بررسی صحت عملکرد سیستم‌های تشخیص‌نفوذ توسط عامل‌های متحرک

امیرحسین پی‌براه
دانشکده کامپیوتر – دانشگاه صنعتی امیرکبیر
payberah@ce.aut.ac.ir

بابک صادقیان
دانشکده کامپیوتر – دانشگاه صنعتی امیرکبیر
basadegh@ce.aut.ac.ir

چکیده

یکی از مسائل مطرح در طراحی سیستم‌های تشخیص‌نفوذ تامین امنیت خود سیستم است. در این مقاله ایده بکارگیری جزئی به نام بازرس را در سیستم‌های تشخیص‌نفوذ بدین منظور مطرح می‌کنیم. سیستم بازرسی می‌تواند معماری‌های مختلفی داشته باشد که ما سه رویکرد معماری پیشنهاد می‌کنیم که عبارتند از بازرس محلی، بازرس متمرکز و بازرس متحرک. با در نظر گرفتن این سه نمونه بازرس، آزمایشاتی را در محیط شبکه محلی بر روی آنها انجام دادیم و از نظر زمان پاسخ، میزان افزایش بار شبکه و میزان افزایش بار سیستم با یکدیگر مقایسه کردیم. نتایج حاصل از آزمایشات نشان داد که عملکرد بازرس محلی در مقایسه با دو نمونه دیگر دارای زمان پاسخ و اضافه بار کمتر است، اما مشکلی که در این معماری وجود دارد، مشکل قابلیت گسترش سیستم بازرسی می‌باشد. این نتیجه نشان می‌دهد که استفاده از بازرس محلی در شبکه‌های محلی کوچک مناسب است، اما با افزایش وسعت شبکه محلی استفاده از بازرس محلی به علت مشکل بودن گسترش آن کارامد نمی‌باشد. علاوه بر این در سیستم‌های توزیع‌شده تشخیص‌نفوذ نیز بازرس محلی کارایی مناسبی را نشان نمی‌دهد. در این موارد معماری مناسب برای بازرسی استفاده از معماری بازرس متحرک است. در ادامه این مقاله نیز در مورد چگونگی حرکت و همچنین تعداد بازرس‌های متحرک آزمایشاتی انجام داده‌ایم.

کلمات کلیدی

بازرس، سیستم تشخیص‌نفوذ، بازرس محلی، بازرس متمرکز، بازرس متحرک

۱- مقدمه [1]

یکی از تجهیزاتی که در ایمن‌سازی شبکه نقش مهمی‌را بازی می‌کند سیستم‌های تشخیص‌نفوذ هستند. این سیستم‌ها همانطور که از نام آنها بر می‌آید وظیفه بررسی سیستم‌ها و شبکه‌های کامپیوتری را بر عهده دارند و هر گونه عملی را که سعی در ایجاد اختلال و نفوذ داشته باشد را گزارش می‌دهند. اگر هر یک از سیستم‌های امنیتی شبکه (که سیستم‌های تشخیص‌نفوذ از جمله آنها می‌باشد) به نوعی از عملکرد صحیح باز بماند، ایمنی مورد نظر دچار مشکل می‌شود. برای رفع این مشکل در این مقاله ایده

بکارگیری جزئی به نام بازرس مطرح شده است. این جزء که به عنوان بخش اضافی سیستم تشخیص‌نفوذ در نظر گرفته شده است وظیفه بررسی صحت وجودی و عملکردی سیستم تشخیص‌نفوذ را بر عهده دارد. وظیفه بازرس، بررسی سیستم‌های تشخص‌نفوذ به منظور یافتن مشکلی در عملکرد آنها، در ساختار فرایند سیستم و نهایتاً در پیکربندی سیستم‌های تشخیص‌نفوذ می‌باشد. برای انجام این کار یک سیستم تشخیص‌نفوذ را می‌توان از دو دیدگاه مورد بررسی قرار داد. یک دیدگاه، نگاه به سیستم تشخیص‌نفوذ به عنوان ابزاری است که باید انواع حملات را تشخیص دهد و دیدگاه دیگر نگاه به سیستم تشخیص‌نفوذ به عنوان یک فرایند است که باید صحت وجودی آن بررسی شود.

در این مقاله سعی کرده‌ایم تا مساله بازرس را مورد بررسی قرار دهیم و معماری‌های مختلف را مطرح کنیم و کارایی هر یک را با یکدیگر مقایسه کنیم. با توجه به این مطلب، ساختار مقاله در ادامه به ترتیب زیر است: در بخش دو تعاریف اولیه سیستم را ارائه می‌کنیم، در بخش سه انواع معماری‌های مختلف برای بازرس‌ها را شرح می‌دهیم و در بخش چهار این معماری‌ها را از لحاظ زمان پاسخ، میزان بار شبکه و میزان بار سیستم با یکدیگر مقایسه می‌کنیم. در بخش پنج، نگاه دقیق‌تری به بازرس متحرک می‌اندازیم و آن را از لحاظ تعداد بازرس‌ها و همچنین نحوهٔ حرکت مورد بررسی قرار می‌دهیم.

۲- تعاریف اولیه

در این بخش مفاهیم پایه‌ای که در این مقاله مورد استفاده قرار گرفته است، شرح داده می‌شود. مفاهیمی که تعریف آنها ضروری به نظر می‌رسد، مفهوم بازرس و عامل‌های متحرک می‌باشد که در این مقاله از آنها استفاده شده است.

۲-۱- مفهوم بازرسی [2]

بازرسی عبارت است از یک روش خودکار که فعالیت‌های رخ داده در یک سیستم را جمع‌آوری می‌کند و سپس آنها را مورد بررسی و آنالیز قرار می‌دهد. با توجه به این تعریف، فعالیت‌هایی که برای سیستم تشخیص‌نفوذ تعریف می‌کنیم که توسط بازرس مورد بررسی قرار بگیرد عبارتند از تشخیص یا عدم تشخیص نفوذ، تغییر در پیکربندی سیستم تشخیص‌نفوذ، میزان بار سیستم تشخیص‌نفوذ بر روی پردازنده، میزان بار مصرفی سیستم تشخیص‌نفوذ از حافظه، تغییر در شماره فرایند سیستم تشخیص‌نفوذ و یا در شماره فرایند پدر سیستم، تغییر مالکیت سیستم و نهایتاً تغییر در checksum فرایند سیستم. هر کدام از این موارد که به عنوان فعالیت مورد نظر تعریف شد، توسط بازرس مورد بررسی قرار می‌گیرد و در صورت تشخیص مشکلی در هر یک از موارد فوق، آن را خبر می‌دهد.

۲-۲- عامل‌های متحرک [3, 4]

اگر بخواهیم عامل را از دید یک کاربر ساده تعریف کنیم عبارت است از برنامه‌ای که از طرف کاربر موظف می‌شود تا کارهایی را برای او انجام دهد و بدین ترتیب کاربر را در پیشبرد اهدافش کمک می‌کند. اما اگر بخواهیم آن را به صورت دقیق‌تر تعریف کنیم، می‌توان آن را به ترتیب زیر ارائه کرد:

عامل شیءای است که:

- در یک محیط اجرایی فعالیت می‌کند.
- دارای خصوصیات اصلی زیر می‌باشد:

- واکنشی[1]، خودمختاری[2]، هدفمند[3]، اجرای مستمر
- ممکن است دارای خصوصیات اختیاری زیر باشد:
  - برقراری ارتباط[4]، جابجایی[5]، یادگیری[6]

از نظر قابلیت جابجایی، عامل‌ها را می‌توان به دو دسته تقسیم کرد: عامل غیرمتحرک و عامل متحرک. عامل غیرمتحرک تنها بر روی میزبانی که شروع به فعالیت کرده، باقی می‌ماند و ادامه فعالیت می‌دهد، در حالیکه عامل متحرک بر روی میزبانی که شروع به فعالیت کرده باقی نمی‌ماند و می‌تواند بین میزبان‌های متفاوت حرکت کند.

۳- معماری‌های بازرس [5, 6, 7, 8, 9]

در این بخش به معرفی رویکردهای معماری مورد استفاده برای پیاده‌سازی بازرس‌ها پرداخته می‌شود. قبل از آنکه به بیان رویکردها پرداخته شود، لازم است که در مورد معماری کلی سیستم بازرسی شرحی داده شود تا بدین ترتیب جایگاه بازرس در آن بهتر مشخص شود. سیستمی که در نظر گرفته‌ایم به این ترتیب است که شبکه‌ای داریم که میزبان‌های این شبکه هر یک دارای سیستم تشخیص‌نفوذی می‌باشند. در کنار هر سیستم تشخیص‌نفوذ، سنسوری به منظور جمع‌آوری بعضی از فعالیت‌های مورد نظر که در بخش ۲-۱ به آنها اشاره شد قرار دارد. بعد از جمع‌آوری اطلاعات توسط سنسورها، سیستم بازرس با توجه به معماری‌ای که دارد با آن اطلاعات برخورد می‌کند. حال با توجه به این مطلب به معرفی رویکردهای معماری که برای برخورد با این اطلاعات تعریف کردیم، می‌پردازیم:

- **ارسال اطلاعات هر سیستم به یک نقطه مرکزی برای بازرسی (بازرس متمرکز)**

در این روش اطلاعات جمع‌آوری شده توسط سنسورهای هر میزبان به صورت مداوم به یک نقطه پردازشگر مرکزی ارسال می‌شود. در این معماری بازرس در نقطه پردازشگر مرکزی قرار دارد و اطلاعات ارسالی از تمام میزبان‌ها را در آن نقطه مورد بررسی قرار می‌دهد.

- **وجود یک بازرس به صورت محلی بر روی هر سیستم (بازرس محلی)**

روش دیگری که برای بازرسی سیستم‌ها می‌تواند مطرح شود، قرار دادن یک بازرس بر روی هر میزبان به صورت دائم است. در این روش بازرس در کنار سنسور قرار دارد و اطلاعات جمع‌آوری شده توسط آنها را در همان محل مورد بررسی قرار می‌دهد. با استفاده از این روش مشکل ترافیک ارسالی بر روی شبکه و نقطه پردازشگر مرکزی که در روش قبل مطرح شده بود، حل می‌شود.

- **قرار دادن یک عامل متحرک به عنوان بازرس (بازرس متحرک)**

روش سومی‌که برای بازرسی سیستم‌ها می‌تواند مطرح شود استفاده از عامل‌های متحرک است. در این روش بازرس یا بازرس‌هایی در سطح شبکه حرکت می‌کنند و به روی هر میزبانی که برسند، اطلاعات جمع‌آوری شده توسط سنسور آن میزبان را مورد بررسی قرار می‌دهند.

---

[1] Reactive
[2] Autonomous
[3] Goal-driven
[4] Communicative
[5] Mobile
[6] Learning

۴- کارایی معماری‌های مختلف [10]

در این بخش چگونگی بررسی و مقایسه بین رویکردهای مختلف معماری سیستم بازرس شرح داده می‌شود. محیط انجام آزمایشاتی که فراهم کردیم یک شبکه محلی می‌باشد که بر روی هر میزبان شبکه یک سیستم تشخیص‌نفوذ قرار دارد و در کنار هر سیستم تشخیص‌نفوذ نیز سنسوری برای جمع‌آوری اطلاعات مورد نظر وجود دارد. برای بررسی کارایی معماری‌های مختلف بازرس، آنها را در شرایط مختلف مورد بررسی قرار دادیم و از لحاظ میزان مصرف حافظه، میزان مصرفCPU، بار شبکه و زمان پاسخ با یکدیگر مقایسه کردید. برای انجام این کار پریودهای زمانی مختلفی در نظر گرفتیم که عبارتند از ۵، ۱۰، ۳۰، ۶۰ و ۱۲۰ ثانیه که هر بازرس‌ها در فاصله‌های زمانی بیان شده ارسال می‌شوند.

در سیستم بازرس محلی با توجه به آنکه بازرس بر روی هر میزبان در کنار سیستم تشخیص‌نفوذ و سنسور مستقر است، اطلاعات بعد از جمع‌آوری توسط سنسور می‌تواند مورد بررسی قرار گیرد. در این سیستم بعد از انجام آزمایشات میزان مصرف حافظه و CPU، بار شبکه و زمان پاسخ مطابق جدول ۴-۱ بدست آمد:

جدول ۴-۱- نتایج آزمایش برای حالت بازرس محلی

بازرس حالت محلی					
پریود زمانی	**۵ ثانیه**	**۱۰ ثانیه**	**۳۰ ثانیه**	**۶۰ ثانیه**	**۱۲۰ ثانیه**
میزان مصرف حافظه	2.3 %	2.3 %	2.3 %	2.3 %	2.3 %
میزان مصرف CPU	~ 0 %	~ 0 %	~ 0 %	~ 0 %	~ 0 %
بار شبکه	258 bps	170 bps	49 bps	45 bps	40 bps
زمان پاسخ	5009 ms	10010 ms	30012 ms	60017 ms	120031 ms

همانطور که در جدول ۴-۱ مشاهده می‌شود، با توجه به ساده بودن فرایند بازرس، میزان استفاده از پردازنده در بازرس محلی آنقدر کم است که در حدود صفر می‌باشد. علاوه بر این نتایج آزمایشات بر روی ارسال بار بر روی شبکه نشان می‌دهد که میزان این بار (که ارسال نتایج کار بازرس به مدیر شبکه است) بسیار کم و ناچیز است.

در قدم بعد آزمایشی که انجام شد بررسی بر روی عملکرد بازرس مرکزی است. در این معماری، بازرس بر روی یک میزبان مرکزی مستقر است و سنسورها بعد از جمع‌آوری اطلاعات از سیستم تشخیص‌نفوذ خود، اطلاعات را به آن بازرس مرکزی می‌فرستند. در جدول ۴-۲ نتایج کار برای حالت متمرکز آورده شده است:

جدول ۴-۲- نتایج آزمایش برای حالت بازرس متمرکز

بازرس حالت Client/Server					
پریود زمانی	**۵ ثانیه**	**۱۰ ثانیه**	**۳۰ ثانیه**	**۶۰ ثانیه**	**۱۲۰ ثانیه**
میزان مصرف حافظه	2.3 %	2.3 %	2.3 %	2.3 %	2.3 %
میزان مصرف CPU	0.4 %	0.3 %	0.1 %	~ 0 %	~ 0 %
بار شبکه	13.5 kbps	7 kbps	2.4 kbps	1.3 kbps	0.7 kbps
زمان پاسخ	5202 ms	10164 ms	30184 ms	60168 ms	120222 ms

همانطور که در جدول ۴-۲ نشان داده شده است، میزان مصرف پردازنده برای پریودهای کمتر، بالاتر از مواقعی است که پریود زمانی زیاد می‌شود. این مساله به این دلیل است که در پریودهای زمانی کوتاه بازرس کار خود را با فاصله‌های زمانی کمتری انجام

می‌دهد و نتیجه این کار بالا رفتن مصرف پردازنده است. همچنین میزان مصرف پردازنده در مقایسه با حالت بازرس محلی بیشتر است. علت امر این است که در این حالت باید سنسور اطلاعات جمع‌آوری شده را به صورت یک ارتباط برای بازرس متمرکز بفرستد، که این عمل میزان پردازش بیشتری در مقایسه با عمل بازرس محلی دارد. یکی از پارامترهایی که در جداول نشان داده شده است، زمان پاسخ می‌باشد. منظور از زمان پاسخ، مدت زمانی است که بازرس کار خود را آغاز می‌کند تا زمانی که خروجی لازم را تولید می‌کند. همانطور که در جدول ۴-۲ نشان داده شده است، زمان پاسخ بازرس متمرکز در مقایسه با زمان پاسخ بازرس محلی بیشتر است. علت این مساله این است که در بازرس متمرکز زمانی لازم است تا اطلاعات در محل بازرس مرکزی جمع‌آوری شوند و سپس آنالیز شوند، در حالیکه در بازرس محلی این تاخیر زمانی وجود ندارد. علاوه بر این انجام آزمایشات بر روی بار ارسالی شبکه نشان می‌دهد که ترافیک این معماری که نتیجه ارسال اطلاعات جمع‌اوری شده توسط سنسورها بر روی شبکه است در مقایسه با ترافیک بازرس محلی که تنها نتایج آزمایشات را ارسال می‌کرد از حجم بیشتری برخوردار است. همچنین این آزمایشات به ما نشان داد که با افزایش پریود زمانی میانگین میزان بار عبوری بر روی شبکه کم شده است. علت امر این است که با افزایش پریود زمانی، اطلاعات ارسالی با فاصله‌های زمانی بیشتری بر روی شبکه ارسال می‌شوند که نتیجه آن کاهش میانگین بار ارسالی بر روی شبکه است.

در سومین قدم، معماری بازرس متحرک مورد بررسی قرار گرفت. در این معماری بازرس که به صورت عامل متحرک می‌باشد بر روی میزبان‌های مختلف در سطح شبکه حرکت می‌کند و اطلاعات جمع‌آوری شده توسط سنسورها را آنالیز می‌کند. در جدول ۴-۳ می‌توان نتایج آزمایش انجام شده را برای حالت بازرس متحرک را مشاهده کرد.

جدول ۴-۳- نتایج آزمایش برای حالت بازرس متحرک

بازرس مبتنی بر عامل‌های متحرک					
پریود زمانی	**۵ ثانیه**	**۱۰ ثانیه**	**۳۰ ثانیه**	**۶۰ ثانیه**	**۱۲۰ ثانیه**
میزان مصرف حافظه	8.2 %	5.8 %	5.7 %	5.7 %	5.7 %
میزان مصرف CPU	2.3 %	1.4 %	0.4 %	0.3 %	0.1 %
بار شبکه	50 kbps	26 kbps	8.5 kbps	4.5 kbps	2.8 kbps
زمان پاسخ	11969 ms	10151 ms	30180 ms	60160 ms	120200 ms

همانطور که در جدول ۴-۳ مشاهده می‌شود، میزان مصرف حافظه و میزان مصرف پردازنده برای بازرس متحرک در مقایسه با دو معماری دیگر بازرس (بازرس محلی و بازرس متمرکز) بیشتر است. علت این مساله قرار داشتن سرویس‌دهنده عامل متحرک بر روی سیستم‌ها است. این سرویس‌دهنده یا agency وظیفه دریافت عامل‌های متحرک را بر عهده دارد. میزان زمان پاسخ بازرس متحرک در مقایسه با بازرس محلی بیشتر است که این مساله به علت زمانی است که بازرس مصرف می‌کند تا در شبکه حرکت و اطلاعات را جمع‌آوری کند. البته این زمان در مقایسه با زمان پاسخ بازرس متمرکز دارای سرعت بیشتری می‌باشد. انجام آزمایشات نشان داد که میزان ترافیک جمع‌آوری شده در بستر مورد آزمایش در مقایسه با دوحالت بازرس محلی و بازرس متمرکز بیشتر است. اما باید توجه داشت در صورتی که وسعت شبکه بیشتر شود، میزان افزایش بار برای بازرس متمرکز بیشتر از بازرس متحرک خواهد بود. در شرایط آزمایش علت افزایش حجم ترافیک شبکه در بازرس متحرک، وجود کد خود بازرس متحرک است. حجم این کد به وسعت شبکه بستگی ندارد و در صورت افزایش وسعت شبکه، این ترافیک تغییر قابل توجهی نمی‌کند، اما در بازرس متمرکز،

میزان ترافیک نسبت مستقیم با وسعت شبکه دارد. به همین دلیل مشخص است که با افزایش وسعت شبکه میزان بار مربوط به بازرس متمرکز از بازرس متحرک بیشتر می‌شود.

یکی از مسائل مهم در بازرس‌ها، مساله قابلیت گسترش آنها می‌باشد. در معماری بازرس متمرکز برای پیکربندی سیستم بازرسی، لازم است که تنها بازرسی را که در نقطه مرکزی قرار دارد پیکربندی کنیم و در معماری بازرس متحرک نیز کافی است در نقطه شروع حرکت بازرس‌ها، آنها را مورد پیکربندی قرار دهیم. در حالیکه در سیستم بازرس محلی، باید به ازای تمام سیستم‌ها عمل پیکربندی صورت گیرد.

با توجه به مطالب گفته شده، می‌توان نتیجه گرفت که استفاده از بازرس محلی در شبکه‌های محلی کوچک به علت بار کم و سرعت بالا به عنوان راه مناسب می‌باشد. اما یکی دیگر از مسائلی که در انتخاب نوع معماری موثر است امکان قابلیت گسترش می‌باشد. همانطور که گفته شد عمل پیکربندی بازرس‌ها در سیستم بازرس محلی به ازای تمام بازرس‌ها باید صورت گیرد که این مساله با گسترش شبکه کار دشواری می‌شود و قابلیت گسترش را با مشکل مواجه می‌کند. به همین دلیل در شبکه‌های بزرگ دو انتخاب وجود دارد که بازرس متمرکز و بازرس متحرک می‌باشد که استفاده از بازرس متمرکز به علت بار زیاد و همچنین single point of failure بودن بازرس مرکزی راه حل مناسبی نیست. در چنین شبکه‌ای راه‌حل برگزیده استفاده از بازرس متحرک است.

۵- بررسی بازرس متحرک

در این دسته از آزمایش‌ها، بین تعداد بازرس‌ها، نحوه حرکت آنها، میزان باری که بر شبکه می‌گذارند و زمان پاسخ آنها برای شبکه‌هایی با تعداد میزبان‌های مختلف مقایسه‌ای انجام می‌شود.

برای انجام این آزمایش دو معیار زمان پاسخ و بار شبکه مورد ارزیابی قرار گرفته است. برای در نظر گرفتن این دو معیار، پارامتری در نظر گرفته شده است به صورت زمان پاسخ x میزان بار شبکه. همانطور که مشخص است، این دو پارامتر نسبت عکس با یکدیگر دارند، به این معنی که هر چه تعداد بازرس‌ها بیشتر باشد، زمان پاسخ کمتر می‌شود و جواب سریع‌تر آماده می‌شود و به دنبال آن بار شبکه افزایش می‌یابد. با توجه به این مطلب باید تعادلی بین آن دو برقرار کرد تا مقدار زمان پاسخ x بار شبکه حداقل شود. فرضی که در انجام آزمایشات این بخش وجود دارد، در نظر گرفتن یک مسیر حرکت مشخص برای بازرس‌ها می‌باشد که شرح آن در ادامه آورده شده است. یک عامل به صورت متوسط یک سیستم تشخیص‌نفوذ را در مدت 300 ms بررسی می‌کند و جواب را برمی‌گرداند و باری که بر شبکه ایجاد می‌کند در حدود 4.5 kbps است. با توجه به این مقادیر می‌توان نسبت بار شبکه به سرعت پاسخ را برای تعداد مختلف بازرس بررسی کرد. این آزمایش برای شبکه‌هایی با تعداد میزبان مختلف در ادامه نشان داده شده است.

در صورتیکه در شبکه دو میزبان دارای سیستم تشخیص‌نفوذ باشند حالات زیر را می‌توان در نظر گرفت. در این شبکه تعداد عامل‌هایی که به عنوان بازرس می‌توان انتخاب کرد یک تا دو عدد خواهد بود (به علت اینکه برای بازرسی دو سیستم تشخیص‌نفوذ حداکثر به دو بازرس نیاز است). در صورتیکه تعداد بازرس‌ها یک عدد باشد میزان باری که بر شبکه می‌گذارد برابر خواهد بود با 4.5 kbps و زمان پاسخ برابر خواهد بود با 600 ms (600 x 4.5 = 2700). در صورتیکه تعداد بازرس‌ها دو عدد در نظر گرفته شود میزان باری که ایجاد می‌کند در حدود 9 kbps و زمان پاسخ آن در حدود 300 ms می‌شود (300 x 9 = 2700). در جدول ۵-۴ این نتایج را می‌توان مشاهده کرد:

جدول ۵-۴- میزان بار و زمان پاسخ برای شبکه‌ای با دو میزبان

شبکه‌ای با دو میزبان			
تعداد عامل	میزان بار	زمان پاسخ	بار x زمان
1	~ 4.5 kbps	~ 600 ms	2700
2	~ 9 kbps	~ 300 ms	2700

در ادامه برای شبکه‌هایی با تعداد میزبان مختلف نتایج بدست آمده نشان داده شده است (جداول ۵-۵، ۵-۶، ۵-۷، ۵-۸ و ۵-۹).

جدول ۵-۵- میزان بار و زمان پاسخ برای شبکه‌ای با سه میزبان

شبکه‌ای با سه میزبان			
تعداد عامل	میزان بار	زمان پاسخ	بار x زمان
1	~ 4.5 kbps	~ 900 ms	4050
2	~ 7.5 kbps	~ 600 ms	4500
3	~ 13.5 kbps	~ 300 ms	4050

جدول ۵-۶- میزان بار و زمان پاسخ برای شبکه‌ای با چهار میزبان

شبکه‌ای با چهار میزبان			
تعداد عامل	میزان بار	زمان پاسخ	بار x زمان
1	~ 4.5 kbps	~ 1200 ms	5400
2	~ 6.75 kbps	~ 900 ms	6075
3	~ 10.5 kbps	~ 600 ms	6300
4	~ 18 kbps	~ 300 ms	5400

جدول ۵-۷- میزان بار و زمان پاسخ برای شبکه‌ای با پنج میزبان

شبکه‌ای با پنج میزبان			
تعداد عامل	میزان بار	زمان پاسخ	بار x زمان
1	~ 4.5 kbps	~ 1500 ms	6750
2	~ 6.3 kbps	~ 1200 ms	7560
3	~ 9 kbps	~ 900 ms	8100
4	~ 13.5 kbps	~ 600 ms	8100
5	~ 22.5 kbps	~ 300 ms	6750

جدول ۵-۸- میزان بار و زمان پاسخ برای شبکه‌ای با شش میزبان

شبکه‌ای با شش میزبان			
تعداد عامل	میزان بار	زمان پاسخ	بار x زمان
1	~ 4.5 kbps	~ 1800 ms	8100
2	~ 6 kbps	~ 1500 ms	9000
3	~ 8.1 kbps	~ 1200 ms	9720
4	~ 11.25 kbps	~ 900 ms	10125
5	~ 16.5 kbps	~ 600 ms	9900
6	~ 27 kbps	~ 300 ms	8100

جدول ۵-۹- میزان بار و زمان پاسخ برای شبکه‌ای با هفت میزبان

شبکه‌ای با هفت میزبان			
تعداد عامل	میزان بار	زمان پاسخ	بار x زمان
1	~ 4.5 kbps	~ 2100 ms	9450
2	~ 5.78 kbps	~ 1800 ms	10404
3	~ 7.5 kbps	~ 1500 ms	11250
4	~ 9.9 kbps	~ 1200 ms	11880
5	~ 13.5 kbps	~ 900 ms	12150

11395	~ 600 ms	~ 19.5 kbps	6
9450	~ 300 ms	~ 31.5 kbps	7

نکته‌ای که در اینجا باید به آن توجه داشت چگونگی حرکت بازرس‌ها در شبکه می‌باشد. واضح است بسته به نحوه حرکت آنها زمان پاسخ و میانگین میزان ترافیک شبکه تغییر خواهد کرد. نحوه حرکت بازرس‌ها در آزمایش فوق، ثابت در نظر گرفته شده است، به این ترتیب که اگر شبکه‌ای با n میزبان در نظر گرفته شود و برای آن m بازرس وجود داشته باشد (n < m)، m-1 بازرس-m 1 میزبان را بازرسی می‌کنند و بازرس m ام سایر میزبان‌های باقیمانده را مورد بررسی قرار می‌دهد. همانطور که در جداول فوق نشان داده شده است، زمانی حاصل پارامتر زمان پاسخ x بار شبکه حداقل می‌شود که تعداد عامل‌ها یا یکی باشد و یا آنکه به تعداد میزبان‌های شبکه باشد. علت این مساله با بیان نحوه حرکت که در ادامه می‌آید توجیه می‌شود.

به منظور نشان دادن تاثیر نحوه حرکت بر زمان پاسخ و میزان بار شبکه، شبکه‌ای با شش میزبان و دو، سه و چهار بازرس در نظر گرفته می‌شود که در آنها می‌توان به روش‌های مختلفی بازرس‌ها را در شبکه حرکت داد. برای بررسی تاثیر حرکت بر زمان پاسخ و بار شبکه، نیز از پارامتر زمان پاسخ x میزان بار شبکه استفاده شده است. با توجه به این مطلب باید تعادلی بین آن دو برقرار کرد تا مقدار زمان پاسخ x بار شبکه حداقل شود. در جدول ۵-۱۰، ۵-۱۱ و ۵-۱۲ نتایج این آزمایشات صورت گرفته در شبکه‌ای با شش میزبان و تعداد دو، سه و چهار بازرس آورده شده است. در جداول نحوه حرکت بازرس‌ها به این ترتیب نشان داده شده است: m (IDSa, IDSb, ..., IDSn) که نشان‌دهنده این مطلب است که بازرس شماره m، IDSهای a، b و ... را بازرسی می‌کند. با توجه به این مطلب، جدول ۵-۱۰ نشان می‌دهد که در صورتی که شبکه‌ای با شش میزبان داشته باشیم، در صورتی که یک بازرس وجود داشته باشد، میزان بار x زمان پاسخ چه مقدار می‌شود و در صورتی که دو بازرس داشته باشیم، این پارامتر چه تغییری می‌کند. در جداول ۵-۱۱ و ۵-۱۲ همین عمل برای شبکه‌هایی با سه و چهار بازرس نشان داده شده است. همانطور که پیشتر نیز گفته شد یک عامل به صورت متوسط یک سیستم تشخیص‌نفوذ را در مدت 300 ms بررسی می‌کند جواب را برمی‌گرداند و باری که بر شبکه ایجاد می‌کند در حدود 4.5 kbps است. با توجه به این موارد می‌توان نتایج را به ترتیب زیر مشاهده کرد:

جدول ۵-۱۰- میزان بار و زمان پاسخ برای شبکه‌ای با شش میزبان و دو بازرس با مسیرهای حرکت متفاوت

شبکه‌ای با شش میزبان			
نحوه حرکت بازرس‌ها	**میزان بار**	**زمان پاسخ**	**بار x زمان**
1 (IDS1) 2 (IDS2, IDS3, IDS4, IDS5, IDS6)	~ 6 kbps	~ 1500 ms	9000
1 (IDS1, IDS2) 2 (IDS3, IDS4, IDS5, IDS6)	~ 7.2 kbps	~1200 ms	8640
1 (IDS1, IDS2, IDS3) 2 (IDS1, IDS2, IDS3)	~ 9 kbps	~ 900 ms	8100

جدول ۵-۱۱- میزان بار و زمان پاسخ برای شبکه‌ای با شش میزبان و سه بازرس با مسیرهای حرکت متفاوت

شبکه‌ای با شش میزبان			
نحوه حرکت بازرس‌ها	**میزان بار**	**زمان پاسخ**	**بار x زمان**
1 (IDS1) 2 (IDS2) 3 (IDS3, IDS4, IDS5, IDS6)	~ 8.1 kbps	~ 1200 ms	9720
1 (IDS1) 2 (IDS2, IDS3) 3 (IDS4, IDS5, IDS6)	~ 10.125 kbps	~ 900 ms	9112.5
1 (IDS1, IDS2) 2 (IDS3, IDS4) 3 (IDS5, IDS6)	~ 13.5 kbs	~ 600 ms	8100

جدول ۵-۱۲- میزان بار و زمان پاسخ برای شبکه‌ای با شش میزبان و چهار بازرس با مسیرهای حرکت متفاوت

شبکه‌ای با شش میزبان			
نحوه حرکت بازرس‌ها	**میزان بار**	**زمان پاسخ**	**بار x زمان**
1 (IDS1) 2 (IDS2) 3 (IDS3) 4 (IDS4, IDS5, IDS6)	~ 11.25 kbps	~ 900 ms	10125
1 (IDS1) 2 (IDS2) 3 (IDS3, IDS4) 4 (IDS5, IDS6)	~ 15 kbps	~ 600 ms	9000

همانطور که گفته شد، میزان بار شبکهx زمان پاسخ هنگامی مناسب است که مقدار حداقل را داشته باشد. با توجه به این مطلب و توجه به جدول ۵-۱۰ که نشان‌دهنده شبکه‌ای با شش میزبان و دو بازرس می‌باشد، مشخص است که پارامتر تعریف شده زمانی مقدار حداقل را می‌گیرد که (IDS1, IDS2, IDS3) 1 و (IDS4, IDS5, IDS6) 2 به این معنی که بازرس شماره یک سه میزبان را بررسی کند و بازرس شماره دو نیز سه میزبان را بررسی کند. این حالت، زمانی را نشان می‌دهد که شبکه به صورت مساوی به بخش‌هایی شکسته شده است و توسط بازرس‌ها مورد بررسی قرار می‌گیرد. با دقت در جدول ۵-۱۱ نیز مشخص است که مقدار حداقل باز زمانی به دست آمده که شبکه به بخش‌های مساوی بین سه بازرس تقسیم شده است - یعنی زمانی که (IDS1, IDS2) 1، (IDS3, IDS4) 2 و (IDS5, IDS6) 3. - مقدار پارامتر بارx زمان پاسخ در این حالت 8100 است که با مقدار حداقل که در جدول ۵-۱۰ بدست آمده بود برابر است. جدول ۵-۱۲ زمانی را نشان می‌دهد که چهار بازرس عمل بازرسی را انجام می‌دهند. همانطور که این جدول نشان می‌دهد، مقادیر بدست آمده در مقایسه با مقادیر جداول ۵-۱۰ و ۵-۱۱ مقدار بیشتری دارد. علت این مطلب این است که شبکه‌ای با شش میزبان را نمی‌توان به صورت مساوی بین چهار بازرس تقسیم کرد. با توجه به این مطلب، نتایج آزمایشات نشان می‌دهد، مقدار حداقلی که در جدول ۵-۱۲ بدست آمده 9000 است که از مقدار 8100 بیشتر است. به این معنی که به دلیل اینکه در حالت اخیر که چهار بازرس وجود داشت، به علت عدم امکان شکستن شبکه به بخش‌های مساوی بین آنها، مقدار پارامتر بدست آمده در مقایسه با حالت‌های دو بازرس و سه بازرس که امکان شکستن شبکه به بخش‌های مساوی بین آنها بود، بیشتر است. با توجه به این مطلب، علت این امر که "حاصل پارامتر بار شبکهx زمان پاسخ برای تعداد یک بازرس و تعداد n بازرس (که n تعداد میزبان‌ها می‌باشد) حداقل می‌شود" و در گذشته به آن اشاره شده بود مشخص می‌شود. در حالت تعداد یک بازرس و n بازرس، به علت اینکه شبکه به صورت مساوی بین بازرس‌ها تقسیم می‌شود، پارامتر زمان پاسخ x بار شبکه مقدار حداقل می‌شود.

۶- نتیجه و جمع‌بندی

در این مقاله سیستم‌های تشخیص‌نفوذ به عنوان یکی از ابزارهای امنیتی شبکه مورد توجه قرار گرفت و شرح داده شد که در صورتی که اگر سیستم تشخیص‌نفوذ به هر دلیل به درستی عمل نکند، مکانیزم امنیتی شبکه دچار مشکل می‌شود. روشی را که به عنوان راه‌حل برای مقابله با این مشکل مطرح کردیم ایده بکارگیری جزئی به نام بازرس بود. این بازرس به عنوان یک عامل وظیفه بررسی سیستم تشخیص‌نفوذ را به عهده دارد. این بازرسی شامل بررسی پارامترهایی مثل بررسی تشخیص یا عدم تشخیص حمله توسط سیستم، بررسی تغییرات در پیکربندی سیستم، میزان سربارهای سیستم تشخیص‌نفوذ و تغییرات دیگری که هر یک می‌تواند بیانگر تغییری در عمل سیستم تشخیص‌نفوذ باشد.

با مطرح کردن ایده بازرس، سه معماری برای آن نیز مطرح کردیم که عبارت بودند از بازرس متمرکز، بازرس محلی و بازرس متحرک. با آزمایشاتی که بر روی این سه معماری انجام شد، این نتیجه بدست آمد که استفاده از بازرس متمرکز در هنگامی که شبکه محلی کوچک باشد قابل استفاده می‌باشد، اما با وسعت شبکه، بکار گرفتن این معماری امکان‌پذیر نیست و در این شرایط راه‌حل مناسب استفاده از بازرس متحرک می‌باشد.

در رابطه با بازرس متحرک نیز بررسی‌هایی را انجام دادیم و آن را از لحاظ تعداد بازرس و نحوه حرکت مورد ارزیابی قرار دادیم. برای مقایسه بین تعداد بازرس‌ها از دو پارامتر زمان پاسخ و میزان بار شبکه استفاده شده است. مشخص است بهترین حالت زمانی است که هم زمان پاسخ و هم میزان بار شبکه کم باشد. به این ترتیب می‌توان گفت بهترین تعداد عامل، زمانی است که حاصل ضرب زمان پاسخ در میزان بار شبکه حداقل شود. با توجه به آزمایشات انجام شده می‌توان دید که بهترین جواب‌ها در زمانی صورت می‌گیرد که یک بازرس تمام میزبان‌ها را بررسی کند و یا آنکه برای هر میزبان یک بازرس مستقل وجود داشته باشد (این حالت زمانی صحیح است که بازرس‌های ۱ تا m-1 میزبان‌های ۱ تا m-1 را بررسی کند و بازرس آخر سایر میزبان‌ها را). البته در صورتی که مسیر حرکت برای بازرس‌ها تغییر داده شود می‌توان برای تعداد بازرس‌های مختلف دیگر نیز جواب بهینه را بدست آورد. در صورتیکه شبکه به صورت مساوی بین بازرس‌ها تقسیم شود می‌توان جواب بهینه را بدست آورد. انتخاب تعداد بازرس‌ها و نحوه حرکت آنها با توجه به سیاست‌های مدیر شبکه صورت می‌گیرد. در صورتی که سرعت پاسخ بالا اهمیت داشته باشد روش برتر قرار دادن یک بازرس برای هر میزبان است، به علت اینکه در این حالت هر میزبان توسط یک بازرس بررسی می‌شود، زمان پاسخ حداقل می‌شود، اما با توجه به اینکه به تعداد میزبان‌ها بازرس وجود دارد، بار ارسالی بازرس‌ها بر روی شبکه حداکثر می‌شود. زمانی که بار شبکه اهمیت دارد می‌توان از یک بازرس برای بررسی کل میزبان‌ها استفاده کرد. به علت اینکه در این حالت تنها یک بازرس وجود دارد، باری که در شبکه ایجاد می‌کند، حداقل است اما چون یک بازرس است و وظیفه بررسی تمام میزبان‌ها را بر عهده دارد، زمان پاسخ آن زیاد می‌شود.

۷- مراجع

[1] Rebecca Gurley Bace، "*Intrusion Detection*"، Macmillan Technical Publishing، 2000

[2] Edward G. Amoroso, "*Fundamentals of Computer Security Technology*", Prentice Hall, 1994

[3] Mats Person، "*Mobile Agent Architectures*"، Defense Research Establishment، 2000

[4] Denny B. Lange, Mitsuru Oshima, "*Programming and Deploying Java Mobile Agents with Aglets*", Addison Wesley, 1998

[5] Christopher Krugel, Thomas Toth, "*Applying Mobile Agent Technology to Intrusion Detection*", Technical University Vienna, 2000

[6] Jose Durate، Luiz Fernando، "*Micael: An Autonomous Mobile Agent System to Protect New Generation Networked Applications*"، URFJ – Rio de Janeiro، 2001

[7] Midori Asaka, Atsushi Taguch, Shigeki Goto, "*The Implementation of IDA: An Intrusion Detection Agent System*", IPA, Waseda University, 1998

[8] Christopher Krugel، Thomas Toth, "*Sparta, A Mobile Agent based Intrusion Detection System*"، Technical University Vienna، 2000

[9] Jai Suunder، Jose Omar، "*An Architecture for Intrusion Detection using Autonomous Agents*"، Purdue University، 1998

[10] Richard P. Lippmann, David J. Fried, "*Evaluating Intrusion Detection Systems: The 1998 DARPA Off-line Intrusion Detection Evaluation*", Lincoln Laboratory MIT, 1999