آشنایی با Honeypot ها

Honeypot ها یک تکنولوژی جدید می باشند 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 Honeypot ها شروع به رشد کردند و به وسیله ابزارهای امنیتی قوی توسعه یافتند و رشد آنها تا به امروز ادامه داشته است. هدف این مقاله تعریف و شرح واقعی Honeypot می باشد و بیان منفعت ها و مضرات آنها و اینکه آنها در امنیت چه ارزشی برای ما دارند.

تعریف

قدم اول در فهم اینکه Honeypot چه می باشند بیان تعریفی جامع از آن است. تعریف Honeypot می تواند سخت تر از آنچه که به نظر می رسد باشد. Honeypot ها از این جهت که هیچ مشکلی را برای ما حل نمی کنند شبیه دیواره های آتش و یا سیستمهای تشخیص دخول سرزده نمی باشند. در عوض آنها یک ابزار قابل انعطافی می باشند که به شکلهای مختلفی قابل استفاده هستند.آنها هر کاری را می توانند انجام دهند از کشف حملات پنهانی در شبکه های IPv6 تا ضبط آخرین کارت اعتباری جعل شده! و همین انعطاف پذیریها باعث شده است که Honeypot ها ابزارهایی قوی به نظر برسند و از جهتی نیز غیر قابل تعریف و غیر قابل فهم!!

البته من برای فهم Honeypot ها از تعریف زیر استفاده می کنم:

یک Honeypot یک منبع سیستم اطلاعاتی می باشد که با استفاده از ارزش کاذب خود اطلاعاتی از فعالیتهای بی مجوز و نا مشروع جمع آوری می کند.

البته این یک تعریف کلی می باشد که تمامی گونه های مختلف Honeypot ها را در نظر گرفته است. ما در ادامه مثالهای مختلفی برای Honeypot ها و ارزش امنیتی آنها خواهیم آورد. همه آنها در تعریفی که ما در بالا آورده ایم می گنجند ، ارزش دروغین آنها برای اشخاص بدی که با آنها در تماسند. به صورت کلی تمامی Honeypot ها به همین صورت کار می کنند. آنها یک منبعی از فعالیتها بدون مجوز می باشند. به صورت تئوری یک Honeypot نباید هیچ ترافیکی از شبکه ما را اشغال کند زیرا آنها هیچ فعالیت قانونی ندارند. این بدان معنی است که تراکنش های با یک Honeypot تقریبا تراکنش های بی مجوز و یا فعالیتهای بد اندیشانه می باشد. یعنی هر ارتباط با یک Honeypot می تواند یک دزدی ، حمله و یا یک تصفیه حساب می باشد. حال آنکه مفهوم آن ساده به نظر می رسد (و همین طور هم

است) و همین سادگی باعث این هم موارد استفاده شگفت انگیز از Honeypot ها شده است که من در این مقاله قصد روشن کردن این موارد را دارم.

فواید Honeypot ها

Honeypot مفهوم بسیار ساده ای دارد ولی دارای توانایی های قدرتمندی می باشد.

1. داده های کوچک دارای ارزش فراوان: Honeypot ها یک حجم کوچکی ار 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 Honeypot فقط در حد چندین مگابایت باید ذخیره کنیم. به جای تولید 10000 زنگ خطر در یک روز آنها فقط 1 زنگ خطر را تولید می کنند. یادتان باشد که Honeypot ها فقط فعالیتهای ناجور را ثبت می کنند و هر ارتباطی با Honeypot می تواند یک فعالیت بدون مجوز و یا بداندیشانه باشد. و به همین دلیل می باشد که اطلاعات هر چند کوچک Honeypot ها دارای ارزش زیادی می باشد زیرا که آنها توسط افراد بد ذات تولید شده و توسط Honeypot ضبط شده است. این بدان معنا می باشد که تجزیه و تحلیل اطلاعات یک Honeypot آسانتر (و ارزانتر) از اطلاعات ثبت شده به صورت کلی می باشد.

2. ابزار و تاکتیکی جدید : Honeypot برای این طراحی شده اند که هر چیزی که به سمت آنها جذب می شود را ذخیره کنند. با ابزارها و تاکتیکهای جدیدی که قبلا دیده نشده اند.

3. کمترین احتیاجات: Honeypot ها به کمترین احتیاجات نیاز دارند زیرا که آنها فقط فعالیتهای ناجور را به ثبت می رسانند. بنابراین با یک پنتیوم قدیمی و با 128 مگابایت RAM و یک شبکه با رنج B به راحتی می توان آن را پیاده سازی کرد.

4. رمز کردن یا IPv6 : بر خلاف برخی تکنولوژیهای امنیتی (مانند IDS ها) Honeypot خیلی خوب با محیطهای رمز شده و یا IPv6 کار می کنند. این مساله مهم نیست که یک فرد ناجور چگونه در یک Honeypot گرفتار می شود زیرا Honeypot ها خود می توانند آنها را شناخته و فعالیتهای آنان را ثبت کنند.

مضرات Honeypot ها

شبیه تمامی تکنولوژیها ، Honeypot ها نیز دارای نقاط ضعفی می باشند. این بدان علت می باشد که Honeypot ها جایگزین تکنولوژی دیگری نمی شوند بلکه در کنار تکنولوژیهای دیگر کار می کنند.

1- محدودیت دید : Honeypot ها فقط فعایتهایی را می توانند پیگیری و ثبت کنند که به صورت مستقیم با آنها در ارتباط باشند. Honeypot حملاتی که بر علیه سیستمهای دیگر در حال انجام است را نمی توانند ثبت کنند به جز اینکه نفوذگر و یا آن تهدید فعل و انفعالی را با Honeypot داشته باشد.

2- ریسک : همه تکنولوژیهای امنیتی دارای ریسک می باشند. دیوارهای آتش ریسک نفوذ و یا رخنه کردن در آن را دارند. رمزنگاری ریسک شکستن رمز را دارد، IDS ها ممکن است نتوانند یک حمله را تشخیص دهند. Honeypot ها مجزای از اینها نیستند. آنها نیز دارای ریسک می باشند. به خصوص اینکه Honeypot ها ممکن است که ریسک به دست گرفتن کنترل سیستم توسط یک فرد هکر و صدمه زدن به سیستمهای دیگر را داشته باشند. البته این ریسکها برای انواع مختلف Honeypot ها فرق می کند و بسته به اینکه چه نوعی از Honeypot را استفاده می کنید نوع و اندازه ریسک شما نیز متفاوت می باشد.ممکن است استفاده از یک نوع آن ، ریسکی کمتر از IDS ها داشته باشد و استفاده از نوعی دیگر ریسک بسیار زیادی را در پی داشته باشد.ما در ادامه مشخص خواهیم کرد که چه نوعی از Honeypot ها دارای چه سطحی از ریسک می باشند.