEPT terminalserver.foobar.edu

#

# If you're going to protect the portmapper use the name "rpcbind" for the

# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.

#

sshd,vsftpd : 10.106.3.127,LOCAL