نوشته شده توسط root
چهارشنبه ، 5 اسفند 1388 ، 11:29 - آخرین بروزرسانی چهارشنبه ، 5 اسفند 1388 ، 12:30

می دانیم در سیستم عامل هایی مانند Unix یک راه ارتباط برقرار کردن با سیستم و انجام کار ها روشی به نام ssh می باشد که شما به ssh به سیستم وصل شده و کار هایی را در سیستم انجام می دهید . فرض کنید سیستمی که شما می خواهید بر روی آن کار کنید در فاصله دوری از شما قرار دارد و با خطوط مزخرف اینترنت توانایی وصل شدن به صورت گرافیکی با برنامه هایی مانند VNC را به سیستم ندارید . در این حالت بهترین راه استفا ده از ssh است که حتی با خطوط واقعا مزخزف up-Dial نیز شما می توانید به سیستم وصل شده و کار های خود را انجام دهید.

می شوید وصل آن به خواهید می که را دستگاهی password و username شما از سیستم به شدن وصل هنگام در ssh خواهد و با این یوزر name و پسورد می توانید به سیستم وصل شوید.

یکی از روش های حمله کردن به یک سیستم این است که تلاش می کنند با ssh به سیستم وصل شده و کار های مخرب انجام دهند . معمولا hacker یا cracker با برنامه هایی مانند nmap چک می کند که آیا سیستم مورد نظر دارای پورت باز است یا نه . مثلا چک می کند آیا پورت ۲۲ که برای ssh استفاده می شود باز هست یا نه و اگر باز بود سعی می کند با دادن به بتواند تصادفی طور به شاید تا دهد می انجام قدر این کار این . کند نفوذ سیستم آن به هایی password و username آن سیستم وصل شود و خراب کاری کند .

مثلا در سیستمی که الان این post را برا ی شما می فرستم از دو ماه گذشته در حدود 40000 بار با IP های مختلف تلاش شده است که ssh کنند و باعث خرابکاری در این سیستم شوند . این حملات در بعضی مواقع آنقدر شدید بوده این تعداد بوده سابق شوروی های کشور و چین مانند هایی کشور از اکثرا که است رسیده روز یک در ۲۰۰۰ به مواقع بعضی در ssh است ..

با مقابله برای خوب . شود می استفاده سیستم به نفوذ برای که انست حمله نوع یک توان می زیادرا تعداد به کردن ssh حمله های ssh ی چه باید کرد ؟

۱- سعی کنید حتما از فایروال استفاده کنید که در FreeBSD می توانید از فایروال هایی مانند PF یا IPFW استفاده کرد و با استفاده از rule هایی که در این فایروال ها تعریف می کنید می توانید تا اندازه زیادی جلوی حمله های ssh را گرفت .

۲- فایل زیر باز کنید و تغییرات زیر را در آن اعمال کنید.

نوشته شده توسط root
چهارشنبه ، 5 اسفند 1388 ، 11:29 - آخرین بروزرسانی چهارشنبه ، 5 اسفند 1388 ، 12:30

/etc/ssh/sshd_config

برای وصل شدن با ssh به صورت پیش فرض از پورت یا درگاه ۲۲ استفاده می شود پس اولین مکار این است که این پورت را تغییر دهید پس در فایل بالا عبارت port 22 **را به عبارت** port 678 **تغییر می دهیم**

Port 678

۳- سعی کنیم که در این فایل تعریف کنیم که چه IP هایی حق ssh دارند و به صورت پیش فرض با هر IP و از هر جا می توان ssh را انجام داد ولی با محدود کردن IP می توان تعریف کردن فقط از چه جاهایی می توان ssh کرد . پس در فایل بالا خط زیر را وارد می کنیم .

ListenAddress 192.168.0.1

این یعنی که برای ssh فقط 192.168.0.1 **اجازه دارد .**

۴- ssh می تعریف بالا فایل در پس باشد می ریسک کمترین دارای دو ره شما نسخه که است مختلفی های ورژن دارای کنیم برای ssh از ورژن شماره ۲ استفاده شود .پس خط زیر را قرار می دهیم

Protocol 2

۵- در سیستم عامل هایی مانند Unix یوزری وجود دارد به نام root که همکاره سیستم می باشد و دارای قدرت مطلق در سیستم است و توانایی آن مانند یوزر administrator در windows می باشد . اکثر hacker ها و cracker ها اولین ssh خود را با یوزر root انجام می دهند چون می دانند که این یوزر حتما وجود دارد . پس بهتر است در فایل بالا تعریف کنیم که اجازه ssh به یوزر روت داده نشود تا اگر چنانچه کسی توانست پسورد root را به دست آورد با آن login نشود . پس در فایل بالا عبارت های زیر را وارد می کنیم .

PermitRootLogin no
DenyUsers root

۶- معمولا در سیستم عامل های Unix مانند همه چیز ثبت می شود که این ثبت شدن به فرد یا مدیر server اجازه می دهد تا بعدا اگر مشکلی به وجود آمد بتواند پیگیری کند . ssh نیز از این قانون مجزا نیست و به صورت IP ثبت می گردد که در چه زمانی با چه IP فردی تلاش کرده است که به سیستم وصل شود . می توانیم یک پیام در هنگام ssh قرار داد تا به فرد های قانون اگر که . باشد می اخطار نوع یک واقع در و دهد می انجام را کاری چه دارد که شود یادآوری کننده ssh دیجیتال اعمال شود می توان با این پیغام یک برگ برنده در دست داشت.

برای قرار دادن پیغام در هنگام ssh باید فایلی به نام

/etc/ssh.go.txt

را ویرایش کرد و عبارت مورد نظر را که می تواند چیزی شبیه به زیر باشد در ان قرار داد

This is a private server!!! All ssh login attempts are logged and monitored by our staff.
All unauthorized login attempts will be investigated and repoeted to local authorities.
If you have any login problem please contact helpdesk us at Phone: 845454515454 or email us Email: support@mycorop.com

بعد از قرار دان متن بالا باید به فایل

/etc/ssh/sshd_config

بگوییم که این متن در کجا قرار دارد پس در این فایل عبارت زیر را قرا ر می دهم

Banner /etc/ssh.go.txt

خوب حالا تغییرات اعمل شده را ذخیره می کنیم و از فایل conf **ی که برای** ssh **است خارج می شویم و** ssh **را ریست می کنیم تا تغییرات اعمال شده کار کند . در** FreeBSD **برای ریست** ssh **دستور زیر را در ترمینال تایپ می کنم**

/etc/rc.d/sshd restart

خوب اگر قبلا به صورت زیر login **می کردیم**

ssh -l mostafa 192.168.0.1

حالا به این صورت ssh **می کنیم**

ssh -p 678 mostafa@192.168.0.1

می بینیم که تعریف کرده ایم برای ssh **از پورت** 678 **استفده شود.**