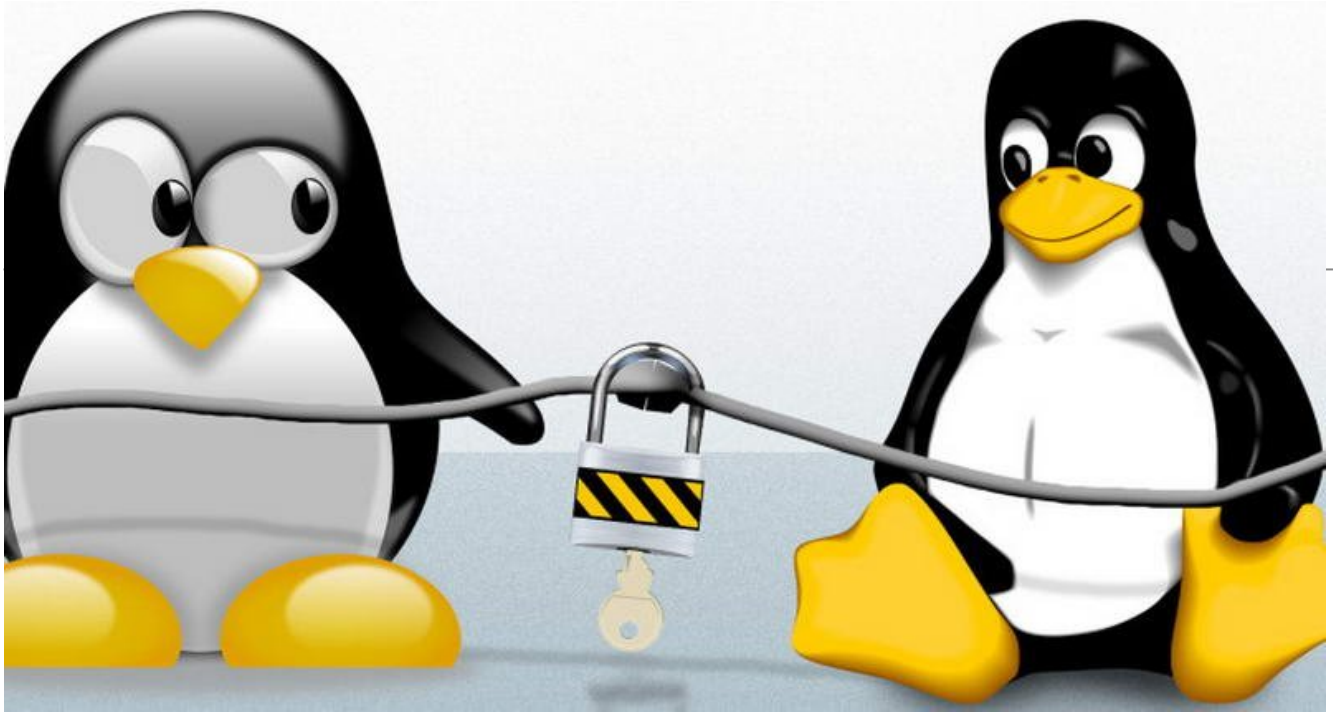
راهکارهایی برای افزایش امنیت یک سرور لینوکسی

چگونه سرور لینوکس امن‌تری داشته باشیم؟



سرورهای لینوکس برای موارد متعددی از جمله فایل سرور برای مدیریت و نگهداری فایل‌ها، وب سرور برای میزبانی سایت‌های اینترنتی، میل سرور برای برای ساخت و مدیریت ای‌میل و بسیاری از موارد دیگر مورد استفاده قرار می‌گیرند. هر چند استفاده و نگهداری از سرورهای خانگی و خصوصی به دلیل عدم ارتباط آنها با شبکه اینترنت بسیار راحت‌تر است، اما در صورتی که سرور شما به شبکه جهانی اینترنت متصل باشد برای نگهداری و محافظت از آن باید ضوابط و نکات امنیتی مربوط به آن را نیز رعایت کرد. کسانی که تازه با سیستم‌عامل لینوکس آشنا شده‌اند و قصد دارند سرور اختصاصی خود را مدیریت کنند، باید چند نکته ضروری را رعایت کنند که ما در این مقاله قصد داریم به آنها بپردازیم.

چیزهایی را نصب کنید که به آن نیاز دارید

اگر قصد دارید یک سرور راه‌اندازی کنید، ممکن است با خود بگویید که من ۴۰ گیگابایت فضای ذخیره‌سازی در اختیار دارم؛ بنابراین می‌توانم هر نرم افزار و سرویسی را که مایل هستم نصب کنم. از لحاظ تئوری حرف شما درست است، شما مالک سرور هستید و به لطف نرم افزارهای منبع باز سیستم عامل لینوکس هر چیزی را که مایل باشید را می‌توانید نصب کنید. اما نباید این موضوع را فراموش کنید که حتی غیر قابل نفوذترین سرورها نیز ممکن است با بهره برداری از اجزای آسیب پذیر و اصلاح نشده‌ای که در آن سرور در حال اجرا هستند مورد حمله قرار بگیرند.

برای در اختیار داشتن یک سرور امن اولین قانون این است که سرور خود را تا حد امکان خلاصه و ساده نگه دارید. تنها پکیج‌هایی را که واقعا به آن نیاز دارید، نصب کنید. اگر از قبل پکیج‌های ناخواسته‌ای روی سرور شما نصب شده است آنها را پاکسازی کنید. هر چه بسته‌های نرم افزاری شما کمتر باشد احتمال مواجه شدن با باگ‌ها و حفره‌های نرم افزاری نیز کمتر می‌شود. قبل از نصب هر گونه نرم افزار و بسته‌های وابسته (مثل ownCloud)، شما باید اسناد مرتبط با آن پکیج را مطالعه کرده و تنها مواردی که به آن نیاز دارید را نصب کنید.

چیزهایی را اجرا کنید که به آن نیاز دارید

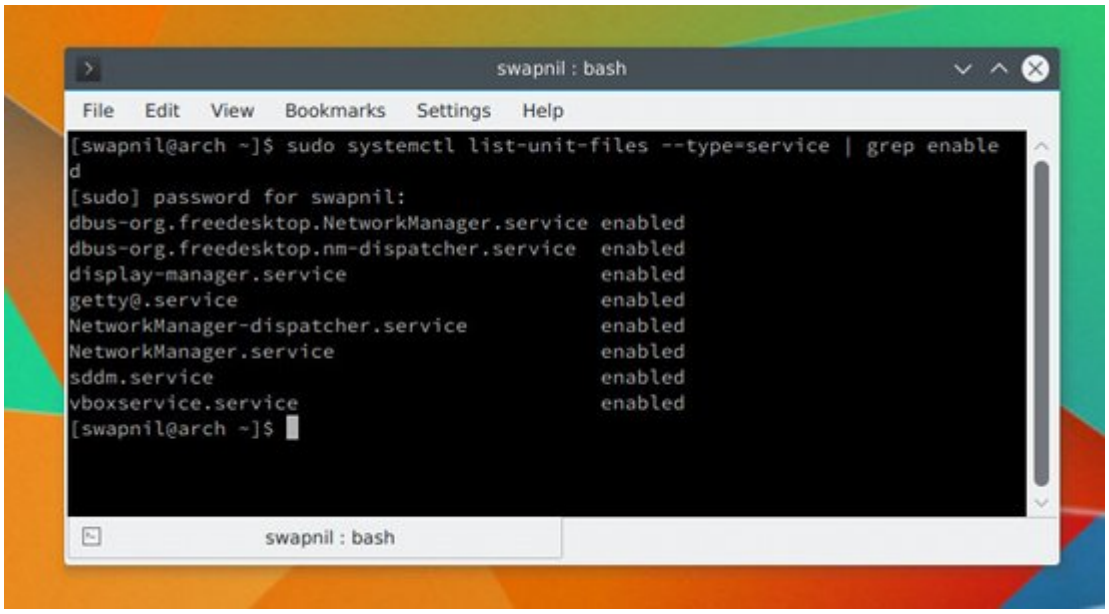
دومین قانون برای راه اندازی و حفظ امنیت یک سرور لینوکس این است که تنها سرویس‌هایی را که به آن نیاز دارید، اجرا کنید. خیلی از توزیع‌ها و پکیج‌ها ممکن است در زمان راه اندازی سرویس‌های خاصی را روی پورت‌های متفاوت اجرا کنند که می‌تواند خطرات امنیتی را به همراه داشته باشد. بنابراین ترمینال را باز کرده و فرمان زیر را اجرا کنید:

```
netstat -npl
```

خروجی این فرمان به شما نشان می‌دهد که کدام سرویس‌ها روی کدام پورت‌ها در حال اجرا هستند. اگر شما به سرویسی برخورد کردید که نباید اجرا شود آن را متوقف کنید. شما همچنین باید مراقبت سرویس‌هایی که فعال بوده و در زمان راه اندازی سیستم اجرا می‌شوند نیز باشید. با اجرای فرمان زیر می‌توانید این موضوع را تحت نظر قرار

دهید:

systemctl list-unit-files --type=service | grep enabled



بر اساس نوع سیستم، شما ممکن است یک خروجی شبیه به آن چه در تصویر بالا مشاهده می‌کنید را دریافت کنید. اگر با هر نوع سرویس ناخواسته مواجه شدید می‌توانید آن را با فرمان قدرتمند systemctl غیر فعال کنید:

systemctl disable service_name

محدود کردن دسترسی به سرور

درست شبیه به موردی که شما کلیدهای خانه خود را تنها در اختیار کسانی قرار می‌دهید که می‌شناسید، امکان دسترسی به سرور خود را نیز باید از دسترس افراد غریبه دور نگه دارید. این قانون به وضوح مشخص می‌کنند که شما باید دسترسی به سرور خود را محدود کنید. توجه داشته باشید که انجام این کار به تنهایی راه نفوذ خرابکاران به سرور شما را مسدود نمی‌کند، اما انجام آن می‌تواند لایه‌های امنیتی سرور شما را افزایش داده و امکان نفوذ به آن را دشوارتر کند.

هیچ گاه با حساب کاربری Root به سرور وارد نشوید

استفاده از حساب کاربری مدیریت ارشد یا همان روت برای ورود به سرور از طریق ssh به هیچ وجه کار درستی نیست. بنابراین بهترین کار این است که امکان دسترسی کاربر روت به سرور را از طریق ssh غیر فعال کنید. اما قبل از انجام این کار باید یک حساب کاربری ایجاد کنید که بتوانید با این حساب از طریق ssh به سرور وارد شده و وظایف مدیریتی را انجام دهید. به یاد داشته باشید که همیشه بعد از لاگین کردن به سرور می‌توانید در صورت نیاز به کاربر روت منتقل شوید.

برای اضافه کردن یک کاربر جدید در توزیع‌های مختلف لینوکس شیوه‌های متفاوتی وجود دارد. به عنوان مثال، توزیع Red Hat/CentOS از فرمان useradd و توزیع Ubuntu/Debian از فرمان adduser استفاده می‌کنند.

برای ایجاد یک کاربر جدید در Red Hat/CentOS از فرمان زیر استفاده کنید (swapnil نام کاربر فرضی ما است):

useradd swapnil

سپس با استفاده از فرمان زیر یک کلمه عبور برای این کاربر تعریف کنید:

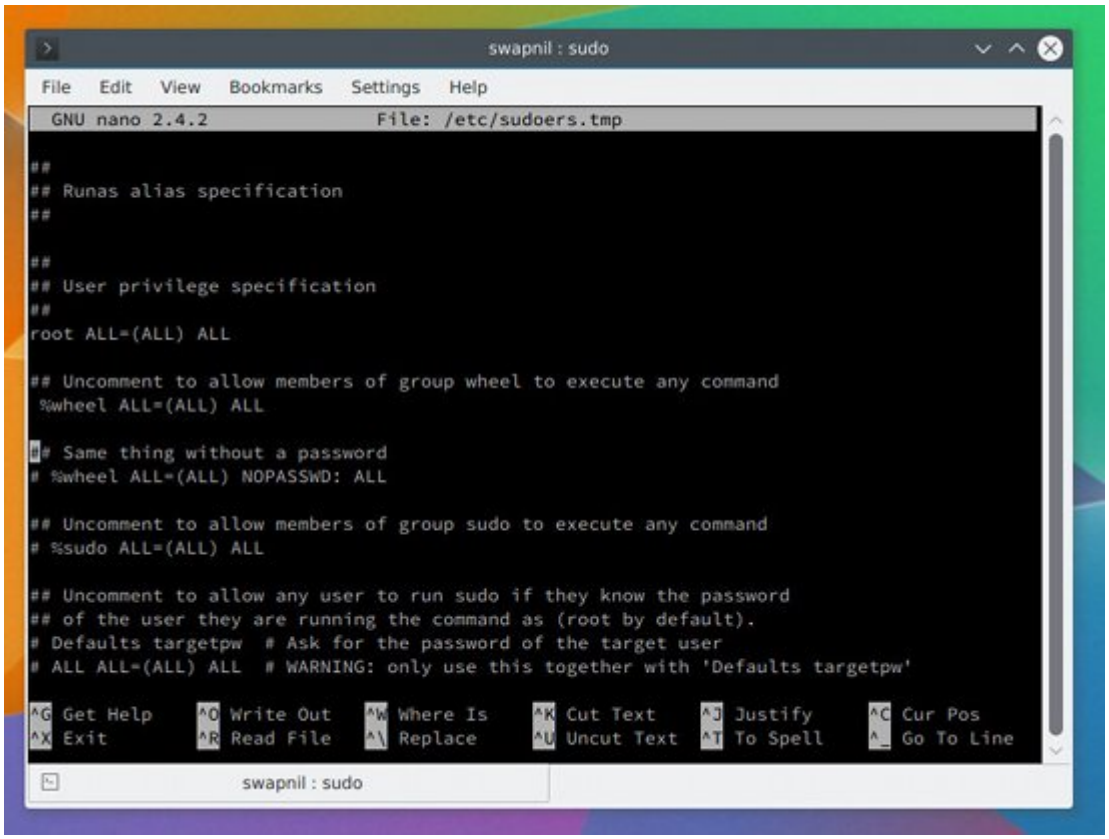
passwd swapnil

بعد از وارد کردن این فرمان از شما درخواست می‌شود که یک کلمه عبور جدید برای این کاربر وارد کنید. حالا باید به این کاربر امکان برخورداری از توانایی‌های sudo را اعطا کنید. برای این منظور فرمان زیر را اجرا کنید:

EDITOR=nano visudo

سپس طبق تصویر زیر به دنبال این خط بگردید

 # %wheel ALL=(ALL) ALL



خط را از حالت کامنت خارج کنید. نماد # در ابتدای هر خط نشان دهنده کامنت بودن (توضیحات) آن خط است و با برداشتن این نماد خط نیز از حالت کامنت خارج و به فرمان تبدیل می‌شود. بعد از انجام این کار خط شما به این شکل در خواهد آمد:

%wheel ALL=(ALL) ALL

حالا فایل را ذخیره و از آن خارج شوید. اگر این کاربر به گروه wheel تعلق ندارند شما می‌توانید به راحتی با استفاده از فرمان زیر آن را به این گروه اضافه کنید:

 # usermod -aG wheel swapnil

در سیستم‌های اوبونتو از این فرمان استفاده کنید:

adduser swapnil

به سوالاتی که سیستم از شما می‌پرسد پاسخ دهید که شامل ایجاد یک کلمه عبور جدید برای این کاربر است. بعد از ساخته شدن این کاربر با استفاده از فرمان زیر قدرت‌های sudo را به او اعطا کنید:

gpasswd -a swapnil sudo

یک پنجره ترمینال جدید دیگر باز کنید و سعی کنید با این کاربر جدیدی که ساخته‌اید وارد سرور شوید و از طریق sudo فرامین مدیریتی را انجام دهید. اگر این کار به درستی انجام شد مراحل بعد را دنبال کنید.

غیرفعال کردن امکان ورود با کاربر root

بعد از طی کردن مراحل قبل حالا نوبت آن است که امکان دسترسی کاربر root را غیرفعال کنیم. با این کار دیگر هیچ کس نمی‌تواند از طریق ssh یا روش‌های دیگر به عنوان کاربر روت وارد سیستم شود. برای انجام این کار فایل پیکربندی sshd را باز کنید:

```
nano /etc/ssh/sshd_conf
```

سپس خط زیر را پیدا کرده و آن را از حالت کامنت خارج کنید:

```
#PermitRootLogin no
```

حالا فایل را ذخیره کرده و از آن خارج شوید، بعد سرویس را با استفاده از فرمان زیر ری‌استارت کنید:

```
service ssh restart
```

یا:

```
systemctl restart sshd
```

توجه: در این مرحله هنوز نباید از سرور خارج شوید. ابتدا باید امتحان کنید که آیا می‌توانید با موفقیت و با استفاده از حساب کاربری که قبلا ساخته‌اید از طریق ssh وارد سرور شوید. یک پنجره جدید از ترمینال باز کرده و با استفاده از حساب کاربری که قبلا ایجاد کرده بودید به سرور لاگین کنید، اگر همه چیز به خوبی کار کرد حالا می‌توانید با خیال راحت از حساب کاربری روت خارج شوید.

تغییر دادن پورت

دومین تغییری که ما قصد داریم در فایل پیکربندی sshd اعمال کنیم، عوض کردن پورت پیش فرض است. این کار بیشتر به منظور افزایش یک لایه امنیتی از طریق در ابهام قرار دادن شماره پورت صورت می‌گیرد. فرض کنید یک شرکت خدمات امنیتی با استفاده از چند وسیله نقلیه یک شکل قصد داشته باشد یک فرد مهم را جابجا کند. در این حالت فرد حمله کننده نمی‌تواند تشخیص دهند که شخص مورد نظر در کدام یک از این وسایل نقلیه سوار شده است. تغییر دادن پورت پیش فرض نیز امکان تشخیص درست آن را برای هکر دشوار می‌کند.

فایل sshd_config را باز کنید (این بار از طریق فرمان sudo، چرا که دیگر شما نمی‌توانید با استفاده از حساب کاربری روت به سرور وارد شوید):

```
sudo nano /etc/ssh/sshd_conf
```

سپس این خط را پیدا کنید:

```
#Port 22
```

خط را از حالت کامنت خارج کرده و یک شماره پورت دیگر را برای آن انتخاب کنید. قبل از انتخاب یک شماره جدید اطمینان حاصل کنید که این پورت توسط سرویس دیگری روی سرور شما استفاده نشده باشد. برای بدست آوردن شماره پورت‌های رایج و استفاده نکردن از آنها می‌توانید از مقاله موجود در **ویکی پدیا** استفاده کنید. برای نمونه می‌توانید از پورت1977 استفاده کنید:

```
Port 1977
```

سپس فایل را ذخیره کرده و از آن خارج شوید و یک بار سرویس sshd را ری‌استارت کنید. یک بار دیگر قبل از خارج شدن از سرور با باز کردن یک پنجره ترمینال دیگر و لاگین کردن با استفاده از الگوی زیر تنظیمات خود را بررسی کنید:

ssh -p{port_number}@server_IP

مثال:

ssh -p1977

This e-mail address is being protected from spambots. You need JavaScript enabled to view it

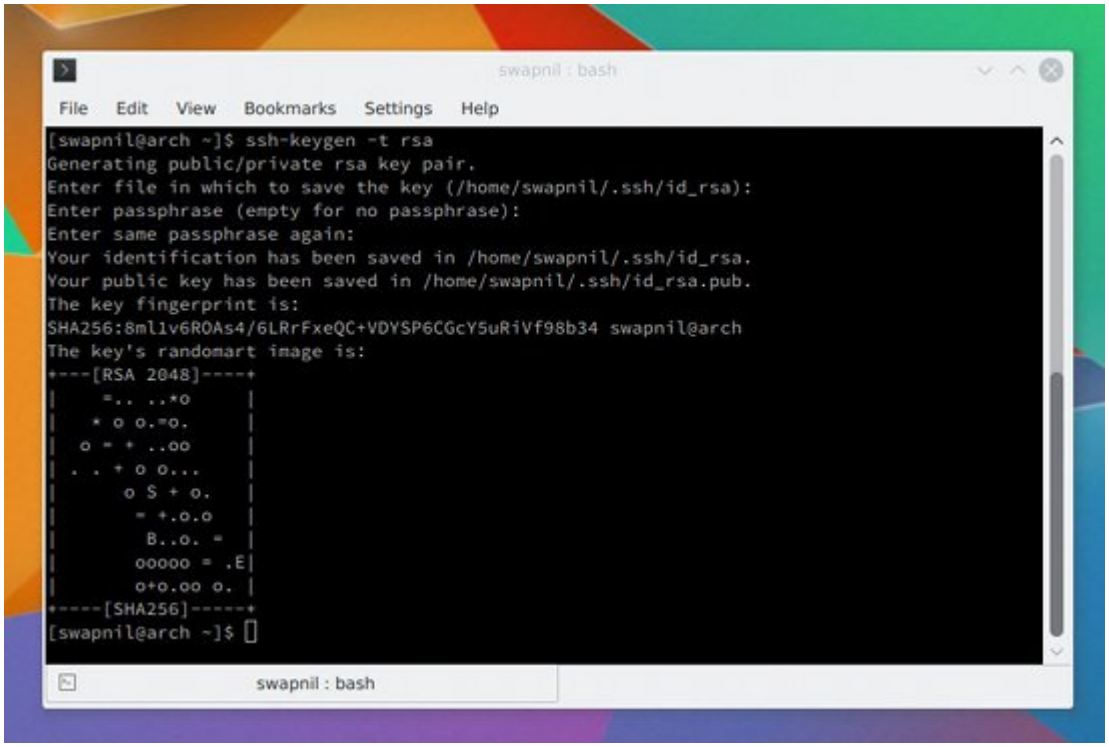
اگر توانستید با موفقیت به سرور وارد شوید کارها به درستی انجام شده است.

لاگین کردن بدون نیاز به کلمه عبور

شما می‌توانید با غیرفعال کردن نیاز به وارد کردن کلمه عبور راحت‌تر و سریع‌تر به ssh لاگین کنید. همچنین با غیرفعال کردن کامل احرازهویت به وسیله کلمه عبور یک لایه امنیتی دیگر را نیز اضافه کنید. به یاد داشته باشید که با فعال کردن این قابلیت تنها می‌توانید از طریق سیستمی که کلیدهای ssh را در آن ایجاد کرده‌اید به سرور خود متصل شوید.

برای شروع ابتدا کلید ssh را با استفاده از فرمان زیر در سیستم محلی خود ایجاد کنید:

ssh-keygen - t rsa



بعد از اجرای این فرمان چند سوال از شما پرسیده می‌شود، شما می‌توانید مکان این کلید را در موقعیت پیش فرض خود رها کنید و با استفاده از یک گذر واژه حدس زدن آن را دشوار کنید. در مرحله بعد شما باید این کلیدها را به سرور کپی کنید تا با این کلید هر دو سیستم (محلی و سرور) بتوانند با یک دیگر ارتباط برقرار کنند.

cat ~/.ssh/id_rsa.pub | ssh -p 1977 swapnil@remote-server ";mkdir -p ~/.ssh && cat

>> ~/.ssh/authorized_keys"

حالا سعی کنید با استفاده از یک پنجره ترمینال دیگر به سرور دسترسی پیدا کنید. اگر همه چیز به درستی انجام شده باشد دیگر برای ورود از شما کلمه عبور پرسیده نخواهد شد.

انجام این مرحله بیشتر از این که جنبه افزایش امنیت داشته باشد برای سهولت در انجام کار مورد استفاده قرار می‌گیرد. اما در مجموع با غیرفعال کردن کامل احراز هویت به وسیله کلمه عبور شما می‌توانید مقداری امنیت سرور خود را نیز بالا ببرید. فایل sshd_config را باز کرده و این خط کامنت شده را پیدا کنید:

#PasswordAuthentication yes

سپس آن را از حالت کامنت خارج کنید و مقدار آن را از yes به no تغییر دهید، حالا فایل را ذخیره و از آن خارج شوید. بعد سرویس sshd را ری‌استارت کنید. یک بار دیگر، همچنان ارتباط خود با سرور را در پنجره فعلی باقی نگه دارید. یک ترمینال جدید باز کرده و به سرور لاگین کنید (دقت کنید که این کار بدون پرسیدن کلمه عبور انجام شود).

نقطه ضعف انجام این تنظیمات این است که حالا شما تنها می‌توانید از طریق سیستمی که کلیدهای ssh را در آن ایجاد کرده‌اید به سرور متصل شوید. بنابراین اگر برای دسترسی به سرور از چند کامپیوتر مختلف استفاده می‌کنید نباید از این روش استفاده کنید.

نتیجه‌گیری

مطالب ارائه شده در بالا یکسری از ملاحظات عمومی برای کاربران جدید بودند که بتوانند با رعایت کردن آنها سرور شخصی خود را امن‌تر راه‌اندازی کنند. اما باید توجه داشته باشید که خرابکاران و متجاوزان همیشه یک مرحله از ما جلوتر هستند. آنها برای نفوذ به سرور شما تمام حفره‌های موجود را بررسی می‌کنند. بنابراین بهترین کار این است که همیشه یک **نسخه پشتیبان** از محتوای سرور خود در اختیار داشته باشید تا در صورت از دست رفتن آن به هر دلیلی (از جمله حملات سایبری) بتوانید آن را سریعا جایگزین کنید. کارشناسان توصیه می‌کنند همیشه قبل و بعد از اعمال تغییرات روی سرور خود نیز از محتوای آن پشتیبان تهیه کنید. با این کار اگر به هر دلیلی سرور شما به درستی کار خود را انجام نداده و دچار مشکل شد می‌توانید با استفاده از نسخه پشتیبان به مرحله قبلی بازگردید.

==========

شاید به این مقالات هم علاقمند باشید:

دو پروژه‌ای که امنیت شبکه ملی اطلاعات را تضمین می‌کنند!

پردازنده سروری پرقدرت جدید Xeon E7 v4

مهرماه یک تغییر بزرگ در اینترنت جهان رخ می‌دهد!

شروع به کار اولین مرکز داده ابری ایران با ظرفیت ۶ پتابایت

رشد بازار سوییچ‌های اترنت برای خدمات ابری و مراکز داده

چرا این روزها حال اینترنت خوب نیست و پشت‌سرهم هک می‌شویم؟

راهنمای خرید سرور برای کسب‌وکارهای کوچک و متوسط

سریع‌ترین شبکه غیرقابل ردیابی جهان طراحی شد

منبع:

لینوکس‌دات‌کام
تاریخ انتشار:
07 شهریور 1395

نشانی منبع:
https://www.shabakeh-mag.com/tricks/network-tricks/4260/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%B3%D8%B1%D9%88%D8%B1-%D9%84%DB%8C%D9%86%D9%88%DA%A9%D8%B3-%D8%A7%D9%85%D9%86%E2%80%8E%D8%AA%D8%B1%DB%8C-%D8%AF%D8%A7%D8%B4%D8%AA%D9%87-%D8%A8%D8%A7%D8%B4%DB%8C%D9%85%D8%9F