نوشته شده توسط root
دوشنبه ، 5 مهر 1389 ، 10:59 - **آخرین بروزرسانی دوشنبه ، 5 مهر** 1389 ، 11:49

یکی از حمله هایی که معمولا بر روی سیستم عامل های شبیه به Unix **زیاد انجام می شود حمله از نوع** ssh **است . در این حمله افراد سعی می کنند با** username **و** password **های فرضی به یک سیستم یونیکسی نفوذ کرده واختیار سیستم را به دست گیرند .**

برای مقابله با این روش ها بهترین راه حل استفاده از یک firewall **قوی با** rule **های کار آمد است تا بتوان به راحتی جلوی حمله کننده ها را گرفت . اگر از فایروال استفاده نمی کنید می توانید در** FreeBSD **از یک برنامه کاربردی و قدرتمند به** denyhosts **استفاده کنید با این برنامه و با تنظیمات آن به راحتی می توانید جلوی حمله های** ssh **را گرفته و می توانید ایمیلی مبنی بر حمله** ssh **را دریافت کنید .**

برای نصب این برنامه در FreeBSD **کافی است بعد از آپدیت نمودن** port **های خود در ترمینال دستور زیر را تایپ کنید**

```
cd /usr/ports/security/denyhosts/
make install clean
```

بعد از مدتی برنامه مورد نظر نصب خواهد . خوب برای کانفیگ باید کار های زیر را انجام دهید . اولین کار این است که کاری کنیم هنگامی که سیستم شروع به کار می کند برنامه denyhosts **شروع به کار کند . خوب برای استارت را زیر عبارت باید سیستم بوت هنگام در** denyhosts

```
denyhosts_enable="YES"
```

در فایل

/etc/rc.conf

قرار می دهیم . در مر حله بعد فایل زیررا با استفاده از یک ویرایشگر مانند vi **یا** nano **باز می کنیم**

/etc/hosts.allow

و عبارت های زیر را در آن قرار می دهیم و تغییرات را ذخیره می کنیم

```
sshd : /etc/hosts.deniedssh : deny  sshd : ALL : allow
```

حال به شاخه

نوشته شده توسط root
دوشنبه ، 5 مهر 1389 ، 10:59 - آخرین بروزرسانی دوشنبه ، 5 مهر 1389 ، 11:49

/etc

می رویم و با استفاده از دستور touch **فایلی به نام** denissh.hosts **ایجاد می کنیم**

touch /etc/hosts.deniedssh

بعد از کار های بالا حالا نوبت آن است که فایل کانفیگ مربوط به denyhosts **را با توجه به نیاز خود ویرایش کنیم .**
فایل کانفیگ denyhosts **در مسیر زیر وجود دارد**

/usr/local/etc/denyhosts.conf

فایل conf.denyhosts **را با استفاده از یک ویرایشگر مانند** vi **باز می کنم و در آن دنبال عبارت زیر یا قسمت زیر می گردم**

BLOCK_SERVICE:

در این قسمت ما می توانیم تنظیم کنیم که بر نامه چه سرویس هایی را باید مورد بررسی قرار دهد و آنها را نظارت کند و چون من می خواهم فقط با این برنامه جلوی حملات ssh **را بگیرم لذا علامت**

#

از جلوی عبارت زیر بر می داریم

BLOCK_SERVICE = sshd

خوب به برنامه تعریف کردیم از بین service **هایی که در سیستم من کار می کنند فقط** service **مربوط به** ssh **را مورد بررسی قرار دهد .**

حال در فایل کانفیگ denyhosts **دنبال عبارت زیر می گردم**

DENY_THRESHOLD_INVALID

در این قسمت به برنامه تعریف می کنیم که اگر کسی حمله از نوع ssh **را بر روی سیستم من انجام داد بعد از چند بار حمله این برنامه جلوی حمله را بگیرد و** IP **حمله کننده را بلوک یا** block **کند . من برای خود عدد ۲ را انتخاب کرده ام که این بستگی به نیاز شما دارد و شما می توانید اعداد دیگری را نیز انتخاب کنید . البته لازم به یادآوری است این برنامه به** login **ها یا درخواست** ssh **هایی که از طرف یوزر تعریف شده بر روی سیستم واکنشی نشان نمی دهد و جلوی آن را نمی گیرد . فرض کنید من یوزری به نام** mfaridi **دارم و با این یوزر از جای دیگر تلاش می کنم به سیستم خودم**

نوشته شده توسط root
دوشنبه ، 5 مهر 1389 ، 10:59 - آخرین بروزرسانی دوشنبه ، 5 مهر 1389 ، 11:49

وصل شوم ولی بنا به دلایلی پسورد خود را اشتباه وارد می کنم . این برنامه اول چک می کند آیا چنین یوزری بر روی سیستم وجود دارد یا نه اگر وجود داشت به اجازه ssh های بیشتری را می دهد و اگر وجود نداشت بعد از ۲ بار تلاش دستگاه حمله کننده را برای همیشه در فهرست سیاه خود قرار می دهد و دیگر من با آن IP نمی توانم به سیستم وصل شوم.

حال دنبال عبارت زیر می گردم

DENY_THRESHOLD_VALID

در اینجا تعریف می توان بکنم که یوزر موجود بر روی سیستم چند بار می تواند برای ssh تلاش کند این به درد جایی می خورد که کسی بداند شما به چه یوزری به سیستم login می شوید ولی پسورد ندارد . من برای این قسمت 5 را در نظر گرفته ام.

حال دنبال عبارت زیر می گردم

DENY_THRESHOLD_ROOT

در اینجا می توانیم تعریف کنیم که اگر کسی خواست با یوزر root به سیستم وصل شود بعد از چند بار تلاش IP فرد حمله کننده در لیست سیاه قرار گیرد و جلوی login و تلاش برای ssh را بگیرد که به طور پیش فرض عدد 1 است و عالی است .

این برنامه قسمت های دیگری برای کانفیگ دارد که با توجه به نیاز خود می توانید از آن استفاده کنید.

اگر دوست دارید بعد از هر بار تلاش برای ssh به سیستم ایمیلی دریاف کنید و با ایمیل آگاه شوید در فایل کانفیگ بگردید زیر عبارت دنبال denyhosts

ADMIN_EMAIL

و در جلوی عبارت email_admin ایمیل خود را وارد کنید تا ایمیل ها به آن آدرس فرستاده شود .

خوب من تغییرات مورد نیاز خودم ار اعمال کردم حال برای استارت denyhosts در FreeBSD عبارت زیر را در ترمینال تایپ می کنم

/usr/local/etc/rc.d/denyhosts start

نوشته شده توسط root
دوشنبه ، 5 مهر 1389 ، 10:59 - **آخرین بروزرسانی دوشنبه ، 5 مهر** 1389 ، 11:49

با این دستور برنامه شروع به کار می کند و شما با دستور زیر می توانید چک کنید که آیا این برنامه در لیست process **قرار دارد یا نه**

```
ps -aux | grep deny
```

خوب خروجی به من نشان می دهد که برنامه کار می کند .

منتظر ایمیل باشید تا ببینید چه کسانی تلاش می کنند به سیستم شما ssh **کنند .**

لازم به یادآوری است هیچ چیزی جای یک Firewall **خوب با** rule **هایی مستحکم را نمی گیرد . این برنامه به** python **وابستگی دارد . خرابی پایتون یعنی از کار افتادن برنامه پس به فکر فایروال باشید.**