دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

مقطع: کارشناسی

گرایش: نرم‌افزار

راهنمای راه‌اندازی و نصب Firewall

فروردین ۱۳۹۹

فهرست مطالب

صفحه

بخش اول آشنایی با Firewallها..... ۳

بخش دوم دریافت و نصب UFW..... ۵

بخش سوم پیکره‌بندی ufw..... ۷

بخش چهارم آشنایی با IPTables..... ۱۰

بخش اول

آشنایی با Firewallها

وقتی شـما مدیریت یک سـرور را به عهده می‌گیرید، یکی از ابتدایی‌ترین مواردی که میبایسـت به آن در راستای ارتقا امنیت سیستم توجه کنید، نصب و راه‌اندازی فایروال یا دیوار آتش[1] می‌باشد. لینوکس از یک سـیسـتم پیشـرفته به نام IPTables به منظور مدیریت فایروال بهره می‌برد. افراد زیادی پیکره‌بندی و مدیریت فایروال از طریق IPTablesرا کمی پیچیده می‌دانند، از این رو جایگزین‌هایی همانند UFW[2] مطرح می‌شـوند. UFW یک رابط کاربری مبتنی بر خط فرمان در اختیار کاربر قرار می‌دهد که به کاربر این امکان را می‌دهد تا به نحو ساده‌تری از IPTables استفاده کند. این ابزار نسخه گرافیکی نیز دارد نام آن GUFW می‌باشد.

سیستم عامل ویندوز، از یک دیوار آتش پیش‌فرض استفاده می‌کند که به صورت پیش‌فرض نصب و فعال است. پیکره بندی این دیوارآتش عموما نیازی به تغییر دادن پیش فرض‌ها ندارد و حتی در صورت نیاز به تغییر در تنظیمات آن، به دلیل وجود رابط گرافیکی قدرتمند، بسیار ساده می‌باشد.

در این گزارش، تمرکز ما برروی بحث فایروال در سـیسـتم عامل لینوکس و هم‌چنین بحث IPTables می‌باشد. در ادامه به نصب، راه اندازی و پیکره بندی این موارد می‌پردازیم.

---

[1] Firewall

[2] Un-complicated Firewall

بخش دوم

دریافت و نصب UFW

برای نصب UFW ابتدا یک سیستم لینوکسی مهیا می‌کنیم. این سیستم عامل می‌تواند سیستم عامل موجود بر روی سیستم شما و یا یک ماشین مجازی باشد. پس اطمینان از اتصال لینوکس به اینترنت، یه صفحه ترمینال باز کرده و دستور زیر را وارد کنید (در اینجا ما از یک سیستم عامل مبتنی بر Debian استفاده کرده‌ایم، لذا از Package Manager مختص آن یعنی apt استفاده کرده‌ایم):

Sudo apt-get install ufw

بعد از وارد کردن دستور بالا، ufw دانلود و نصب می‌شود. نسخه گرافیکی آن یعنی gufw نیز از طریق وارد کردن دستور زیر قابل دریافت است:

Sudo apt-get install gufw

ابزار ufw بصورت پیش‌فرض، بعد از نصب، غیرفعال می‌باشد. وضعیت آن را می‌توانید از طریق دستور زیر مشاهده کنید:

Sudo ufw status

برای فعال کردن فایروال می‌توانیم از دستور استفاده کنیم:

Sudo ufw enable

بخش سوم

پیکره‌بندی ufw

یکی از ابتدایی‌ترین مواردی که می‌توان در ufw تنظیم کرد، کنترل ترافیک ورودی و خروجی از سیستم می‌باشد. برای این کار می‌توانیم Default Rules را تغییر دهیم. همانطور که از اسم آن مشخص است، Default Rules تنظیمات استاندارد و پیش‌فرضی می‌باشد که پیکره‌بندی فایروال را تسهیل می‌بخشند. برای رد شدن یا نشدن ترافیک ورودی، می‌توان از یکی از موارد زیر استفاده کرد:

Sudo ufw default [deny/allow] incoming

برای ترافیک خروجی نیز از دستور زیر می‌توان استفاده کرد:

Sudo ufw default [deny/allow] outgoing

حال فرض کنید، فایروال سرور خود را تنظیم کرده‌ایم و تمام ترافیک ورودی را از طریق د ستور بالا، بلاک کرده‌ایم. این کار مشکلات زیادی دارد. یکی از اولین مشکلات زیادی که با آن مواجه می‌شویم، این است که دیگر نمی‌توانیم از طریق SSH به آن متصل شویم، چراکه اتصال ما به سرور نیز یک ترافیک ورودی محسوب می‌شود، بنابراین تلاش‌های خودمان نیز، توسط سرور رد می‌شوند و قادر به وصل شدن به سرور نخواهیم بود. بنابراین، درمورد این شرایط نیاز داریم که پورت مربوط به سرویس SSH که پورت شماره ۲۲ می‌باشد را، در ورودی سیستم باز کنیم. برای اینکار، دستور زیر را در ترمینال وارد می‌کنیم:

Sudo ufw allow ۲۲/tcp

که در دستور بالا:

Sudo: اجرای دستور در حالت SuperUser

Ufw: نام فایروال

Allow: برای اجازه دادن

عدد ۲۲: شماره پورت مورد نظر که میخواهیم قانون allow بر روی آن اجرا شود

Tcp: پروتکل مورد نظر (گزینه دیگر udp می‌باشد)

می‌باشند.

توجه داشته باشید که برخی از موارد در ufw از طریق یک سری rule پیش‌فرض نیز قابل تنظیم هستند. برای مثال، عملیات دستور بالا که پورت ۲۲ TCP را برای ما فعال می‌کرد، از طریق دستور زیر نیز قابل انجام است:

Sudo ufw allow ssh

از آن جاییکه مرسوم است برروی پورت ۲۲ سرویس ssh فعال باشد، تنها با وارد کردن کلمه کلیدی ssh نیز می‌توان این سرویس را فعال کرد.

ممکن ا ست برروی سرور خود ابزاری دا شته با شید که نیاز به باز بودن یک سری پورت دا شته با شد، برای جلوگیری از اتلاف وقت می‌توانید از د ستور زیر برای باز کردن چند پورت به صورت همزمان استفاده کنید:

Sudo ufw allow ۲۰۰:۲۵۰/udp

دستور بالا پورت‌های udp را از شماره ۲۰۰ تا ۲۵۰ باز می‌کند.

به منظور لیســـت کردن ruleهایی که تا به حال برای فایروال تعریف کرده‌ایم می‌توانیم از دســـتور زیر استفاده کنیم:

Sudo ufw status numbered

حال فرض کنید می‌خواهیم یکی از ruleهایی که ســاخته‌ایم را از بین ببریم ولی دســتور غیر فعال کردن آن را بلد نیستیم، بدین منظور می‌توانیم آن rule را پاک کنیم تا غیرفعال شود. در این صورت دستور زیر را وارد می‌کنیم:

Sudo ufw delete ۴

که در دستور بالا می‌بایست بعد از کلمه کلیدی delete، شماره rule مورد نظر را از دستور پیشین یعنی status numbered برداشته و در آن جا قرار دهیم.

اگر می‌خواهید فایروال را به حالت اولیه برگردانید، می‌توانید از دستور زیر استفاده کنید:

Sudo ufw reset

بخش چهارم

آشنایی با IPTables

مدیریت ترافیک شبکه یکی از مهم‌ترین کارهایی است که یک مدیر شبکه/سیستم می‌بایست با آن مواجه شود. یک مدیر شبکه باید فایروال را به طوری تنظیم کند که نیازهای سیستم و کاربران سیستم چه درمورد ترافیک‌های ورودی و چه درمورد ترافیک‌های خروجی برطرف شود، به طوری که سیستم در مقابل حملات امن باشد. هنگام مطرح شدن این نیاز سیستم است که IPTables مطرح می‌شود. Iptableها ابزارهایی برای مدیریت Ruleهای فایروال‌های مبتنی بر خط فرمان [۳] می‌باشند که به مدیر سیستم امکان مدیریت ترافیک ورودی و خروجی را به وسیله یک سری Configuration Table Rules می‌دهند.

IPTables ماژول فایروال کرنل لینوکس می‌باشد که هم از IPV۴ و هم از IPV۶ پشتیبانی می‌کند. IPTableها هم در حالت stateless یعنی تنها کنترل State مبدا و مقصد و هم در حالت stateful یعنی کنترل تمامی stateهای مربوط به connectionها، قابل استفاده است. همچنین از قابلیت System Loging نیز بهره‌مند می‌باشد که برای بررسی دقیق‌تر شبکه توسط مدیر سیستم سودمند می‌باشد.

یکی از امکانات موجود در IPTables، قابلیت تعیین محدودیت برای تعداد پکت در ثانیه و یا حتی connection در ثانیه می‌باشد. این قابلیت در زمینه جلوگیری از حملات DoS می‌تواند کارا باشد.

IPTableها از یک سری جدول استفاده می‌کنند که این جدول‌ها زنجیرهایی دارند، هر کدام از این زنجیرها یک یا چند Rule تعریف شده توسط کاربر [۴] و یا درون سیستمی [۵] دارند. به کمک این جدول‌ها مدیر یک سیستم می‌تواند به درستی ترافیک شبکه را فیلتر کند.

جدول‌های IPTables به طور کلی به ۳ دسته تقسیم می‌شوند:

- جدول Filter: این جدول، جدول پیش‌فرض و در واقع همان فایروال می‌باشد و تمامی پالیسی‌های مرتبط با فایروال درون آن قرار می‌گیرد. این جدول تعدادی زنجیر درون سیستمی برای موارد زیر دارد:

---

[۳] Command Line

[۴] User Defined

[۵] Built-in

- ✓ Input: پکت‌هایی به مقصد سوکت‌های محلی[۶] (پکت‌های ورودی). یعنی پکت‌هایی که ورودی سیستمی هستند که فایروال بر روی آن است، برروی این زنجیر می‌روند
- ✓ Forward: پکت‌هایی که از طریق سیستم مسیریابی[۷] می‌شوند (پکت‌هایی که سیستم ما آن را دریافت و به سمت سیستمی دیگر مسیریابی می‌کند)
- ✓ Output: پکت‌هایی که به صورت محلی تولید می‌شوند (پکت‌هایی که سیستم ما تولید می‌کند، یعنی مبدا آن سیستم ما می‌باشد)

- جدول NAT: جدولی است که وقتی مورد استفاده قرار می‌گیرد که یک پکت می‌خواهد از شبکه محلی خارج و یا به آن داخل شود (از gateway).حله شامل موارد زیر می‌باشد:
  - ✓ PreRouting: برای هشدار دادن به هنگام فرارسیدن یک پکت، مورد استفاده قرار می‌گیرد
  - ✓ Output: برای هشدار دادن به هنگام تولید پکت‌های محلی (پکت‌هایی که سیستم ما تولید کرده) مورد استفاده قرار می‌گیرد
  - ✓ Postrouting: برای هشدار دادن به هنگام خروج پکت‌ها از سیستم مورد استفاده قرار می‌گیرد
- جدول Mangle: جدولی است که کارهای مرتبط با QoS نظیر توزیع بار[۸]، تغییر سرآیند[۹]های پکت‌ها نظیر سرآیندهای TCP و دیگر موارد مورد استفاده قرار می‌گیرد. در واقع بجای پردازش IP و پورت مبدا و هم‌چنین IP و پورت مقصد در طول گذر پکت از سیستم، با یک بیت آن را مشخص و پردازش می‌کند تا از پردازش زیاد جلوگیری شود. تا نسخه ۲,۴ کرنل لینوکس این جدول تنها ۲ زنجیر داشت، اما از آن به بعد شامل ۵ زنجیر می‌باشد:
  - ✓ PreRouting: برای پکت‌های ورودی به شبکه از gateway

---

۶ Local Sockets

۷ Route

۸ Load Balance

۹ Header

- ✓ Output: پکت‌های تولید شده توسط سیستمی که فایروال بر روی آن است
- ✓ Input: برای پکت‌های ورودی به سیستمی که فایروال بر روی آن است
- ✓ PostRouting: برای پکت‌های خروجی از شبکه(از gateway)
- ✓ Forward: برای پکت‌هایی که توسط سیستمی که فایروال بر روی آن است، مسیریابی می‌شوند

برای شروع از دستور زیر برای چک کردن ruleهای موجود استفاده می‌کنیم:

Iptables –L –n -v

کاربرد هر کدام از فلگ‌های استفاده شده، به سادگی از طریق help قابل مشاهده هستند:

Iptables -h

برای مثال اگر رفتار مشکوکی از یک IP ببینیم، میتوانیم به وسیله دستور زیر آن را بلاک کنیم:

Iptables –A INPUT –s xxx.xxx.xxx.xxx –j DROP

که در این دستور:

A- برای append کردن rule جدید به زنجیره فعلی

INPUT نام زنجیره

s- برای مشخص کردن IP مبدا

j- برای تعیین مقصد بسته است که در اینجا با اننتخاب DROP آن بسته مردود می‌شود

به وسیله دستور زیر می‌توانیم همین کار را تنها بر روی پروتکل TCP انجام دهیم:

iptables -A INPUT -p tcp -s xxx.xxx.xxx.xxx -j DROP