نکاتی در مورد امنیت سرور

CentOS

گردآوری توسط میلاد آجیلیان

۲۴ دی ۹۱

www.AryanRad.com

به نام خدا

مطمعا با کارهای که اینجا گفته شده امنیت سرور شما ۱۰۰ درصد نمیشه اما بی تاثیر هم نیست
بیشتر درمورد تنظیمات توسط فایل sshd_config صحبت شده

توجه : در تمامی مراحل باید دسترسی های کاربر روت داشته باشین.

توجه : در بعضی از موارد برای این که تغییرات اعمال بشه نیاز به ریستارت کردن ssh هست ، **به هیچ عنوان اتصال ssh خودتون قطع نکنین** چون ممکنه دیگه نتونین وصل بشین !! برای ریستارت کردن ssh فقط از دستور زیر استفاده کنین :

```
/etc/init.d/sshd restart
```

مطالب بر اساس سایت اصلی CentOS هست

با تشکر ویژه از استاد امینی

۱) رمز ورود مشکل انتخاب کنید :

انتخاب پسورد قوی خیلی مهمه که متاسفانه بهش توجه هم نمیشه !! اگر یک پسورد معمولی انتخاب کردین حتما همین الان برین تغییرش بدین :دی . خیلی راحت میتونین ببینین که تا الان چند بار سعی شده وارد اکانت شما بشن .
با دستور lastb و از طریق فایل /var/log/secure میتونین به این اطلاعات دسترسی داشته باشین که چند نمونش رو براتون مثال میزنم

 # پنج تا از بیشترین حمله های اخیر به اکانت های شما :

```
lastb | awk '{print $1}' | sort | uniq -c | sort -rn | head -5
```

لیستی مثل لیست زیر بهتون میده :

```
1289  root
41    oracle
40    viktor
36    linux
34    user1
```

 # پنج اکانتی که بیشترین حمله بهشون شده :

```
awk 'gsub(".*sshd.*Failed password for (invalid user )?", "") {print $1}' /var/log/secure*
| sort | uniq -c | sort -rn | head -5
```

 # پنج آی پی که بیشترین حمله رو به شما کردن :

```
awk 'gsub(".*sshd.*Failed password for (invalid user )?", "") {print $3}' /var/log/secure* |
sort | uniq -c | sort -rn | head -5
```

در CentOS کاربر root میتونه هر نوع پسوردی برای خودش انتخاب کنه چه ساده و چه مشکل ، پس حتما سعی کنین پسورد مشکلی رو انتخاب کنین ، یک پسورد خوب شامل اعداد ، حروف کوچک و بزرگ ، کارکتر های خاص میشه.

۲) نصب برنامه "DenyHosts" برای بلاک کردن خودکار کاربرای خطرناک :

این برنامه با برسی فایل /var/log/secure و لاگین های ناموفق در ssh به صورت خودکار با وارد کردن آی پی در فایل /etc/hosts.deny اونا رو بلاک میکنه.
برای دسترسی به تنظیمات این برنامه میتونین فایل /etc/denyhosts.conf ببینید.

برای نصب از دستورات زیر استفاده کنین :

```
yum install denyhosts
chkconfig denyhosts on
service denyhosts start
```

۳) تغییر پرت پیشفرض :

در بیشتر حملاتی که انجام میشه قطعا اولین پرتی که امتحان خواهد شد پرت پیش فرضه که ۲۲ هست ، پس پیشنهاد میکنم هرچه زودتر این پرت رو هم تغییر بدین.
برای تغییر پرت باید فایل /etc/ssh/sshd_config ویرایش کنین.
فایل باز کنید :

```
Nano /etc/ssh/sshd_config
```

دنبال عبارت Port 22 بگردین ، شما باید ۲۲ به یک پرت دیگه که استفاده نمیکنن تغییر بدین بهتره بیشتر از ۱۰۲۴ باشه (;

۴) پرتکل ۱ رو ببندید :

ssh از طریق دو تا پرتکل ارتباط خودش رو برقرار میکنه. یکی پرتکل ۱ که قدیمی و ناامن هست ، یکی هم پرتکل ۲ که جدیدتره . بیشتر کاربرای ssh از پرتکل ۲ استفاده میکنن اما بهتر که شما کلا پرتکل ۱ رو غیرفعال کنین.
برای این کار باز هم باید فایل ssh_config ویرایش کنین و داخل فایل به دنبال خط زیر بگردین
Protocol 2,1
تغیرش بدین به
Protocol 2

۵) ورود از طریق root غیر فعال کنید :

هیچ دلیل نداره کاربر root هم بتونه مثل بقیه کاربرا لاگین کنه !!! وقتی شما میتونید با استفاده از دستور su مجوز های روت داشته باشین پس بهتره کلا لاگین توسط کاربر root غیرفعال کنین
برای این کار باید فایل sshd_config ویرایش کنین.
داخل فایل دنبال عبارت زیر بگردین
PermitRootLogin yes
و yes به no تغییر بدین
توجه داشته باشین قبل از خروج ssh یک کاربر دیگه برای ورود بعدی بسازین :دی

۶) برای ورود از کلید اختصاصی استفاده کنین (بیشتر برای مدیریت سرور های پرکار)

با این کار برای اتصال به سرور به کلیدی که داخل سیستم شما ذخیره میشه نیاز هست ، اگر کلید نباشه با نام کاربری و رمز عبور صحیح هم نمیشه وارد سرور شد.
این کار بیشتر برای سرور های پیشنهاد میشه که زیاد بهشون لاگین میکنین و حال ندارین هر دفعه یوزر و پس وارد کنین !!
داخل فایل sshd_config عبارت PasswordAuthentication no وارد کنید.
در کل این روش زیاد پیشنهاد نمیشه !!

۷) تعداد لاگین های هم زمان رو کم کنین :

شما بیاید تعداد کاربرای که میتونن در آن واحد به سرور وارد بشن رو محدود کنین. برای این کار باید فایل sshd_config ویرایش کنید.
درون فایل به دنبال عبارت زیر بگیردین
MaxStartups 10
و اونو به صورت زیر تغییر بدین :
MaxStartups 3:50:10
با این کار در آن واحد فقط سه کاربر میتونن وارد سرور بشن

۸) حداکثر زمان لاگین به سیستم رو کم کنید :

به صورت پیش فرض در زمان لاگین شدن ۲ دقیقه فرصت داده میشه که با موفقیت وارد بشین ، اما خوب این مدت زمان زیاده و شما برای ورود خیلی کمتر از این نیاز دارین ، وقتی مدت زمان کم کنین فرصت کمتری هم به حمله کننده میدین
برای این کار داخل فایل sshd_cofig عبارت زیر پیدا کنین :
LoginGraceTime 2m
و مقدار اونو به ۳۰ ثانیه تغییر بدین

۹) فقط به گروه و کاربر های خاص اجازه ورود بدین :

در حالت عادی هر گروه و کاربری میتونه وارد ssh بشه و برای وارد شدن تلاش کنه ، اما شما میتونین فقط به تعدادی کاربر خاص و یک گروه خاص اجازه دسترسی رو بدین برای این کار داخل فایل sshd_config عبارت زیر پیدا کنین :
AllowUsers
هر کاربری که میخواین رو روبروش وارد کنید
نام های کاربری با یک فاصله از هم جدا میشن
میتونید از کارکتر های مثل * هم استفاده کنین (به عنوان مثال *milad تمام کاربرانی که نام کاربریشون با milad شروع میشه)
برای گروه های کاربری هم دنبال
AllowGroups
بگردین و هرگروهی که میخواین وارد کنید

۱۰)فقط به آی پی های خاص اجازه دسترسی بدین :

شما میتونی فقط به آی پی های خاصی اجازه دسترسی به سرور بدین (به قول یکی از استاد های خوبم شما که داخلی ایران هستید و مطمعا با آی پی خارج از ایران به سرورتون وصل نمیشین میتونین اجازه دسترسی رو فقط به رنج آی پی های ایران بدین :دی)
برای این کار اول از همه باید دسترسی کل آی پی ها رو قطع کنین !!! برای این کار فایل

```
/etc/hosts.deny
```

ز
باز کرده و
sshd: ALL
قرار بدین
توجه : اگر در این حالت از سرور خارج بشین تموم شده دیگه :دی ، کلا دیگه دسترسی نخواهید داشت ! پس خیلی حواستون جمع کنین

بعد باید فایل زیر باز کنید

```
/etc/ hosts.allow
```

e
و آی پی آدرس های که باید دسترسی داشته باشن وارد کنید

نمونه :

```
sshd: 192.168.1.0/255.255.255.0
sshd: 10.0.0.0/255.0.0.0
sshd: 24.42.69.*
sshd: 24.42.69.201
```

لطفا نظرات ، پیشنهاد و مشکلات رو به بنده انتقال بدین تا ویرایش کنم
برای این کار میتونید از طریق ایمیل miladdevelop@gamil.com یا از طریق وب سایت آرین راد و یا تاپیک مربوطه در انجمن sod با من در ارتباط باشین.

با تشکر