Analysing Performance issues of open-source intrusion detection systems in high-speed networks

Journal of Information Security and Applications(Elsevier)(Apr 2020)

The University of Auckland, Northwestern University

21 citations

بررسی و تحلیل کاراپودن سیستم‌های تشخیص نفوذ متن‌باز در شبکه‌های پهن‌باند

باتوجه به گسترش روزافزون شبکه‌ها و متداول‌شدن استفاده از آنها، حجم تبادل و انتقال اطلاعات نیز بالاتر رفته و امروزه در بیشتر شبکه‌ها نرخ گذر اطلاعات به بیش از ۱۰۰گیگابیت‌درثانیه رسیده است. سیستمهای تشخیص نفوذ نمیتوانند به درستی این حجم از ترافیک و فعالیت را کنترل کنند(این حجم از ترافیک منجر به رهاشدن تعداد زیادی از بسته‌ها و در نتیجه پایین‌آمدن کارایی این سیستم‌ها خواهدشد). این مقاله قصد دارد دقت تشخیص، میزان رهاشدن بسته‌ها، میزان منابع مصرفی و غیره را برای سامانه‌های تشخیص نفوذ متن‌باز سوریکاتا و اسنورت را در شبکه‌هایی با نرخ‌گذر ۱۰۰گیگابیت‌برثانیه بررسی کند. همچنین معیارهای ذکرشده را برای تنظیمات متفاوت این دو سیستم(متفاوت با تنظیمات پیشفرض)و در جریانات متفاوت با مدت زمان متغیر و حجم‌های دیگر ترافیک نیز اندازه می‌گیرد. در آخر راهکارهایی برای بهبود دو سامانه برای شبکه‌های پهن‌باند ارائه می‌دهد.

اسنورت تقریباً مکانیزم ساده‌تری به نسبت رقیب خود دارد و بر پایه تطابق امضا هست. اما سوریکاتا ویژگی‌های جدیتر و مدرنتری دارد از جمله پشتیبانی‌از اسکریپت که بهتر می‌تواند در شناسایی بدافزارها کمک کند. این دو سامانه از کتابخانه‌های خارجیLibpcap ,AF_Packet,PF_RING استفاده می‌کنند. برای بحث تطابق الگوها نیز از دو الگوریتمAho-corasic ویاregular expressionها می‌توان‌استفاده‌کرد. بنا به تحقیقات انجام شده قبلی، با مکانیزم‌های موجودlibpcap وAF_PACKET در پهنای باند بالای ۴۰ گیگابیت بر ثانیه نرخ‌رهاشدن بسته‌ها در این دو سیستم به بالای ۹۹درصد می‌رسد(باAF_PACKET برای ترافیک های کمتر از ۶۰ گیگابیت بر ثانیه اوضاع بهتر می‌شود).به کمکXDP در سوریکاتا میتوان ۱۰۰گیگابیت در ثانیه را کنترل کرد، اما تنها می‌توان از یک خط قانون استفاده کرد.

این مقاله این دو سامانه تشخیص نفوذ را در سه مرحله ارزیابی می‌کند:

- ترافیکی شامل چندین جریانTCP با حجم بسته‌های۱۵۰۰بایت تولید می‌کند و همچنین نرخ‌گذر را از ۱۰ گیگابیت‌درثانیه به ۱۰۰ گیگابیت‌درثانیه افزایش می‌دهد. و کارایی(این‌که چه تعداد از بسته ها را دور می‌اندازند)هر دو سامانه را اندازه می‌گیرد.
- دقت تشخیص این دو سامانه را با یک حجم زیادی از ترافیک که شامل داده‌ها مربوط به بدافزار هم هست، بررسی می‌کند. و برای خطوط قانون تعریف شده پیش فرض نیز این کار را انجام می‌دهد.
- در مرحله بعد دقت این دو سامانه را با ترافیک واقعی(شامل پروتکل‌های مختلف، جریانات متعدد با طول زمانی متفاوت)ارزیابی می‌کند.

در هرکدام از این آزمایش‌ها از این محیط استفاده می‌کند: یک ارسال‌کننده که بسته‌ها را تولیدمیکند و یک دریافت‌کننده که بر روی آن دوسامانه تشخیص نفوذ نصب شده‌است و بسته‌ها و جریان‌ها را پردازش می‌کند.

در هرکدام از این آزمایش‌ها تعداد بسته‌های دریافتی، تعداد بسته‌های رهاشده، میانگین استفاده از پردازشگر و حافظه مصرفی را اندازه می‌گیرد. پس از بررسی نتیجه آزمایش‌ها به این نتیجه می‌رسیم که قابلیت چندنخی که به نسخه‌های جدید دو سامانه اضافه شده‌است، باعث بهبودشان شده است. این سامانه‌ها در ترافیک۶۰گیگابیت در ثانیه باوجود رهاشدن تعدادی از بسته‌ها، دقت خوبی دارند. اما در ترافیک‌های بالاتر به مشکل خواهندخورد. همچنین با افزایش تعداد جریانات در ترافیکهای بسیارپایین‌تر نیز به مشکل خواهندخورد. همانطور که اشاره شد، استفاده از مکانیزم‌ها و کتابخانه‌های دیگر به‌جای تنظیمات پیشفرض و بهبود خط قوانین تعریف‌شده پیشفرض ب میتوان بهبود عملکرد سامانه‌های مذکور را در برخی شرایط بهبود داد(البته نه به صورت چشمگیری).

راهکارهایی که در این مقاله به آنها اشاره شده‌است:

- بااستفاده از چندین نمونه از سامانه‌های مذکور میتوان بارترافیکی را بینشان به صورت متعادلی تقسیم کرد.
- برای بهبود سرعت ضبط بسته‌ها می‌توان از DPDK استفاده کرد که با استفاده از آن حتی قادر خواهیم‌بود در ترافیک ۱۰۰گیگابیت‌برثانیه را بدون دورانداختن بسته ای تحمل کنیم.

ارتباط با موضوع انتخابی:

- معیارهایی که برای بررسی عملکرد این دو سامانه در نظرگرفته شده است، می تواند در مقاله استفاده شود: تعداد بسته‌های دریافتی، تعداد بسته‌های رهاشده، میانگین پردازشگر و حافظه مصرفی .
- به عنوان راهکار بررسی و آزمایش مثلاً می‌توان در ابتدا تنها ترافیک معمول اما با نرخ بالا را ارسال کرد.
- می‌توان برای داده‌های تست مواردی را در نظر گرفت که شامل جریانات معتدد باشند و طول(بازه) هر کدام نیز متغیر باشد.
- استفاده از چندین نمونه و مفهوم loadbalancing نیز می‌تواند به عنوان یک راهکار مورد بررسی قرارگیرد.
- استفاده از چارچوب DPDK نیز می‌تواند باعث بهبود ضبط و بررسی بسته‌ها شود.
- استفاده از XDP ؟؟؟