禪

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] (ownCloud [redacted])

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
```


swapnil : bash
File
Edit
View
Bookmarks
Settings
Help
swapnil : bash

```
[swapnil@arch ~]$ sudo systemctl list-unit-files --type=service | grep enable
d
[sudo] password for swapnil:
dbus-org.freedesktop.NetworkManager.service enabled
dbus-org.freedesktop.nm-dispatcher.service  enabled
display-manager.service                     enabled
getty@.service                              enabled
NetworkManager-dispatcher.service           enabled
NetworkManager.service                      enabled
sddm.service                                enabled
vboxservice.service                         enabled
[swapnil@arch ~]$ 
```

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

swapnil : sudo
File
Edit
View
Bookmarks
Settings
Help
swapnil : sudo

```
  GNU nano 2.4.2              File: /etc/sudoers.tmp

##
## Runas alias specification
##


##
## User privilege specification
##
root ALL=(ALL) ALL

## Uncomment to allow members of group wheel to execute any command
 %wheel ALL=(ALL) ALL

## Same thing without a password
# %wheel ALL=(ALL) NOPASSWD: ALL

## Uncomment to allow members of group sudo to execute any command
# %sudo ALL=(ALL) ALL

## Uncomment to allow any user to run sudo if they know the password
## of the user they are running the command as (root by default).
# Defaults targetpw  # Ask for the password of the target user
# ALL ALL=(ALL) ALL  # WARNING: only use this together with 'Defaults targetpw'

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line
```

[illegible] (Debian) [illegible] # [illegible]. [illegible] [illegible] [illegible] [illegible]. [illegible] [illegible] [illegible] [illegible] [illegible]:

%wheel ALL=(ALL) ALL

[illegible] wheel [illegible]. [illegible] [illegible]:

 # usermod -aG wheel swapnil

[illegible]:

adduser swapnil

[illegible] sudo [illegible]:

gpasswd -a swapnil sudo

root [illegible]

root [illegible] ssh [illegible] sshd [illegible]:

nano /etc/ssh/sshd_conf

[illegible]:

#PermitRootLogin no

[illegible]:

service ssh restart

[illegible]:

systemctl restart sshd

[illegible]: [illegible] ssh [illegible].

[illegible]

sshd [illegible].

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 پورت 1977 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

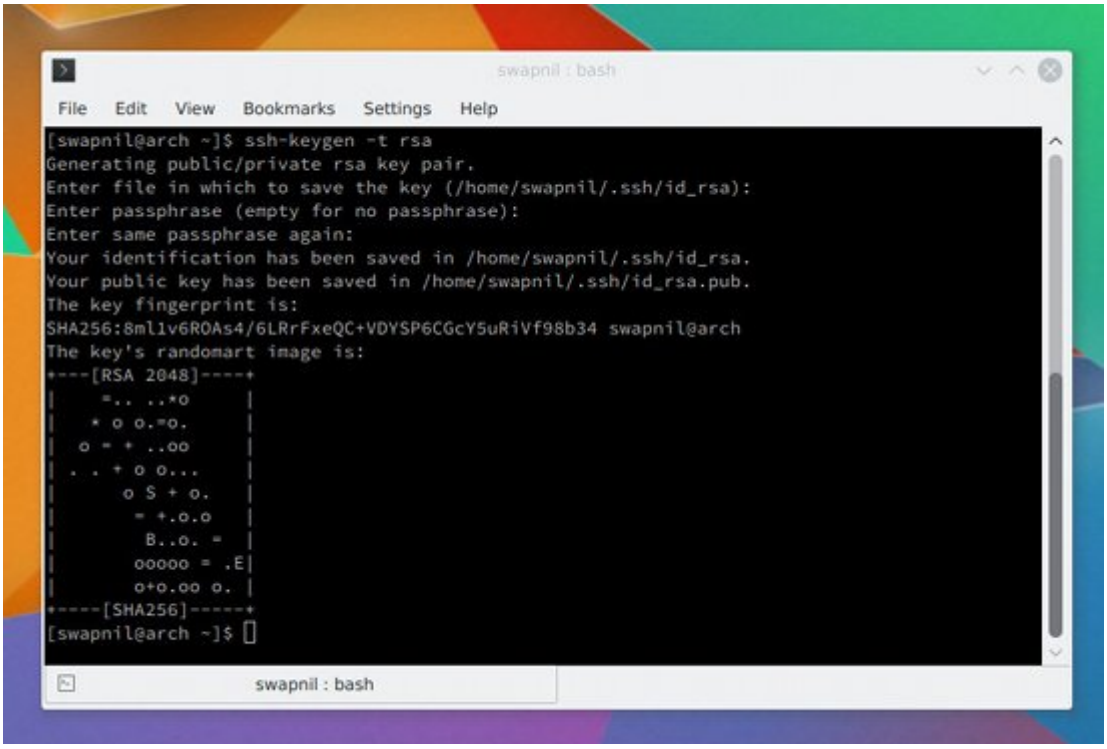
اگر توانستید با موفقیت به سرور وارد شوید کارها به درستی انجام شده است .

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
```



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

#PasswordAuthentication yes

[illegible]

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 !

intel
Intel® Xeon® Processor
E7 v4

پردازنده سروری پرقدرت جدید **Xeon E7 v4**

مهرماه یک تغییر بزرگ در اینترنت جهان رخ میدهد !









AFR@NET
Internet & E-Comm

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

نویسنده :
محسن آقاجانی
منبع :
لینوکسداتکام
دسته بندی:
ترفند شبکه
تاریخ انتشار :
12:00 - 07/06/1395
برچسب:
امنیت_سرور_لینوکس - لینوکس - سرور - سرور_لینوکس - امنیت_سرور

نشانی
□□□□: 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