دانلودمقاله پیادهسازی دیوارهی آتشْ در لینوکسِ ازطریق نگهداری Iptables

چکیده

تأمین امنیتَ شبکهُ، بخش حساسی از وظایف هر مدیر شبکه محسوب می‌شود. از آنجاییکه ممکن است محافظتِهای متفاوتی موردنیاز باشد، لذا مکانیزمّ های گوناگونی هم برای تأمین امنیت در شبکه وجود دارد. یکی از این مکانیزمها استفاده از دیوارآتش می‌باشد. مدیر شبکه باید درک بالایی از انواع دیوار آتش، نقاط قوت و ضعف هر نوع، حملاتْ تهدید کننده َی هر نوع، معماری ُهای دیوار آتش، تأثیرات آن بر شبکه و کاربران، سیاستٌ امنیتی سازمان و همچنین نیازهای فنی پیادهسازیٌ داشته باشد تا بتواند راهحل مناسب را انتخاب و بهدرستی پیادهسازی نماید و سپس آن را مورد آزمایش قرار دهد. در همین راستا، سیستم عاملٌ Linux برای پیادهسازی نرم افزاری دیوارآتش فیلترکنندهَّی بسته، ابزاری را به نامiptablesدر اختیار کاربر قرار می‌دهد تا با استفاده از دستورات این ابزار بتواند قوانینٌ و فیلترهای موردنیاز را برای کنترل مطلوب دسترسی، خواه از داخل شبکه به خارج و خواه بالعکس، پیکربندی نماید.

کلمات کلیدی:Iptables, firewall, linux, ipfilter, udp, tcp

مقدمه

دیوارهآتشiptablesتوسط پروژهی netfilterتوسعه یافته و از زمان ارائهی linuxبا هستهی ۴,۲در ژانویهی ۴۰۰۲ به عنوان قسمتی از linux در اختیار عموم قرار گرفته، طی سالها ویژگیهای iptablesبهبود یافته و آن را به یک فایروال قدرتمند با بیشتر قابلیتهایی که عموماً در دیوارهایآتش تجاری پیدا میشود تبدیل کرد. برای مثال iptablesقابلیتهای جامع ردیابی وضعیت پروتکل، بررسی کاربرد بسته ها توسط لایه، کاهش نرخ، و یک مکانیسم قدرتمند جهت تعیین نمودن یک سیاست فیلتر کردن را ارائه میدهد. تمامی نسخههای اصلی linuxشامل iptablesهستند و خیلی از این نسخهها نیز از همان ابتدای نصب،کاربر را وادار به استفاده از یک سیاست iptablesمیکنند. تفاوت اصطلاح netfilterوiptablesدر جامعه ی linuxمنجر به سردرگمیهای فراوانی شده که اکنون به توضیح این دو اصطلاح میپردازیم. نام رسمی که توسطlinux برای تمامی پروژههای فیلترکردن بستهها و ابزارهای ایجاد تغییر در بستهها فراهم شده netfilterاست. گرچه این اصطلاح همچنین

برای یک frameworkدرون هستهی linuxنیز به کاربرده میشود. که از این frameworkمیتوان جهت قرار دادن توابع درون پشتههای شبکه در مراحل مختلف استفاده کرد. از طرفی دیگرiptablesزnetfilter frameworkبه منظور قرار دادن توابع طراحی شده برای اجرای عملیات (مانند فیلتر کردن)بر روی بستهها درون پشتههای شبکه استفاده می کند. شما میتوانید به netfilterبه عنوان ابزاری جهت فراهم نمودن frameworkهایی که iptablesبا استفاده از آنها نقش دیوارآتش را ایفا میکند نگاه کنید. اصطلاح iptablesهمچنین به ابزاربخش کاربر گفته میشود که خط فرمان را می شکند، یک سیاست دیوارآتش را به هسته القا میکند. اصطلاحاتی مانند جداول، زنجیرها، همتاها و هدفها در متن iptablesمعنا پیدا میکنند(.Gregor N.Purdy,2004 Netfilter)خود، ترافیک را فیلتر نمی کند و صرفاً به توابعی که قادر به فیلتر کردن ترافیک هستند اجازه میدهد تا در محل مناسب در هسته قرار بگیرند. پروژهی netfilterهمچنین چندین قطعه از شالودهی هسته (مانند ردیابی ارتباط،loggingیا واقعه نگاری)را نیز تامین میکند. هر سیاست iptablesمیتواند از این تسهیلات جهت اجرای هر نوع فرایند ویژهی پردازش بسته استفاده کند(.Gregor N.Purdy,2004)

فیلتر کردن بستهها به وسیلهی iptables

دیوارآتشiptablesبه کاربر و یا وسیله اجازه میدهد کنترل زیادی بر روی بستههای ipکه با یک سیستم linuxدر ارتباط هستند داشته باشد.که این کنترل درون هستهی linuxاعمال میشود یک سیاست میتواند توسط iptables ساخته شود و به عنوان یک ناظرترافیک فعال عمل کند نحوهی کار این ناظر به این صورت خواهد بود که بستههایی که

اجازهی عبور ندارند از بین میروند و بستههایی که عبور میکنند جمع میشوند و به مسیر مورد نظرشان میروند یا مطابق نیازمندیهای شبکهی محلی تغییر میکنند. یک سیاست iptablesبراساس دسته ای از قوانین مرتب که عملیات مورد نیاز جهت برخورد با گروههای مختلف بستهها را توصیف می کند ساخته میشود. هر قانون iptablesبه یک زنجیر درون
یک جدول مربوط میشود. یک زنجیرiptablesمجموعهای از قوانین است که یا مقایر یا
هماهنگ و یا مشابه با موارد مربوط به بستههایی است که ویژگیهای مشترکی دارند(مانند مسیریابی شدن به سمت سیستم .linuxو یا دور کردن از سیستم). شکل زیر نشان میدهد که چگونه بستهها درون هسته از جدولهای natfilter میگذرند(.Rash.Michael,2007)

شکل-۲ نحوهی عبور بستههای درون هسته از جدول Natfilters

نصبiptables

به دلیل اینکه iptablesبه دو بخش اساسی تقسیم میشود (ماژولهای هسته و برنامه مدیریت بخش کاربر)نصبiptablesشامل کامپایل کردن و نصب کردن هستهی لینوکس و قسمت باینری مربوط به کاربر میشود کد منبع هسته شامل تعداد زیادی زیر سیستم و تواناییهای ضروری فیلتر کردن بسته را دارا میباشد که به صورت پیش فرض فعال شدهاند. در برخی از هستههای)۴,۲و همهی هستههای (۴,۲گزینههای کامپایل netfilterبهصورت پیش فرض فعال نبودند اما طی سالها به دلیل رسیدن نرمافزارهایی که توسط پروژهی netfilterتولید میشوند به سطح کیفیت بالا، نگهدارندگان هسته احساس کردند که نرم افزار به حدی رسیده است که استفاده از iptablesدرlinuxنباید نیازمند کامپایل مجدد هسته باشد. هستههای کنونی به شما اجازه میدهند تا با یک سیاست iptablesبهصورت پیش فرض بستهها را فیلتر کنید. مهمترین گام در ساخت یک سیستم linuxکه بتواند بهعنوان یک فایروال iptablesکار کند پیکربندی و کامپایل مناسب هستهی linuxاست تمامی پردازشهای سنگین شبکه و کارهای مقایسه در iptablesدرون هسته انجام میشود(.Gregor N.Purdy,2004

پیکربندی هسته

قبل از شروع به کامپایل باید یک فایل پیکربندی هسته ایجاد کنیم. خوشبختانه فرایند ساخت این فایل به صورت خودکار توسط توسعهدهندگان هسته ایجاد شده و برای راه اندازی آن تنها نیاز به یک دستور داریم(درون دایرکتوری.(/usr/src/linux-2.6.20.1دستور make menuconfigواسطncursesرا راه اندازی میکند که در آن می توان گزینههای مختلف کامپایل را انتخاب کرد(شما میتوانید به ترتیب با دستورات make xconfigوmake configواسطهای xwindowsو terminalرا فراخوانی کنید)در اینجا ما واسطncurses15را انتخاب کردیم چون تعادل خوبی بین واسطspartanو واسط نسبتاً گران xwindowsایجاد میکند. واسط ncursesهمچنین به آسانی با پیکربندی یک هستهی linuxاریموت شدهٌ درمیانٌ یک جلسهً sshبدون نیاز به ارسال یک ارتباطxwindowsهماهنگ میشود(. Rash.Michael,2007)

پس از اجرای make menuconfigچندین بخش پیکربندی از گزینههای میزان پیشرفتگی کد تا روالهای کتابخانه ارائه میشوند.بیشتر گزینههای کامپایل netfilterبرای هستهی سری۲,۶درون بخشی به نامnetwork packet filtering frameworkدر زیر networking options>networkingقرار دارد. برخی از مهمترین گزینههایی که باید در قسمت فایل پیکربندی هسته فعال شوند عبارتند از: ردیابی ارتباطnetfilter، ثبت کردن و فیلتر کردن بستهها. دو بخش پیکربندی اضافی در بخش netfilter(network packet filtering framework)وجود دارند که عبارتند از پیکربندی مرکز netfilterو پیکربندی.(Rash.Michael,2007)ip:netfilter

پیکربندی مرکزnetfilter

قسمتcore netfilter configurationشامل چندین گزینهی مهم است که همگی باید فعال شوند.

Comment match support× FTP support× Length match support Limit match support

MAC address match support

MARK target support Netfilter connection tracking support Netfilter LOG over NFNETLINK interface Netfilter netlink interface Netfilter Xtables support State match support String match support

پیکربندیip:netfilter

پس از اتمام پیکربندی بخشcore netfilter configurationبه بخشnetfilter configurationمیرویم که گزینههایی که در این بخش باید فعال شوند به ترتیب زیر هستند:

ECN target support× Full NAT× IP address range match support

IP tables support (required for filtering/masq/NAT) IPv4 connection tracking support (required for NAT) LOG target support MASQUERADE target support Owner match support Packet filtering

raw table support (required for NOTRACK/TRACE) Packet mangling Recent match support× REJECT target support× TOS match support TOS target support TTL match support TTL target support ULOG target support

اتمام پیکربندی هسته

پس از پیکربندی هستهی ۴,۲,۴۰,۲با پشتیبانیهای مورد نیاز توسط واسط menuconfigبا انتخابexitو تایید پیام do you wish to save your new kernel configuration?پیکربندی را ثبت کنید. پس از این مرحله به

قسمت پوستهی فرمان برمیگردید که در آن قسمت میتوانید با استفاده از دستورات زیر پیکربندی netfilterحاصل را امتحان کنید .

grep ” _NF_” .config× $ grep NETFILTER . config $

کامپایل و نصب هسته

اکنون که پیکربندی هسته به پایان رسید به سراغ کامپایل کردن و نصب آن میرویم. جهت نصب و کامپایل هستهی ۴,۲,۴۰,۲دون قسمت bootدستورات زیر را اجرا
کنید(.Suehring.S and Zeigler.R,2005)
make $ su – Password: # mount /boot $

cd /usr/src/linux-2.6. 20 .1 # make install && make modules_install #

نتیجهی موفقیت آمیز دستورات بالا اعلام می کند که bootloaderباید پیکر بندی شود و در نهایت هستهی ۴,۲,۴۰,۲جدید را بوت کنیم. در این قسمت ازgrub bootloaderو محل/dev/hda2برای بخش ریشه استفاده میکنیم با استفاده از ویرایشگر دلخواه خطوط زیر را به قسمت/boot/grub/grub.confاضافه میکنیم(Suehring.S and
Zeigler.R,2005).

title linux-2.6.20.1× root (hd0,0) kernel /boot/vmlinuz-2.6.20.1 root=/dev/hda2