مروری اجمالی بر چگونگی عملکرد Sourcefire IPS

مرجان اسحاقی

Baharti Vidyapeeth University, India, m.esehaghi@gmail.com

چکیده- این روزها بیشتر شبکه ها داینامیک هستند و تهدیدات امنیتی به شدت و با سرعت در حال متحول و پیچیده شدن می باشند راهکارهای امنیتی استاتیک قدیم دیگر جوابگوی شبکه های امروزی نیستند . به همین دلیل است که زیرکی و باهوشی افراد سازمان های فناوری اطلاعات در زمینه امنیت بیشتر کارامد و مهم هست تا سخت کوشی آنها .امروزه مدیران امنیت نیازمند این امر هستند که مانیتورینگ و مدیریت حفاظت در برابر تهدیدات را از چندین جهت انجام دهند وآمادگی پاسخ به هر گونه بحران و تهدید را در هر زمان داشته باشند .آنها گاهی اوقات وقت کافی برای استفاده از تمام ابزارهای امنیتی و مانیتورینگ و همچنین به روز رسانی ابزارهای موجود را ندارند.همچنین در اکثر موارد توانایی تبحر لازم در اینگونه ابزارها را نخواهند داشت.در روش های قدیمی که از راهکارهای استاتیک استفاده می شد ،خیلی از سازمان ها این راهکارها را در پروسه های امنیتی دیگر شبکه نیز پیاده سازی می کردند .وجود این پروسه های استاتیک باعث ایجاد ناپایداری در ساختار امنیتی شبکه می شود. اکثر IPSهای قدیمی بر اساس تهدیدات شناخته شده قدیمی شبکه را محافظت می کردند و هیچ تمهیداتی در مورد تهدیدات ناشناخته نداشتند.همچنین تحقیقات نشان داده است که تنها ۶ درصد از رخنه های امنیتی شبکه توسط راهکارهای امنیتی ابزارهای خریده شده توسط سازمان ها تشخیص داده شده است و این امر که یکی دیگر از نگرانی های متخصصان امنیتی بود بیشتر به دلیل ناتوانی کاربران امنیتی از تفسیر و بررسی اخطارها ی بیشمار IPS ها بوده است .یکی از ویژگی های بارز Source fire ، RNA یا هوشمندی بلادرنگ شبکه می باشد که محافظت در برابر هر گونه تهدید و آسیب پذیری اعم از شناخته شده و ناشناخته را محقق می کند و در کنار آن با استفاده از خاصیت Context و Visibility کاربر امنیت را قادر به تمایز قائل شدن بین اخطارها می نماید.

مقدمه:

IPS که مخفف Intrusion Prevention System می باشد سیستم کشف نفوذ می باشد که شبکه را بر اساس رفتار های مشکوک و مخرب مانیتور می کند و به صورت real-time هشدار داده و حملات را بلاک می کند. IPS تکامل یافته IDS می باشد.

IDS (Intrusion Detection System) یا سیستم پیشگیری از نفوذ تنها می تواند حملات را تشخیص دهد ولی توانایی بلاک کردن انها را ندارد.

به همین دلیل امروزه از IPS بیشتر به عنوان Inline blocking mode و از IDS به عنوان Passive detecting mode یاد می شود.

اما سیستم های کشف نفوذ قدیمی مشکلاتی داشتند. IPS های قدیمی مدیر امنیت را درگیر تعداد بسیار زیادی از رویدادهای نا مربوط می کرد و این امر باعث سر در گمی و اتلاف وقت مدیر امنیت می شد و همچنین اساس کار این سیستمها بر مبنای Black box یا جعبه سیاه بود و مدیر سیستم هیچ ذهنیتی از چگونگی عملکرد نداشت و از آنجایی که IPS آخرین امید امنیتی هر شبکه ای بود ، این کمبود کارآیی و نفوذ پذیری شبکه باعث مشکلات زیادی در حوزه امنیت می شد.[۲]

نشانه های یک IPS کارآمد به شرح زیر بود:

- تشخیص دادن حمله
- دادن یک سری اطلاعات متنی مبنی بر اینکه چه کسی و چه چیزی و کجا و چرا و در چه زمانی این حمله را انجام داده است
- قانع کردن مدیرامنیت که حمله کاملا کنترل شده و شبکه در امنیت کامل به سر می برد

در اینجا بود که محققان Sourcefire IPS را معزفی کردند که شامل تمام این موارد بوده و کمی و کاستی های IPSهای قدیمی را جبران کرد.

قبل از توضیح در مورد Sourcefire IPS لازم هست تا کمی در مورد زنجیره مقابله با حملات توضیح داده شود

تمهیداتی که در برابر حملات انجام می شود در سه مرحله انجام می گیرد:

- تمهیدات قبل از حمله
- تمهیدات در حین حمله
- تمهیدات پس از حمله

۱- تمهیدات قبل از حمله: که شامل کشف حمله ، اجرای عملیاتی در برابر حمله و مقاوم کردن شبکه در برابر حمله می باشد . این تمهیدات توسط تکنولوژی هایی همچون Firewall و VPN و UTM و NGFW و NAC انجام می شود.

۲- تمهیدات در حین حمله :که شامل تشخیص حمله و بلاک کردن منبع حمله و دفاع در برابر آن می باشد که توسط تکنولوژی هایی چون NGIPS و Web Security و Email Security انجام می شود.

۳- تمهیدات بعد از حمله : که شامل توجه ، تضمین و ترمیم که با تکنولوژی هایی چون Advanced Malware Protection و Network Behavior Analysis انجام می گیرد.

اما Visibility و Contextual دو ویژگی نوین امنیتی هستند که اساس کار Source fire IPS بوده و هر سه مرحله را پوشش می دهند.[۹]

Source fire IPS

Source fire که در واقع به 3D system معروف است به دلیل ۳ ویژگی که با D آغاز می شود. " Discover , Determine , Defend " که به معنی دارا بودن ساختاری با خصوصیات کشف ، تعیین و دفاع در برابر حملات است ، تشخیص و طبقه بندی ترافیک شبکه ،که درصد تشخیص نادرست حمله بسیار پایین هست یا به بیان دیگر مدیر امنیت را قادر به کشف درست تهدید در زمان رخداد آن می کند و مقدار شدت و اثر آن خطر را تعیین کرده و در عین حال امنیت را فارغ از اینکه این تهدید در چه محدوده ای از شبکه اتفاق افتاده باشد، با متوقف کردن تهدید برقرار می نماید.

شکل ۱ :نداشتن تصویری که این فرد به چه منظور قصد وارد شدن به این ساختمان را دارد.

3D System در واقع یک سیستم مدیریت مرکزی است که به صورت Context عمل می کند همراه با agentهایی که شبکه را در برابر تهدیدات امنیتی حمایت می کند.هنگامیکه IPS با یک پکت که احتمال حمل داده ها و کد های مخرب هست مواجهه می شود توانایی بررسی کامل و صحیح آن را ندارد مگر اینکه توانایی Contextرا داشته باشد. به طور مثال اگر شما فردی را در حال وارد شدن به ساختمانی را ببینید شما هیچ تصوری از اینکه این فرد به چه منظور وارد این ساختمان می شود ندارید مگر اینکه از شرایط حاکم بر آن مکان و زمان و حالات و طرز پوشش آن فرد واتفاقات اخیر اطراف آن محل داشته باشید .این مثال دقیقا همانند وارد شدن یک پکت می باشد و اطلاعات برای بررسی های بیشتر به همان ویژگی Context بر می گردد.پس بنابراین با وجود ویژگی Context کاربر امنیتی شبکه می تواند اوالویت مابین اخطارهای IPS قائل شده و می تواند تصمیم بگیرد که کدام اخطار نیاز به بررسی های بیشتری دارد و مهم تر و در حالت بحرانی تر است.

در این مقاله بیشتر تاکید بر دو ویژگی خاص Source fire شده است که این تکنولوژی نوین را متمایز از دیگران کرده است این دو ویژگی عبارتند از:

- هشیاری بلادرنگ شبکه
- هشیاری بلارنگ کاربر

هشیاری بلادرنگ شبکه Real-Time Network Awareness

وقتی از مارکس رانوم که یکی از مدیران ارشد امنیتی شبکه می باشد سوال پرسیده شد که ضعیف ترین حلقه در زنجیر شبکه کدام قسمت است ،پاسخ او چیزی نبود غیر از هشیاری شبکه یا Network Awareness .[۸] متخصصان امنیتی همگی بر این عقیده اند که بزگترین مشکل برای کاربران امنیتی شبکه آگاهی از این است که چه چیزی هم اکنون در شبکه در حال انجام است.

در واقع RNA با جمع آوری اطلاعات در مورد شبکه اعم از سیستم عامل ها و برنامه های نصب شده بر روی دستگاه های شبکه همچنین نقاط محتمل آسیب پذیزی آنها ، میتواند حملات محتمل را اولویت بندی کرده و رسیدگی کند.به طور مثال هنگامیکه یک پکت شامل کدهای مخرب برای آسیب زدن به Windows هست این پکت نمی تواند تهدیدی برای سیستم هایی که سیستم عامل آنها Linux می باشد باشد .بنابراین با این راهکار RNA باعث کاهش تعداد رویدادهای IPS می شود.

RNA با استفاده از خصوصیتی به نام (RNA – Recommended Rules) RRR به چابکی و هوشیاری IPS کمک بیشتری می کند. RRR با استفاده از اطلاعات در مورد سیستم عامل و سرویس های در حال اجرا در شبکه پیشنهاد اجرای بهترین و مناسبترین Rule را می دهد.این امر باعث افزایش سرعت کار ایمن سازی و جلوگیری از اتلاف زمان کاربران امنیتی سیستم می شود.

در کل RNA مدیریت امنیت را قادر می سازد که Visibility کامل از شبکه داشته باشد وهمچنین با دانستن آنچه در شبکه در حال اتفاق هست بهترین تصمیم امنیتی را اتخاذ نماید.

Sourcefire 3D System با توصیف یک Ipmact Vlue برای هر رویداد یا Event محدوده شدت محتمل هر تهدیدی را مشخص کرده تا کاربر امنیت بتواند تصمیمات قاطعانه تر و صحیح تر در بهترین محدوده زمانی انجام دهد.

IMPACT FLAG RATING & COLOR	ADMINISTRATION ACTION
	Act Immediately , Vulnerable
	Investigate , Potentially Vulnerable
	Good to know ,Currently Not Vulnerable
	Good to know ,Unknown Target
	Good to know ,Unknown Network
	Good to know , Blocked

جدول ۱ :Impact Value or Impact Flag table [۸]

هشیاری بلادرنگ کاربر Real-Time User Awareness

بسیاری از سازمان ها RNA را با RUA یا همان Real-Time User Awareness برای بالا بردن Visibility در شبکه ترکیب می کنند. نگرانی مدیر امنیت شبکه به محض تشخیص یک رویداد تهدید آمیز این است که این رویداد توسط کدام کاربر شبکه با چه IP در حال انجام است .در شبکه های خیلی بزرگ تشخیص این امر کار بسیار پیچیده و مشکلی است که کاربر را در میان هزاران IP بتوان پیدا کرد.

RUA با استفاده از LDAP و Active Directory domains به عنوان منبع اطلاعات کاربران هوشمندی کاربر شبکه را برقرار می شازد.[۸]

نتیجه گیری :

با حضور و پیشرفت سریع تهدیدات امنیتی شبکه ها یافتن ابزاری برای مواجهه با این ابزارها امری اجتناب ناپذیر است. اما برخلاف تلاش بسیار زیاد ، مدیران امنیتی شبکه ها و انجام هزینه های گزاف برای خرید اینگونه ابزار ها همچنان شاهد آسیب پذیری های بسیاری بوده اند .این مشکل در IPS های قدیمی بیشتر ناشی از فقدان Visibility و Context بود که کاربر امنیت را ناتوان از تشخیص رخنه ها و آسیب های شبکه می ساخت. Sourcefire IPS با فراهم کردن این دو ویژگی کاربر را بسیار آگاه تر و هوشیار تر از گذشته از آنچه در حال اتفاق در شبکه است می سازد تا راهکارهای امنیتی در زمان موثر اعمال شود و شبکه از تهدیدات در امان باشد. اما در عمل هنوز هم خیلی از کاربران امنیتی رضایت چندان زیادی از Sourcefire نشان نمی دهند که یکی از مشکلات عمده آنها بی مورد بودن هزینه زیاد برای خریداری این تکنولوژی برای سازمان می باشد.این امر قابل توجه هست که برای خریداری هر تکنولوژی جدید ابتدا ساختار موجود شبکه باید مورد بررسی قرار بگیرد که آیا با این ساختار موجود انجام این هزینه کارآمد هست یا خیر.با این حال بسیاری از کارشناسان متبحر امنیت هیچ تردیدی در انجام این هزینه گزاف در برابر امکانات جدید و موثر آن از جمله احراز هویت کاربران و مدیریت فعالیت آنها و همچنین توانایی شفاف بودن عملیات های حاکم بر شبکه نداشته اند. با این حال هنوز تولید کنندگان ویروس ها و Malware ها و دیگر تهدیدات در حال پیدا کردن رخنه های جدید در شبکه ها هستند که حتی Sourcefire IPS هم ممکن هست در تشخیص آنها توانایی کافی را نداشته باشد. یکی از این تهدید ها تهدیدات zero-day است که IPS های نسل جدید هم گاهی ناتوان در برابر تشخیص و دفاع در برابر آنها هستند.

مراجع:

[1] Sourcefire Seminar Series 2014 Road American Roadshow, Cisco

[2] Introduction to the Cisco Sourcefire Next Generation Intrusion Prevention Systems,Wes Bateman, Consulting Security Engineer,BRKSEC-1030

[3] Towards Next-GenerationIntrusion Detection ,Robert Koch ,Institut für Technische Informatik (ITI) ,Universität der Bundeswehr ,Munich, Germany 2011 3rd International Conference on Cyber Conflict

[4] Next Generation Security , Mahmoud Rabi Consulting Systems Engineer – Security, cisco live

[5] Next Generation Intrusion Prevention Is… So Yesterday Exploring the evolution of network intrusion detection and prevention , John Pirc Chief Strategy Officer Bricata ,www.bricata.com

[6] Sourcefi re IPS™ (Intrusion Prevention System) www.sourcefire.com

[7] www.slideshare.com

[8] www.Sourcefire.com

[9] www.cisco.com

[10] www.scmagazine.com

[11] www.ndm.net