نما
مجله الکترونیکی پژوهشگاه اطلاعات و مدارک علمی ایران
شماره دوم دوره پنجم
تاریخ انتشار این مقاله: ۵ آذر ۱۳۸٤

برقراری امنیت شبکه با Honeypot

گردآوري : معصومه صحرائی کلجاهی
kalejahi@hotmail.com
دانشجوي دوره کارشناسي ناپيوسته نرم افزار کامپيوتر
دانشگاه جامع علمی کاربردی مرکز تراکتورسازي تبريز

چکیده :
همه ما بارها و بارها شنیده ایم که فلان هکری را دستگیر کردند ویا فعالیتهای غیر قانونی عده ای از خرابکاران اینترنتی را برملا ساختند و همچنین می دانیم که هکرها و نفوذگران افراد بسیار باهوش وشاید هم تیز هوشی هستند که نسبت به کاری که انجام می دهند اطلاع کافی دارند و به راحتی اثری از فعالیتهای خود بر جا نمی گذارند که قابل شناسائی باشند پس چگونه این نوابغ روزگار در دام مأموران برقراری امنیت شبکه گرفتار می شوند ؟Honeypot یکی از ابزارهائی است که متخصصین برخورد با هکرها و مدیران شبکه از آن برای شناسایی و به دام انداختن هکرها ونفوذگران استفاده می کنند . در این مقاله ضمن معرفی Honeypot و انواع آن ،اهمیت تکنولوژی Honeypot در برقراری امنیت شبکه ها و نحوه گرفتار شدن هکرها در دام متخصصین شبکه را بررسی می کنیم .
کلیدواژه ها : Honeypot - امنیت شبکه های کامپیوتری

تعریفHoneypot :
یک منبع سیستم اطلاعاتی می باشد که بر روی خود اطلاعات کاذب وغیر واقعی دارد وبا استفاده از ارزش واطلاعات کاذب خود سعی در کشف وجمع آوری اطلاعات و فعالیت های غیرمجاز و غیر قانونی بر روی شبکه
می کند.به زبان ساده Honeypot 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 (Attacker) قرار بگیرد و با ا ستفاده 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.
نحوه تشخیص حمله و شروع عملکرد Honeypot :
در مسیر منتهی به Honeypot نباید هیچ ترافیکی ایجاد شود یعنی هر گونه ارتباطی با Honeypot فعالیت غیرمجاز و غیر قانونی محسوب شده و می تواند یک دزدی ، حمله و یا سرقت محسوب شود.

مزایای Honeypot :
۱- جمع آوری بسته های اطلاعاتی کم حجم ولی با ارزش :
Honeypot ها حجم کوچکی از اطلاعات را جمع آوری می کنند .مثلاً به جای ثبت روزانه ۱GB داده توسط سایر تکنولوژی های برقراری امنیت اطلاعات ، Honeypot مثلاً ۱MB اطلاعات جمع آوری می کند ولی چون مطمئن هستیم که اطلاعاتی که یک Honeypot جمع آوری می کند مربوط به فعالیتی غیر مجاز است در نتیجه این اطلاعات بسیار مفید بوده و تجزیه و تحلیل حجم کوچکی ازاطلاعات آسان و ارزان است.
۲- ابزارها و تاکتیکها ی جدید :
Honeypot ها طراحی شده اند تا هر چیزی که به سمتشان منتهی می شود ثبت کنند بنابراین Honeypot می تواند ابزارها و تاکتیکهایی جدید را که هکرها به کمک آنها به سیستم حمله می کنند را ثبت کند.

۳- نیاز به کمترین سخت افزار برای پیاده سازی :

در یک کامپیوتر Pentium که دارای ۱۲۸MBRAM است قابل پیاده سازی است.
۴- قابل پیاده سازی در محیط های IPV6 و رمز شده :
بر خلاف اغلب تکنولوژیهای امنیت (مثل سیستمهایIDS) که در محیط های رمز شده بخوبی کارنمی کنند Honeypot به راحتی قابل پیاده سازی در این محیط ها است و در این محیط ها به خوبی کار می کند.
۵- سادگی :
Honeypot ها بسیار ساده اند زیرا الگوریتم پیچیده ای ندارند که بخواهند توسعه یابند جداول حالت ندارند که نیاز به پشتیبانی داشته باشند.
۶-شناسایی نقاط ضعف سیستم :
مدیر سیستم می تواند با مشاهده تکنیک ها و روشهای استفاده شده توسط نفوذگر بفهمد که سیستم چگونه شکسته می شود و نقاط آسیب پذیر سیستم را شناسایی و نسبت به ترمیم آنها اقدام کند.هدف اصلی یکHoneypot شبیه سازی یک شبکه است که نفوذگران سعی می کنند به آن وارد شوند اطلاعاتی که بعد از حمله به یکHoneypot به دست می آید می تواند برای کشف آسیب پذیری های شبکه فعلی و رفع آنها استفاده شود.

تقسیم بندی Honeypot از نظر کاربرد :

۱)Production Honeypot
۲)Research Honeypot

Production Honeypot :

این نوع سیستم وقتی که سازمان می خواهد شبکه و سیستم هایش را با کشف و مسدود کردن نفوذگران حفاظت کند و نفوذگر را از طریق قانون در دادگاه مورد پیگیرد قرار دهد مورد استفاده قرار می گیرد.
Honeypot هایی که کاربرد Production دارند به سه طریق می توانند در برابر حملات از شبکه محافظت کنند .
۱)به روش Prevention (پیشگیری)
۲)به روش Detection (کشف یا شناسايي)
۳)به روش Response (پاسخ)

Prevention :

در بعضي از حملات نفوذگران با استفاده از ابزارهایی رنجی از شبکه ها را پویش می کنند تا آسیب پذیری سرورهای موجود در شبکه راشناسایی کنند این ابزارها پس از پیدا کردن آسیب پذیریهای موجود در سیستم به این سیستمها حمله می کنند در روش پیشگیریHoneypot سرعت این گونه حملات را کند می کند و حتی بعضی اوقات آنها را متوقف نیز می کند به این دسته از Honeypotها،Honeypotهاي چسبنده (Sticky) مي گویند در این روش Honeypot هنگام پویش توسط نفوذگر نسبت به آدرسهایی که در شبکه موجودنیست واکنش نشان میدهد Labrea Tarpit جزو این دسته از Haneypot ها است .
به طور کلی هدف پیشگیری (Prevention) کند کردن سرعت عملیات نفوذگر و توقف حمله است.
Detection (کشف یا شناسايي) :
وظیفه اش عمل کشف و شناسایی ناتوانی های بخش پیشگیری است کشف یک حمله کار بسیارمشکلی است. وقتی یک حمله شناسایی شود می توان خیلی سریع به آن واکنش نشان دادو آن را متوقف و یا حداقل اثرش را کم کرد می توان از تکنولوژیهای امنیتی مثل IDSو فایلهاي ثبت وقایع(Log) در مرحله شناسایی استفاده کرد ولی بدلیل اینکه این تکنولوژی ها داده های زیادی را ثبت می کنند تجزیه و تحلیل آنها زمانبر است و بسیاری از این داده ها غیر مفید بوده و در شناسایی نفوذگر و اهدافش ما را کمک نمی کنند و در محیط های رمز شده نیز بخوبی کار
نمی کنند.Honeypot ها در کشف و ردیابی یک حمله نسبت به تکنولوژیهای مذکور برتری دارند.Honeypotها داده های کم و با درجه اطمینان درستی بالاتری جمع آوری می کنند که تجزیه و تحلیل آنها آسان بوده و ارزش بیشتری دارند. همچنین Honeypotها در محیط های رمز شده نیز می توانند بخوبی کار کنند.

Response (پاسخ) :

یکی از چالشهایی که هر سازمانی می تواند با آن روبرو شود این است که بعد از شناسایی و کشف حمله چگونه به آن پاسخ دهد معمولا در پاسخ مناسب به یک حمله دو مشکل وجود دارد. اول اینکه اکثر سیستمهایی که مورد حمله قرار

گرفته اند را نمی توان بخاطر تجزیه و تحلیل مناسب از کار انداخت زیرا online بودن آنها امری ضروری و حیاتی است دوم اینکه حتی اگر سیستم را نیز از کار بیاندازیم به دلیل وجود کثرت داده ها در سیستم تشخیص داده های متعلق به نفوذگر آسان نیست. بنابراین استفاده از Honeypot در چنین سازمانی این امکان را فراهم
می کند که درمواقع لزوم برای تجزیه وتحلیل کامل داده ها آنها را از شبکه خارج کنیم بدلیل اینکه Honeypot همیشه فعاليتهاي غير قانوني و بد انديشانه را ذخيره می کند بنابراین مطمئن هستیم که اطلاعات موجود در آنها مربوط به یک هکر و یا یک نفوذگر است و به همین دلیل است که تجزیه وتحلیل یکHoneypot هك شده بسیار آسانتر از یک سیستم واقعی است ودر نتیجه می توان در برابر حمله پاسخ سریع ومؤثری داد.

Research Honeypot :

اين نوع سيستم وقتي كه سازمان مي خواهد فقط امنیت شبکه وسیستمهای خود را با آموختن روشهای نفوذ، منشأ نفوذ، ابزارها و Exploit هاي مورد استفاده نفوذگر مستحکم تر کند، استفاده می شود.

تقسیم بندی Honeypot از نظر میزان تعامل با نفوذگر :

Honeypot ها از لحاظ میزان تعامل ودرگیری با نفوذگر به سه دسته تقسیم می شود.

1)Low Interaction Honeypots (Honeypot هاي با تعامل كم)

2)Medium Interaction Honeypots (Honeypot هاي با تعامل متوسط)

3)High Interaction Honeypots (Honeypot هاي با تعامل بالا)

Interaction نوع ارتباطی که نفوذگر با Honeypot دارد را مشخص می کند.

Low Interaction Honeypots :

ارتباط وفعالیتی محدود با نفوذگر دارند ومعمولاً با سرویسها وسیستم عاملهای شبیه سازی شده کار می کنند وسطح فعالیت نفوذگر را محدود به سطوح شبیه سازی شده می کنند. به عنوان مثال Low Interaction honeypot مي تواند شامل یک WindowsServer2000 به همراه سرویسهاي مثل Telnet و FTP باشد. یک نفوذگر می تواند ابتدا با استفاده از Telnet روي Honeypot نوع سیستم عامل آن را تشخیص داده سپس با حدس زدن رمز عبور و یا با هر روش دیگری وارد شبکه شود بدون اینکه اطلاع داشته باشد که در یک Honeypot گرفتار شده است. بر اساس فعالیتی که نفوذگر در Honeypot انجام مي دهد.Honeypot مي تواند اطلاعات زیر را جمع آوری کرده و در اختیار متخصص شبکه قرار دهد.

۱) زمان نفوذ نفوذگر و یا هکر به سیستم

۲) پروتکلی که از آن استفاده کرده

۳) آدرس FTP مبدا ومقصد

در این نوع Honeypot ، نفوذگر نمی تواند هیچ گونه ارتباطی با سیستم عامل برقرار کندو این مسأله میزان خطر را کاهش میدهد چون پیچیدگیهای سیستم عامل حذف می شود وبه دلیل اینکه ما سطح فعالیت نفوذگر را محدود کرده ایم بنابراین اعمالی که نفوذگرانجام می دهد محدود شده ودر نتیجه Honeypot اطلاعات محدودی را می تواند ثبت کند. این نوع Honeypot فقط قادر به شناسایی حمله های شناخته شده است ونمی تواند حمله های ناشناخته را تشخیص دهد. سادگی نگهداری وتوسعه Honeypot کم واکنش همچنین پایین بودن ریسک خطر آن از نقاط قوت Honeypot کم واکنش محسوب می شود.

ازاین Honeypotها میتوان برای اهداف Production استفاده کرد.

Medium Interaction Honeypots (Honeypot با تعامل متوسط) :

Honeypot با تعامل متوسط در مقایسه با Honeypot نوع کم واکنش امکان بیشتری برای تعامل با نفوذگر فراهم
می کند ولی هنوز هم نفوذگر هیچ ارتباطی با سیستم عامل نداردDaemonهاي جعلی فراهم شده پیشرفته ترند و دانش بیشتری راجع به سرویسهایارائه شده دارند. در این حالت میزان خطر افزایش می یابد. احتمال اینکه نفوذگر یک حفره امنیتی یا یک نقطه آسیب پذیری پیدا کند بیشتر است زیرا پیچیدگی Honeypot افزایش می یابد نفوذگر امکان بیشتری برای ارتباط با سیستم وبررسی آن دارد و راحتتر فریب می خورد. همچنین با توجه به تعامل بیشتر، امکان انجام حمله های پیچیده تری وجود دارد که می توان با ثبت و آنالیز کردن آنها به نتایج دلخواه دست یافت. همانطوریکه گفته شد نفوذگر هیچ ارتباطی با سیستم عامل ندارد و در سطح برنامه های کاربردی فعالیت می کند. توسعه یک Honeypot با تعامل متوسط کاری پیچیده و زمانبر است. باید دقت شود که تمام Daemonهای جعلی تا جایی که ممکن است ایمن شوند. نسخه های توسعه یافته

ایـن سـرویسـها نبـاید دارای همـان آسـیب پذیـری هـای نسـخه های واقعی باشند زیرا این اصلي ترین دلیل جایگزینی آنها با نسـخه هـای جعـلی اسـت. کسـی که می خواهد چنین سیستمی را طراحی و پیاده سازی کند، باید از دانش خوبی در مورد پروتکلهـا، سـرویسـها و برنامـه هـای کـاربردی ارائـه شـده بـرخوردار باشـد ازایـن Honeypotهـا میتـوان هـم برای اهداف دسته Research و هم برای اهداف دسته Production استفاده کرد.

High Interaction Honeypot :

یـکی از اهـداف نفوذگرامکـان دسترسـی بـه اطلاعـات در ماشـینی کـه به اینترنت وصل است می باشد این نوع Honeypot چنیـن امکـانی را در اختیـار نفوذگر قرار می دهد. به محض اینکه نفوذگر این امکان را پیدا کند کار اصلی او شروع می شود در ایـن نـوع Honeypot مـا یـک سیسـتم واقـعی را در اختیـار نفوذگـر قـرار مـی دهیم و هیچ چیزی شبیه سازی شده نیست و نفوذگـر بـا سیسـتم عـامل واقعی و شبکه واقعی سرو کار دارد و میزان دسترسی وی به شبکه بیشتر است در نتیجه میزان عمـلی که می تواند انجام دهد بیشتر شده و Honeypot می تواندفعالیت بیشتری از نفوذگر و اهداف مورد نظر وی جمع آوری کند.ازاین Honeypotها میتوان برای اهداف دسته Research استفاده کرد.

مزایای استفاده از High Interaction Honeypot :

متخصص شبکه با تجزیه و تحلیل اطلاعات Honeypot می تواند اطلاعات زیر را در مورد نفوذگر بدست آورد.

- نفوذگران بیشتر از چه ابزارها و Exploit هایی استفاده می کنند
- از چه کشورهایی هستند
- به دنبال چه نقاط آسیب پذیری هستند
- میزان دانش آنها درمورد نفوذگری
- جمع آوری اطلاعات واسناد زیاد برای تحلیل
- بـه دلیل وسیع بودن سطح فعالیت نفوذگر اغلب این نوع Honeypot ها رفتارهایی ازفردنفوذگررا به مانشان می دهند که ما انتظارنداشته ایم ویا نمی توانسته ایم حدس بزنیم.

معایب استفاده از High Interaction Honeypot :

- طراحی ، مدیریت ونگهداری آن فوق العاده زمانبر است
- سیستم باید دائماً تحت نظرباشد درغیر این صورت نه تنها هیچ کمکی نمی کند بلکه خودش به عنوان یک نقطه خطریا حفره امنیتی مطرح می شود
- دارای ریسک بالا

زیـرا نفوذگـر یـک سیسـتم واقـعی رادراختیـار دارد وممـکن اسـت بـه سیسـتم هـای اصـلی شـبکه صـدمه بـزند .بنابراین هیچ سیستمی بر روی شبکه را نمی توان امن در نظر گرفت .

نتیجه گیری:

بـا توجـه بـه گسـترش کاربرد کامپیوتر در جوامع بشری ،مکانیزه کردن اطلاعات وتبادل آن امری اجتناب ناپذیر است.هر سیستم مکـانیزه ای آسـیب پذیـری خـاص خـود را دارد. تبادل اطلاعات از طریق شبکه های کامپیوتری و مخصوصاً اینترنت آسیب پذیری وریسـک تغییرمحتویـات آن توسـط نفوذگـر ،هکـرو حتـی صـدمه دیـدن سیسـتم را دارد.بنابراین حفظ امنیت سیستم واطلاعات ضـروری مـی باشـد. اسـتفاده از تکنولـوژی های برقراری امنیت شبکه تا حدی می تواند این ریسک را کاهش دهد.Honeypot یـکی از ایـن تکنولـوژی هایی است که با شناسایی اهداف واعمال نفوذگر ونقاط ضعف سیستم ، در کنار سایر تکنولوژی های امنیتی مارادر حفظ امنیت سیستم مان یاری می نماید.

تقدیر وتشکر :

در نهـایت از زحمـات اسـتاد محتـرم جنـاب آقـای مهنـدس میزرابیگی که درتهیه این مقاله اینجانب را یاری فرمودند کمال تشکر وقدردانی را دارم .

منابع: