Intrusion Detection System

شناسایی حمله در مکانیزم های دفاعی برای پیشگیری از وقوع حمله مهم است. IDS (Intrusion Detection System) از ابزاری است که در شبکه به این منظور استفاده می شود.

سیستم IDS به صورت یک ابزار در شبکه با نرم افزاری که کار مونیتورینگ ترافیک عبوری را انجام می‌دهد، نصب می‌شود. معمولا دیوار آتش به همراه IDS کار تشخیص حمله را انجام می‌دهند. اگر از درون یک LAN به سمت بیرون حرکت کنید ابتدا به IDS سپس به دیوار آتش می‌رسید و پس از آن به شبکه بیرونی(اینترنت) می‌رسید. زیرا دیوار آتش یا از عبور بسته ممانعت می نماید و یا بسته را عبور می دهد. بنابراین ترافیک گسیل شده از شبکه بیرون در صورتی که از دیوار آتش عبور نمود توسط IDS بررسی می شود تا در مورد مشکوک بودن رفتار آن تصمیم‌گیری شود. در عمل این دو ابزار در یک آدرس IP می‌توانند پیاده‌سازی شوند. به علت منحرف نمودن توجه مهاجم از وجود ابزار امنیتی در شبکه، معمولا سیستم‌های امنیتی را در غالب یک مسیریاب، سوییچ در شبکه قرار می‌دهیم.

یک IDS کار مونیتور نمودن ترافیک شبکه و سرکشی به فایلهایlog راانجام میدهد. به این ترتیب هرگونه تخلف از سیاستهای امنیتی معمول شبکه را تشخیص می‌دهد.

انواع متفاوتی از این سیستم تعریف شده است. سیستم هایی که بر مبنای رفتار ترافیک شبکه، تنظیمات پورت‌ها، بر اساس نشانه‌ها و رفتار یک حمله که در منبع سیستم IDS ذخیره شده است و تغییر ترافیک با این الگو تطابق داده می‌شود، بر اساس تخطی از الگوی رفتاری معمول یک کاربر و یا سایر مشخصه ها به تشخیص یک حمله می‌پردازد و هشداری مبنی بر احتمال حمله را می‌دهد. سیستمIDS کار مقابله با حمله و سد آن را نیز عهده دار می‌باشد.

سیستم‌های IDS ای که رفتار آماری غیر عادی را تشخیص می‌دهند(behavior-based) وسیستم‌هایی که بر روی سگمنت‌های شبکه و ترافیک آنها به صورت بلادرنگ شنود و تحلیل می‌نمایند، سیستمهای مبتنی بر شبکه می‌باشند که در واقع نشانه‌ها را تشخیص می‌دهند . این سیستمها شامل یک برنامه لایه کاربرد به همراه NIC می‌باشند. ترافیک بقیه سگمنتهای آن شبکه و یا بقیه خطوط ارتباطی همانند خطوط تلفن مونیتور نمی شوند.

سیستم‌های کارآمد باید بتوانند هر نوع حمله‌ای را با ترکیبی از این روش‌ها و بدون تلف نمودن منابع سیستم، داده‌های بلادرنگ و قابل اعتمادی از شبکه را بدست آورند. این سیستم ها برای مقابله با حمله DOS کاربرد دارند.

می توان IDS را کنار سوییچ‌ها نصب نمود و با استفاده از پورت‌های خاص این ابزار که خاصیت یک هاب را دارند، ترافیک عبوری از سوییچ را به IDS فرستاد (forward) می شود به این ترتیب یک سیستم محافظتی خاموش در شبکه قرار داده‌ایم.

سیستم هایIDS مشکلاتی نیز دارند:

برخی هکرها حوصله زیادی در عملی نمودن حمله خود دارند. برخی حمله‌ها بر اساس تغییرات بسیار کند ترافیک عبوری و با گذشت زمان زیاد به وقوع می پیوندند و این یعنی سیستم IDS باید نمونه‌های زیادی از اطلاعات را در

پایگاه داده ذخیره و تحلیل نماید! و تشخیص حمله نیازمند هزینه فضای حافظه ها و تحلیل رفتاری طولانی مدت شبکه است.

در مواردی مشخصه‌ها و شناسه‌هایی که در بخش کاربرد سیستم IDS تنظیم می‌شوند مانند نوع سیستم عامل و شماره نسخه آن و platform مربوطه باعث می‌شود حملاتی که به صورت موردی و یا با فرمت جدید انجام می شود از دید دور بماند. این نوع سیستمIDS به شدت به سیستم عامل و منابع خود وابسته است و برای داشتن شبکه سالم به پشتیبانی و به روز شدن مداوم نیازمند است تا شناسایی آسیب‌پذیری‌های جدید و هماهنگی با آنها را به خوبی انجام دهد. در واقع داشتن دید سازگار با تغییرات نوع حمله ها نیازمند همراهی با تغییرات کاربردها و امکانات مهاجمان می‌باشد.

در مورد سیستم‌های IDS که بر اساس رفتار ترافیک عبوری تصمیم‌گیری می‌نمایند، به روز شدن و پشتیبانی ضرورت کمتری دارد. آنها بر اساس تحلیل ترافیک به تصمیم‌گیری می‌پردازند.

گاهی سیستم آنقدر حساس تنظیم شده است که با کوچکترین تغییر و تحولی در شبکه هشدار می‌دهد و این موقع‌هاست که مدیر شبکه شاکی از این ابزار محافظتی ترجیح می‌دهد خود با ترفندهای دستی همانند بستن پورت ICMP، کنترل دسترسی به ترافیک و برخی محدودیت های دیگر، خود به trace شبکه برای مقابله با حملات بپردازد.

نرم‌افزارهایی open source در شبکه با هسته Linux, Unix تعریف می‌شوند که ادعا می‌نمایند به scan پورتها می‌پردازند و به ما در کنترل شبکه کمک می‌نمایند. این نرم‌افزارها گاهی از طریق Back door های تعریف شده به شنود ترافیک مشغولند.

نرم‌افزاری مانند snort که در عمل به همراه یک موتور IDS میتواند یک سیستم تشخیص نفوذ را ایجاد کند توسط مهاجم برای استراق سمع بسته های مربوط به دیگران استفاده می شود.

سیستم‌های محافظتی دیگری بجز IDS همانند دیوار آتش و ... نیز وجود دارند.