نویسنده : هومن تصدیقی Tasdighi@aidagroups.com

۱. مقدمه :

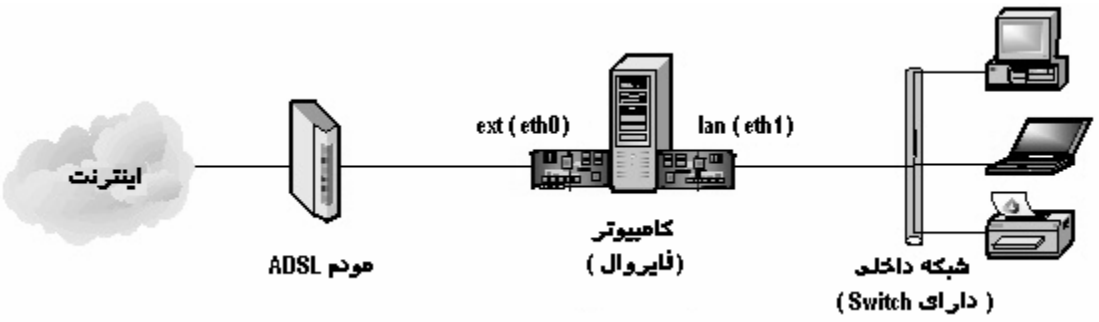
موضوع مورد بحث در این مقاله، مفهوم جداول، زنجیرها (Chains) و قوانین (Rules) می باشد و اینکه به چه شکل می توان از آنها استفاده نمود تا یک کامپیوتر دارای سیستم عامل Linux را به یک فایروال تبدیل نمود.

در این مقاله هدف بررسی مجموعه دستورات لازم برای آنکه یک فایروال توسط IPTables راه اندازی شود، نمی باشد؛ بلکه فقط توسط یک نقشه فیزیکی شبکه سعی دارد تا جریان بسته و جایگاه جداول را در IPTables ارائه نماید. این دیاگرام می تواند سنگ بنای معرفی ویژگی ها، دستورات، و مفاهیم IPTables به شکل غیر فنی باشد. این مقاله صرفاً جنبه آشنایی برای افراد تازه کار داشته و در مقاله های بعدی موجود در سایت www.aidagroups.com می توانید اطلاعات تخصصی در مورد IPTables و نحوه پیکربندی آن بدست آورید.

۲. شبکه مُدل مورد استفاده :

بسیاری از متخصصان، دنیای شبکه و تجهیزات را به آن دلیل بر برنامه نویسی ترجیح می دهند که در دنیای شبکه همه چیز فیزیکی بوده و احساس راحتی بیشتری نسبت به دنیای برنامه نویسی بدست می آورند! درست یا غلط، من نیز همین خط مشی را برای این مقاله بر می گزینم. اجازه دهید در این مقاله بحث خود را بر روی یک شبکه واقعی که در طرح آن در شکل ۱ آمده است، متمرکز نماییم. با این شبکه سعی خواهیم کرد تا در دنیای جالب و تا حدی پیچیده Netfilter و IPTables به کنکاش بپردازیم.

شبکه مورد بررسی در این مقاله از یک کامپیوتر پنتیوم IV ، دارای 512MB حافظهٔ RAM که بر روی مادربورد Gigabyte قرار دارد و دارای دو کارت شبکه از نوع D_link 538TX می باشد و در بازار کشورمان نیز بسیار فراوان است، تشکیل می گردد.



شکل ۱ – شبکه مورد بررسی در این مقاله

متاسفم! قرار بود این مقاله برای تازه کاران باشد. بنابراین اجازه دهید همان سیاست قبلی را دنبال کنیم. به عنوان مدل در این مقاله از این کامپیوتر PC با دو کارت شبکه (Network Interface Card = NIC)، استفاده می کنیم. همانگونه که در دنیای سیستم عامل Linux مرسوم است، این دو کارت با اسامی eth0 و eth1 در شکل فوق نشان داده شده اند. Eth مخفف کلمه Ethernet بوده و نشان دهنده آن است که این کارت ها، کارت شبکه می باشند.

یکی از این کارت های شبکه به یک سوئیچ متصل شده است. این سوئیچ شبکه داخلی سازمان را تشکیل داده است که در شکل نیامده است. بنابراین شبکه داخلی سازمان دارای توپولوژی star (ستاره ای) میباشد. کارتی که به شبکه داخلی متصل می گردد، در شکل با نام lan نشان داده شده است. گاهی در کتاب ها به آن کارت آبی (نشانه اطمینان و عدم وجود خطر) و یا کارت Internal (به معنی داخلی) نیز می گویند.

کارت دوم به یک مودم ADSL متصل شده و از طریق آن به اینترنت دسترسی دارد. این کارت در شکل با نام ext که مخفف کلمه External (به معنی خارجی است)، مشخص شده است. چون این کارت به سمتی که در آن خطر وجود دارد، گاهی به این کارت، کارت قرمز نیزمی گویند. هدف از ایجاد این شبکه آن است که بتوان شبکه داخلی را تحت کنترل داشت و توسط فایروال جلوی نفوذ افراد مزاحم از اینترنت به شبکه داخلی را گرفت.

با این طرح، اجازه دهید معرفی مفاهیم پایه IPTables را آغاز نماییم. فقط به خاطر داشته باشید، این مقاله یک مرجع کامل IPTables نیست و فقط سعی دارد جای آن چیزی را که در بسیاری از مقالات تخصصی خالی است، پرکند.

۳. معرفی بسته نرم افزاری IPTables :

در زیر معرفی مختصری که در سایت رسمی پشتیبانی از IPTables به آدرس www.netfilter.org آمده است، ارائه می گردد:

Netfilter و IPTables ساختاری نرم افزاری درون کرنل 2.4.x و کرنل 2.6.x می باشد که باعث می شود به کمک آن بتوان packet filtering (فیلتر کردن بسته های پرتکل معرفی)، NAT (ترجمه آدرس شبکه) و سایر اعمال مربوط به بسته ها (mangle) را انجام داد.

اجازه دهید در مورد بعضی از اطلاعات موجود در تعریف فوق توضیح دهم.

- بسته ها (Packet)، واحد داده پروتکلی است که در لایه شبکه مدل OSI در حال عمل می باشد. "واحد داده پروتکل" با کلمه مخفف PDU که از عبارت Protocol Data Unit می باشد، نشان داده می شود. PDU ها برای پروتکل های مختلف و در لایه های متفاوت OSI با یکدیگر تفاوت دارد. مثلاً PDU (یعنی واحد داده پروتکل) در لایه ۲، فریم می باشد در حالیکه در لایه ۳، بسته است.

  گاهی اوقات اصطلاح PDU باعث سردرگمی تازه واردان به دنیای شبکه می گردد. مثلاً وقتی می گویند PDU در

حال حرکت بر روی رسانه (سیم) و یا در لایه دوم، منظور فریم است. بسته ها که مربوط به لایه سوم (یعنی Network) می باشند، درون فریم ها قرار می گیرند. در صورتیکه با ساختار یک بسته آشنا باشیم، می توانیم محتویات آنرا وارسی کرده و براساس این محتویات و به کمک قوانینی خاص، به انتخاب از بین بسته ها بپردازیم. یکی از وظایف مهم IPTables نیز همیم می باشد که براساس قوانین (rule)، محتویات بسته ها را بررسی کرده و به بعضی اجازه عبور بدهد و یا جلوی عبور گروهی دیگر را بگیرد.

- IPTables یک نرم افزار است. کسانی که با نسخه های قدیمی تر خانواده Linux مانند Read Hat 7.x سروکار داشته اند، IPChain را به خاطر می آورند. IPChain یک فایروال قدیم است که به نوعی پدر بزرگ IPTable محسوب می گردد!

IPTables به کمک Netfilter ساخته شده است و دارای مجموعه ای از دستورات خاص خط فرمانی است که توسط آن می توان قوانین را نوشت. مثلاً طبق این قوانین می گوییم اگر بسته ها از کامپیوتر با آدرس IP، 192.168.0.1 بود، آنها را حذف کن!

- NAT که مخفف Network Address Translation می باشد و به معنی "ترجمه آدرس شبکه" است، استانداردی است که باعث می گردد، برای انتقال بسته های داده بر روی شبکه داخلی از یک مجموعه آدرس IP و برای ترافیک خارجی از مجموعه دیگری از آدرس های IP استفاده شود. در شکل ۱، کامپیوتر موجود بین دو شبکه داخلی و خارجی، می تواند نقش یک وسیله ترجمه کننده آدرس IP یا NAT را بازی کند. این کامپیوتر، آدرس های IP موجود در سمت داخلی شبکه را به آدرس های IP خارجی که بر روی سمت خارجی شبکه و یا اینترنت مورد استفاده هستند، ترجمه میکند. یکی از دلایل این کار و استفاده از NAT آن است که کاربران می توانند آدرس های داخلی خود را از دید کاربران بیرونی مخفی کرده و به آنها یک آدرس دیگر را نشان دهند.

امکان راه اندازی NAT در سیستم عامل Windows 2003، خانواده های مختلف Linux و روترهای Cisco وجود دارد.

- Mangling به معنای "پیچاندن" و یا "تغییر فرم دادن" و ... می باشد! در دنیای IPTable این اصطلاح زیاد شنیده می شود. ولی چه چیزی قرار است تغییر یابد؟ Mangling (یا تغییر محتویات) به کرنل این امکان را می دهد تا محتویات فیلدهای خاصی در Header مربوط به بسته ها را تغییر دهد.

ولی چرا باید محتویات فیلدها تغییر یابد؟ حتماً توضیح در مورد NAT را فراموش نکرده اید. وظیفه NAT آن بود که یک آدرس را به آدرس دیگری تبدیل کند. مثلاً آدرس IP فرستنده یک بسته از 192.168.0.5 به 80.40.50.60 عوض شود. آدرس فرستنده در یکی از فیلدهای Header ذخیره شده است و به کمک Mangling می توان محتویات این فیلد را تغییر داد.

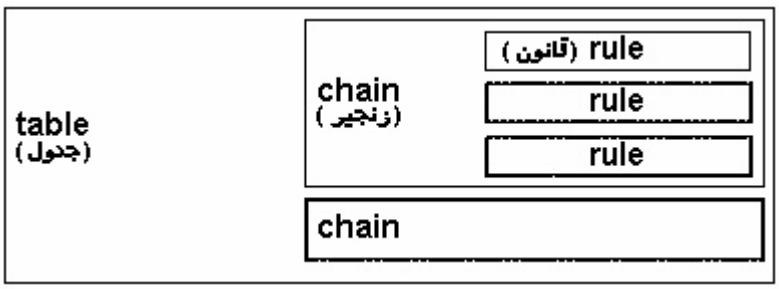
- Netfilter مانند تعدادی قلاب درون کرنل می باشد که به ماجول های درون کرنل اجازه می دهد تا هر دفعه که یک بسته از قلابی عبور می کند، یک تابع را صدا بزند و در صورت نیاز عکس العملی نشان دهد. IPTables از قلاب های کرنل استفاده نموده و هر وقت بسته ای عبور می کند، پیش از آنکه بتواند به یک شبکه خاص ارسال گردد، آنرا چک می کند.

برای آنکه بتوان از IPTables استفاده نمود، باید قابلیت پشتیبانی از آن در کرنل ایجاد شده باشد و سرویس نیز باید پیکربندی و اجرا شده باشد. خوشبختانه این ویژگی در اکثر خانواده های Linux وجود دارد ولی ممکن است به دلایلی فعال نباشد و یا در حالت متوسط فعال شده باشد و با حداکثر قدرت کار نکند! علت آن است که IPTables وقتی به حالت حداکثر فعال گردد، بسیار سخت گیر می شود و ممکن است بسیاری از اعمال جاری شبکه ای نیز از کار بیفتد.

با راه اندازی فایروال، تعدادی قانون (rule) و زنجیر (chain) ایجاد می گردد و برای بسته هایی که می خواهند بین شبکه های متصل به فایروال انتقال یابند، استفاده می گردد.

۴. ساختار IPTables :

برای استفاده از IPTables باید با اجزاء سازنده آن آشنا شد. فایروال IPTables دارای ۳ عنصر اصلی میباشد که در شکل ۲ آمده است. این ۳ بلاک سازنده ساختار فایروال عبارتند از: جدول، زنجیر و قانون.



شکل ۲ – اجزاء سازنده فایروال IPTables

Rule یا قانون، دربرگیرنده دستوری است که برای انتخاب بسته ها و انجام یک کار بر روی آن باید بکار رود. مثلاً:
تمام بسته های ارسال شده از مبدا 192.168.0.1، حذف شوند. یا آدرس IP مبدا تمام بسته های ارسال شده از کامپیوتر 192.168.0.5 به 80.40.50.60 تغییر یابد.
این موارد دو نمونه rule را نشان می دهند که خود از یک بخش مربوط به انتخاب و دسته بندی و یک بخش مربوط به یک

عملکرد تشکیل می گردند.

Chain یا زنجیر، مجموعه ای از قوانین می باشد. مثلاً دو قانون بالا می توانند با یکدیگر تشکیل یک chain به نام testchn را بدهند.

Table یا جدول، مجموعه ای از زنجیرها می باشد. مثلاً chain فوق با دو chain دیگر به نام های فرضی mainchn و changechn تشکیل یک جدول به نام input_tbl را بدهند.

IPTables به شکل پیش فرض دارای ۳ جدول اصلی به نام های filter ، nat و mangle می باشد. البته میتوان برحسب نیاز جداول دیگری را نیز به این مجموعه اضافه نمود. این جداول توسط کاربران و برای دسته بندی chain ها و rule های تعریف شده توسط خودشان کاربرد دارد. هر زمانی هم که بخواهند جداول خود را حذف نمایند ولی ۳ جدول پیش فرض filter ، nat و mangle قابل حذف نیستند.

در زیر توضیحی در مورد هر کدام از جداول سه گانه فوق ارائه می گردد:

- جدول filter : در بر گیرنده کلیه قوانین و chain های فیلتر نمودن بسته ها می باشد. مثلاً قوانین مربوط به حذف بسته های ارسالی از سوی شبکه 172.16.0.0 و یا صدور مجوز عبور برای بسته های ارسالی از کامپیوتر 10.10.5.8 و ... همگی در این جدول قرار می گیرند. علاوه بر اینها می توان قوانینی در این جدول تعریف کرد که بسته های مربوط به یک پورت و پروتکل خاص مثلاً پورت ۸۰ که مربوط به پروتکل http (یا همان وب) است اجازه عبور داشته باشند ولی بسته های مربوط به پورت ۲۱ یا پروتکل ftp اجازه عبور نداشته باشند. پس وظیفه اصلی این جدول نگهداری قوانین فیلتر کننده و یا قوانینی است که فیلتر نمی کنند. عمل فیلتر کردن و یا فیلتر نکردن براساس معیارهای گوناگون مانند آدرس IP مبدا و مقصد و یا شماره پورت و ... صورت می پذیرد.

  جدول nat : توضیح در مورد nat را که به خاطر دارید. این جدول در بر گیرنده کلیه قوانین و chain هایی است که وظیفه ترجمه آدرس IP را برعهده دارند. بعنوان مثال قانون زیر را در نظر بگیرید:

  اگر بسته ای از کامپیوتر 10.10.10.8 ارسال شد، آدرس IP فرستنده را به 80.50.60.90 تغییر بدهید.

  این قانون عملی در مورد فیلتر انجام نمی دهد، بلکه عمل ترجمه آدرس را انجام می دهد. بنابراین جای آن در جدول filter نبوده و باید در جدول nat قرار گیرد.

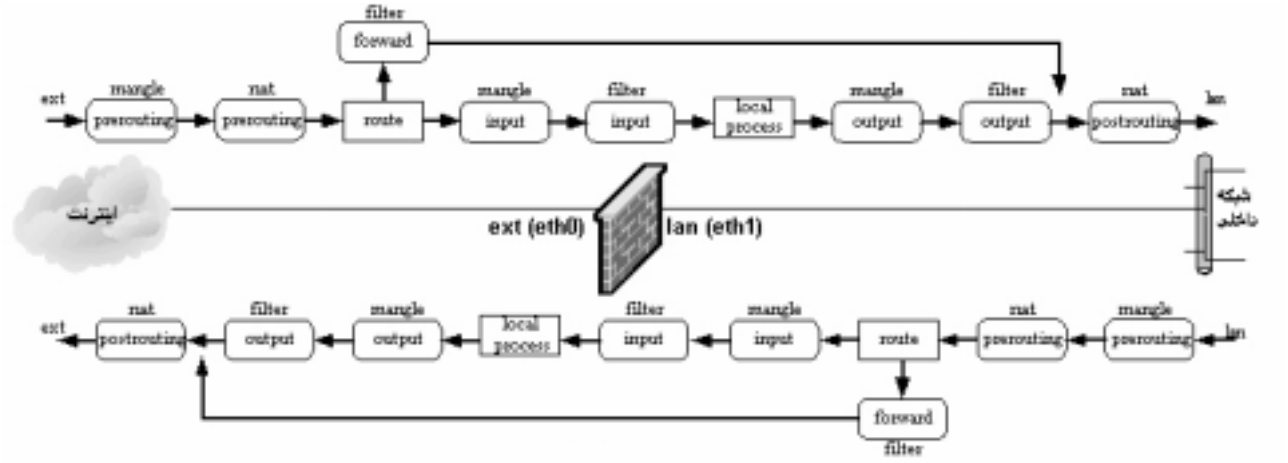
- جدول mangle : کلیه اعمال پیشرفته، مربوط به دستکاری فیلدهای header در بسته های ارسالی در شبکه توسط قوانین موجود در این جدول صورت می گیرد. تفاوت جدول nat و mangle در آن است که فقط قوانین مربوط به تغییر آدرس IP و یا پورت در جدول nat قرار می گیرند ولی سایر قوانین مربوط به تغییر فیلدهای header که در حالت پیشرفته کاربرد دارند، در جدول mangle جای می گیرند.

درون هر کدام از این جداول، تعدادی chain به شکل پیش فرض قرار می گیرد. از جمله این chain ها میتوان به ۸ عدد

chain اصلی که در زیر آمده است، اشاره کرد:

۱. جدول filter : chain های input، forward و output
۲. جدول nat : chain های prerouting و postrouting
۳. جدول mangle : chain های prerouting ، input و output

البته این ها فقط تعدادی از chain های پیش فرض بوده و علاوه بر تمام chain های پیش فرض امکان ساخت chain توسط کاربران نیز وجود دارد.
شکل ۳ نشان می دهد که در شبکه مدل مورد بحث در این مقاله، نحوه حرکت بسته ها چگونه می باشد و قوانین موجود در جدول های IPTable، در چه نقاطی بسته های ورودی و یا خروجی به فایروال را مورد بررسی قرار می دهند.



شکل ۳ – نحوه حرکت بسته ها در شبکه مدل و جایگاه هر جدول

مدیر شبکه می تواند کل ساختار IPTables و یا فقط قسمتی از آن را بر روی هر اینترفیس کامپیوتر فعال نماید. عملکرد IPTables باعث می شود تا یک کامپیوتر تبدیل به فایروال گردد.
همانطور که در شکل ۳ مشخص است، مسیر حرکت یک بسته از شبکه خارجی به داخل و برعکس در دو نمودار جدا نشان داده شده است. جریان بسته درون این ساختار بدین شکل می باشد:
به هنگام ورود یک بسته به فایروال از طریق کارت شبکه eth0، اولین قسمت زنجیر prerouting در جدول mangle می باشد. این ترکیب را با mangle / prerouting نشان می دهیم. اگر به یاد داشته باشید، mangling (تغییر محتویات) باعث می شود که کرنل بتواند فیلدهای خاصی در header را تغییر دهید. قوانین موجود در این زنجیر این عمل را ممکن می سازند.
از mangle / prerouting ، بسته وارد nat / prerouting می شود. قبلاً بیان گردید که nat برای ترجمه آدرس IP از یک

شبکه به شبکه دیگر بکار می رود. قوانین موجود در این زنجیر، می توانند آدرس IP مقصد و یا آدرس پورت مقصد را عوض کنند.

بنابراین اگر بر روی یک فایروال IPTables بخواهیم قوانینی بنویسیم که تمام بسته های ورودی به فایروال از سوی کاربران اینترنتی، اگر مربوط به پروتکل http بودند، به سمت آدرس 192.168.5.5 روی شبکه داخلی هدایت شوند، باید در nat / prerouting ، آدرس مقصد تمام بسته های ورودی مربوط به http را به 192.168.5.5 تغییر داد.

بنابراین به خاطر داشته باشید :

nat / prerouting برای تغییر آدرس IP مقصد و یا آدرس پورت مقصد می باشد. بخش Route که در شکل آمده است، یک جدول یا زنجیر و یا rule نباشد. Roué فقط قسمتی است که تصمیم می گیرد بسته باید به کدام زنجیر و کدام جدول ارسال شود. اساس تصمیم گیری نیز آدرس IP مقصد است. بنابراین بخش route (مسیریابی) ، آدرس IP مقصد بسته را check می کند. اگر آدرس IP مقصد بسته، مساوی آدرس IP خود فایروال باشد، معلوم است که بسته برای فایروال ارسال شده و route بسته را به قسمت input / mangle ارسال می نماید. اگر آدرس IP مقصد هر چیز دیگری باشد، route بسته را به filter / forward می فرستد.

قسمت filter / input ، تمام بسته هایی را که می خواهند به فایروال وارد شوند را مورد بررسی قرار میدهد. این زنجیر حاوی قوانینی است که معین می کند آیا یک بسته مورد قبول می باشد و یا باید بلاک شود. به عبارت ساده یک فیلتر کننده بسته یا packet-filter می باشد.

یک قسمت دیگر بر روی شکل با عنوان local process یا پراسس های محلی مشخص شده است. بعضی از پراسس های موجود بر روی فایروال ممکن است بخواهند از طریق کارت شبکه با سایر وسایل و سرویس های موجود روی شبکه ارتباط برقرار نمایند. یک مثال از این دسته می تواند ping کردن کامپیوترهای دیگر از پشت فایروال، و یا موجود بودن سرویس DNS و یا سرویس NTP بر روی کامپیوتر فایروال باشد.

این نوع بسته ها ابتدا به mangle / output وارد می شوند. زنجیر mangle / output عملکردی شبیه به mangle / prerouting دارند. ولی تفاوت در این است که فقط بسته هایی که توسط خود فایروال تولید می شوند، به زنجیر mangle output / وارد می شوند.

زنجیر filter / output ، بسته هایی را که از فایروال خارج می شوند را مدیریت می کند. این زنجیر شامل قوانینی هستند که مشخص می کنند که آیا یک بسته باید موردقبول قرار گیرد و یا بلاک شود. به عبارت ساده، این بخش نیز یک packet-filter می باشد. در مسیر موازی، زنجیر filter / forward بسته هایی را که از شبکه خارجی به سمت شبکه داخلی فرستاده می شوند را مورد بررسی قرار داده و براساس ویژگیهای بسته آنرا حذف کرده و یا به آن اجازه عبور می دهند.

nat / postrouting ، آخرین نقطه در مسیر حرکتی بسته ها می باشد. این زنجیر در بر گیرنده قوانینی است که توسط آن

می توان آدرس IP مبدا و یا شماره پورت مبدا یک بسته عبوری را تغییر داد. پس یادآوری می کنیم زنجیر nat / prerouting در برگیرنده قوانینی است که آدرس IP مقصد و یا پورت مقصد را عوض می کنند ولی در nat / postrouting قوانینی داریم که آدرس IP مبدا و شماره پورت مبدا را عوض می کنند.

۵. خلاصه :

IPTables یک فایروال است که به کمک ابزار Netfilter ، ساخته شده است. نسل قبل از IPTables با نام IPchains شناخته می شود. درون IPTables ، جداول، زنجیرها و قوانین را داریم. زنجیرها در ارتباط خاصی با یکدیگر قرار دارند که در شکل ۳ نشان داده شد. به شکل خلاصه کاربرد هرکدام از جداول و زنجیر درون آنها مطابق جدول ۱ می باشد:

نام زنجیر / نام جدول	توضیح
mangle / prerouting	به ندرت استفاده می شود
nat / prerouting	تغییر آدرس IP مقصد و پورت مقصد
filter / forward	انتقال (forward) بسته از یک شبکه به شبکه دیگر و کنترل آن
nat / postrouting	تغییر آدرس IP مبدا و پورت مبدا
filter / input	زنجیر input که بسته های ورودی به خود فایروال را چک می کند
mangle / input	به ندرت استفاده می شود
mangle / output	به ندرت استفاده می شود
filter / output	زنجیر output که بسته های خروجی از خود فایروال را چک می کند

جدول ۱ – خلاصه کاربرد هر جدول و زنجیر درون آن

این مقاله صرفاً معرفی ساختار IPTables بوده و جهت آشنایی با مفاهیم اولیه مطرح در این فایروال ارائه گردیده است. اطلاعات بدست آمده از این متن، پایه مورد نیاز برای آشنایی و استفاده هوشمندانه از دستورات فایروال IPTables و پیکربندی آن می باشد. یکی از توانایی های متخصصان واحد امنیت شرکت "آینده یاوران داده های امن" ، تنظیم و پیکربندی انواع فایروال سخت افزاری و نرم افزاری، از جمله IPTables می باشد.

مهندس هومن تصدیقی

۱۳۸۵/۲/۲۰