تفاوت‌های دو سامانه قدرتمند تحت شبکه

سامانه‌های تشخیص نفوذ یا سامانه‌های پیشگیری از نفوذ، کدام‌یک بهتر هستند؟

سامانه‌های تشخیص نفوذ IDS (سرنام Intrusion Detection Systems) ترافیک شبکه را برای پیدا کردن امضاهایی که با حملات سایبری شناخته‌شده یکسان هستند، تحلیل و ارزیابی می‌کنند. در نقطه مقابل سامانه‌های پیشگیری از نفوذ IPS (سرنام Intrusion Prevention Systems) ضمن تحلیل بسته‌های اطلاعاتی بر مبنای نوع حمله‌ای که شناسایی کرده‌اند، قادرند، فرآیند تحویل بسته‌ها به شبکه را متوقف کرده و مانع از آن شوند تا حمله به شبکه به سرانجام برسد.

سامانه تشخیص نفوذ

یک سامانه تشخیص نفوذ، ابزاری (نرم‌افزاری یا سخت‌افزاری) است که برای شناسایی تهدیدات امنیتی که یک سامانه میزبان یا شبکه را نشانه رفته‌اند، استفاده می‌شود. برای درک بهتر عملکرد سامانه‌های تشخیص نفوذ به شکل 1 دقت کنید.

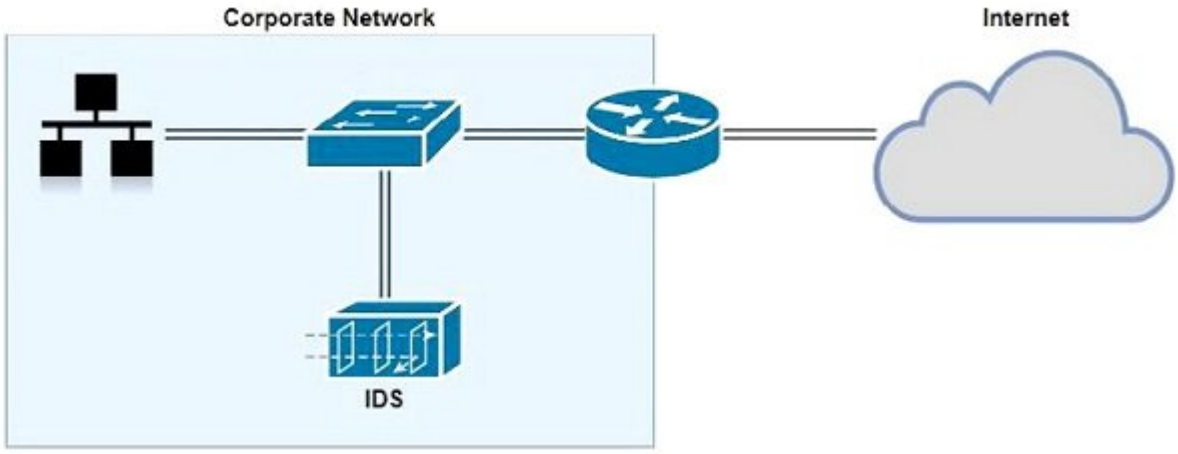
شکل 1 به‌وضوح نشان می‌دهد، یک سامانه تشخیص نفوذ برای اجتناب از به وجود آوردن زمان انتظار یا تاخیر در ترافیک شبکه به‌صورت خطی به شبکه متصل نشده، بلکه به یکی از پورت‌های سوییچ متصل شده تا یک کپی از ترافیک شبکه را برای تجزیه‌وتحلیل دریافت کند. علاوه بر این، اگر سامانه تشخیص نفوذ غیرفعال شده یا ارتباطش با شبکه قطع شود، روی عملکرد شبکه تاثیر منفی نخواهد گذاشت. بااین‌حال، از آنجا که تنها یک کپی از ترافیک را دریافت می‌کند و مدل استقرار و پیاده‌سازی آن خطی نیست (یعنی، ترافیک شبکه از طریق سامانه تشخیص نفوذ عبور نمی‌کند)، تنها پس از آن‌که تهدیدی شناسایی شد، سامانه تشخیص نفوذ هشداری صادر می‌کند و به همین دلیل نمی‌تواند از بروز یک حمله به شبکه ممانعت به عمل آورد. همین مسئله لزوم به‌کارگیری یک ابزار واکنش‌گرا را به تهدیداتی همچون سامانه پیشگیری از نفوذ دوچندان می‌کند.

سامانه پیشگیری از نفوذ

یک سامانه پیشگیری از نفوذ IPS، دستگاهی است که برای تشخیص و مسدودسازی تهدیدات امنیتی روی یک سامانه میزبان یا شبکه نصب می‌شود. همان‌گونه که شکل 2 نشان می‌دهد یک سامانه پیشگیری از نفوذ بر مبنای توپولوژی‌ای که شبکه بر مبنای آن طراحی‌شده است به‌صورت خطی در یک شبکه قرار می‌گیرد.

استقرار مستقیم در شبکه باعث می‌شود تا همه ترافیک شبکه از طریق دستگاه IPS عبور کرده و هرگونه کد مخرب یا حمله بالقوه‌ای که ممکن است شبکه را با خطر جدی روبه‌رو کند توسط سامانه پیشگیری از نفوذ شناسایی شود. اگر سامانه تشخیص نفوذ یک تهدید احتمالی را شناسایی کند، حسگرهای سامانه هشداری تولید کرده و مانع از آن می‌شوند تا ترافیک مخرب/ بارداده به شبکه وارد شده یا از آن خارج شوند. نکته بسیار مهمی که باید به آن توجه داشته باشید این است که یک سامانه پیشگیری از نفوذ باید در پشت دیوارآتش و نه در مقابل دیوارآتش و روبه‌روی مدخل ورود اینترنت به شبکه قرار گیرد. اگر یک سامانه پیشگیری از نفوذ در مقابل اینترنت که به آن منطقه غیرقابل

اعتماد گفته می‌شود قرار گیرد، ممکن است هشدارهای متعددی را تولید کند. برخی از این هشدارها ممکن است مثبت کاذب یا حتی ترافیک ناخواسته باشند. همان‌گونه که در توپولوژی شکل 2 مشاهده می‌کنید، سامانه پیشگیری از نفوذ به‌صورت خطی و به‌منظور نظارت و جلوگیری از حملات بالقوه قرار می‌گیرد. البته این‌کار هزینه‌هایی به همراه دارد که از آن جمله می‌توان به تأخیر یا زمان انتظار، کاهش عملکرد شبکه، مسدود شدن ترافیک در اثر از کار افتادن سامانه پیشگیری از نفوذ اشاره کرد.



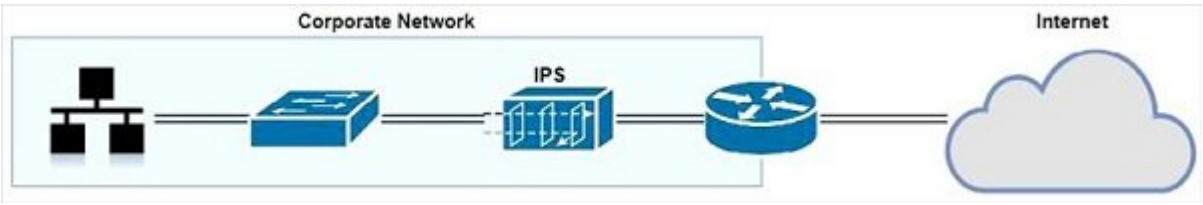
انواع سامانه‌های تشخیص نفوذ و پیشگیری از نفوذ

سامانه‌های فوق به دو شکل میزبان‌محور و شبکه‌محور استفاده می‌شوند. یک سامانه تشخیص نفوذ میزبان‌محور HIDS (سرنام Host-based Intrusion Detection System) یا سامانه پیشگیری از نفوذ میزبان محور HIPS (سرنام Host-based Intrusion Prevention system) به‌طور مستقیم روی یک دستگاه کلاینت همچون یک کامپیوتر مجهز به ویندوز 10 نصب می‌شوند. بااین‌حال، اگر هر یک از این دو سامانه روی یک ماشین محلی نصب شوند، HIDS/HIPS تنها قادر به نمایش ترافیک ورودی یا خروجی به/از ماشین محلی هستند. در چنین حالتی اگر تهدیدی به شبکه وارد شود،
HIDS/HIPS نمی‌تواند ترافیک مخرب را شناسایی و فیلتر کند، مگر این‌که ترافیک به ماشین محلی وارد شود. در یک سامانه تشخیص نفوذ مبتنی بر شبکه یا سامانه پیشگیری از نفوذ مبتنی بر شبکه، نرم‌افزار روی بخشی از شبکه نصب می‌شود. مزیت استفاده از چنین سامانه‌ای این است که می‌تواند ترافیک عبوری را نشان دهد و این پتانسیل را دارد تا تهدیدات را در سراسر شبکه شناسایی و متوقف کند.

تشخیص ترافیک مخرب

اکنون که تا حدودی با نحوه کار سامانه‌های تشخیص و پیشگیری از نفوذ آشنا شدیم، وقت آن رسیده تا چگونگی عملکرد این دو سامانه را در شناسایی ترافیک مخرب، از ترافیک سالم بررسی کنیم. سامانه‌های IDS/IPS از راهکارهای زیر برای شناسایی ترافیک مخرب از ترافیک سالم استفاده می‌کنند.
راهکار مبتنی بر امضا: از یک الگوی ویژه برای مقایسه ترافیک شبکه با پارامترهای خاص استفاده می‌کند تا اطمینان حاصل کند ترافیک شبکه مخرب نیست. در روش فوق از برنامه ضدویروسی که روی یک سامانه برای مقابله با ویروس‌ها و سایر بدافزارها نصب‌شده، استفاده می‌شود. البته توجه داشته باشید، اگر روی سامانه‌ای ویروسی در حال اجرا باشد و برنامه ضدویروس امضا آن ویروس را درون بانک اطلاعاتی خود نداشته باشد، سامانه‌های مبتنی بر این روش موفق به تشخیص تهدید نشده و هیچ‌گونه هشداری را تولید نخواهند کرد. درست است که شناسایی مبتنی بر امضا پیاده‌سازی ساده‌ای دارد، اما در مقابل قادر نیست هرگونه تهدید خارج از امضای موجود را در بانک اطلاعاتی IDS/IPS تشخیص دهد. بنابراین، تشخیص مبتنی بر امضا در حفاظت از سامانه‌ها در برابر تهدیدات جدید کارآمد نیست.
در راهکار مبتنی بر خط‌مشی: سامانه‌های IDS/IPS به‌گونه‌ای پیکربندی شده‌اند تا تهدیدات را بر اساس خط‌مشی‌های امنیتی فناوری‌اطلاعات سازمان شناسایی کنند. به‌عنوان‌مثال، خط‌مشی یک سازمان به این صورت تعریف‌شده که ترافیک Telnet باید محدود شود. از آنجا که Telnet از پورت 23 و پروتکل TCP استفاده می‌کند، قاعده تعریف‌شده باید مطابق با نوع ترافیک تعریف شود تا سامانه هشدار درستی صادر کرده و ترافیک مطابقت داده‌شده به‌درستی

مسدود شود.
در راهکار مبتنی بر رفتار غیر عادی: سامانه IDS/IPS برای ترافیکی که قرار است از یک سیستم یا شبکه عبور کند، خط پایه‌ای را ترسیم می‌کند. در ادامه سامانه از این خط اولیه برای ارزیابی شرایط مطلوب با شرایطی که ترافیک مشکوکی به شبکه وارد شده یا در حال خروج از شبکه است، استفاده می‌کند. در چنین شرایطی یک ناهنجاری بیانگر یک نفوذ به شبکه است. برای مثال، فرض کنید 100 بسته TCP-SYN از اینترنت در حال ورود به شبکه هستند و قرار است این بسته‌ها به یکی از سرورها تحویل داده شوند، اما در این میان مشکلی وجود دارد. فرستنده بسته‌های TCP-SYN باید با یک بسته TCP-ACK پاسخی را ارسال کند، اما این‌کار را انجام نمی‌دهد، بنابراین احتمال وقوع یک حمله سیل‌آسای SYN زیاد است. در چنین شرایطی سامانه پیشگیری از نفوذ مانع از آن می‌شود تا بسته‌ها به درون شبکه وارد شوند. لازم به توضیح است، برای ایجاد یک خط پایه که وضعیت عادی و ترافیک منظم شبکه را نشان می‌دهد، از روش‌هایی همچون شبکه‌های عصبی و الگوریتم‌های یادگیری ماشین استفاده می‌شود، زیرا قرار است برای رفتارهای عادی در یک شبکه الگوها و قواعد خاصی را پیدا و تعریف کرد و رفتارهایی که منطبق بر این الگوها هستند، رفتارهای عادی در نظر گرفته‌شده و رفتارهایی که خارج از عرف هستند و انحراف معیار آن‌ها فراتر از مقدار آمار پیش‌بینی شده است، به‌عنوان یک رفتار غیر عادی فرض شوند. به‌عنوان‌مثال، فرض کنید برای یک کارمند پیش‌بینی‌شده دو یا چهار بار در طول روز به شبکه وارد شده یا از آن خارج شود، حال این کارمند بیست مرتبه در طول روز چنین کاری انجام می‌دهد، چنین کاری به‌عنوان یک رفتار غیرمتعارف در نظر گرفته می‌شود. در مجموع باید به این حقیقت اذعان داشته باشیم که شناسایی رفتارهای عادی از رفتارهای غیر عادی کار چندان ساده‌ای نیست و سامانه‌هایی که از چنین روشی استفاده می‌کنند، هشدارهای مثبت کاذب با نرخ خطای بالایی را تولید می‌کنند که باعث می‌شود متخصصان شبکه به شکل کاملا محدودشده از چنین رویکردی استفاده کنند.
رویکرد مبتنی بر اعتماد: در رویکرد شناسایی مبتنی بر اعتماد، سامانه IPS نتایج به‌دست‌آمده از تهدیدات را با منابع معتبری همچون Cisco Talos مرتبط می‌کند.



تعامل سامانه‌های تشخیص نفوذ (IDS) و سامانه‌های پیشگیری از نفوذ (IPS)

سامانه‌های تشخیص نفوذ (IDS) و سامانه‌های پیشگیری از نفوذ (IPS) هر دو از ملزومات مهم و زیربنایی شبکه‌ها هستند. IDS و IPS بسته‌های اطلاعاتی یک شبکه را با پایگاه داده خود که شامل امضای حملات سایبری است، مقایسه کرده و هر بسته‌ای را که مشخصاتش با اطلاعات پایگاه داده مطابقت داشته باشد را به‌عنوان یک تهدید در نظر می‌گیرند. اصلی‌ترین تفاوت دو سامانه فوق در این است که IDS یک سامانه نظارتی است، درحالی‌که IPS یک سامانه کنترلی است.
سامانه‌های تشخیص نفوذ برای ابزارهای نظارت و تشخیصی هستند و قرار نیست بر مبنای رویکرد خود کاری را انجام دهند، درحالی‌که IPS بر مبنای محتویات یک بسته اطلاعاتی مانع از آن می‌شود تا ترافیک مخرب به درون یک شبکه انتقال پیدا کند. در این زمینه عملکرد IPS شباهت خیلی زیادی به چگونگی عملکرد یک دیوار آتش دارد که بر مبنای یک آدرس آی‌پی مانع از ورود ترافیک به شبکه می‌شود. سامانه‌های تشخیص نفوذ به‌منظور پیدا کردن علائمی که نشان می‌دهند، هکرها در حال استفاده از یک تهدید سایبری شناخته‌شده برای به سرقت بردن اطلاعات یا نفوذ به شبکه هستند، ترافیک شبکه را زیر نظر گرفته و آن را تجزیه‌وتحلیل می‌کنند.
سامانه‌های تشخیص نفوذ فعالیت فعلی شبکه را با اطلاعات مرتبط با تهدیدات که درون بانک اطلاعاتی خود قرار دارند، مقایسه می‌کنند تا رفتارهای مخاطره‌آمیزی همچون نقض قوانین امنیتی، وجود نرم‌افزارهای مخرب یا پویشگرهای پورت‌ها را پیدا کنند. اما سامانه‌های پیشگیری از نفوذ درست در میان یک دیوارآتش و جهان خارج از شبکه‌های ارتباطی سازمان قرار می‌گیرند تا بتوانند در زمان تشخیص یک تهدید امنیتی هشداری را تولید کنند. بیشتر فروشندگان محصولات IDS/IPS توانسته‌اند سامانه‌های پیشرفته‌تر پیشگیری از نفوذ را که همراه با دیوارهای آتش بوده و در قالب فناوری مدیریت یکپارچه (UTM) می‌توانند عملکرد هر دو سامانه را ارائه کنند، به بازار عرضه کنند. برخی از سامانه‌ها عملکرد هر دو فناوری IDS و IPS را در قالب یک مجموعه واحد ارائه می‌دهند.

تفاوت‌های میان IDS و IPS

هر دو فناوری سامانه پیشگیری از نفوذ و سامانه تشخیص نفوذ بسته‌های شبکه را خوانده و محتوای بسته‌ها را با تهدیدات شناخته‌شده ثبت‌شده درون بانک‌های اطلاعاتی مقایسه می‌کنند. اما همان‌گونه که اشاره شد، IDS تنها یک ابزار تشخیص و نظارت بوده و خودش عملی را انجام نمی‌دهد، اما IPS یک سامانه کنترلی است که بسته‌ها را بر مبنای قواعد قبول یا رد می‌کند. IDS به یک سامانه مکمل یا متخصصی نیاز دارد تا نتایج به‌دست‌آمده را بررسی کرده و اقدامات بعدی را انجام دهد. اما هدف از به‌کارگیری سامانه پیشگیری از نفوذ به دام انداختن بسته‌های خطرناک است تا موفق نشوند به هدف مشخص‌شده برسند. سامانه پیشگیری از نفوذ تا حد زیادی منفعل‌تر از یک سامانه تشخیص نفوذ است و ضروری است که بانک اطلاعاتی سامانه فوق با اطلاعات تهدیدات جدید به‌روز شود.

کلام پایانی

تیم‌های امنیتی با تهدیدات روبه رشدی همچون نقض داده‌ها و ورود بدافزارها به زیرساخت‌های ارتباطی یک سازمان روبه‌رو هستند، درحالی‌که بودجه سازمان‌ها برای مقابله با تهدیدات سایبری محدود است. در چنین شرایطی سامانه‌های IDS / IPS به یاری سازمان‌ها و تیم‌ها آماده و با خودکارسازی برخی از فرآیندهای مرتبط با شناسایی و دفع تهدیدات امنیتی، حفاظت از اطلاعات حساسی که ممکن است خواسته یا ناخواسته از شبکه یک سازمان خارج شوند، حصول اطمینان از پیاده‌سازی درست خط‌مشی‌های سازمان و مقابله با تهدیدات آتی بر مبنای تهدیداتی که به‌تازگی دفع شده‌اند، به میزان قابل‌توجهی امنیت یک شبکه را بهبود می‌بخشند

تاریخ انتشار:

20 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16012/%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%AA%D8%B4%D8%AE%DB%8C%D8%B5-%D9%86%D9%81%D9%88%D8%B0-%DB%8C%D8%A7-%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%BE%DB%8C%D8%B4%DA%AF%DB%8C%D8%B1%DB%8C-%D8%A7%D8%B2-%D9%86%D9%81%D9%88%D8%B0%D8%8C-%DA%A9%D8%AF%D8%A7%D9%85%E2%80%8C%DB%8C%DA%A9-%D8%A8%D9%87%D8%AA%D8%B1-%D9%87%D8%B3%D8%AA%D9%86%D8%AF%D8%9F