دانلودمقاله هانیپات و کاربرد آن در امنیت کامپیوتر و شبکههای کامپیوتری

چکیده

هانیپاتها۱ یک تکنولوژی جدید میباشند که قابلیتهای فراوانی برای جامعه امنیتی دارند. البته مفهوم آن در ابتدا به صورتهای مختلفی تعریف شده بود به خصوص توسط Cliff Stoll در کتاب .« The Cuckoos Egg » از آنجا به بعد بود که هانیپاتها شروع به رشد کردند و به وسیله ابزارهای امنیتی قوی توسعه یافتند و رشد آنها تا به امروز ادامه داشته است. هانیپات یکی از ابزارهایی است که متخصصین برخورد با هکرها و مدیران شبکه از آن برای شناسایی و به دام انداختن هکرها و نفوذگران استفاده میکنند. این مقاله تعریف و شرح واقعی هانیپاتو محل قرار گرفتن هانیپات در سیستم کامپیوتری و کاربرد آن در تامین امنیت کامپیوتر و شبکه های کامپیوتری و بیان منافع و مضرات آنها و اینکه در امنیت کامپیوتر چه ارزشی هائی دارند، و نیز معرفی هانیپات و انواع آن، اهمیت تکنولوژی هانیپات در برقراری امنیت شبکهها و نحوه گرفتار شدن هکرها در دام متخصصین شبکه را مورد بررسی قرار می-دهد.

کلمات کلیدی: هانیپات ، دیواره های آتش، ۲IPS ،IDS2، امنیت کامپیوتر.

مقدمه:

استفاده از شبکههای کامپیوتری در چندین سال اخیر رشد فراوانی کرده و سازمانها و مؤسسات اقدام به برپایی شبکه نمودهاند. هر شبکه کامپیوتری باید با توجه به شرایط و سیاستهای هر سازمان، طراحی و پیادهسازی گردد. در واقع شبکههای کامپیوتری زیر ساختهای لازم را برای به اشتراک گذاشتن منابع در سازمان فراهم میآورند؛ در صورتیکه این زیر ساختها به درستی طراحی نشوند، در زمان استفاده از شبکه مشکلات متفاوتی پیش آمده و باید هزینههای زیادی به منظور نگهداری شبکه و تطبیق آن با خواستههای مورد نظر صرف شود.

چه خوب بود اگر تمامی سیستمهای کامپیوتری از امنیت کامل برخوردار بودند. ولی متاسفانه امنیت کامل شبکههای کامپیوتری محال است و به این زودیها نمیتوان انتظار داشت سیستمهای کامپیوتری از امنیت کامل بهرهمند شوند. زیرا حتی اگر این سیستمها کاملا امن باشند و ورود هرگونه عامل خارجی تهدیدکننده امنیت،

به این سیستمها محال باشد، همچنان امکان سوء استفاده عوامل داخلی در این سیستم ها وجود دارد (صفائی،.(۱۳۸۶

به منظور مقابله با نفوذگران به سیستمها و شبکههای کامپیوتری، روشهای متعددی تحت عنوان روشهای کشف ترافیک مخرب در)IDSسیستم های تشخیص نفوذ) و IPS (سیستم های جلوگیری از نفوذ) ایجاد گردیده است که عمل نظارت بر وقایع اتفاق افتاده در یک سیستم یا شبکه کامپیوتری را بر عهده دارد. روشهای تشخیص مورد استفاده عبارتند از: اکتشاف بر پایه امضا، اکتشاف بر پایه سیاست گذاریهای سازمان، اکتشاف بر پایه وضعیتهای غیر عادی و اکتشاف بر پایه تکنیک ظرف عسل.

اکتشاف بر پایه تکنیک ظرف عسل از یک سرور ساختگی یا زائد برای جذب حملات استفاده مینماید. سیستمهای ظرف عسل به ندرت در حفاظت از محیط بکار گرفته میشوند. فروشندههای آنتی ویروس و سایر عوامل امنیتی تمایل دارند از این سیستمها برای تحقیقات خود استفاده نمایند .(Sullivan ,۲۰۰۷)

هانی پات چیست؟

همانطور که میدانید دیواره های آتش مدت ها مهم ترین و بهترین ابزار امنیتی برای جلوگیری و کشف نفوذ به کامپیوتر ها و شبکه ها بودند. افزایش کمی و کیفی نفوذ و اخلال در اینترنت ، نیاز به استفاده از ابزار کمکی پیشرفته تری در کنار دیواره های آتش را اجتناب ناپذیر می نمود IDS .ها نتیجه منطقی چنین نیازی بودند .البته آنها هیچ گاه جایگزین سلف خود نشدند، بلکه به موازات آنها یک لایه امنیتی اضافی به شبکه ها افزودند IDS .ها در امر کشف و

شناسایی و واکنش نسبت به اخلال و نفوذ باهوش تر و انعطاف پذیرتر عمل می کنند .دراین قسمت به معرفی عنصر امنیتی دیگری بنام هانی پات میپردازیم .

هانی پات یک منبع سیستم اطلاعاتی با اطلاعات کاذب است که برای مقابله با هکرها و کشف و جمعآوری فعالیتهای غیرمجاز در شبکههای رایانهای بر روی شبکه قرار میگیرد.

هانی پاتها کامپیوترهایی هستند که ابزاری برای مصالحه هستند، کامپیوترهایی که یا واقعی هستند و یا شبیهسازی شدهاند. در نمونههای اولیه، هانیپاتها گرایش به مطالعه و طعمهدادن به مهاجمین انسانی داشتهاند، اما به همان اندازه میتوانند برای دستگیری کرمها نیز استفاده شوند (بشری راد ، حبیبی لشکری ، ۱۳۹۱).

قدم اول در فهم اینکه هانی پاتها چه می باشند بیان تعریفی جامع از آن است. هانی پات یک منبع سیستم اطلاعاتی می باشد که بر روی خود اطلاعات کاذب و غیرواقعی دارد و با استفاده از ارزش و اطلاعات کاذب خود سعی در کشف و جمع آوری اطلاعات و فعالیت های غیرمجاز و غیر قانونی بر روی شبکه می کند. به زبان ساده هانی پات یک سیستم یا سیستمهای کامپیوتری متصل به شبکه و یا اینترنت است که دارای اطلاعات کاذب بر روی خود می باشد و از عمد در شبکه قرار می گیرد تا به عنوان یک تله عمل کرده و مورد تهاجم یک هکر یا نفوذگر قرار بگیرد و با استفاده از این اطلاعات آنها را فریب داده و اطلاعاتی از نحوه ی ورود آنها به شبکه و اهدافی که در شبکه دنبال می کنند جمع آوری کند.

هم چنین هانی پات یک ماشین ویژه در شبکه است که به عنوان طعمه برای نفوذگران استفاده میشود. به طور عمدی بر روی آن سیستم عامل آلوده به یک Trojan Horse1،Back Door2 یا سرویسدهندهای ضعیف و دارای اشکال نصب میشود تا به عنوان یک ماشین قربانی، نفوذگران را به خود جذب کرده و مشغول نگه دارد.

همچنین ممکن است بر روی چنین ماشینی اطلاعات غلط و گمراه کنندهای برای به اشتباه انداختن نفوذگر نیز گذاشته شود.

یک سیستم هانی پاتعملاً هیچ فایدهای برای مقاصد سرویس دهی ندارد بلکه ماشین فداکاری است که با جذب نفوذگران و گمراه کردن آنها با اطلاعات غلط، از دسترسی به سرویس دهندههای حساس جلوگیری میکند. اطلاعات غلط ممکن است ساعتها یک نفوذگر را معطل کند. در ضمن تشخیص این نکته که سیستم موردنظر آیاواقعاً ضعف دارد یا آنکه یک هانی پات است برای نفوذگر چندان ساده نیست.

به صورت کلی تمامی هانی پاتها به همین صورت کار می کنند. آنها یک منبعی از فعالیتهای بدون مجوز می باشند. به صورت تئوری یک هانی پات نباید هیچ ترافیکی از شبکه ما را اشغال کند زیرا آنها هیچ فعالیت قانونی ندارند. این بدان معنی است که تراکنش های با یک هانی پات تقریبا تراکنش های بی مجوز و یا فعالیتهای بد اندیشانه می باشد. یعنی هر ارتباط با یک هانی پات می تواند یک دزدی ، حمله و یا یک تصفیه حساب باشد. حال آنکه مفهوم آن ساده به نظر می رسد و همین سادگی موجب میزان استفاده شگفت انگیز از هانی پات ها شده است .

در جنگ بین نفوذگران و مدیران امنیت شبکه، داشتن اطلاعات نشانه قدرت است. به عنوان یک مدیر امنیت شبکه، هر چه بیشتر در مورد دشمنتان و روشهای حمله او بدانید بهتر میتوانید از خودتان در مقابل او دفاع کنید.استفاده از هانی پات ها یکی از روشهایی است که میتوانیم اطلاعاتی در مورد دنیای نفوذگران به دست آوریم.

یک هانی پات عنصر یا عضوی از شبکه است که منابع و داده هایش را در معرض حمله و نفوذ قرار داده ایم. این حرف یعنی اینکه هرچیزی را که به عنوان هانی پات در شبکه در نظر گرفته ایم ، حتما و عمدا می خواهیم مورد نفوذ ، بررسی ، حمله و سوء استفاده قرار گیرد.پس یادمان نرود، هانی پات ها برای ما راه حل یا به اصطلاح ۳Solution نیستند. آنها قرار نیست که هیچ چیز خرابی را آباد کنند! اما با این حال یک ابزار امنیتی خوب به حساب می آیند.این که چگونه از این ابزار استفاده می کنید، بستگی به اهداف مورد نظر شما دارد.یک هانی پات ممکن است صرفا سیستمی باشد که یک یا چند سیستم یا برنامه دیگر را شبیه سازی میکند.ممکن است محیطی برای به دام انداختن نفوذ گران باشد و یا یک سیستم استاندارد از پیش ساخته شده باشد.صرف نظر از اینکه یک هانی پات ایجاد می کنیم و از آن استفاده می کنیم ، کارایی و ارزش آن به این است که مورد حمله قرار گیرد.

اهداف

اهدافی که هانی پاتها دنبال میکند را می توان به صورت زیر نام برد ۱-۳ پیشگیری: با منابع غیر معتبری که در اختیار حمله کنندگان قرار می دهد، در واقع از در خطر قرار گرفتن سیستم واقعی جلوگیری می شود و این یک عمل پیشگیرانه است.

۲-۳ کشف: در اغلب شبکه های موجود در سازمانها، فعالیت محصولات دارای پیچیدگی فراوانی می باشند که کشف حملات را مشکل می سازد. حال انکه در هانی پات این پیچیدگی وجود ندارد و جریانهای ورود و خروج به آن کاملا روشن است.

۳-۳ واکنش: فعالیت محصولات اشاره شده در بالا،باعث می شود تیم پاسخگویی به حوادث نتواند به درستی تشخیص دهد که چه اتفاقی افتاده است.از طرف دیگر در اغلب مواقع تیم پاسخگویی به اختلالات قادر نیست

اطلاعاتی از سیسیتم در معرض خطر قرار گرفته، جمع آوری کند ولی برای سیستم هانی پات چنین محدودیتی وجود ندارد.

۳-۴ پژوهش:یکی از مهمترین مباحث در امنیت،گرد آوری(داشتن) اطلاعات دشمن است.هانی پات به عنوان یک ابزار پژوهشی، در نیل به این هدف،کمک شایانی به سازمانهای پژوهشی و دانشگاهی می کند.(دهستانی،(۱۳۹۰

نحوه تشخیص حمله و شروع عملکرد هانی پات :

در مسیر منتهی به هانی پات نباید هیچ ترافیکی ایجاد شود یعنی هر گونه ارتباطی با هانی پات فعالیت غیرمجاز و غیر قانونی محسوب شده و می تواند یک دزدی ، حمله و یا سرقت محسوب شود.

بتازگی یک ربات به سراغ سایتی۱ رفت تا بلکه بتواند آدرسهای ایمیل را بیابد. اما چون این وب سایت با ابزار پروژه هانی پات تجهیز شده بود میتوانست بفهمد که چه شرکتی اسپم میفرستد. هانی پات شبیه یک تله برای اسپمرها عمل میکند بدین شکل که وقتی یک جستجوگر ایمیل آدرس به وب سایت میرسد به صفحه ای برخورد میکند که هانی پات درست کرده و در آن یک آدرس ایمیل منحصر بفرد گذاشته است. این ایمیل آدرس به نحوی تنظیم میشود که مطابق آدرس IP2 همان جستجوگر برچسب میخورد. هانی پات میتواند آدرس IP ربات و روز و زمان برداشت صفحه ساختگی را ثبت کند و هر ایمیلی که به آدرس ایمیل کنترلی ارسال میشود را دریافت میکند. آدرسهای ایمیل کنترلی، منحصر بفرد هستند لذا پروژه میتواند آدرس IP های رباتها را جمع کند و هر ایمیل ارسالی را ثبت نماید بدین ترتیب هر سایتی میتواند نهایتا جستجوگر غیرقانونی و شرکتی که در ورای آن قرار دارد را شناسایی نماید. با این شناسایی قدم بعدی آغاز میشود و آن اقدام وب مسترها برای بلوک کردن ربات جستجوگر است. در واقع چون در این پروژه بمرور لیستی از آدرسهای IP اسپمرها تهیه و در اختیار قرار میگیرد، میتوان تمام آنها را بلوک کرد.

دلایل استفاده از هانی پات
هانی پات ها به دو دلیل استفاده میشوند :

اول این که نقاط ضعف سیستم را بشناسیم. مدیر سیستم میتواند با مشاهده تکنیکها و روشهای استفاده شده توسط نفوذگر بفهمد سیستم چگونه شکسته میشود و نقاط آسیبپذیر سیستم را شناسایی و نسبت به ترمیم آنها اقدام کند.

دلیل دوم جمعآوری اطلاعات لازم برای تعقیب و ردگیری نفوذگران است. با توجه به آنکه نفوذگر یک سیستم ضعیف و آسیبپذیر را در شبکه کشف میکند بنابراین تمام تلاشهای بعدی او پیرامون سیستم هانی پات (که یک هدف قلابی است) متمرکز میشود. میتوان یک سیستم تشخیص نفوذ (IDS) را در کنار این سیستم نصب کرد تا تلاشهای نفوذگران برای حمله به این هدف قلابی را گزارش دهد و شما بتوانید این موضوع و مبدا آن را پیگیری کنید.

این در حالی است که هانی پات همزمان از شبکه واقعی در برابر حملات مراقبت میکند.

هدف اصلی یک هانی پات شبیهسازی یک شبکه است که نفوذگران سعی میکنند به آن وارد شوند. اطلاعاتی که بعد از حمله به یک هانی پات به دست میآید، میتواند برای کشف آسیبپذیریهای شبکه فعلی و رفع آنها استفاده شود.

فواید هانی پات داده های کوچک دارای ارزش فراوان:

هانی پاتها حجم کوچکی از داده ها را جمع آوری می کنند. به جای اینکه ما در یک روز چندین گیگابایت اطلاعات را در فایلهای ثبت رویدادها ذخیره کنیم توسط هانی پات فقط در حد چندین مگابایت باید ذخیره کنیم. به جای تولید ۱۰۰۰۰ زنگ خطر در یک روز آنها فقط یک زنگ خطر را تولید می کنند. یادتان باشد که هانی پات ها فقط فعالیتهای غیر مجاز را ثبت می کنند و هر ارتباطی با هانی پات می تواند یک فعالیت بدون مجوز باشد. به همین دلیل اطلاعات هر چند کوچک هانی پات دارای ارزش زیادی می باشد زیرا آنها توسط هانی پات ضبط شده اند. این بدان معنا می باشد که تجزیه و تحلیل اطلاعات یک هانی پات آسانتر (و ارزانتر) از اطلاعات ثبت شده به صورت کلی می باشد.

ابزارها و تاکتیکها ی جدید :

هانی پات ها طراحی شده اند تا هر چیزی که به سمتشان منتهی می شود ثبت کنند بنابراین هانی پات می تواند ابزارها و تاکتیکهایی جدید را که هکرها به کمک آنها به سیستم حمله می کنند را ثبت کند.