مجله رویکردهای نوین در تحقیقات علوم پایه، فنی و مهندسی
سال اول، شماره ۲، بهمن ۱۳۹۷
ISSN: ۲٦٤٥-٥٤٣٩
www.jonarbset.ir

Honeypot در امنیت شبکه

پریسا آزاده ، مهشید قاهری تبریزی ، فرشید صهبا

چکیده

شبکه رایانه‌ای و اینترنت هر روز در حال گسترش هستند. شبکه‌های کامپیوتری به کاربر اجازه دسترسی به پایگاه داده‌های محلی و دوردست را می‌دهند. شبکه و امنیت در صنایع موضوعات مهمی هستند؛ چون نقص در سیستم می‌تواند موجب مشکلات عمده‌ای شود. سیستم تشخیص نفوذ (IDS) برای نظارت بر فرآیندهای یک سیستم یا یک شبکه جهت بررسی تهدیدات استفاده می‌شود و به مدیر شبکه حمله را هشدار می‌دهد. IDS تنها برای صنایع با مقیاس بزرگ راه‌حل ارائه می‌کند، اما هیچ راه‌حلی برای صنایع با مقیاس کوچک وجود ندارد؛ بنابراین مدل Honeypot برای حل مشکل صنایع با مقیاس کوچک پیشنهاد شده است. تعریف Honeypot کار سختی است، چراکه آن‌ها در پیشگیری، تشخیص، جمع‌آوری اطلاعات و کارهای دیگری مورد استفاده قرار می‌گیرند، اما حالت دفاعی ندارند و به عبارتی کار امنیتی نمی‌کنند اما بر امنیت شبکه به شدت تأثیر می‌گذارند. این مدل، فعالیت‌های مهاجمان را ثبت می‌کند و برای تمام این فعالیت‌ها یک log نگه می‌دارد. تمرکز این مقاله جلوگیری از حملات مهاجمان خارجی و داخلی و حفظ فایل لاگ با استفاده از honeypot به‌وسیله ماشین مجازی است.

واژه‌های کلیدی: Honeypot، log، IDS

مقدمه

امنیت شبکه برای بهبود صنایع وابسته به اینترنت جهت افزایش تجارت و ارائه خدمات، مورد نیاز است. بنابراین امنیت شبکه نگرانی اولیه صنایعی است که اطلاعات مهم را تأمین می‌کنند. در سال‌های اخیر در این نوع صنایع، مبالغ کلان جهت ایجاد و حفظ امنیت هزینه شده است. سیستم‌های تشخیص نفوذ (IDS) یک تکنولوژی تشخیصی هستند که هدف آن‌ها این است که فعالیت‌های غیرمجاز یا خرابکارانه را شناسایی کرده و درباره آن‌ها به متخصصان امنیت هشدار دهند؛ در صورتی که فایروال‌ها یک تکنولوژی پیشگیرانه به شمار می‌آیند، آن‌ها از ورود مهاجمان به شبکه یا سیستم‌های کامپیوتری جلوگیری می‌کنند. صنایع کوچک با استفاده از شبکه محلی باید سطح امنیتی خود را بالا نگه‌دارند؛ زیرا پایگاه داده، سرور و مشتری‌ها تنها توسط خودشان اداره می‌شوند. از آنجا که حفظ امنیت برای شبکه داخلی همواره چالش بزرگی برای مدیران است، بنابراین یک راه‌حل مناسب برای امن کردن شبکه داخلی یک شبکه کوچک مورد نیاز است. هانی پات یک ابزار امنیتی است و نقشی ضروری در امنیت سازمان‌ها، بسیار بیش‌تر از firewall و IPS ایفا می‌کند. این مقاله، راه‌حل را برای استفاده از Honeypot پیشنهاد می‌کند.

بررسی Honeypot

Honeypotیک سیستم غیر تولیدی است که برای بهره‌برداری از مهاجم و توجه به تکنیک‌های حمله مورد استفاده قرار می‌گیرد. یک هانی پات با هویتی نفوذپذیر به وظایف خود می‌پردازد؛ به عبارت دیگر یک سیستم اطلاعاتی است که ارزش آن به استفاده غیرمجاز و ممنوع دیگران از آن است. هدف Honeypot نه تنها توجه، بلکه مقابله با خطر و حذف آن است. .از آنجایی که Honeypotها در اشکال و اندازه‌های مختلفی وجود دارند، ارائه تعریف جامعی از آن کار بسیار سختی است. تعریف یک Honeypot نشان‌دهنده نحوه کار آن و یا حتی هدف آن نیست. Honeypotها تکنولوژی هستند که ارزش آن‌ها به تعامل مجرمان با آن‌ها بستگی دارد. تمامی Honeypotها بر اساس یک ایده کار می‌کنند: هیچ‌کس نباید از آن‌ها استفاده کند و یا با آن‌ها تعامل برقرار نماید، هر تعاملی با Honeypot غیرمجاز شمرده شده و نشانه‌ای از یک حرکت خرابکارانه به شمار می‌رود.

در امنیت شبکه، از Honeypotها برای شناسایی مهاجمان استفاده می‌شود و از حملات آن‌ها یاد می‌گیرد و سپس امنیت سیستم را بر اساس آن تغییر داده و توسعه می‌دهد. سوراخ‌های حلقه امنیت شبکه را می‌توان با کمک اطلاعات ارائه شده توسط Honeypot پوشش داد. Honeypot را می‌توان به عنوان یک سیستم کامپیوتری متصل به شبکه برای بازرسی از آسیب‌پذیری‌های یک کامپیوتر یا یک شبکه دانست. نقاط ضعف را می‌توان به طور جمعی یا به تنهایی از هر سیستم بررسی کرد، زیرا یک ابزار منحصر به فرد برای مطالعه درباره مهاجمان و استراتژی‌های آن‌ها در شبکه است. Honeypotها معمولاً ماشین‌های مجازی هستند که مانند یک سیستم واقعی عمل می‌کنند. در واقع سیستمی است که در شبکه سازمان قرار می‌گیرد، اما برای کاربران آن شبکه هیچ کاربردی ندارد و در حقیقت هیچ یک از اعضای سازمان حق برقراری هیچ‌گونه ارتباطی با این سیستم را ندارند. این سیستم دارای یک سری ضعف‌های امنیتی عمدی است. از آنجایی که مهاجمان برای نفوذ به یک شبکه همیشه به دنبال سیستم‌های دارای ضعف می‌گردند، این سیستم توجه آن‌ها را به خود جلب می‌کند و با توجه به اینکه هیچ‌کس حق ارتباط با این سیستم را ندارد، پس هر تلاشی برای برقراری ارتباط با این سیستم، یک تلاش خرابکارانه از سوی مهاجمان محسوب می‌شود. در حقیقت این سیستم نوعی دام است که مهاجمان را فریب داده و به سوی خود جلب

می‌کند و به این ترتیب علاوه بر امکان نظارت و کنترل کار مهاجمان، این فرصت را نیز به سازمان می‌دهد که فرد مهاجم را شناسایی کند و از سیستم‌های اصلی شبکه خود دور نگه دارد.

Honeypotها حتی در بزرگ‌ترین شبکه‌ها، به حداقل منابع احتیاج دارند. در حقیقت، یک Honeypot حتی لازم نیست که حتماً یک کامپیوتر باشد. این سیستم می‌تواند هر نوع نهاد دیجیتالی باشد (معمولاً از آن به عنوان Honeytoken یاد می‌شودکه هیچ ارزش واقعی ندارد).

انواع Honeypotها بر اساس سطح تعامل

۱- تعامل کم:

Honeypotهای با تعامل کم، با شبیه‌سازی سیستم‌ها و سرویس‌ها کار می‌کنند و فعالیت‌های مهاجمان نیز صرفاً شامل همان چیزهایی می‌شود که سرویس‌های شبیه‌سازی شده اجازه می‌دهند. استفاده از هانی پات‌های با تعامل کم ساده‌تر است، چرا که آن‌ها معمولاً از پیش با گزینه‌های مختلفی برای اجرا کردن تنظیم شده‌اند. فقط کافی است شما انتخاب کرده و کلیک کنید، بلافاصله یک Honeypot را با سیستم عامل، سرویس‌ها و رفتار مورد نظر خود در اختیار دارید. این Honeypot می‌تواند تا ۱۳ سیستم عامل مختلف را شبیه‌سازی کرده و ۱۴ سرویس مختلف را نظارت نماید. به عنوان مثال‌هایی از Honeypot با تعامل کم می‌توان به HoneyD، Specter و KFSensor اشاره کرد.

۲- تعامل زیاد:

Honeypotهای با تعامل بالا، کل سیستم عامل و برنامه‌ها را به طور حقیقی برای تعامل با مهاجمان فراهم می‌آورند. آن‌ها چیزی را شبیه‌سازی نمی‌کنند، بلکه کامپیوترها و سیستم عامل‌هایی واقعی هستند که برنامه‌هایی واقعی دارند که آماده نفوذ توسط مهاجمان هستند. مزایای استفاده از این دسته از هانی پات ها بسیار قابل توجه است. آن‌ها برای این طراحی شده‌اند که حجم زیادی از اطلاعات را به دست آورند. این دسته از Honeypotها بارها و بارها ثابت کرده‌اند که قابلیت کشف فعالیت‌های جدید، از پروتکل‌های IP غیراستاندارد مورد استفاده برای کانال‌های دستورات پنهانی گرفته تا تونل زدن IPv٦ در محیط IPv٤ برای پنهان کردن ارتباطات را دارا هستند. به عنوان مثال‌هایی از Honeypot با تعامل زیاد می‌توان به Decoy Server و Honeynet اشاره کرد.

۳- تعادل میانه:

به منظور پوشش خلأ موجود بین هانی پات‌های با تعامل کم و زیاد، هانی پات‌هایی با عنوان هانی پات با سطح تعامل میانه ارائه شدند. در این نوع هانی پات‌ها فاصله بین ۲ نوع اول پوشش داده شده است. در هانی پات با سطح عملکرد میانه، معماری و ساختاری شبیه هانی پات با سطح تعامل کم دارند اما رفتاری شبیه هانی پات با سطح تعامل زیاد را ارائه می‌دهند و امروزه این نوع هانی پات‌ها جزء پرکاربردترین هانی پات‌ها قلمداد می‌شوند.

Honeypot برای صنایع با مقیاس کوچک

Honeypot وقتی برای صنعت در مقیاس کوچک طراحی شود، اطلاعات سیستم شبکه را حفظ می‌کند و سوابق همه فایل‌های لاگ شبکه را حفظ می‌کند. اطلاعات کامل مهاجم جمع‌آوری و تمام فعالیت‌ها را ثبت می‌کند. Honeypot برای صنعت با مقیاس کوچک، با تنظیم ۲ یا ۳ ابزار با هم پیاده‌سازی می‌شود. این ابزارها برای جمع‌آوری اطلاعات حمله‌کنندگان استفاده می‌شوند. بسته‌های خارج از شبکه می‌توانند وارد سیستم شوند. این می‌تواند برای اسکن پورت به منظور شناخت پورت‌های باز و بسته استفاده شود. کامپیوتر مجازی می‌تواند برای ارائه اطلاعات جعلی به حمله‌کننده عمل کند. مجموعه‌ای از سرویس‌ها بر روی شبکه شبیه‌سازی شده‌اند، به طوری که Honeypot باید شبیه یک ماشین واقعی به حمله‌کننده باشد.

این سرویس‌ها عبارت‌اند از:

- HTTP
- POP۳
- FTP
- TELNET

این‌ها سرویس‌های اصلی هستند که Honeypot می‌تواند کار کند و امنیت شبکه را از هکرها تأمین کند.

هدف از Honeypot

شما می‌توانید با استفاده از Honeypotها از شبکه خود در برابر حملات انسانی غیر خودکار نیز محافظت نمایید. این ایده مبتنی بر فریب یا تهدید است. در این روش شما، مهاجمان را گیج کرده و زمان و منابع آن‌ها را تلف می‌کنید. به طور هم‌زمان سازمان شما قادر است که فعالیت مهاجم را تشخیص داده و در نتیجه برای پاسخگویی و متوقف کردن آن فعالیت زمان کافی در اختیار داشته باشد. این موضوع حتی می‌تواند یک گام نیز فراتر رود، اگر مهاجمان بدانند که سازمان شما از هانی پات استفاده می‌کند ولی ندانند که کدام سیستم‌ها هانی پات هستند، ممکن است به طور کلی از حمله کردن به شبکه شما صرف نظر کنند. در این صورت Honeypot یک عامل تهدید برای مهاجمان به شمار رفته است. یک نمونه از Honeypotهایی که برای این کار طراحی شده‌اند، Honeypot Decepti است.

تشخیص حملات

یک راهی که هانی پات‌ها با استفاده از آن، از سازمان شما محافظت می‌کنند، تشخیص حملات است. از آنجایی که تشخیص، یک اشکال و یا نقص امنیتی را مشخص می‌کند، حائز اهمیت است. صرف نظر از این که یک سازمان تا چه اندازه امن باشد، همواره اشکالات و نقایص امنیتی وجود دارند. چرا که حداقل نیروی انسانی در پروسه امنیت درگیرند و خطاهای انسانی همیشه دردسر سازند. با تشخیص حملات، شما می‌توانید به سرعت به آن‌ها دسترسی پیدا کرده، و خرابی آن‌ها را متوقف ساخته یا کم نمایید.

ثابت شده است که تشخیص، کار بسیار سختی است. تکنولوژی‌هایی مانند سنسورهای سیستم تشخیص نفوذ و لاگ‌های سیستم‌ها، به دلایل مختلف چندان مؤثر نیستند. این تکنولوژی‌ها داده‌های بسیار زیادی تولید کرده و درصد خطای تشخیص

نادرست آن، بسیار بالاست. همچنین این تکنولوژی‌ها قادر به تشخیص حملات جدید نیستند و نمی‌توانند در محیط‌های رمز شده یا IPv٦ کار کنند. به طور معمول هانی پات‌های با تعامل کم، بهترین راه حل برای تشخیص هستند. چرا که به کار گرفتن و نگهداری این هانی پات‌ها ساده‌تر بوده و در مقایسه با هانی پات‌های با تعامل بالا، ریسک کمتری دارند.

پاسخگویی به حملات

Honeypotها با پاسخگویی به حملات نیز می‌توانند به سازمان‌ها کمک کنند. زمانی که یک سازمان یک مشکل امنیتی را تشخیص می‌دهد، چگونه باید به آن پاسخ دهد؟ این مسئله معمولاً می‌تواند یکی از چالش برانگیزترین مسائل یک سازمان باشد. معمولاً اطلاعات کمی درباره اینکه مهاجمان چه کسانی هستند، چگونه به آنجا آمده‌اند و یا اینکه چقدر تخریب ایجاد کرده‌اند وجود دارد. در این شرایط، داشتن اطلاعات دقیق در مورد فعالیت‌های مهاجمان بسیار حیاتی است. دو مسئله با پاسخگویی به رویداد آمیخته شده است. اول اینکه بسیاری از سیستم‌هایی که معمولاً مورد سوء استفاده قرار می‌گیرند، نمی‌توانند برای تحلیل شدن از شبکه خارج گردند. سیستم‌های تجاری مانند Mail Server یک سازمان، به حدی مهم هستند که حتی اگر این سیستم هک شود، ممکن است متخصصان امنیت نتوانند سیستم را از شبکه خارج کنند و برای تحلیل آن بحث نمایند. به جای این کار، آن‌ها مجبورند به تحلیل سیستم زنده در حالی که هنوز سرویس‌های تجاری را ارائه می‌کند، بپردازند. این موضوع باعث می‌شود که تحلیل اتفاقی که رخ داده، میزان خسارت به بار آمده، و تشخیص نفوذ مهاجم به سیستم‌های دیگر سخت باشد.

مشکل دیگر این است که حتی اگر سیستم از شبکه خارج گردد، به حدی آلودگی داده وجود دارد که تشخیص اینکه فرد مهاجم چه کاری انجام داده است بسیار سخت است. منظور از آلودگی داده، داده‌های بسیار زیاد در مورد فعالیت‌های گوناگون (مانند ورود کاربران، خواندن حساب‌های ایمیل، فایل‌های نوشته شده در پایگاه داده و غیره) است که باعث می‌شود تشخیص فعالیت‌های معمول روزانه از فعالیت‌های فرد مهاجم سخت باشد.

هانی پات‌ها برای هر دوی این مشکلات راه حل دارند. آن‌ها می‌توانند به سرعت و سهولت از شبکه خارج گردند تا یک تحلیل کامل بدون تأثیر بر کارهای روزانه انجام گیرد. همچنین از آنجایی که این سیستم‌ها فقط فعالیت‌های خرابکارانه یا تأیید نشده را ثبت می‌کنند، کار تحلیل بسیار ساده‌تر خواهد بود و داده‌های بسیار کمتری باید بررسی شوند. ارزش هانی پات‌ها به این است که آن‌ها قادرند به سرعت اطلاعات عمیق و پرفایده را در اختیار سازمان قرار دهند تا بتواند به یک رویداد پاسخ دهد. هانی پات‌های با تعامل بالا بهترین گزینه برای پاسخگویی هستند. برای پاسخگویی به نفوذگران، شما باید دانش عمیقی در مورد کاری که آن‌ها انجام داده‌اند، شیوه نفوذ، و ابزارهای مورد استفاده آن‌ها داشته باشید. برای به دست آوردن این نوع داده‌ها، شما احتیاج به هانی پات‌های با تعامل بالا دارید.

مزایای استفاده از Honeypot :

- Honeypotها فقط زمانی که کسی یا چیزی با آن‌ها ارتباط برقرار کند داده‌ها را جمع‌آوری می‌نمایند، در نتیجه صرفاً مجموعه‌های بسیار کوچکی از داده‌ها را جمع می‌کنند، که البته این داده‌ها بسیار ارزشمندند. سازمان‌هایی که هزاران پیغام هشدار را در هر روز ثبت می‌کنند، با استفاده از Honeypotها ممکن است فقط صد پیغام هشدار را

ثبت نمایند. این موضوع باعث می‌شود که مدیریت و تحلیل داده‌های جمع‌آوری شده توسط Honeypotها بسیار ساده‌تر باشد.

- Honeypotها موارد خطاهای تشخیص اشتباه را کاهش می‌دهند. یکی از مهم‌ترین چالش‌های اغلب سیستم‌های تشخیصی این است که پیغام‌های هشدار دهنده خطای زیادی تولید کرده و در موارد زیادی، این پیغام‌های هشدار دهنده واقعاً نشان دهنده وقوع هیچ خطری نیستند. یعنی در حالی یک رویداد را تهدید تشخیص می‌دهند که در حقیقت تهدیدی در کار نیست. هر چه احتمال این تشخیص اشتباه بیشتر باشد، تکنولوژی تشخیص دهنده بی‌فایده‌تر می‌شود. Honeypotها به طور قابل توجهی درصد این تشخیص‌های اشتباه را کاهش می‌دهند، چرا که تقریباً هر فعالیت مرتبط با Honeypotها به طور پیش فرض غیرمجاز تعریف شده است. به همین دلیل Honeypotها در تشخیص حملات بسیار مؤثرند.
- Honeypotها می‌توانند حملات ناشناخته را تشخیص دهند. چالش دیگری که در تکنولوژی‌های تشخیصی معمول وجود دارد این است که آن‌ها معمولاً حملات ناشناخته را تشخیص نمی‌دهند. این یک تفاوت بسیار حیاتی و مهم بین Honeypotها و تکنولوژی‌های امنیت کامپیوتری معمولی است که بر اساس امضاهای شناخته شده یا داده‌های آماری تشخیص می‌دهند. تکنولوژی‌های تشخیصی مبتنی بر امضا، در تعریف به این معنا هستند که ابتدا باید هر حمله‌ای حداقل یک بار انجام شده و امضای آن شناسایی گردد و سپس با استفاده از آن امضا، در موارد بعدی شناخته شود. تشخیص مبتنی بر داده‌های آماری نیز از خطاهای آماری رنج می‌برد. Honeypotها طوری طراحی شده‌اند که حملات جدید را نیز شناسایی و کشف می‌کنند. چرا که هر فعالیتی در ارتباط با Honeypotها غیر معمول شناخته شده و در نتیجه حملات جدید را نیز معرفی می‌کند.
- هانی پات‌ها فعالیت‌های رمز شده را نیز کشف می‌کنند. به تدریج که تعداد بیشتری از سازمان‌ها از پروتکل‌های رمزگذاری مانند SSH، IPsec و SSL استفاده می‌کنند، این مسئله بیشتر خود را نشان می‌دهد. Honeypotها می‌توانند این کار را انجام دهند، چرا که حملات رمز شده با هانی پات به عنوان یک نقطه انتهایی ارتباط، تعامل برقرار می‌کنند و این فعالیت توسط Honeypot رمزگشایی می‌شود.
- Honeypot با IPv٦ کار می‌کند. اغلب Honeypotها صرف نظر از پروتکل IP از جمله IPv٦، در هر محیط IP کار می‌کنند.
- Honeypotها بسیار انعطاف‌پذیرند و می‌توانند در محیط‌های مختلفی مورد استفاده قرار گیرند. همین قابلیت انعطاف‌پذیری Honeypotهاست که به آن‌ها اجازه می‌دهد کاری را انجام دهند که تعداد بسیار کمی از تکنولوژی‌ها می‌توانند انجام دهند یعنی جمع‌آوری اطلاعات ارزشمند به خصوص علیه حملات داخلی.
- حتی در بزرگ‌ترین شبکه‌ها Honeypotها به حداقل منابع نیاز دارند. یک کامپیوتر پنتیوم قدیمی و ساده می‌تواند میلیون‌ها آدرس IP یا یک شبکه بسیار بزرگ را نظارت نماید.

نتیجه‌گیری

امنیت شبکه موضوع مهمی است که مدیران را با چالش‌های زیادی روبه‌رو کرده است. استفاده از هانی پات به دلیل کاهش هزینه، مدیریت و تحلیل آسان داده‌های جمع‌آوری شده و همچنین کاهش درصد تشخیص‌های اشتباه، یک راه حل مناسب

برای امن کردن شبکه داخلی است. به دلیل اینکه هانی پات را می‌توانیم با استفاده از ماشین‌های مجازی نیز پیاده‌سازی کنیم، استفاده از آن برای سازمان‌ها احتیاج به تجهیزات پیچیده‌ای ندارد.

هانی پات‌ها فعالیت مهاجم را تشخیص داده و به مدیر شبکه گزارش مفید و ارزشمند ارائه می‌دهند در نتیجه برای پاسخگویی و متوقف کردن آن فعالیت فرصت کافی وجود دارد. همچنین این امکان را فراهم می‌کند که سازمان بتواند تمامی سیستم‌ها را نسبت به حملات مشابه ایمن کند. در نتیجه هانی پات‌ها راه حل‌های مناسبی را برای برقرار کردن امنیت شبکه ارائه می‌دهند.

منابع

Gurleen Singh., Sakshi Sharma, Prabhdeep Singh “Design and develop a Honeypot for small scale organization “in IJITEE. Vol ۲, issue-۳, Feb۲۰۱۳.

Abbas Azimi “Honeypot and Honeynet”

Abhishek Sharma “Honeypots in Network Security” in ijtra. Vol ۱, issue-۵, Nov ۲۰۱۳.

Deniz Akkaya – Fabien Thalgott, “Network Security Using Honeypot” IEEE, June ۲۰۱۰.

Y.K.Jain, S. Singh “Honeypot based Secure Network System” in IJCSE. Vol ۳. No.۲ Feb ۲۰۱۱.

C K Shyamala, N Harini, Dr T R Padomanabhan – Cryptography and Security, May ۲۰۱۱.