

# evitar ingreso ftp-linux

```
Ubuntu23 - VMware Workstation 17 Player (Non-commercial use only)
10 de ago 09:53
atomo@atomo-virtual-machine: ~$ sudo apt install vsftpd -y
[sudo] contraseña para atomo:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  vsftpd
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 47 no actualizados.
Se necesita descargar 123 kB de archivos.
Se utilizarán 326 kB de espacio de disco adicional después de esta operación.
Des:1 http://ar.archive.ubuntu.com/ubuntu jammy/main amd64 vsftpd amd64 3.0.5-0ubuntu1 [123 kB]
Descargados 123 kB en 0s (262 kB/s)
Preconfigurando paquetes ...
Seleccionando el paquete vsftpd previamente no seleccionado.
(Leyendo la base de datos ... 212596 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../vsftpd_3.0.5-0ubuntu1_amd64.deb ...
Desempaquetando vsftpd (3.0.5-0ubuntu1) ...
Configurando vsftpd (3.0.5-0ubuntu1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /lib/systemd/system/vsftpd.service.
Procesando disparadores para man-db (2.10.2-1) ...
atomo@atomo-virtual-machine:~$
```

```
Ubuntu23 - VMware Workstation 17 Player (Non-commercial use only)
10 de ago 09:54
atomo@atomo-virtual-machine: ~$ tail -f /var/log/auth.log
(Leyendo la base de datos ... 212596 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../vsftpd_3.0.5-0ubuntu1_amd64.deb ...
Desempaquetando vsftpd (3.0.5-0ubuntu1) ...
Configurando vsftpd (3.0.5-0ubuntu1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /lib/systemd/system/vsftpd.service.
Procesando disparadores para man-db (2.10.2-1) ...
atomo@atomo-virtual-machine:~$ tail -f /var/log/auth.log
Aug 10 09:53:16 atomo-virtual-machine sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Aug 10 09:53:20 atomo-virtual-machine groupadd[5194]: group added to /etc/group: name=ftp, GID=138
Aug 10 09:53:20 atomo-virtual-machine groupadd[5194]: group added to /etc/gshadow: name=ftp
Aug 10 09:53:20 atomo-virtual-machine groupadd[5194]: new group: name=ftp, GID=138
Aug 10 09:53:20 atomo-virtual-machine useradd[5200]: new user: name=ftp, UID=132, GID=138, home=/srv/ftp, shell=/usr/sbin/nologin, from=none
Aug 10 09:53:20 atomo-virtual-machine usermod[5207]: change user 'ftp' password
Aug 10 09:53:20 atomo-virtual-machine chage[5214]: changed password expiry for ftp
Aug 10 09:53:20 atomo-virtual-machine chfn[5218]: changed user 'ftp' information
Aug 10 09:53:29 atomo-virtual-machine sudo: pam_unix(sudo:session): session closed for user root
Aug 10 09:53:40 atomo-virtual-machine snort[1426]: [1:1917:6] SCAN UPnP service discover attempt [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.35.1:60986 -> 239.255.255.250:1900
0
```

```
Ubuntu23 - VMware Workstation 17 Player (Non-commercial use only)
Player 10 de ago 09:56
Actividades Terminal
atomo@atomo-virtual-machine: ~
GNU nano 6.2 /etc/fail2ban/jail.local *
1 [sshd]
2 enable = true
3
4 [vsftpd]
5 enable = true
6

^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación M-U Deshacer
^X Salir ^R Leer fich. ^N Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea M-E Rehacer
```

```
Ubuntu23 - VMware Workstation 17 Player (Non-commercial use only)
Player 10 de ago 09:58
Actividades Terminal
atomo@atomo-virtual-machine: ~
atomo@atomo-virtual-machine:~$ sudo nano /etc/fail2ban/jail.local
[sudo] contraseña para atomo:
atomo@atomo-virtual-machine:~$ ls /etc/fail2ban/filter.d/
3proxy.conf          domino-smtp.conf    mysqld-auth.conf    selinux-common.conf
apache-auth.conf     dovecot.conf        nagios.conf         selinux-ssh.conf
apache-badbots.conf  dropbear.conf       named-refused.conf  sendmail-auth.conf
apache-botsearch.conf drupal-auth.conf    nginx-botsearch.conf sendmail-reject.conf
apache-common.conf   ejabberd-auth.conf  nginx-http-auth.conf sieve.conf
apache-fakegooglebot.conf exim-common.conf    nginx-limit-req.conf slapd.conf
apache-modsecurity.conf exim.conf           nsd.conf            softethervpn.conf
apache-nohome.conf   exim-spam.conf      openhab.conf        sogo-auth.conf
apache-noscript.conf freeswitch.conf     openwebmail.conf    solid-pop3d.conf
apache-overflows.conf froxlor-auth.conf   oracleims.conf       squid.conf
apache-pass.conf     gitlab.conf         perdition.conf      squirrelmail.conf
apache-shellshock.conf grafana.conf        phpmyadmin-syslog.conf sshd.conf
assp.conf            groupoffice.conf    php-url-fopen.conf  stunnel.conf
asterisk.conf        gssftpd.conf        portsentry.conf     suhosin.conf
bitwarden.conf       guacamole.conf      postfix.conf         tine20.conf
botsearch-common.conf haproxy-http-auth.conf proftpd.conf         traefik-auth.conf
centreon.conf        horde.conf           pure-ftp.conf        uwimap-auth.conf
common.conf          ignorecommands      qmail.conf           vsftpd.conf
counter-strike.conf  kerio.conf          recidive.conf        webmin-auth.conf
courier-auth.conf    lighttpd-auth.conf  roundcube-auth.conf  wuftpd.conf
courier-smtp.conf    mongodb-auth.conf
```

```
Ubuntu23 - VMware Workstation 17 Player (Non-commercial use only)
10 de ago 09:58
atomo@atomo-virtual-machine: ~
atomo@atomo-virtual-machine:~$ sudo nano /etc/fail2ban/jail.local
[sudo] contraseña para atomo:
atomo@atomo-virtual-machine:~$ ls /etc/fail2ban/filter.d/
3proxy.conf          domino-smtp.conf      mysqld-auth.conf      selinux-common.conf
apache-auth.conf      dovecot.conf          nagios.conf            selinux-ssh.conf
apache-badbots.conf   dropbear.conf         named-refused.conf     sendmail-auth.conf
apache-botsearch.conf drupal-auth.conf      nginx-botsearch.conf   sendmail-reject.conf
apache-common.conf    ejabberd-auth.conf    nginx-http-auth.conf   sieve.conf
apache-fakegooglebot.conf exim-common.conf      nginx-limit-req.conf   slapd.conf
apache-modsecurity.conf exim.conf             nsd.conf               softethervpn.conf
apache-nohome.conf    exim-spam.conf        openhab.conf           sogo-auth.conf
apache-noscript.conf  freeswitch.conf       openwebmail.conf       solid-pop3d.conf
apache-overflows.conf froxlor-auth.conf     oracleims.conf         squid.conf
apache-pass.conf      gitlab.conf           pam-generic.conf       squirrelmail.conf
apache-shellshock.conf grafana.conf          perdition.conf         sshd.conf
assp.conf             groupoffice.conf      phpmyadmin-syslog.conf stunnel.conf
asterisk.conf          gssftpd.conf          php-url-fopen.conf     suhosin.conf
bitwarden.conf        guacamole.conf        portsentry.conf        tine20.conf
botsearch-common.conf haproxy-http-auth.conf postfix.conf            traefik-auth.conf
centreon.conf          horde.conf            proftpd.conf           uwimap-auth.conf
common.conf           ignorecommands        pure-ftpd.conf         vsftpd.conf
counter-strike.conf   kerio.conf            qmail.conf             webmin-auth.conf
courier-auth.conf     lighttpd-auth.conf    recidive.conf          wuftpd.conf
courier-smtp.conf     mongodb-auth.conf     roundcube-auth.conf    xinetd-fail.conf
```

```
Símbolo del sistema - ftp 192
C:\Users\Usuario>ftp 192.168.35.137
Conectado a 192.168.35.137.
220 (vsFTPd 3.0.5)
200 Always in UTF8 mode.
Usuario (192.168.35.137:(none)): redes
331 Please specify the password.
Contraseña:
530 Login incorrect.
Error al iniciar la sesión.
ftp> |
```

```
Ubuntu23 - VMware Workstation 17 Player (Non-commercial use only)
10 de ago 10:28
atomo@atomo-virtual-machine: ~
atomo@atomo-virtual-machine:~$ tail -f /var/log/vsftpd.log
tail: no se puede abrir '/var/log/vsftpd.log' para lectura: Permiso denegado
tail: no queda ningún fichero
atomo@atomo-virtual-machine:~$ sudo tail -f /var/log/vsftpd.log
[sudo] contraseña para atomo:
Thu Aug 10 10:25:34 2023 [pid 5546] CONNECT: Client "::ffff:192.168.35.1"
Thu Aug 10 10:25:57 2023 [pid 5545] [redes] FAIL LOGIN: Client "::ffff:192.168.35.1"
```

```
Ubuntu23 - VMware Workstation 17 Player (Non-commercial use only)
10 de ago 10:32
atomo@atomo-virtual-machine: ~
atomo@atomo-virtual-machine:~$ tail -f /var/log/vsftpd.log
tail: no se puede abrir '/var/log/vsftpd.log' para lectura: Permiso denegado
tail: no queda ningún fichero
atomo@atomo-virtual-machine:~$ sudo tail -f /var/log/vsftpd.log
[sudo] contraseña para atomo:
Thu Aug 10 10:25:34 2023 [pid 5546] CONNECT: Client "::ffff:192.168.35.1"
Thu Aug 10 10:25:57 2023 [pid 5545] [redes] FAIL LOGIN: Client "::ffff:192.168.35.1"
Thu Aug 10 10:31:30 2023 [pid 5600] CONNECT: Client "::ffff:192.168.35.1"
Thu Aug 10 10:31:39 2023 [pid 5599] [cafe] FAIL LOGIN: Client "::ffff:192.168.35.1"

iTop Screen Recorder
La captura de pantalla se ha guardado en:
C:\Users\Usuario\Desktop\8.jpg
```