Islamic Republic Of Iran Security Team
Www.IrIsT.Ir

Installing DrWEB Antivirus

نصب کردن آنتی ویروس DrWEB برای اجرا در کنترل پنل سرور لینوکس

با عرض سلام و خسته نباشید.

در این مقاله ما قدم به قدم به نحوه نصب کردن آنتی ویروس DrWEB سرور لینوکس و اجرای آن در کنترل پنل می پردازیم.

۱- نصب کردن DrWEB

خوب شما اول از همه باید نسخه RPM را از لینک زیر دانلود کنید:

http://www.sald.com/get.html

حالا به نصب این rpm می پردازیم:

```
# rpm -Uvh ftp://ftp.drweb.ru/pub/unix/drweb-4.30-glibc.2.3.i586.rpm
```

و به وسیله این فرمان آن را اجرا کنید:

```
# /opt/drweb/drwebd start
```

خوب حالا بهتون میگم که چطوری به صورت اتوماتیک دیتابیس اون آپدیت می شه.
این فرمان رو وارد کنید:

```
00 12 * * * /opt/drweb/update/update.pl
```

به همین سادگی.

خوب حالا می رسیم سر اصل مطلب.

۲- نصب و پیکربندی DrWEB Exim

بر روی سرور, drweb-exim رو از سایت زیر دریافت کنید :

http://www.sald.com/get.html

و از حالت فشرده در بیارید:

```
tar xzvf drweb-exim-4.29.12-F-linux.tar.gz
```

حالا ما باید فایلهای drweb-exim را در یک دایرکتوری مناسب کپی کنیم:

```
# cp -r drweb-exim/etc/drweb/* /etc/drweb/
# cp -r drweb-exim/opt/drweb/doc/* /opt/drweb/doc/
# cp -r drweb-exim/opt/drweb/drweb-* /opt/drweb/
```

حالا با یک ویرایشگر خوب این فایل رو باز کنید:

/etc/drweb/drweb_exim.conf

و

AdminMail = postmaster>

رو به

AdminMail = you@yourdomain.com>

تغییر دهید.
و سپس این فرمان رو بزنید:

```
# /opt/drweb/drweb-exim --check_only --check_user=drweb
```

۳- پیکربندی Exim

اکنون ما باید تغییراتی رو در ۲ فایل برای استفاده بهتر ایجاد کنیم.

فایل اول /etc/exim.conf

بعد از باز کردن این فایل دستورات داخلی باید به شکل زیر باشد:

```
###### begin exim.conf ########

[skipped]>

###########################
# Runtime configuration file for Exim #
###########################

trusted_users = drweb
trusted_groups = drweb

[skipped]


#!!# message_filter renamed system_filter
system_filter = /etc/antivirus.exim
message_body_visible = 5000

>system_filter_pipe_transport = filter_pipe
system_filter_reply_transport = address_reply

[skipped]

###########################
```

```
# TRANSPORTS CONFIGURATION #
########################## ORDER DOES NOT MATTER #
# Only one appropriate transport is called for each delivery. #
########################## A transport is used only when referenced from
a director or a router that
# successfully handles an address.

# This transport is used for delivering messages over SMTP connections.

begin transports

filter_pipe:
driver = pipe
user = drweb
group = mail
return_fail_output

>

###### end exim.conf ########>
```

و همچنین فایل /etc/antivirus.exim که ما باید به آخرین خط, این کد را اضافه کنیم:

```
###### begin antivirus.exim #######>>

# to prevent from mail loop, skip already scanned message
if $received_protocol is "drweb-scanned"
then
finish
endif


>pipe "/opt/drweb/drweb-exim -f $sender_address -- $recipients"


>>finish



###### end antivirus.exim ########>>
```

٤- Restart کردن آنتی ویروس

اکنون برای رستارت کردن از این فرمان استفاده کنید:

```
# /etc/rc.d/init.d/exim restart
```

نکته: شما به این فایلها برای تغییرات نیاز دارید:

```
etc/exim.conf

/etc/antivirus.exim
```

که بهتره یک بک آپ از این ۲ تا فایل تهیه کنید.

به پایان این مقاله رسیدیم و باید بگم که این مقاله به منظور آشنایی شما با نحوه نصب آنتی ویروس و همچنین بالا بردن سطح امنیتی سرور لینوکس می باشد که امیدوارم به مورد قبول شما قرار گرفته شده باشه.

پایان.

خوب این بحث هم به پایان رسید و اگر مشکلی وجود داشت به بزرگواری خودتون ببخشید و اعلام کنید تا این مشکل را برطرف نماییم.

:::::یک تشکر ویژه از **مدیران و بچه های تیم IrIsT**::::

با تشکر از همگی:

نویسنده: **مدیر تیم IrIsT™ (امیر موسوی)**

صفحه اصلی سایت: **Www.IrIsT.Ir**

تالار گفتمان سایت: **Www.IrIsT.Ir/forum/**

ایمیل: **Admin@IrIST.Ir**

کپی برداری فقط با ذکر لینک کامل مقاله و همچنین نام سایت مجاز می باشد.