با توجه به افزایش کمیت و کیفیت نفوذگری‌ها در عصر اینترنت و پیدایش روش‌های جدید و پیچیده نفوذگری، نیاز به استفاده از IDSها رفته رفته غیرقابل اجتناب می‌گردد

سیستم‌های کشف و ردیابی نفوذگری (IDS)

علی دریس‌زاده

IDSها (سرنام Intrusion Detection System) یا سیستم‌های کشف و ردیابی نفوذگری، امروزه به یکی از مهم‌ترین اجزای ساختار امنیتی شبکه‌ها تبدیل شده‌اند. شاید اسم‌شان را شنیده باشید یا چیزهایی درباره آن‌ها بدانید. شاید هم تنها از روی اسم‌شان دربارهٔ عملکردشان حدس‌هایی می‌زنید. در این صورت ممکن است با خود بگویید: شبکهٔ شرکت یا سازمان ما از یک یا چند دیواره آتش (Firewall) خوب بهره می‌برد، در این صورت چه نیازی ممکن است به تهیه و نصب چنین سیستمی داشته باشیم؟ در یک کلام، IDSها دقیقاً کاری را انجام می‌دهند که نام‌شان بازگو می‌کند: آن‌ها یک سری نفوذگری‌ها و اخلال‌گری‌های محتمل را کشف می‌کنند. اگر بخواهیم روشن‌تر بگوییم، باید گفت که این سیستم‌ها سعی می‌کنند حملات و یا سوءاستفاده‌های انجام شده از کامپیوترها را شناسایی و با اعلام خطر و ارسال هشدار، آن‌ها را به فرد یا افراد مسؤول اطلاع دهند. اما واقعاً این سیستم‌ها چه تفاوتی با دیواره‌های آتش دارند؟ اگر چه IDSها را می‌توان در کنار دیواره‌های آتش توأمان مورد استفاده قرار داد، اما این دو ابزار امنیتی را نباید با یکدیگر یکسان فرض نمود. با مراجعه به مقاله فایروال در شمارهٔ ۱۸ ماهنامه، حتماً به خاطر می‌آورید که دیواره آتش را می‌توان یک نگهبان یا مأمور امنیتی جلوی در ورودی یک خانه یا ساختمان فرض کرد. اگر به این مأمور گفته باشید که از ورود بعضی افراد خاص به ساختمان جلوگیری کند، او این کار را برای‌تان انجام خواهد داد. همچنین می‌تواند کیف دستی مراجعین را بررسی کند تا چنان‌چه محتوایی برخلاف قوانین تعریف شده داشته باشد، از ورود شخص ممانعت کند. اما یک به ظاهر مأمور اداره پست که درون کیفش یک اسلحه حمل می‌کند، چطور؟ نگهبان شما ممکن است اصلاً درون چنین کیفی را بررسی نکند. اصلاً شاید یک مهاجم از روی نرده و حفاظ دور خانهٔ شما عبور کند یا یک تونل به زیر آن بزند! گرچه انواع مختلف دیواره‌های آتش درجات هوشمندی متفاوتی دارند، اما در نحوهٔ انجام عملیات امنیتی خود، چندان انعطاف‌پذیر نیستند. همچنین، گرچه آن‌ها با ارائه دسته‌ای از گزارش‌ها و ثبت تلاش‌های نفوذگری در فایل‌های ثبت، شما را از این تلاش‌ها آگاه می‌سازند، اما این گزارشات معمولاً چندان واضح و روشنگر نیستند. صرفاً ثبت مجموعه‌ای از وقایع هستند. داستان IDSها از این‌جا شروع می‌شود ... .

در این شماره:

- سیستم‌های کشف و ردیابی نفوذگری
- درآمدی بر نفوذگری بی‌خطر

از این پس به طور مشخص و اختصاصی، تحت عنوان «امنیت» مباحث مرتبط با امنیت ارتباطات در شبکه‌ها، حفظ حریم خصوصی کاربران و مقابله با نفوذگری را دنبال خواهیم کرد. ناگفته نماند که دومین مقاله سرآغاز بحثی است که با عنوان «کبریت بی‌خطر» در چند شماره آتی مجله پی‌گرفته می‌شود.

IDSها، لزوم و کلیّات

امیدوارم آن چه تاکنون گفته شد باعث اجحاف در حق دیواره‌های آتش نشده باشد! این درست که IDSها در کشف و تشخیص حملات و نفوذگری‌ها از دیواره‌های آتش به مراتب انعطاف‌پذیرتر هستند، اما واقعیت این است که مقایسه این دو با یکدیگر چندان هم منطقی نیست. تعریف واژهٔ Security یا امنیت را در مورد کامپیوترها و شبکه‌ها، از اولین مقالهٔ مفاهیم بنیادی امنیت شبکه در شمارهٔ ۱۴ به خاطر می‌آورید؟

"Computer Security عبارت است از فرآیند شناسایی و جلوگیری از هرگونه دسترسی و استفادهٔ غیرمجاز از یک کامپیوتر." تعریفی که بر دو مفهوم اساسیِ جلوگیری و ممانعت (Prevention) و کشف و شناسایی (Detection) بنا شده است. اگرچه هم دیواره‌های آتش هم IDSها، در هر دو جنبهٔ یاد شده از مفهوم امنیت انجام وظیفه می‌کنند و به این ترتیب گاهی وقت‌ها حوزهٔ کاری مشترکی پیدا می‌کنند، اما باید توجه داشت که وظیفهٔ اصلی یک دیوارهٔ آتش ممانعت و وظیفهٔ اصلی و کارایی یک IDS در شناسایی می‌باشد. آن‌ها را مکمل‌های منطقی دیواره‌های آتش می‌نامند. در عین حال با توجه به افزایش کمیت و کیفیت نفوذگری‌ها در عصر اینترنت و پیدایش روش‌های جدید و پیچیده نفوذگری، نیاز به استفاده از IDSها رفته رفته غیرقابل اجتناب

می‌گردد، چرا که آن‌ها می‌توانند انواع متنوع و پیچیده‌تری از نفوذها و اخلال‌گری‌ها را شناسایی کنند، در صورت امکان، خودشان از این اقدامات جلوگیری کنند و در غیر این‌صورت با اعلام یک هشدار به موقع، این وظیفه را به ما واگذار کنند.

هر چه‌قدر سایت و شبکه مهم‌تری داشته باشید، استفاده از یک IDS ضروری‌تر خواهد بود. ممکن است در این برهه از زمان و در حالی که در کشور ما در بسیاری از شرکت‌ها و سازمان‌های بزرگ هنوز حتی از دیواره‌های آتش نرم‌افزاری هم استفاده نمی‌شود، صحبت کردن از IDS غیرضروری بنماید، اما دلایل ذکر شده در بالا ضرورت آشنایی با آن‌ها و به کارگیری تدریجی‌شان را ضروری می‌سازد.

شاید برای‌تان جالب باشد که بدانید در ایالات متحده تقریباً تمامی شرکت‌های بزرگ و اکثر سازمان‌های متوسط از یکی از انواع IDS استفاده می‌کنند. این در حالی است که IDSها معمولاً گران‌تر از دیواره‌های آتش هستند. برخی از آن‌ها چند هزار دلار قیمت دارند، اگرچه انواع چند صد دلاری و حتی ارزان‌تر آن‌ها هم موجودند. حملات انجام شده از نوع DoS (ممانعت از سرویس‌دهی) به Amazon.com و eBay در فوریهٔ ۲۰۰۰، نیاز به وجود روش‌های مؤثر در کشف و تشخیص نفوذگری و اخلال را به خصوص برای فروشندگانِ روی خط و دست اندرکاران تجارت الکترونیک بیش از پیش آشکار نمود. همچنین، تجربه نشان داده است که در میان وقایع مختلفی که امنیت یک شبکه کامپیوتری را به خطر می‌اندازند، حملات و نفوذهای داخلی بخش عمده را تشکیل می‌دهند (براساس بعضی آمارها گاه تا ۸۵ درصد) و سایر موارد، تلاش‌هایی برای ممانعت از سرویس‌دهی و نفوذ به شبکه، از محیط خارج را شامل می‌شوند. سیستم‌های کشف و تشخیص نفوذگری یا IDSها تا این لحظه بهترین و مؤثرترین انتخاب برای شناسایی و پاسخگویی به حملات درونی و بیرونی محتمل به شبکه یک سازمان محسوب می‌شوند. پیش از پرداختن به دلایل این ادعا می‌خواهم یک حرف تکراری بزنم! و آن این‌که: هیچ ابزار امنیتی و از جمله IDSها هرگز امنیت کامل شبکه شما را تضمین نخواهند کرد، اما هنگامی که در کنار اعمالی چون تعیین خط مشی‌های امنیتی (Security policy)، ارزیابی نقاط ضعف سیستم‌ها (Vulnerability assessment)، رمز کردن داده‌ها (data encryption)، اعتبارسنجی و مجوزدهی (authorization و authentication) و

به طور کلی IDSها سه عملکرد امنیتی اصلی دارند: نظارت و بررسی، کشف و ردیابی و عکس‌العمل و واکنش

استفاده از دیواره‌های آتش، از IDS هم استفاده کنید، به میزان قابل توجهی امنیت شبکه خود را ارتقاء داده‌اید.

این را هم به خاطر داشته باشید که هر چقدر با ابزار مدرن‌تر و مؤثرتری سر و کار داشته باشید، نحوه بکارگیری و استفاده مناسب از آن نیز دشوارتر می‌شود. بنابراین بهره‌وری خوب از یک IDS نیاز به دانش و مدیریت مناسب دارد. به طور کلّی IDSها سه عملکرد امنیتی اصلی دارند:

نظارت و بررسی یا monitoring، کشف و ردیابی یا detection و عکس‌العمل و واکنش یا respond. IDSها از خط مشی‌هایی (Policy) برای تعریف مجموعه‌ای از وضعیت‌ها و رویدادها (events) استفاده می‌کنند. هرگاه چنین رویدادهایی تشخیص داده و آشکار شوند، IDS اعلام خطر می‌کند یا به عبارتی یک پیغام هشدار (alert) ارسال می‌کند. به عبارت دیگر چنان‌چه یک رویداد خاص، عامل یک واقعهٔ امنیتی تشخیص داده شود، به هنگام اتفاق افتادنِ آن رویداد، پیام هشدار ایجاد و ارسال می‌شود. IDSها این هشدارها را به اشکال مختلفی مانند فراخوانی (page)، ارسال نامه الکترونیکی، ارسال یک SNMP Trap و... به administrator یا مسؤول IDS می‌فرستند و فرد مسؤول به این ترتیب متوجه می‌شود که ممکن است اقدامی در جهت اخلال در شبکه صورت گرفته باشد (Protocol = SNMP Simple Network Management یک پروتکل ارتباطی است برای جمع‌آوری اطلاعات از ادوات مختلف در شبکه TCP/IP).

بعضی IDSها نه تنها قادر به شناسایی یک رویداد خاص و ارسال هشدار هستند، بلکه می‌توانند به طور خودکار به رویداد مذکور پاسخ داده و عکس‌العمل نشان دهند. نمونه‌های چنین عکس‌العملی می‌تواند قطع کردن ارتباط یک کاربر، غیرفعال کردن یک شناسه و حساب کاربری و یا اجرای دسته‌ای از اسکریپت‌ها باشد. به طور خلاصه می‌توان گفت که شناسایی تهاجم (Intrusion Detection) عبارت است از فرآیند نظارت و بررسی کامپیوترها و شبکه‌ها به منظور کشف نفوذها و فعالیت‌های غیرمجاز و همچنین دستکاری و تغییر در فایل‌ها. IDSها همچنین می‌توانند ترافیک‌های شبکه را نظارت و بررسی کنند و به این ترتیب دریابند که یک سیستم، هدف یک تهاجم شبکه‌ای، مثلاً یک حمله از نوع ممانعت از سرویس‌دهی یا Denial Of Service، قرار گرفته است.

انواع IDS

IDSها در دو نوعِ host-based و network-based موجودند، گرچه برخی انواع جدیدشان ترکیبی از هر دو قابلیت را دارا هستند. هر یک از این دو نوع، رهیافت خاص خود را برای نظارت و نیز حفاظت از داده‌ها دارند و هریک دارای مزایا و معایب خاص خود هستند. به طور خلاصه، IDSهای host-based داده‌های موجود روی هر کامپیوتر را به طور جداگانه مورد بررسی قرار می‌دهند، در حالی که IDSهای network-based داده‌های رد و بدل شده میان کامپیوترها را مورد بازرسی قرار می‌دهند.

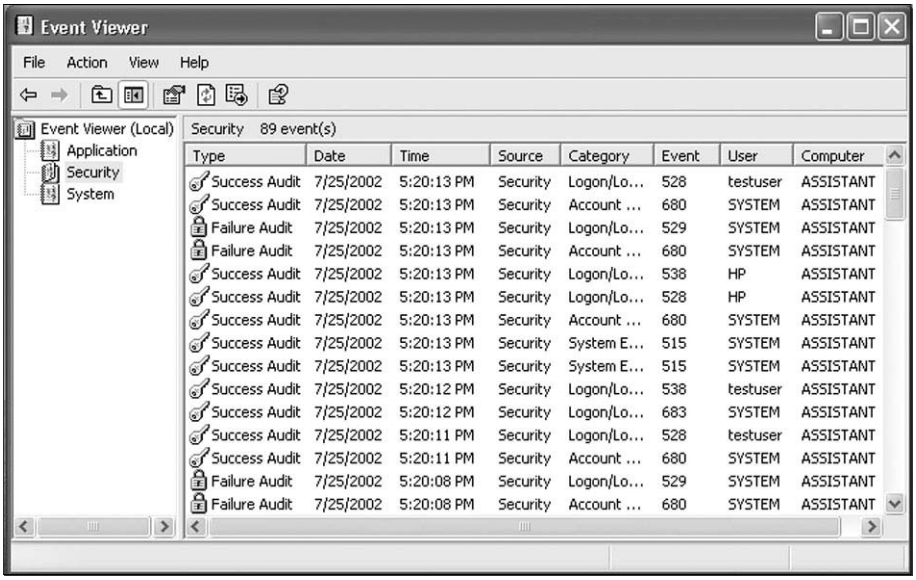
IDSهای مبتنی بر میزبان (کامپیوتر) (Host-Based IDS)

IDSهای مبتنی بر میزبان یا HIDSها معمولاً بسته‌های نرم‌افزاریی هستند که روی کامپیوتری که قرار است از آن محافظت کنند، قرار می‌گیرند. بسیاری از آن‌ها از system logها، audit logها و event logهای سیستم عامل‌ها و برنامه‌های کاربردی مختلف برای ارائه گزارش یا ارسال هشداری که مبتنی بر عملکرد پردازش‌های سیستم/کاربر هستند، استفاده می‌کنند. HIDSها

اعمال مختلفی برای کشف یک حمله به یک میزبان انجام می‌دهند. یکی از معمول‌ترین کارهایی که این نوع IDS برای شما انجام می‌دهد، بررسی و حصول اطمینان از درستی و سالم بودن فایل‌های سیستم می‌باشد (file integrity). HIDSها در امور مربوط به امنیت فایل‌ها عملکرد خوبی دارند. مواردی همچون تشخیص این که آیا فایل‌های مهم و حساس یک سیستم مورد تغییر یا دستکاری قرار گرفته‌اند یا خیر و یا ردیابی دستیابی غیرمجاز یک کاربر به فایل یا فایل‌هایی که خارج از حیطهٔ مجاز و سطح دسترسی داده شده به کاربر می‌باشند. یک IDS مبتنی بر میزبان برای نیل به این مقصود، یک بار فایل‌های سیستم مورد نظر را مورد بررسی قرار می‌دهد و یک به اصطلاح Signature یا نشانهٔ به رمز درآمده برای هریک از این فایل‌ها در وضعیت کنونی‌شان برای خود ایجاد می‌کند (Cryptographic Signature). پس از آن، IDS هر چند وقت یک بار فایل‌ها را با این نشانه‌ها مقایسه و بررسی می‌کند و چنان‌چه به تغییر و تفاوتی برخورد کند، شما را مطلع می‌سازد. البته این نشانه‌ها باید با هر بار انجام تغییرات در فایل‌ها و افزودن برنامه‌ها و Patchها توسط خود شما، به‌روز شوند. همچنین باید مطمئن باشید زمانی که این نشانه‌ها نصب یا به‌روز می‌شوند، سیستم در معرض خطر و نفوذ احتمالی نباشد، چرا که اگر برخی از فایل‌ها پیشاپیش مورد دستکاری قرار گرفته باشند، بعدها تصور غلطی از سالم بودن‌شان خواهید داشت. بهترین زمان برای نصب یک IDS مبتنی بر میزبان، زمانی است که تازه کامپیوتر میزبان را پیکربندی و آماده کرده‌اید و پیش از اتصال آن به شبکه، IDS را روی سیستم تنظیم کرده‌اید. واضح است که پس از روی خط آمدن، نفوذگران ممکن است تغییراتی روی سیستم به وجود بیاورند که تخمین‌های شما و HIDS را دچار اشکال کند.

از مزایا و ویژگی‌های IDSهای host-based می‌توان موارد زیر را ذکر کرد:

- اطلاعات صریحی در مورد این که چه کسی در چه زمانی چه کاری را به چه مقصدی انجام داده است، ارائه می‌کنند! یعنی معمولاً مبداء، مقصد، زمان و نوع عمل انجام شده را مشخص می‌کنند. در چنین حالتی نیاز به محاسبه و مقایسه و ارزیابی برای فهمیدن مفهوم یک گزارش یا هشدار نخواهید داشت و می‌توانید به راحتی دربارهٔ فرد یا برنامه‌ای که مسبب انجام عملی است، تصمیم بگیرید.



Type	Date	Time	Source	Category	Event	User	Computer
Success Audit	7/25/2002	5:20:13 PM	Security	Logon/Lo...	528	testuser	ASSISTANT
Success Audit	7/25/2002	5:20:13 PM	Security	Account ...	680	SYSTEM	ASSISTANT
Failure Audit	7/25/2002	5:20:13 PM	Security	Logon/Lo...	529	SYSTEM	ASSISTANT
Failure Audit	7/25/2002	5:20:13 PM	Security	Account ...	680	SYSTEM	ASSISTANT
Success Audit	7/25/2002	5:20:13 PM	Security	Logon/Lo...	538	HP	ASSISTANT
Success Audit	7/25/2002	5:20:13 PM	Security	Logon/Lo...	528	HP	ASSISTANT
Success Audit	7/25/2002	5:20:13 PM	Security	Account ...	680	SYSTEM	ASSISTANT
Success Audit	7/25/2002	5:20:13 PM	Security	System E...	515	SYSTEM	ASSISTANT
Success Audit	7/25/2002	5:20:13 PM	Security	System E...	515	SYSTEM	ASSISTANT
Success Audit	7/25/2002	5:20:12 PM	Security	Logon/Lo...	538	testuser	ASSISTANT
Success Audit	7/25/2002	5:20:12 PM	Security	Logon/Lo...	683	SYSTEM	ASSISTANT
Success Audit	7/25/2002	5:20:11 PM	Security	Logon/Lo...	528	testuser	ASSISTANT
Success Audit	7/25/2002	5:20:11 PM	Security	Account ...	680	SYSTEM	ASSISTANT
Failure Audit	7/25/2002	5:20:08 PM	Security	Logon/Lo...	529	SYSTEM	ASSISTANT
Failure Audit	7/25/2002	5:20:08 PM	Security	Account ...	680	SYSTEM	ASSISTANT

شکل ۱: نمایی از Event viewer ویندوز اکس‌پی. می‌توانید آن را یک IDS ابتدایی به حساب آورید.

- HIDSها کمتر ممکن است به اشتباه اعلام خطر کنند، چرا که همان‌طور که گفته شد اطلاعات‌شان مستقیماً به افراد و برنامه‌های مشخص مربوط می‌شود.
- ترافیک شبکه‌ای کمتری نسبت به IDSهای مبتنی بر شبکه ایجاد می‌کنند.

در عین حال این نوع IDSها نقاط ضعفی هم دارند، از جمله این‌که قابلیت انتقال خوبی روی سیستم عامل‌های مختلف ندارند. معمولاً برای هر نوع سیستم عامل باید یک نرم‌افزار IDS مبتنی بر میزبان نوشت. همچنین از آن‌جایی که در یک شبکه بزرگ با تعداد زیادی میزبان یا گره (node) مواجه هستیم، جمع‌آوری انبوهی از اطلاعات جداگانه و خاص برای هر یک از کامپیوترها می‌تواند کاری سخت و ناکارآمد باشد و نهایتاً این‌که چنان‌چه یک مهاجم و نفوذگر به نحوی عمل جمع‌آوری اطلاعات روی یکی از کامپیوترها را غیرفعال سازد، برنامهٔ IDS موجود روی آن کامپیوتر عملاً به هیچ کاری نمی‌آید.

برخی منابع بسته‌های نرم‌افزاری HIDS عبارتند از:

- Intruder Alert از AXENT Technologies به آدرس www.axent.com
- Tripwire از Tripwire Security Systems به آدرس www.tripwiresecurity.com
- POLYCENTER Security Intrusion Detector از شرکت Digital به آدرس www.digital.com
- Kane Security Monitor (برای سرورهای NT و Novell) از شرکت Security Dynamics به آدرس www.securitydynamics.com
- Cybercop Monitor از Nerwork Associates به آدرس www.nai.com (ویژگی‌های network-based هم دارد)،
- Computer Misuse Detection System (CMDS) از شرکت ODS Networks به آدرس www.ods.com
- همچنین ابزارها و برنامه‌هایی چون Windows NT/2000 Security Event Logs و یا Syslog یونیکس و BSM سولاریس را می‌توان نوعی IDS مبتنی بر میزبان دانست.
- RealSecure، ITA، Squire و Entercept از دیگر محصولات تجاری معروف از این دسته هستند.

IDSهای مبتنی بر شبکه Network-Based IDS

بسته‌هایی که ارائه‌کنندهٔ این نوع IDS می‌باشند، معمولاً سیستم‌هایی اختصاصی هستند که تمامی یک بخش یا Segment از شبکه را از بیرون و گاهی از درون یک دیوارهٔ آتش مورد نظارت و بررسی قرار می‌دهند. این سیستم‌ها معمولاً از دو بخش ناظر (monitor یا Sniffer یا Sensor) و عامل (agent) تشکیل شده‌اند.

ناظر (monitor) یک دستگاه و یا یک بستهٔ نرم‌افزاری است که شبکه را به منظور یافتن بسته‌های اطلاعاتی مشکوک مورد بررسی و پویش قرار می‌دهد. عامل (agent) نرم‌افزاری است که معمولاً به طور جداگانه روی هریک از کامپیوترهای مورد نیاز قرار می‌گیرد و نقش ارسال اطلاعات را به صورت بازخورد به ناظر برعهده دارد. همچنین ممکن است بخش دیگری به نام کنسول مدیریت (management console) هم

وجود داشته باشد که به شکلی مطمئن (با اعتبارسنجی و رمزنگاری) به ناظر متصل می‌شود و از آن گزارش دریافت می‌کند و نیز به تبادل اطلاعات مربوط به تنظیم و پیکربندی سیستم می‌پردازد. در بیشتر موارد، کار اصلی IDSهای مبتنی بر شبکه، جمع‌آوری بسته‌های اطلاعاتی ورودی به شبکه و بررسی آن‌ها بر پایهٔ دسته‌ای از عوامل است تا از این طریق بفهمند آیا این بسته‌ها مسبب یکی از انواع حملات شناخته شده و یا فعالیت‌های مشکوک می‌باشند یا خیر.

در حقیقت برخلاف IDSهای مبتنی بر میزبان و به جای بررسی اطلاعاتی که روی یک کامپیوتر قرار دارند و یا از آن سرچشمه می‌گیرند، این نوع IDSها با استفاده از تکنیک‌هایی مانند packet-sniffing یا کالبدشکافی بسته‌ها، داده‌ها را از درون بسته‌های اطلاعاتی TCP/IP (و یا سایر پروتکل‌ها) که در حال رفت و آمد در شبکه می‌باشند، استخراج می‌کنند. این مراقبت و نظارت بر ارتباطات میان کامپیوترها باعث می‌شود که NIDSها در کشف و تشخیص نفوذگری‌های انجام شده از محیط بیرونی شبکه مورد حفاظت، عنصر مؤثر و کارآمدی به حساب بیایند.

از مزایا و ویژگی‌های IDSهای مبتنی بر شبکه می‌توان به موارد زیر اشاره کرد:

- کارایی خوب در برابر حملات مبتنی بر DoS و ربودن پهنای باند. این نوع حملات خارجی با هدف سوءاستفاده و یا استفادهٔ بیش از حد (overload) از منابع شبکه صورت می‌گیرند. بسته‌هایی که حاوی یا ایجادکنندهٔ این نوع حملات هستند به خوبی توسط IDSهای network-based شناسایی می‌شوند.
- کارایی خوب در برابر دستیابی‌های غیرمجاز خارجی. هنگامی که یک کاربر غیرمجاز به یک کامپیوتر log in می‌کند یا در این راستا سعی می‌کند، این IDSهای مبتنی بر میزبان هستند که بهتر از هر عنصر امنیتی دیگری چنین رویدادی را تشخیص می‌دهند، اما تشخیص کاربران غیرمجاز پیش از اقدام به ورود به سیستم بهتر از هر ابزار دیگری از عهدهٔ IDSهای مبتنی بر شبکه بر می‌آید.
- به نوع سیستم عامل یا یک برنامه کاربردی خاص وابسته نیستند، چرا که در سطح بسته‌ها عمل می‌کنند. همچنین برای اجرا و گرفتن نتیجه از آن‌ها، نیازی به دانستن مجوزها و کلمات عبور سیستم عامل و همچنین برنامه‌های کاربردی ندارید.

این نوع IDSها نیز البته دارای نقاط ضعفی می‌باشند. مهم‌ترین نقطه ضعف این IDSها به هنگام کار در شبکه‌های سریع (۱۰۰Mbps و بالاتر) و نیز مواجهه با بسته‌های رمز شده می‌باشد. در مورد اول چنان‌چه NIDS برخی بسته‌ها و داده‌ها را به دلیل سرعت بالای انتقال‌شان از دست بدهد، آن‌گاه از جمع‌آوری و تجزیه تحلیل صحیح آن‌ها باز می‌ماند و در مورد دوم چنان‌چه ترافیک شبکه رمز شده باشد، IDS نشانه‌های یک حمله را نمی‌تواند تشخیص بدهد. NIDSها در شبکه‌های سوئیچ شده نیز دچار مشکل می‌شوند.

برخی منابع بسته‌های نرم‌افزاری NIDS عبارتند از:

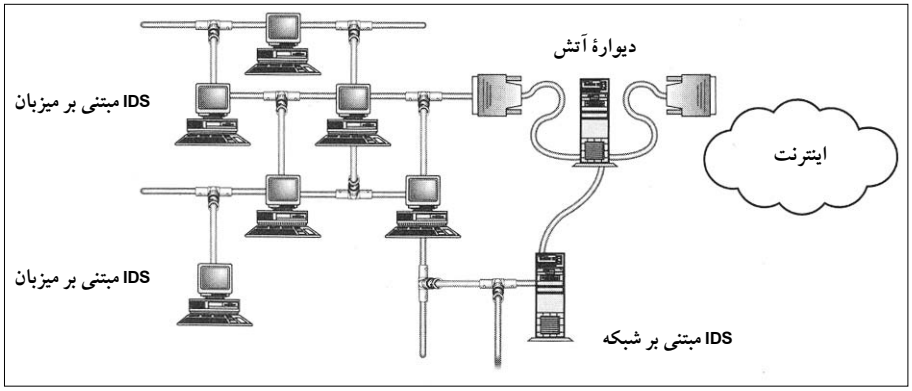
- NetRanger از Cisco Systems به آدرس www.cisco.com
- ISS RealSecure به آدرس www.iss.net
- Cybercop Monitor از Network Associates به آدرس www.nai.com (ویژگی‌های host-based هم دارد)
- SessionWall-3 از Computer Associates به آدرس www.abirnet.com
- Anzen Flight Jacket به آدرس www.anzen.com
- Shadow، Snort!، Dragon، NFR و Netprowler

چند نام تجاری و معروف دیگر از این دسته هستند.

چگونگی قرار گرفتن IDS در شبکه

شکل ۲ یکی از روش‌های متداول قرارگیری و نصب IDS در شبکه را نشان می‌دهد.

هر IDS مبتنی بر میزبان بر روی یک کامپیوتر سرویس‌دهنده در شبکه نصب و اجرا می‌شود. IDS مبتنی بر شبکه، درون شبکه و بلافاصله پشت دیواره آتش قرار دارد. البته باید توجه داشت که این راه‌حل تنها روشِ ممکن نیست. مثلاً می‌توان یک IDS مبتنی بر شبکه را به گونه‌ای نصب کرد که بخش ناظر یا sensor آن به ناحیهٔ DMZ (شبکهٔ متصل به هر دو شبکه داخلی و خارجی، رجوع کنید به ماهنامه شبکه شماره ۱۸) و دیگر بخش‌های آن به شبکه داخلی متصل باشد.



شکل ۲: نحوهٔ قرارگیری IDS در ساختار یک شبکه نمونه

خیلی وقت‌ها یک IDS مبتنی بر شبکه را درون DMZ قرار می‌دهیم. در این حالت فرض کرده‌ایم که یک دیوارهٔ آتش داریم و یک DMZ نیز ایجاد کرده‌ایم. اگر IDS را پشت دیواره آتش قرار دهیم، آن گاه می‌تواند حملات پروتکل‌ها و منابعی که از دیواره آتش عبور می‌کنند و همچنین حملات کاربران داخلی شبکه را شناسایی و آشکار کند. به شکل ۳ توجه کنید.

اکنون IDS مبتنی بر شبکه می‌تواند برای آشکارسازی یا واکنش به یک حمله یا دسترسی غیرمجاز یکی از کارهای زیر را انجام دهد:

- یک نامه الکترونیک، فراخوان یا SNMP trap ارسال کند.
- یک ارتباط مبتنی بر TCP را بلوکه کند یا به کلی از بین ببرد.
- یک اسکریپت تعریف شده توسط کاربر یا برنامه خاصی را اجرا کند (مثلاً برخی سرویس‌های شبکه‌ای را به ترتیب اولویت shutdown کند).

تکنیک‌های IDS

هر یک از دو نوع IDSها (host-based و network-based) از ۴ تکنیک اصلی برای کشف و ردیابی نفوذگران استفاده می‌کنند: anomaly detection یا نمونه‌های غیرمتعارف، signature (misuse) detection یا کشف از روی نشانه یا سوءاستفاده، target monitoring یا نظارت بر هدف و سرانجام stealth probes یا کاوش‌های نهانی.

۱ـ تشخیص نمونه‌های غیرمتعارف (Anomaly Detection)

IDS یک مرز نرمال از الگوهای متعارف استفاده از سیستم برای خود ترسیم و تعریف می‌کند. هر رفتار یا رویدادی که به میزان زیادی

پرسش و پاسخ‌های اتصال به اینترنت

چرا Outlook Express خود به خود قطع نمی‌کند؟

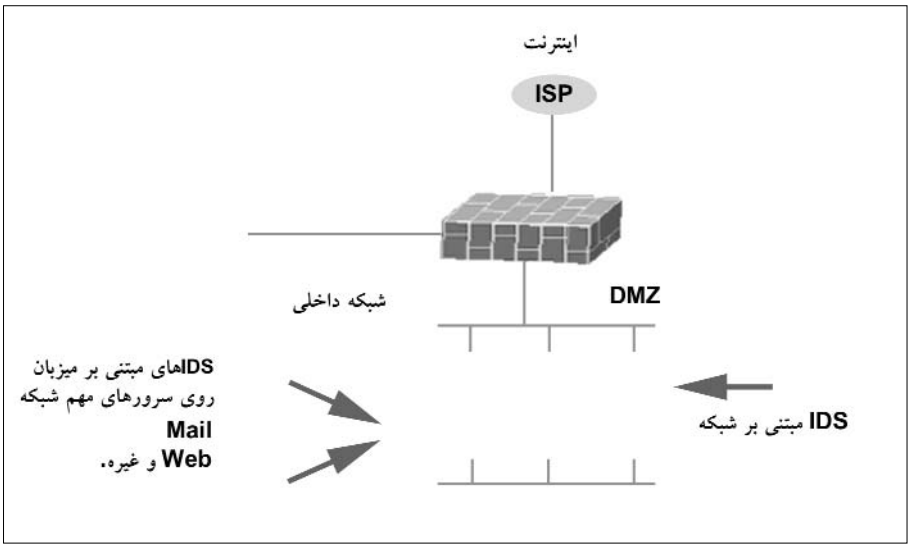
س **من سابقاً از Outlook Express استفاده می‌کردم که گزینه Hang up automatically after sending and receiving آن را انتخاب کرده بودم و همه چیز درست کار می‌کرد. اما اخیراً که آن را به OE 5.5 ارتقاء داده‌ام و همان گزینه را علامت زده‌ام، دیگر بعد از ارسال و دریافت خود به خود ارتباط را قطع نمی‌کند. موضوع چیست؟**

ج این اتفاق شاید به خاطر این باشد که گزینه مذکور دیگر در OE تنظیم نشده باشد. از منوی Tools گزینه Options را انتخاب کرده و به صفحه Connection بروید. نگاه کنید ببینید گزینهٔ ...Hang up علامت خورده باشد و سپس OK کنید. حال، از منوی Tools، گزینه Accounts و سپس Properties را کلیک کرده و به صفحه Connection بروید. گزینهٔ Always connect to this account using را علامت زده و سپس از فهرست کشویی اتصال خود را انتخاب کنید. در پایان، روی Apply و سپس OK کلیک کنید.

چگونه می‌توانم رمز عبورم را باطل کنم؟

س **من با این امید برای شما نامه می‌نویسم که بتوانید مشکل کوچکم را حل کنید. اخیراً به Control Panel رفتم، روی Passwords کلیک کردم و رمز عبوری را برای اینترنت تنظیم نمودم. این کار خیلی آسان بود، ولی حالا که می‌خواهم آن را باطل کنم، هیچ راهی را نمی‌توانم پیدا کنم و نزدیک است فریاد بکشم. من از Windows 98 SE استفاده می‌کنم.**

ج نگران نباشید، حل مشکل شما خیلی راحت است. به پنجره Control Panel بروید و دوباره Passwords را وارد کنید. روی Change Windows Password کلیک و رمز عبور قبلی خود را تایپ کنید. قسمت New Password را خالی بگذارید و در جلوی Confirm New Password هم چیزی ننویسید. حال روی OK و دوباره OK کلیک کنید. حالا دیگر ویندوز از شما رمز عبور نمی‌خواهد.



شکل ۳: توپولوژی یک شبکه با حضور دیوارهٔ آتش، IDSها و ناحیه DMZ

از این الگوها دور باشد، به عنوان یک اخلال‌گری محتمل در نظر گرفته می‌شود. آن چه خلاف قاعده و غیرمتعارف فرض می‌شود، می‌تواند متغیر باشد، اما معمولاً رویدادی که با تناوبی بیشتر یا کمتر از دو مرتبه انحراف از آمار نرمال به وقوع بپیوندد، غیرمتعارف فرض می‌شود. چند مثال برای این شرایط عبارتند از: کاربری که به جای ۱ یا ۲ بار ورود و خروج نرمال از سیستم در طول یک روز، ۲۰ بار این کار را انجام داده است یا کامپیوتری که در ساعت ۲ بعد از نیمه شب مورد استفاده قرار گرفته در حالی که قرار نبوده پس از ساعت اداری روشن باشد. در یک سطح دیگر، این تکنیک می‌تواند الگوهایی در مورد کاربران، از جمله برنامه هایی که به اجرا در می‌آورند را مورد بررسی قرار دهد. مثلاً اگر کاربری از بخش گرافیک یک سازمان ناگهان شروع به دست‌یابی به برنامه‌های حسابداری یا کامپایل کردن کد بنماید، سیستم می‌تواند یک هشدار به راهبر (administrator) خود ارسال کند.

۲ـ کشف از روی نشانه یا سوءاستفاده (Signature یا Misuse Detection)

این روش از دسته‌ای الگوهای شناخته شده از رفتارهای غیرمجاز به منظور پیش‌بینی و کشف تلاش‌های مشابه بعدی استفاده می‌نماید. این الگوهای خاص Signature نامیده می‌شوند. برای IDSهای مبتنی بر میزبان سه بار تلاش ناموفق برای login کردن می‌تواند یک Signature باشد. برای IDSهای مبتنی بر شبکه، Signature می‌تواند یک الگوی خاص باشد که با بخشی از یک بسته همخوانی داشته باشد. به عنوان مثال نشانه‌های مربوط به سربرگ یک بسته اطلاعاتی می‌تواند نشانه یک عمل غیرمجاز، مثلاً اجرای یک FTP غیرعادی باشد. بسته به میزان اهمیت و جدی بودن نشانه یا signature، ممکن است یک عکس‌العمل یا response به عملِ انجام شده و یا یک تذکر یا هشدار به افراد مسؤول ارسال شود.

۳ـ نظارت بر هدف (Target Monitoring)

در این روش به جای جستجو برای یافتن یک مورد غیرمتعارف یا یک نشانه، تغییر و دستکاری احتمالی بعضی فایل‌ها مورد بررسی قرار می‌گیرد. این تکنیک، بیشتر یک شیوه کنترلی تصحیح کننده است. یعنی برای آشکارسازی یک عمل غیرمجاز پس از به وقوع پیوستن آن و به منظور انجام عمل معکوس، طراحی شده است. یکی از راه‌های کشف دستکاری شدن پنهانی فایل‌ها این است که کدهای رمز شده‌ای برای آن‌ها ایجاد شود (cryptographic hash) و در فواصل زمانی معینی با hashهای جدید هر فایل مقایسه شود. پیاده‌سازی چنین سیستمی آسان است، زیرا به نظارت مستمر administrator مدیرشبکه نیاز ندارد. فواصل زمانی بررسی سالم بودن و جامعیت فایل‌ها و نیز این که آیا تمامی آن‌ها و یا صرفاً برخی فایل‌های مهم سیستمی مورد بررسی قرار بگیرند به راحتی قابل تنظیم و کنترل می‌باشد.

۴ـ کاوش‌های نهانی (Stealth probes)

این تکنیک برای ردیابی نفوذگرانی که سعی می‌کنند عملیات‌شان را در دوره‌های زمانیِ طولانی به انجام برسانند، به کار می‌رود. مثلاً یک

نفوذگر در یک دورهٔ زمانی دو ماهه به بررسی ضعف‌های امنیتی و درگاه‌های باز یک سیستم می‌پردازد. سپس دو ماه دیگر صبر می‌کند تا حمله‌اش را واقعاً شروع کند. تکنیک کاوش‌های نهانی مجموعه متنوع و زیادی از داده‌ها را از سیستم جمع‌آوری می‌کند و بر پایهٔ آن به دنبال آثار یک حملهٔ ساخت یافته و اسلوب‌مند در یک بازهٔ زمانی طولانی می‌گردد. در این روش نمونه‌گیری‌های زیادی از سیستم، جهت کشف حملات مرتبط با این شواهد و نمونه‌ها صورت می‌پذیرد. این روش از دو تکنیک رفتار غیرمتعارف و سوءاستفاده برای آشکارسازی رفتارهای مشکوک استفاده می‌کند.

چند نکتهٔ پایانی

بی‌شک وجود و حضور سیستم‌های کشف و تشخیص نفوذگری، یک سطح امنیتی و محافظتی به شبکه شما می‌افزاید. بخصوص اگر دلایلی دارید مبنی بر این که بیش از پیش هدف تهاجم اخلال‌گران قرار می‌گیرید (مثلاً اگر نمونه‌های port scan بی‌شماری در فایل ثبت دیوارهٔ آتش خود مشاهده می‌کنید و یا این‌که مورد یک تهاجم یا نفوذ واقعی قرار گرفته‌اید)، استفاده از IDS ضروری می‌نماید. در عین حال فراموش نکنید که این ابزارهای امنیتی مانند هر وسیلهٔ دیگری می‌توانند معایبی نیز به دنبال داشته باشند. علاوه بر نقاط ضعفی که پیشتر در مورد دو نوع مختلف IDSها بیان شد، به طور کلی همهٔ آن‌ها می‌توانند دارای دو عیب کلی زیر باشند:

ـ False Positives یا اعلام خطرهای اشتباه

اگرچه ممکن است ترجیح بدهید که IDS شما بیشتر حساس باشد تا این که اصلاً بعضی موارد نفوذگری را تشخیص ندهد، اما یک False Positive گاه ممکن است برای‌تان بسیار گران تمام شود. مثلاً اگر IDS را تنظیم کرده‌اید که هرگونه ارتباط یا Connection مشکوک را قطع کند، چنین اشتباهی (اعلام خطر اشتباهی) می‌تواند منجر به قطع ارتباط یک کاربر مشروع از سیستم شما گردد. اگر عامل زمان برای سرویسی که ارائه می‌کنید، مهم باشد (مثلاً یک سایت ویژه تجارت الکترونیک)، این اشتباه، مصیبت‌بار خواهد بود.

ـ کاهش کارایی سیستم

با پیدایش سیستم‌های جدیدتر و سریع‌تر، این عامل البته از اهمیت کمتری برخوردار است، اما به هرحال باید توجه داشت که آنالیز کردن

اگر IDS را تنظیم کرده‌اید که هرگونه ارتباط یا Connection مشکوک را قطع کند، چنین اشتباهی می‌تواند منجر به قطع ارتباط یک کاربر مشروع از سیستم شما گردد.

بسته‌های شبکه و audit logهای سیستم، یک عمل زمان‌بَر و به طور بالقوه مصرف‌کنندهٔ توان پردازنده می‌باشد. به خصوص اگر شبکه شلوغ یا سرویس‌دهنده‌ای که داده‌های فراوانی برای آنالیز تولید می‌کند داشته باشید، ممکن است متوجه شوید که سرویس‌های شبکه‌ای یا سرویس‌های موجود روی میزبان‌ها به شکل غیر قابل قبولی کند شده‌اند. بهتر است در صورت امکان پیش از تهیه IDS اطلاع یابید که چه میزان فعالیت برای IDS مورد نظر، زیاد محسوب می‌شود و یا این که ابتدا یک نسخه نمونه و آزمایشی از محصول را روی شبکه خود امتحان کنید.

ـ چنان‌چه سیستم‌ها و شبکه شما به درستی پیکربندی و تنظیم شده باشند، IDS با سایر اجزا و ادوات امنیتی شبکه از جمله دیوارهٔ آتش تداخل وظیفه پیدا نخواهد کرد. در عین حال یک دیوارهٔ آتش نباید به گونه‌ای تنظیم شده باشد که از عملکرد عادی IDS جلوگیری نماید، چرا که IDS یک ابزار کشف و ردیابی است که انتظار می‌رود کلیهٔ نفوذگری‌ها و اقدامات انجام شده در شبکه از جمله آن هایی را که از سایر محصولات امنیتی موجود در شبکه سرچشمه می‌گیرند، جمع‌آوری، بررسی و در صورت لزوم آشکار نماید.

منابع:

Peter Norton and Mike Stockman,

"Network Secyrity Guides"

www.securityfocus.com

Mission Critical Internet Security

Syngress Publishing

www.itsecurity.com

توضیح نویسنده: این مقاله را به آقای محمد رضا اسدی، که نسبت به مجلهٔ شبکه و این جانب در راستای ارائه مقالات بخش امنیت در شبکه ابراز لطف و محبت بسیار داشته اند، تقدیم می‌کنم.