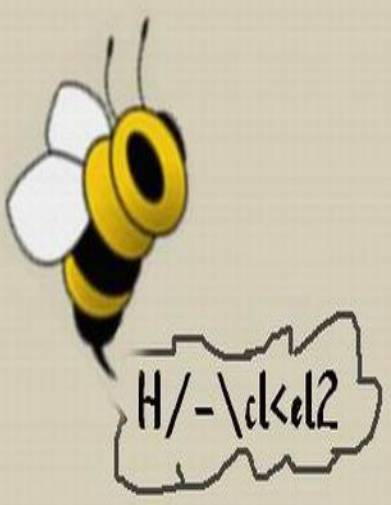
Honey Pot



Author : Satanic Soulful

Satanic Hell

جهنم شیطانی

Honey Pot

مباحثی پیرامون هونی پوت ها

نویسنده: **Satanic Soulful**

تاریخ:10/1/1384

Contact:
Satanic.Soulful@GMail.Com
Satanic_Soulful@Yahoo.Com

Special Tnx 2:
Hell Hacker - Phacker_ir - I_Love_U_mct - **B0rn2h4k**
& X Hulk

ملاحضات:
لازم به تذکر است کلیه مطالب گفته شده تنها جنبه آموزشی دارد و هر گونه استفاده غیر آموزشی به عهده خود کاربر می باشد و نویسنده این مقاله و مدیریت سایت پرشین هکرز و جهنم شیطانی هیچ گونه مسولیتی نسبت به استفاده نادرست از این مقاله را برعهده نمی گیرند!

استفاده از مطالب این مقاله با ذکر نام نویسنده و همچنین گروهای مربوط بلامانع است.

منابع:

ژورنال سیاه – گروه امنیتی کلاه سفیدان کوچه نشین و سایت و **&KfSensor**
Definitions and Value of Honeypots
و راهنمای چند تن از همکلاسی هام و استادانم

به نام خدا

مقدمه:
با توجه به این که هکرهای ایرانی رو به رشد هستند و دیگه بی خیال هک کردن پورتال ها شد ند و رو به هک کردن سرورکردن گفتم مقاله راجبه این ظرف های عسل بدمزه تهیه کنم تا موقعی خدای نکرده زبونم لال در دام این عسل ها نیوفتند.

با گذشتن سال ها به تعداد هکرها و نفوذ کنندگان به سرور ها و شبکه های گسترده اینترنتی افزایش یافت و هر روز اطلاعات بسیار ارزشمندی از قبیل شماره های حساب بانکی ، شماره های کاربری پسورد ها و ... دزدیده می شودند و خسارت های بسیار زیاد از نظر مالی و اعتباری به شرکت های کوچک وبزرگ زده می شود.
حتی یک حمله کوچک گاهی بزرگترین خسارت ها رو وارد میکرد!
بنابراین داشمندان و برنامه نویسان چیره دست سریع دست به کار شودند تا بتوانند جلوی این قبیل حملات رو بگیرند یا به نوعی هکرها رو منحرف کنن.
بهترین طومه برای فریب دادن هکرها اطلاعات نادرست و گمراه کننده ی بود.
پس برنامه نویسان و دانشمندان سخت افزار بعد چندی تالش تنوانستند قطعه و برنامه به نام ظرف عسل یا **Honey Pot** را تولید کنند وظیفه این ظرف عسل گمراه کردن و به دام انداختن نفوذ کننده ها(هکر) است.
این برنامه با دادن اطلاعات نادرست به هکرها باعث میشود تا هکر فکر کند که به اطلاعات مورد نظر خود دست یافته اند و کار را پایان یافته فرض کنند.

Honey Pot چیست؟

ظرف عسل به واقع یک سیستم اطلاعاتی می باشد که با استفاده از منابع خود سعی در کشف و جمع آوری اطلاعات و فعالیتهای غیر مجاز و غیر قانونی بر روی شبکه می کنند. به زبان ساده یک ظرف عسل یک سیستم یا سیستمهای کامپیوتری متصل به شبکه و اینترنت می باشند که بر روی خود دارای اطلاعات کاذب(برای آنکه آب دهان آقا هکر رو آب بیاندازند) می باشند و از عمد بر روی شبکه قرار می گیرند تا به عنوان یک تله عمل کنند و مورد تهاجم یک هکر قرار بگیرند.

هونی پوت ها هم اطلاعات نادرست به یک هکر می دهند وهم باعث به دام افتادن هکر ها میشوند(عجب ظرف عسله بد و شیطونی)

شاید بگید خوب یه فایروال که کار رو تموم میکرد دیگه نیازی به این هونی پوت ها نبود که؟!

خوب بزارید اینجوری براتون بگم

یک ارائه دهنده سرویس اینترنت متوجه می شود که یکی از

کاربرانش به طور مداوم سرورشان را هک کرده و خلاصه کلی خرابکاری به بار می آورد. به دلایل متعدد ردگیری این هکر آسان نیست از این رو متخصصین شبکه آی اس پی به فکر به دام انداختن هکر مربوطه می شوند و بهترین راه برای آنان استفاده از ظرف عسل می باشد.
آنان یک سیستم خود را به این کار اختصاص داده و آن را تبدیل به یک ترمینال سرور می نمایند(ترمینال سرور در واقع کامپویتری ست که شخص می تواند از راه دور به آن از طریق مثلا خط تلفن اتصال پیدا کرده و از منابع آن استفاده کند) و نرم افزارهای مورد نیاز را برای به دام انداختن هکر مربوطه بر روی سیستم کامپیوتر مورد نظر نصب می کنند.
حال آنها وظیفه اشان به پایان رسیده و می بایست منتظر ورود آقا هکره باشند.(دوستانی ازقبیل آقا .... و ... مواظب باشتند گول نخورن)

هکر نوجوان و بی اطلاع ما سرمست از خرابکاری های قبلی خویش و با فکر اینکه هرگز کسی نمی تواند وی را ردیابی کند به ظرف عسل (ترمینال سرور) مثال ما وصل شده و شروع به گشتن و پیدا کردن چاله چوله های سرور می کند.
متخصصین امنیتی در شرکت نیز به عمد تنها سوراخهای امنیتی را بر روی سرور باز گذاشته اند که توسط آنها می توانند هکر فلک زده داستان ما را به دام بیندازند!

با پیگیری کارهای هکر علاوه بر به دام انداختن هکر و یا هکرها، کارشناسان امنیتی به اطلاعات ذیقیمت دیگری نیز می توانند دست پیدا کنند و آن نحوه رخنه هکرها به درون سیستم هایشان می باشد.
اساسا وقتی یک هکر به سروری حمله می کند و یا به کامپیوتری نفوذ می کند آن شبکه و یا سیستم دارای ضعف امنیتی ست و مسلما

مسوول مربوطه اش از وجود این شکاف و روزنه امنیتی مطلع نیست. با بوجود آوردن یک ظرف عسل و پیگیری کنجکاوی های یک هکر می توان به راههایی که وی برای ورود به سیستم استفاده می کند آگاه شد و بدین وسیله جلوی هک شدن سیستم های اصلی را گرفت ؛)

خب ممکن است بگویید چه جالب که می توان به این شکل هکرها را به دام انداخت اما متاسفانه باید بگویم قضیه به این سادگی ها هم نیست و هر تله ای موش نا به کار را به دام نمی اندازد. هکرهای بزرگ تماما دارای سواد بالایی می باشند و علم نفوذ به شبکه را نیز فوت آبند.
حتی کوچک ترین خطا در گونه و جایگذاری ظرف عسل باعث فرار هکر از تله میشود!

آنها از وجود ظرفهای عسل نیز بی اطلاع نیستند و هر زمان بویی ببرند دست از کار خود کشیده و یا با ترفندی متخصصین متفکر و مبارز خویش را ناکام می گذارند.بسته به نوع ظرف عسلی که توسط

کارشناس شبکه تعبیه می شود گاهی امکان ریسک و خرابی کل سیستم توسط هکر وجود دارد.
از سویی دیگر سواد کارشناس برای تعبیه کردن و پیش بینی حرکات هکر و درخواستهایی که به سیستم می فرستد بسیار در نتایج و اطلاعاتی که از سیستم تله گذاری شده بدست خواهد آمد، تاثیر گذار خواهد بود.

تعریف کلی:

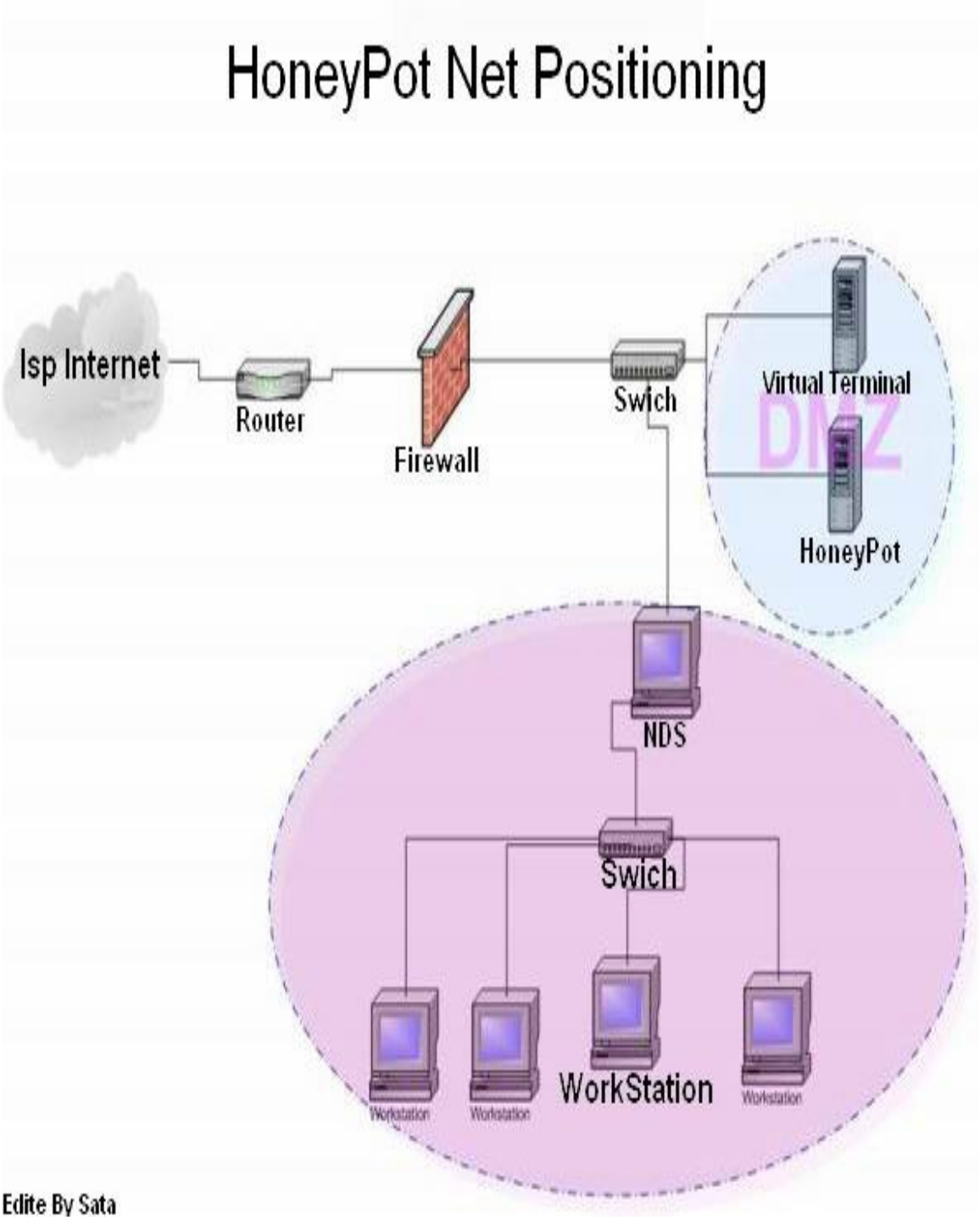
قدم اول در فهم اینکه Honeypot چه مي باشند بیان تعریفي جامع از آن است. تعریف Honeypot مي تواند سخت تر از آنچه که به نظر مي رسد باشد.Honeypot ها از این جهت که هیچ مشکلي را براي ما حل نمي کنند شبیه دیواره هاي آتش و یا سیستمهاي تشخیص دخول سرزده نمي باشند. در عوض آنها یك ابزار قابل انعطافي مي باشند که به شکلهاي مختلفي قابل استفاده هستند.

آنها هر کاري را مي توانند انجام دهند از کشف حملات پنهاني در شبکه هاي IPv6 تا ضبط آخرین کارت اعتباري جعل شده! و همین انعطاف پذیریها باعث شده است که Honeypot ها ابزارهایی قوي به نظر برسند و از جهتي نیز غیر قابل تعریف و غیر قابل فهم!!

البته من براي فهم Honeypot ها از تعریف زیر استفاده مي کنم:

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

شکل زیر جایگزینی یک ظرف عسل را در یک شبکه نشان میدهد



البته اين يك تعريف كلي مي باشد كه تمامي گونه هاي مختلف Honeypot ها را در نظر گرفته است. ما در ادامه مثالهاي مختلفي براي Honeypot ها و ارزش امنيتي آنها خواهيم آورد. همه آنها در تعريفي كه ما در بالا آورده ايم مي گنجند ، ارزش دروغين آنها براي اشخاص بدي كه با آنها در تماسند. به صورت كلي تمامي Honeypot ها به همين صورت كار مي كنند. آنها يك منبعي از فعاليتها بدون مجوز مي باشند. به صورت تئوري يك Honeypot نبايد هيچ ترافيكي از شبكه ما را اشغال كند زيرا آنها هيچ فعاليت قانوني ندارند. اين بدان معني است كه تراكنش هاي با يك Honeypot تقريبا تراكنش هاي بي مجوز و يا فعاليتهاي بد انديشانه مي باشد. يعني هر ارتباط با يك Honeypot مي تواند يك دزدي ، حمله و يا يك تصفيه حساب مي باشد. حال آنكه مفهوم آن ساده به نظر مي رسد (و همين طور هم است) و همين سادگي باعث اين هم موارد استفاده شگفت انگيز از Honeypot ها شده است كه من در اين مقاله قصد روشن كردن اين موارد را دارم.

Honeypot چه كارهايي مي‌تواند انجام دهد؟

با توجه به اين كه از يک Honeypot چه مي‌خواهيم، Honeypot مي‌تواند كارهاي زير را انجام دهد :

- فراهم كردن هشدارهايي در مورد حملات در حال انجام
- معطل كردن نفوذگر و دور نگه داشتن او از شبكة واقعي(نفوذگران پس از شناسايي شبكه، به طور معمول از ضعيف‌ترين و آسيب‌پذيرترين سيستم در شبكه شروع مي‌كنند. زماني كه آن‌ها صرف كلنجار رفتن با اين سيستم قلابي مي‌كنند مي‌تواند يک آسودگي خاطر براي بقية ماشين‌ها ايجاد كند.)
- فراهم كردن امكان مونيتورينگ بلادرنگ حملات صورت گرفته

- فراهم كردن اطلاعاتي در مورد جزئيات حمله (اطلاعاتي از قبيل اين كه نفوذگران چه كساني هستند، چه مي‌خواهند)
- فراهم كردن امكان رديابي و پيگرد قانوني نفوذگر

فوايد Honeypot ها :

Honeypot مفهوم بسيار ساده اي دارد ولي داراي توانايي هاي قدرتمندي مي باشد.

1. داده هاي كوچك داراي ارزش فراوان:

Honeypot ها يك حجم كوچكي ار داده ها را جمع آوري مي كنند. به جاي اينكه ما در يك روز چندين گيگابايت اطلاعات را در فايلهاي ثبت رويدادها ذخيره كنيم توسط Honeypot فقط در حد چندين مگابايت بايد ذخيره كنيم. به جاي توليد 10000 زنگ خطر در يك روز آنها فقط 1 زنگ خطر را توليد مي كنند. يادتان باشد كه Honeypot ها فقط فعاليتهاي ناجور را ثبت مي كنند و هر ارتباطي با Honeypot مي تواند يك فعاليت بدون مجوز و يا بداندیشانه باشد. و به همين دليل مي باشد كه اطلاعات هر چند كوچك Honeypot ها داراي ارزش زيادي مي باشد زيرا كه آنها توسط افراد بد ذات توليد شده و توسط Honeypot ضبط شده است. اين بدان معنا مي باشد كه تجزيه و تحليل اطلاعات يك Honeypot آسانتر (و ارزانتر) از اطلاعات ثبت شده به صورت كلي مي باشد.

2. ابزار و تاكتيكي جديد :

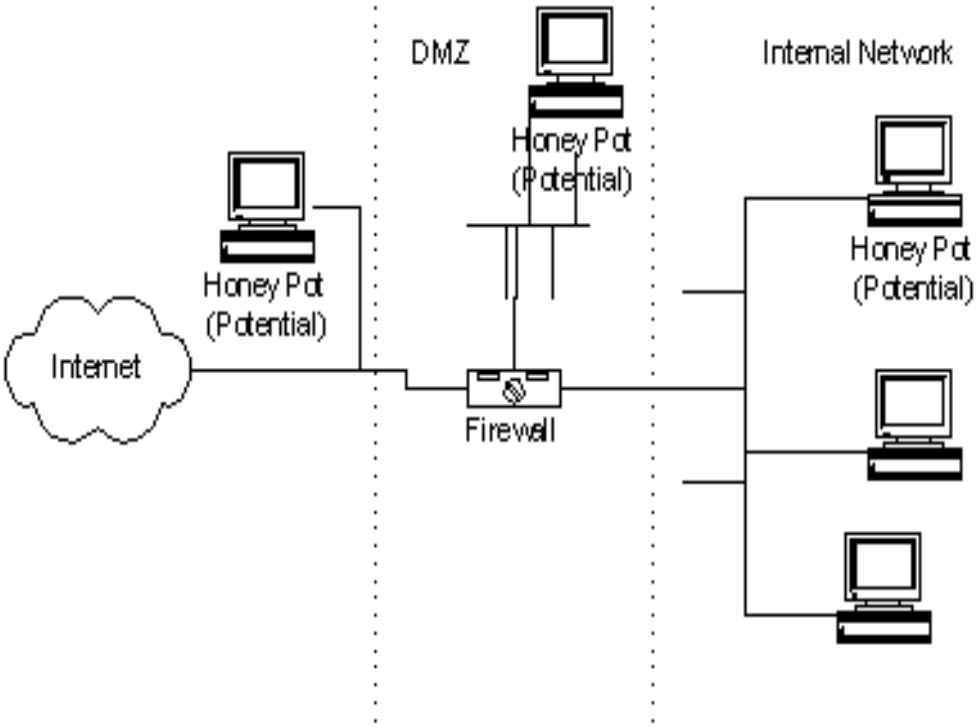
Honeypot براي اين طراحي شده اند كه هر چيزي كه به سمت آنها جذب مي شود را ذخيره كنند. با ابزارها و تاكتيكهاي جديدي كه قبلا ديده نشده اند.

3. كمترين احتياجات:

Honeypot ها به كمترين احتياجات نياز دارند زيرا كه آنها فقط فعاليتهاي ناجور را به ثبت مي رسانند. بنابراين با يك پنتيوم قديمي و با 128 مگابايت RAM و يك شبكه با رنج B به راحتي مي توان آن را پياده سازي كرد.

4. رمز كردن يا IPv6 :

بر خلاف برخي تكنولوژيهاي امنيتي (مانند IDS ها) Honeypot خيلي خوب با محيطهاي رمز شده و يا IPv6 كار مي كنند. اين مساله مهم نيست كه يك فرد ناجور چگونه در يك Honeypot گرفتار مي شود زيرا Honeypot ها خود مي توانند آنها را شناخته و فعاليتهاي آنان را ثبت كنند.



ورود انواع زنبور و ظرف عسل ممنوع!

مضرات Honeypot ها :

شبيه تمامي تكنولوژيها ، Honeypot ها نيز داراي نقاط ضعفي مي باشند. اين بدان علت مي باشد كه Honeypot ها جايگزين تكنولوژي ديگري نمي شوند بلكه در كنار تكنولوژيهاي ديگر كار مي كنند.

بلخره هر نقطعه قوتی نقطه ضعفی هم دارد!

1- محدوديت ديد :

Honeypot ها فقط فعايتهايي را مي توانند پيگيري و ثبت كنند كه به صورت مستقيم با آنها در ارتباط باشند.

Honeypot حملاتي كه بر عليه سيستمهاي ديگر در حال انجام است را نمي توانند ثبت كنند به جز اينكه نفوذگر و يا آن تهديد فعل و انفعالي را با Honeypot داشته باشد.

2- ريسك :

همه تكنولوژيهاي امنيتی داراي ريسك مي باشند. ديوارهاي آتش ريسك نفوذ و يا رخنه كردن در آن را دارند. رمزنگاري ريسك شكستن رمز را دارد، IDS ها ممكن است نتوانند يك حمله را تشخيص دهند. Honeypot ها مجزاي از اينها نيستند. آنها نيز داراي ريسك مي باشند. به خصوص اينكه Honeypot ها ممكن است كه ريسك به دست گرفتن كنترل سيستم توسط يك فرد هكر و صدمه زدن به سيستمهاي ديگر را داشته باشند. البته اين ريسكها براي انواع مختلف Honeypot ها فرق مي كند و بسته به اينكه چه نوعي از Honeypot را استفاده مي كنيد نوع و اندازه ريسك شما نيز متفاوت مي باشد.ممكن است استفاده از يك نوع آن ، ريسكي كمتر از IDS ها داشته باشد و استفاده از نوعي ديگر ريسك بسيار زيادي را در پي داشته باشد.ما در ادامه مشخص خواهيم كرد كه چه نوعي از Honeypot ها داراي چه سطحي از ريسك مي باشند.

چگونگي و شيوه به كار بردن Honeypot ها مي باشد كه ارزش و فوايد و مضرات آنها را مشخص مي كند. در ادامه بيشتر روي آن بحث خواهد شد.

بد از چندی که ظرف های عسل پدید آمد ند و روش موثری برای گمراه کردن نفوذ کنندها و ردیابی آنها بودند این ظرف ها هم کم کم

دارای نوع های خاصی شودند که هر کدام کارهای خاصی را انجام می دهند.

در این بخش با انواع این ظرف های شیطون آشنا میشویم

انوع Honeypot ها :

Honeypot ها در اندازه و شکلهای مختلفی هستند و همین امر باعث شده است که فهم آنها کمی مشکل شود. برای اینکه بتوان بهتر آنها را فهمید همه انواع مختلف آنها را در دو زیر مجموعه آورده ایم:

1- Honeypot های کم واکنش

2- Honeypot های پرواکنش

این تقسیم بندی به ما کمک می کند که چگونگی رفتار آنها را بهتر درک کنیم. و بتوانیم به راحتی نقاط ضعف و قدرت آنها و توانایی ها یشان را روشن تر کنیم. واکنش در اصل نوع ارتباطی که یک نفوذگر با Honeypot دارد را مشخص می کند.

1- Honeypot های کم واکنش

Honeypot های کم واکنش دارای ارتباط و فعالیتی محدود می باشند.آنها معمولا با سرویسها و سیستم های عامل را شبیه سازی شده کار می کنند. سطح فعالیت یک نفوذگر با سطحی از برنامه های شبیه سازی شده محدود شده است. به عنوان مثال یک سرویس FTP شبیه سازی شده که به پورت 21 گوش می کند ممکن است فقط یک صفحه login و یا حداکثر تعدادی از دستورات FTP را شبیه سازی کرده باشد . یکی از فواید این دسته از Honeypot های کم واکنش سادگی آنها می باشد.

نگهداری Honeypot های کم واکنش بسیار راحت و آسان است و خیلی راحت می توان آنها را گسترش داد و ریسک بسیار کمی دارند. آنها بیشتر درگیر این هستند که چه نرم افزارهایی باید روی چه سیستم عاملی نصب شود و همچنین می خواهید چه سرویسهایی را برای آن شبیه سازی و دیده بانی (Monitor) کنید.

همین رهیافت خودکار و ساده آنها است که توسعه آن را برای بسیاری از شرکت ها راحت می کند. البته لازم به ذکر است که همین سرویسهای شبیه سازی شده باعث می شود که فعالیت های فرد نفوذگر محدود شود و همین امر باعث کاهش ریسک می گردد. به این معنی که نفوذگر نمی تواند هیچگاه به سیستم عامل دسترسی پیدا کند و به وسیله آن به سیستم های دیگر آسیب برساند.

یکی از اصلی ترین مضرات Honeypot های کم واکنش این است که آنها فقط اطلاعات محدودی را می توانند ثبت کنند و آنها طراحی می شوند که فقط اطلاعاتی راجع به حملات شناخته شده را به ثبت برسانند.همچنین شناختن یک Honeypot کم واکنش برای یک نفوذگر بسیار راحت می باشد. نگران این نباشید که شبیه سازی شما چه اندازه خوب بوده است زیرا که نفوذگران حرفه ای به سرعت یک Honeypot کم واکنش را از یک سیستم واقعی تشخیص می دهند. از Honeypot های کم واکنش می توان Spector , Honeyd و KFSensor را نام برد.(در صفحات بعد با کی اف سنسور ... بیشتر آشنا می شویم)

2- Honeypot های پرواکنش :

Honeypot های پر واکنش متفاتند. آنها معمولا از راه حل های پیچیده تری استفاده می کنند زیرا که آنها از سیستم عاملها و سرویسهای واقعی استفاده می کنند. هیچ چیزی شبیه سازی شده نیست و ما یک سیستم واقعی را در اختیار نفوذگر می گذاریم.

اگر شما می خواهید که یک Honeypot لینوکس سرور FTP داشته باشید شما باید یک لینوکس واقعی به همراه یک سرویس FTP نصب کنید. فایده این نوع Honeypot دو چیز است. شما می توانید یک حجم زیادی از اطلاعات را به دست آورید. با دادن یک سیستم واقعی به فرد نفوذگر شما می توانید تمامی رفتار او از rootkit های جدید گرفته تا یک نشست IRC را زیر نظر بگیرید. دومین فایده Honeypot های پرواکنش این است که دیگر جای هیچ فرضیه ای روی رفتار نفوذگر باقی نمی گذارد و یک محیط باز به او می دهد و تمامی فعالیتهای او را زیر نظر می گیرد. همین امر باعث می شود که Honeypot های پرواکنش رفتارهایی از فرد نفوذگر را به ما نشان دهند که ما انتظار نداشته ایم و یا نمی توانسته ایم حدس بزنیم!!

بهترین جا برای استفاده از این نوع Honeypot ها زمانی است که قصد داریم دستورات رمز شده یک در پشتی را روی یک شبکه غیر استاندارد IP به دست بیاریم. به هر حال همین امور است که ریسک اینگونه Honeypot ها را افزایش می دهد زیرا که نفوذگر یک سیستم عامل واقعی را در اختیار دارد و ممکن است به سیستم های اصلی شبکه صدمه بزند. به طور کلی یک Honeypot پرواکنش می تواند علاوه بر کارهای یک Honeypot کم واکنش کارهای خیلی بیشتری را انجام دهد.

برای فهم بهتر اینکه Honeypot کم واکنش و پرواکنش چگونه کار می کنند بهتر است دو مثال واقعی در این زمینه بیاوریم. با Honeypot های کم واکنش شروع می کنیم.

محل قرار گرفتن Honeypot در شبکه :

یک Honeypot مي‌تواند در هرجايي که يک سرويس دهنده قادر است قرار بگيرد، واقع شود ولي مطمئناً برخي جاها بهتر از بقيه است.

يک Honeypot با توجه به سرويس‌هاي مورد استفاده مي‌تواند در اينترنت يا اينترانت مورد استفاده قرار گيرد. اگر بخواهيم فعاليت‌هاي خرابکارانة اعضاي ناراضي را در شبکة خصوصي کشف کنيم قرار دادن Honeypot در اينترانت مفيد است. در اينترانت Honeypot پشت ديوارة آتش قرار مي‌گيرد.

در شبکة اينترنت يک Honeypot مي‌تواند در يکي از محل‌هاي زير قرار گيرد :

1-جلوي ديوارة آتش

2-درون DMZ

شکل فوق قرار گرفتن Honeypot را در محل‌هاي گفته شده نشان مي‌دهد.

هر کدام از اين دو مزايا و معايبي دارد که به آن مي‌پردازيم.

با قرار گرفتن Honeypot در جلوي ديوارة آتش، خطر داشتن يک سيستم تحت سيطرة نفوذگر در پشت ديوارة آتش از بين مي‌رود و هيچ خطر اضافي (منتج از نصب Honeypot) متوجه شبکة داخلي نمي‌شود.

يک Honeypot مقداري ترافيک ناخواسته مثل پويش درگاه يا الگوهاي حمله را ايجاد و جذب مي‌کند که با قرار دادن Honeypot

در بيرون از ديوارة آتش چنين وقايعي توسط ديوارة آتش ثبت نمي-شود و سيستم تشخيص نفوذ داخلي (كه در حالت عادي در مواجهه با چنين رخدادهايي هشدار توليد مي‌كند) پيغام هشدار توليد نمي‌كند.

عيب قرار گرفتن Honeypot جلوي ديوارة آتش اين است كه نفوذگران داخلي به راحتي فريب نمي‌خورند، مخصوصاً اگر ديوارة آتش ترافيک خروجي و در نتيجه ترافيک دريافتي Honeypot را محدود كند.

قرار گرفتن Honeypot درون يک DMZ يک راهحل خوب به نظر مي‌رسد به شرطي كه امنيت ديگر سيستم‌هاي درون DMZ در برابر Honeypot برقرار شود. از آن‌جايي كه فقط سرويس‌هاي مورد نياز اجازة عبور از ديوارة آتش را دارند، دسترسي كامل به اغلب DMZها ممكن نيست. به اين دليل و با توجه به اين‌كه تنظيم قوانين مرتبط روي ديوارة آتش كاري زمانبر و مخاطره‌آميز است، در چنين حالتي قرار دادن Honeypot جلوي ديوارة آتش مورد توجه قرار مي‌گيرد.

قرار دادن Honeypot پشت ديوارة آتش، مي‌تواند باعث بروز خطرات امنيتي جديدي در شبكة داخلي شود، مخصوصاً اگر شبكة داخلي توسط ديواره‌هاي آتش اضافي در برابر Honeypot ايمن نشده باشد. توجه داشته باشيد كه اگر Honeypot را پشت يک ديوارة آتش قرار مي‌دهيد، بايد قوانين ديوارة آتش را طوري تنظيم كنيد كه دسترسي از اينترنت مجاز باشد.

بزرگ‌ترين مشكل وقتي به وجود مي‌آيد كه يک نفوذگر خارجي كنترل Honeypot داخلي را در اختيار مي‌گيرد. در اين صورت نفوذگر امكان دسترسي به شبكة داخلي را از طريق Honeypot به دست مي‌آورد. زيرا اين ترافيک، به عنوان ترافيک ورودي به Honeypot در نظر گرفته مي‌شود و از آن‌جايي كه ترافيک ورودي به Honeypot مجاز است، ديوارة آتش جلوي عبور اين ترافيک را

نمي‌گيرد. بنابراين ايمن كردن Honeypot داخلي ضروري است. دليل اصلي قرار گرفتن Honeypot پشت ديوارة آتش شناسايي نفوذگران داخلي است.

بهترين راهحل قرار دادن يک Honeypot درون DMZ به همراه يک ديوارة آتش است. بسته به اين‌كه هدف شناسايي نفوذگران داخلي يا خارجي است، ديوارة آتش مي‌تواند به اينترنت يا اينترانت وصل شود.

در حقيقت شما مي‌خواهيد از طريق Honeypot يک مانور ترتيب بدهيد و به يک دشمن فرضي حمله كنيد يا در مقابل يک دشمن فرضي بايستيد. لذا شرايط را به صورت واقعي تنظيم كنيد.

Trojan Horse-1

Backdoor-2

Intrusion Detection System-3

Social Engineering-4

Sniffer-5

DeMilitarized Zone-6

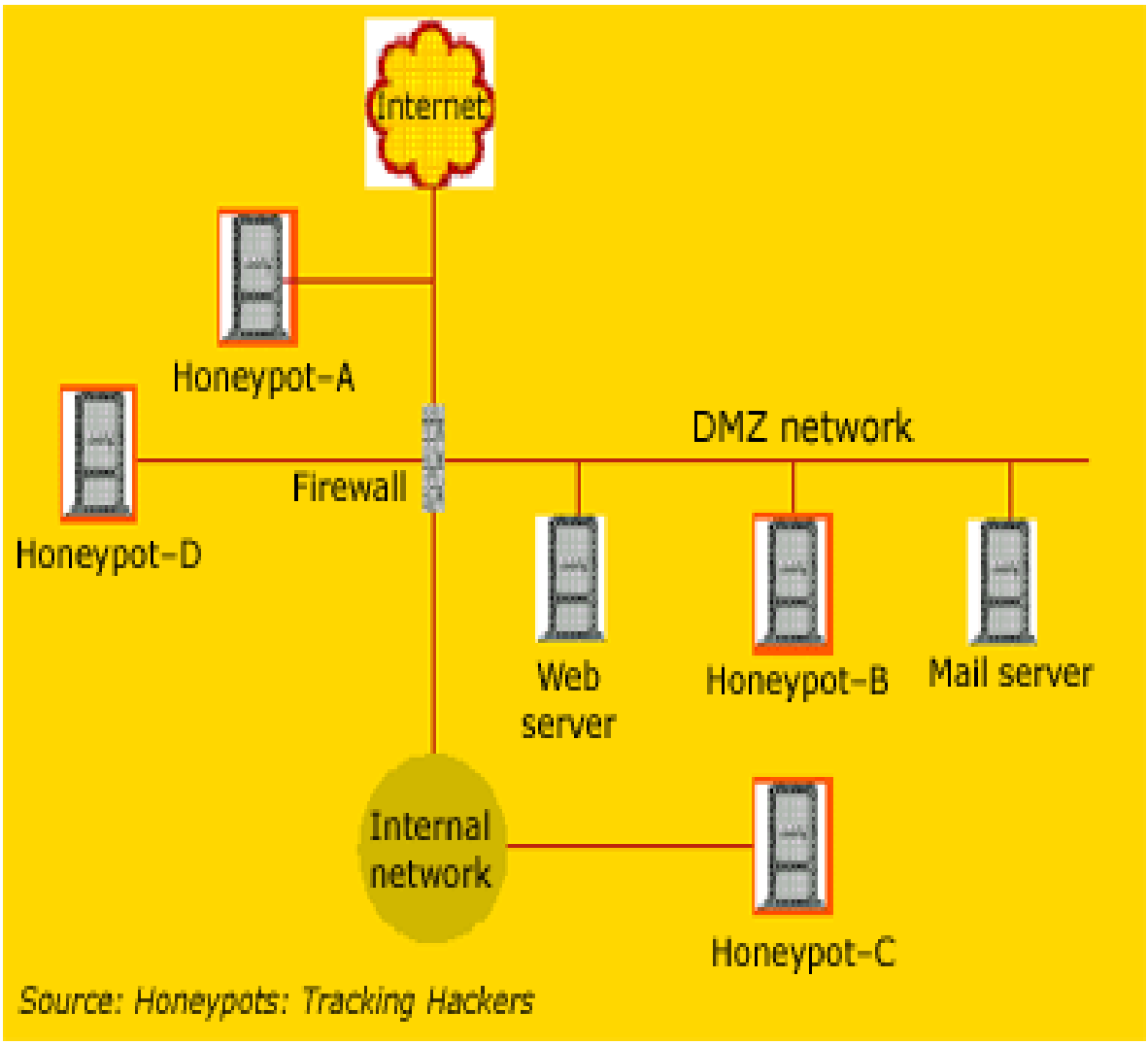


Figure 1. Honeypots can be deployed from a variety of locations. This diagram shows four different possible locations. The optimum location for deployment depends on an array of factors, such as the type of information the organization is interested in gathering, and the level of risk that organization can tolerate to obtain the maximum amount of data.

Honeyd (یک Honeypot کم واکنش) :

Honeyd یک Honeypot کم واکنش است که توسط Niels Provos ساخته شده است. Honeyd به صورت کد باز می باشد

و برای مجموعه سیستم عاملهای یونیکس ساخته شده است.(فکر کنم روی ویندوز هم برده شده است) . Honeyd بر اساس زیر نظر گرفتن IP های غیر قابل استفاده بنا شده است. هر چیزی که قصد داشته باشد با یک IP غیر قابل استفاده با شبکه ارتباط برقرار کند ارتباطش را با شبکه اصلی قطع کرده و با نفوذگر ارتباط برقرار می کند و خودش را جای قربانی جا می زند.

به صورت پیش فرض Honeyd تمامی پورتها TCP و یا UDP را زیر نظر گرفته و تمامی درخواستهای آنها را ثبت می کند. همچنین برای زیر نظر گرفتن یک پورت خاص شما می توانید سرویس شبیه سازی شده مورد نظر را پیکربندی کنید مانند شبیه سازی یک سرور FTP که روی پروتکل TCP پورت 21 کار می کند.وقتی که نفوذگر با یک سرویس شبیه سازی شده ارتباط برقرار می کند تمامی فعالیتهای او را با سرویسهای شبیه سازی شده دیگر ثبت کرده و زیر نظر می گیرد. مثلا در سرویس FTP شبیه سازی شده ما می توانیم نام کاربری و کلمه های رمزی که نفوذگر برای شکستن FTP سرور استفاده می کند و یا دستوراتی که صادر می کند را به دست آوریم و شاید حتی پی ببریم که او به دنبال چه چیزی می گردد و هویت او چیست !

همه اینها به سطحی از شبیه سازی بر می گردد که Honeypot در اختیار ما گذاشته است. بیشتر سرویسهای شبیه سازی شده به یک صورت کار می کنند. آنها منتظر نوع خاصی از رفتارهای هستند و طبق راههایی که قبلا تعیین کرده اند به این رفتارهای واکنش نشان می دهند.

اگر حمله A این را انجام داد از این طریق واکنش نشان بده و اگر حمله B این کار را کرد از این راه واکنش نشان بده!

محدودیت این برنامه ها در این است که اگر نفوذگر دستوراتی را وارد کند که هیچ پاسخی برای آنها شبیه سازی نشده باشد. بنابراین

آنها نمی دانند که چه پاسخی را باید برای نفوذگر ارسال کنند. بیشتر Honeypot های کم واکنش - مانند Honeyd - یک پیغام خطا نشان می دهند. شما می توانید از کد برنامه Honeyd کل دستوراتی که برای FTP شبیه سازی کرده است را مشاهده کنید.

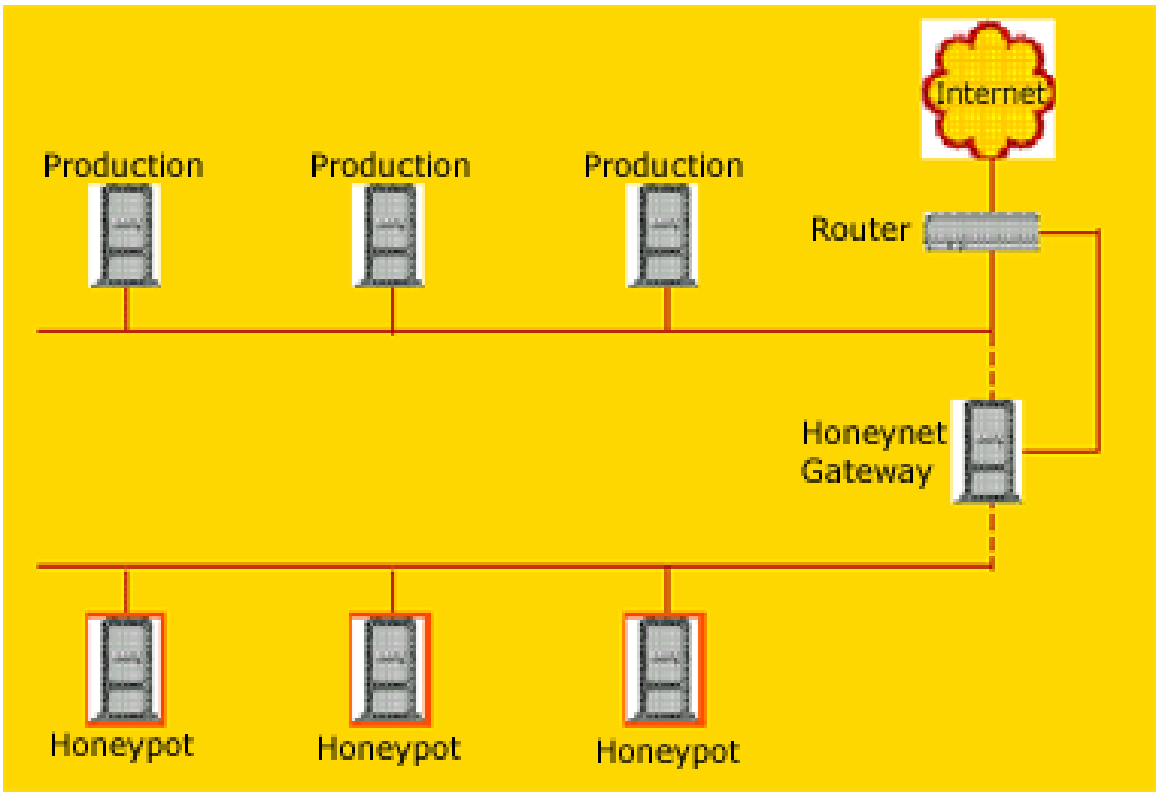


Figure 2. In this Honeynet (a research honeypot used to gather information), the Honeynet Gateway is a Layer 2 bridge that isolates the Honeynet from the rest of the production network. The bridge controls inbound and outbound traffic. Systems are placed in the Honeynet as intended targets for attackers to break into and interact with.

Honeynet ها (یک Honeypot پر واکنش)

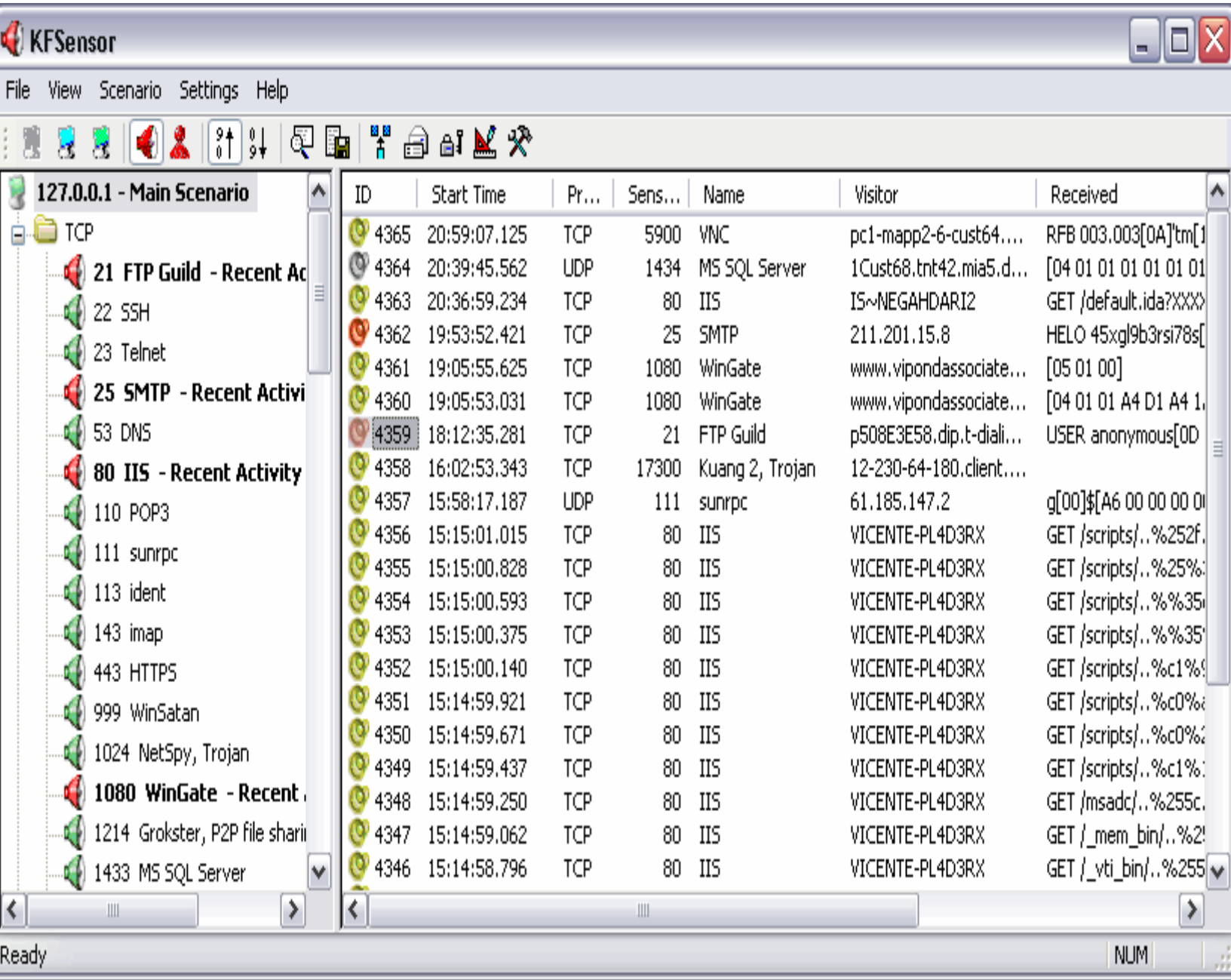
Honeynet یک مثال بدیهی برای Honeypot های پرواکنش می باشد. Honeynet ها یک محصول نمی باشند. آنها یک راه حل

نرم افزاری که بتوان روی یک کامپیوتر نصب شوند نمی باشد. Honeynet ها یک معماری می باشند . یک شبکه بی عیب از کامپیوترهایی که طراحی شده اند برای حملاتی که روی آنها انجام می گیرد. طبق این نظریه ما باید یک معماری داشته باشیم که یک کنترل بالایی را روی شبکه ایجاد کند تا تمامی ارتباطات با شبکه را بتوان کنترل کرد و زیر نظر گرفت.

درون این شبکه ما چندین قربانی خیالی در نظر می گیریم البته با کامپیوترهایی که برنامه های واقعی را اجرا می کنند. فرد هکر این سیستم ها را پیدا کرده و به آنها حمله می کند و در آنها نفوذ می کند اما طبق ابتکار و راهکارهای ما ! یعنی همه چیز در کنترل ما می باشد. البته وقتی آنها این کارها را انجام می دهند نمی دانند که در یک Honeynet گرفتار شده اند. تمامی فعالیت های فرد نفوذگر از نشست های رمز شده SSH گرفته تا ایمیل ها و فایلهایی که در سیستم ها قرار می دهند همه و همه بدون آنکه آنها متوجه شوند زیر نظر گرفته و ثبت می شود. در همان زمان نیز Honeynet تمامی کارهای نفوذگر را کنترل می کند. Honeynet ها این کارها را توسط دروازه ای به نام Honeywall انجام می دهند. این دروازه به تمامی ترافیک ورودی اجازه می دهد که به سمت سیستم های قربانی ما هدایت شوند ولی ترافیک خروجی باید از سیستم های مجهز به IDS عبور کند. این کار به نفوذگر این امکان را می دهد که بتواند ارتباط قابل انعطاف تری با سیستم های قربانی داشته باشد اما در

کنار آن اجازه داده نمی شود که نفوذگر با استفاده از این سیستم ها به سیستم های اصلی صدمه وارد کند.

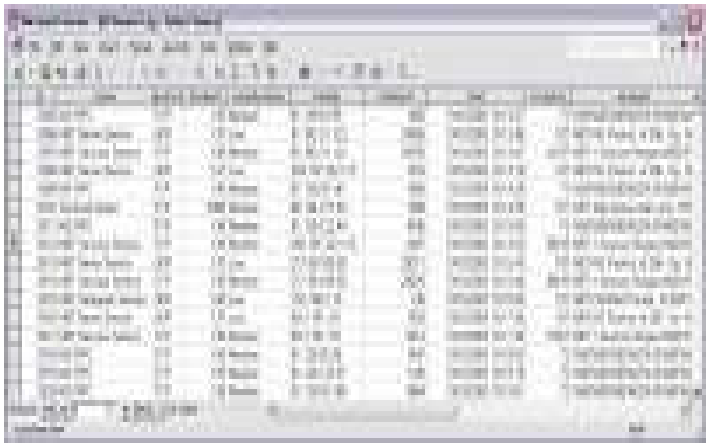
در زیر تصاویری از نرم افزار
KfSensorرامی بینید :



Displays the simulated services on each port. Ports are color coded to indicate recent activity.
The events displayed are from a variety of real life attack.

Icons are colour coded to make it easy to identify recent attacks.

External Database Log



Write your own custom reports in Access, or any other SQL database.

(ببخشید یه مشکل اینترنتی داشتم نشود عکس رو با کیفیت بهتر بگیرم!)

جايگاه Honeypot ها :

حال كه آشنايي ابتدايي با هر دو نوع Honeypot داريم لازم است كه ارزش و جايگاه آنها را در دنياي امنيتي بيان كنيم ، به خصوص در ادامه بيان خواهيم كرد كه چگونه بايد از Honeypot استفاده كنيم.

همانطور كه قبلا اشاره كرديم دو دسته Honeypot داريم كه براي اهداف و تحقيقات ما مورد مطالعه قرار مي گيرند. وقتي از Honeypot ها به صورت محصولات توليد شده براي محافظت از سازمان ها استفاده مي كنيم مي توانند ما را در موارد مختلفي محافظت كنند از جمله مي توان محافظت ، كشف و پاسخ مناسب به يك حمله را بيان كرد. وقتي آنها را در جهت امور تحقيقاتي به كار مي بريم Honeypot ها اطلاعات لازم را براي ما جمع آوري مي كنند. البته اين اطلاعات براي سازمانهاي مختلف فرق مي كند. عده اي شايد بخواهند دشمنان بيروني خود را شناسايي كنند ، يا كارمندان و خريداران خرابكار خود را بشناسند اين سازمانها نيز مي توانند از اين دسته Honeypot ها استفاده كنند.

اگر بخواهيم به صورت كلي بيان كنيم Honeypot هاي كم واكنش به عنوان محصولات توليدي به كار مي روند در صورتيكه Honeypot هاي پرواكنش براي عملياتهاي تحقيقاتي روي شبكه به كار گرفته مي شوند. البته هر كدام از آنهامي توانند در اهداف ديگر نيز به كار روند .

Honeypot هاي توليداتي مي توانند ما را در سه رده زير كمك كنند:

1- پيشگيري (Prevention)
2- رديابي يا كشف(Detection)
3- پاسخ (Response)

Honeypot ها از راههاي مختلفي مي توانند ما را از حملات حفظ كنند. ابتدا حملاتي كه به صورت اتوماتيكي انجام مي شود مثل كرمها و يا Auto-rooter ها . اين حملات به اين صورت كار مي كنند كه نفوذگران با استفاده از بعضي از ابزارها يك رنجي از شبكه ها را پويش كرده تا آسيب پذيري سرورهاي موجود در اين شبكه را پيدا كنند اين ابزارها پس از پيدا كردن آسيب پذيريهاي موجود ، به اين سيستم ها حمله مي كنند. (مانند كرم ساسر كه وقتي سيستمي را آلوده مي كرد به صورت اتوماتيك و به وسيله يك آدرس IP تصادفي ، سيستم ديگري را نيز آلوده مي كرد). روشي كه Honeypot ها براي محافظت شبكه ما از اين گونه حملات استفاده مي كنند اين است كه مي توانند سرعت اينگونه حملات را كند كنند و يا حتي آنها را متوقف كنند! به اين دسته از Honeypot ها Honeypot هاي چسبنده (Sticky) مي گويند.

در اين راه حل Honeypot ها ، آن دسته از آدرس هايي را كه در شبكه استفاده نمي شوند ، در نظر مي گيرند و به آنها واكنش نشان مي دهند. يعني هنگاميكه يك برنامه مخرب يا نفوذگر قصد پويش رنجي از آدرس ها را دارد ، Honypot به آن دسته از آدرس هايي كه در شبكه موجود نمي باشند واكنش نشان مي دهد براي مثال با استفاده از پيغامهاي TCP روند اين گونه حملات را آهسته تر مي كند.

(براي نمونه، با دادن پيغام پنجره صفر ، نفوذگر را در يك گودال هل مي دهد تا نتواند بسته هاي ديگر را ارسال كند) اين امر براي آهسته كردن سرعت انتشار و يا محافظت در برابر كرمهايي كه شبكه داخلي ما را مورد هجوم قرار مي دهند بسيار مناسب است. LaBrea جزو اين دسته از Honeypot ها مي باشد.

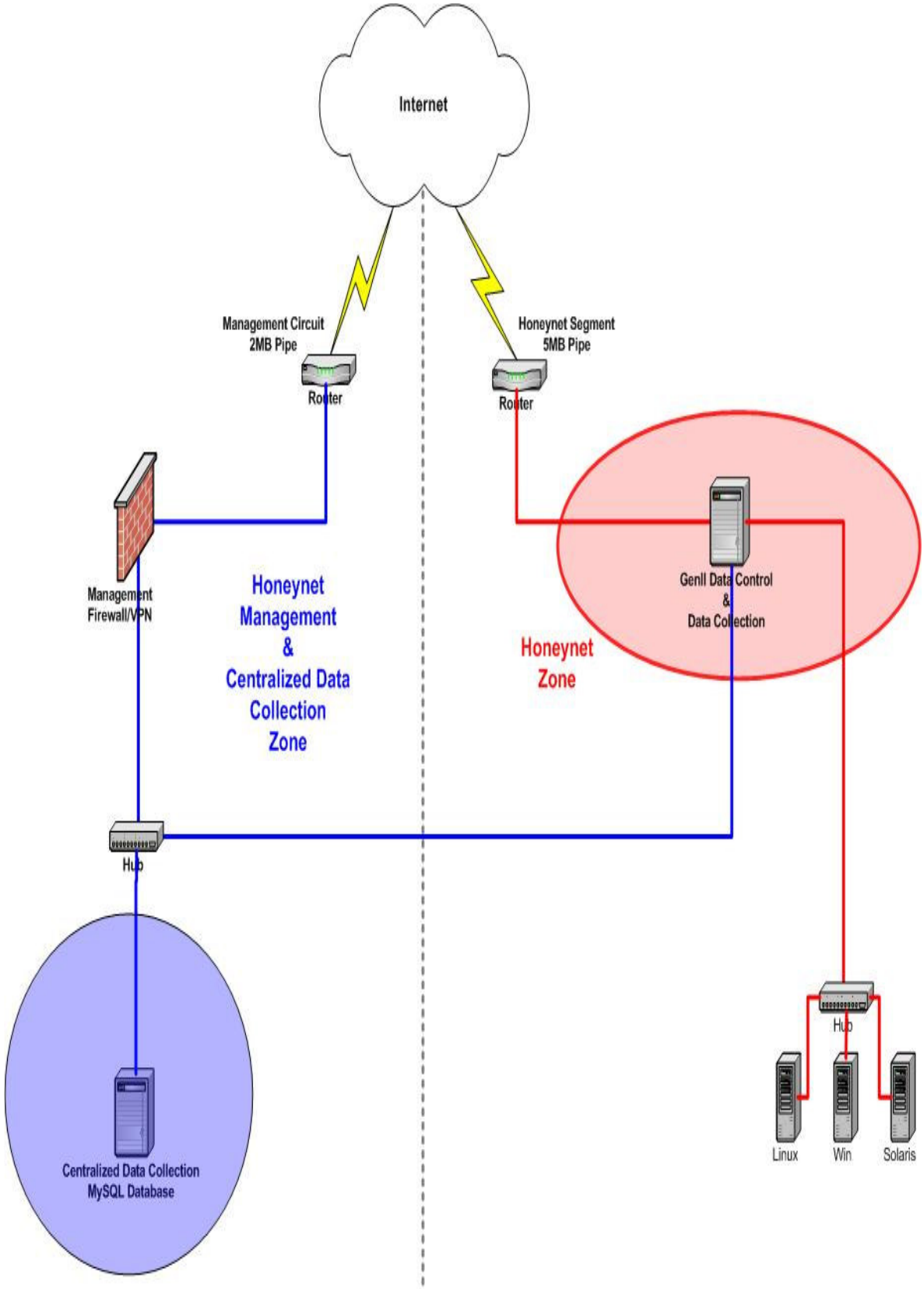
Honeypot هاي چسبنده اغلب به عنوان يك Honeypot كم واكنش شناخته مي شوند.

(البته شما مي توانيد آنها را Honeypot هاي **بدون واكنش** بناميد زيرا كه آنها فقط سرعت نفوذ يك نفوذگر را در شبكه كند مي كنند) Honeypot همچنين مي توانند سازمان شما را از اشخاص نفوذگر محافظت كنند. البته اين كار فقط حيله اي مي باشد كه باعث تهديد و ارعاب نفوذگر مي شود. يعني نفوذگر را گيج و دست پاچه كنيم تا بتوانيم از اين طريق وقت او را به وسيله درگير شدنش با Honeypot بگيريم. در ضمن سازمان شما مي تواند با كشف فعاليتهاي نفوذگر و داشتن زمان لازم براي پاسخ ، اين گونه جملات را متوقف كند.

حتي مي توان يك مرحله بالاتر رفت . اگر نفوذگر بداند كه سازمان شما از Honeypot استفاده مي كند ولي نداند كه كدام سيستم Honeypot مي باشد هميشه يك نگراني در ذهن خود دارد كه « آيا اين يك سيستم حقيقي است يا در يك Honeypot گرفتار شده ام !! » و ممكن است همين نگراني باعث شود كه هيچگاه به فكر نفوذ در شبكه شما نيفتد.

بنابراين Honeypot مي توانند نفوذگران را بترسانند. Deception Toolkit يكي از همين نوع Honeypot هاي كم واكنش مي باشد.

راه دومي كه Honeypot ها به محافظت سازمانها كمك مي كنند از طريق كشف يا رديابي است.عمل **كشف** خيلي بحراني مي باشد كه وظيفه اش شناسايي ناتواني ها و از كار افتادگي هاي بخش **پيشگيري** مي باشد. صرف نظر از اينكه امنيت يك سازمان به چه صورت مي باشد معمولا اتفاقي براي شبكه هاي آنها مي افتد كه باعث بعضي از شكست ها مي گردد. صرف نظر از مشكلات و درگيري هايي كه اشخاص براي كشف يك حمله انجام مي دهند، وقتي يك حمله شناسايي شود مي توان خيلي سريع به آن واكنش نشان داد و آن را متوقف كرد و يا حداقل اثر آن را كمتر كرد. متاسفانه كشف يك حمله بسيار كار مشكلي مي باشد. تكنولوژي هايي مانند IDS ها و فايلهاي ثبت وقايع(log) از جهاتي بدون اثر مي باشند.


Internet
Management Circuit
2MB Pipe
Honeynet Segment
5MB Pipe
Router
Router
Management
Firewall/VPN
Honeynet
Management
&
Centralized Data
Collection
Zone
Honeynet
Zone
GenII Data Control
&
Data Collection
Hub
Hub
Centralized Data Collection
MySQL Database
Linux
Win
Solaris

آنها داده هاي فراواني را توليد مي كنند كه خواندن تمامي آنها زمان فراواني را مي طلبد و بسياري از اين داده ها نيز بيهوده و به درد نخور مي باشند. همچنين آنها در كشف حملات جديد نيز ناتوان مي باشند. حتي نمي توانند با محيط هاي رمز شده و يا IPV6 كار كنند. Honeypot ها براي كشف و رديابي يك حمله نسبت به اين تكنولوژيهاي قديمي برتري دارند. Honeypot داده هاي كم و با قطع و يقين بيشتري جمع آوري مي كند كه ارزش بسيار فراواني دارد.آنها حتي مي تواند حملات جديد و يا كدهاي چند شكلي را به راحتي كشف كنند و مي توانند در محيطهاي رمز شده و IPv6 نيز استفاده شوند.

براي اينكه اطلاعات بيشتري راجع به اين دسته از Honeypot كسب كنيد مي توانيد مقاله Honeypot:Simple,Cost Effective Detection را مطالعه كنيد. به هر جهت Honeypot هاي كم واكنش بهترين راه حل براي كشف مي باشند. ساخت و نگهداري آنها آسان تر از Honeypot هاي پر واكنش مي باشد و همچنين ريسك كمتري نسبت به آنها دارد.

سومين و آخرين راهي كه honeypot ها سازمانهاي ما را محافظت مي كنند **پاسخ**(Response) است. هر زماني كه يك سازمان يك خطا و مشكلي را در شبكه خود تشخيص داد حال چگونه بايد پاسخ دهد؟ همين موضوع مي تواند يكي از چالش هايي باشد كه يك سازمان با آن مواجه مي باشد. معمولا اطلاعات كمي درباره اينكه نفوذگر چه كسي است! و چه كاري مي خواهد انجام دهد!، وجود دارد. در اين وضعيت كوچكترين اطلاعات درباره فعاليت هاي نفوذگر، مهم و حيلاتي است.

معمولا در پاسخ مناسب به يك حمله دو تا مشكل وجود دارد؛ ابتدا اينكه ، بيشتر سيستم هايي كه مورد هجوم قرار گرفته اند را نمي توان براي يك تجزيه و تحليل مناسب ، از كار انداخت . سيستم هاي توليداتي ، مانند سرور پست الكترونيكي براي يك سازمان بسيار مهم

و حياتي مي باشند و حتي اگر متوجه بشوند كه سرور آنها هك شده است باز هم حاضر نيستند اين سيستم ها را از كار بياندازند تا تجزيه و تحليل دقيقي روي آنها انجام شود و پاسخ مناسبي به آن داده شود. در عوض بايد در هنگامي كه اين سيستم ها در حال كار مي باشند آنها را بررسي كرد. همين امر باعث مي شود كه نتوان به درستي پي برد كه چه اتفاق افتاده است و چه مقدار خسارت توسط هكر به سيستم وارد شده است و آيا نفوذگر به سيستم هاي ديگر وارد شده است؟ و يا مي تواند وارد شود!؟

مشكل ديگر در اينجا مي باشد كه حتي اگر سيستم را نيز از كار بياندازيم آنقدر داده در سيستم وجود دارد كه نمي توان به درستي متوجه شد كه كداميك متعلق به نفوذگر است. در عوض Honeypot ها براي چنين كارهايي بسيار عالي مي باشند، زيرا كه آنها را مي توان به آساني از كار انداخت تا تجزيه و تحليل كاملي روي آنها انجام گيرد بدون اينكه به روند كاري سازمان صدمه اي وارد شود. همچنين Honeypot ها تنها فعاليت هاي غير قانوني و بد انديشانه را در خود ذخيره مي كنند و به همين دليل است كه تجزيه و تحليل يك Honeypot هك شده بسيار آسان تر از يك سيستم واقعي مي باشد. هر داده اي كه در Honeypot ذخيره شده است مربوط به فعاليت هاي فرد نفوذگر مي باشد و همين موضوع اين امكان را به يك سازمان مي دهد كه خيلي راحت به اطلاعات مفيدي درباره نوع حمله و هويت نفوذگر پي برده و پاسخ سريع و موثري را به آن دهد. به صورت كلي Honeypot پرواكنش براي پاسخ بهترين گزينه مي باشند. براي پاسخ به يك اخلال ابتدا بايد دانست كه اخلال گر قصد چه كاري را داشته است و چگونه توانسته است كه اخلال ايجاد كند، همچنين از چه ابزارهايي استفاده كرده است. پس براي اين مرحله نياز به Honeypot پرواكنش داريم.

آنچه كه مسلم است ، Honeypot ها يك تكنولوژي جديد مي باشند و هنوز راه فراواني را بايد بپيمايند تا به تكامل برسند. اما آنها براي

بسياري از اهدافي كه يك سازمان براي مسايل امنيتي نياز دارد ، مناسب مي باشند و ما را براي براي پيشگيري از يك نفوذ ، كشف نفوذ و پاسخ به آن كمك مي كنند.

جدول زیر کاربرد هر کدام ازHoneypot ها را با توجه به میزان تعامل آن با نفوذگر نشان می‌دهد:

	production	research
تعامل کم	✓	-
تعامل متوسط	✓	✓
تعامل زیاد	-	✓

مزایا و معایب هر کدام از انواع Honeypot در جدول زیر آمده است:

میزان تعامل با نفوذگر	کم	متوسط	زیاد
ارتباط با سیستم عامل	خیر	خیر	بلی
میزان خطر	کم	متوسط	زیاد
اطلاعات جمع آوری شده	تلاش ها برای ورود به سیستم	درخواست های رسیده از نفوذگر	همه ترافیک سیستم
کنترل کامل بر سیستم	خیر	خیر	بلی
دانش لازم برای توسعه سیستم	کم	زیاد	زیاد
زمان نگهداری سیستم	کم	کم	خیلی زیاد

طرز تشخیص یک هانی پوت(ظرف عسل)از یک سیستم اصلی

برای این کار اول شما رو با یک برنامه آشنا میکنم.

ايستگاه كاري چيست؟

VMware

طراحي شده براي توسعه نرم افزار قدرتمند ماشين مجازي ، دهندگان نرم افزارها و مديران سيستم و كساني است كه مي خواهند در ساختار نرم افزاري شان تغييرات اساسي بدهند.

اين نرم افزار با قدمت بيش از 5 سال و برنده شدن بيش از يک دو جين جوايز بزرگ محصولات نرم افزاري ، توسعه دهندگان نرم پيچيده ترين برنامه هاي تحت شبكه را كه در افزار را قادر مي كند، اجرا مي شوند Net ware يا Linuxويندوزهاي مايكروسافت ، ، اجرا كنندdesktop روي تنها يک رايانه

Virtural) نظير: شبكه بندي مجازي خصيصه هاي ويژه اي به Real time انجام تراكنشها به صورت زنده و (Networking PXE) پشتيباني از drag and drop اشتراک گذاري پوشه ها و يک وسيله ضروري VMware بوت شده) از محيط اجراي از پيش است.

كد زير به شما خواهد گفت كه آيا سيستمي كه كد روي اون اجرا شده تحت VMware كار ميكنه يا خير؟

از VMware خيلي وقت ها براي راه اندازي سرور هاي مجازي ياهاني پات ها استفاده ميشه...

اين كد خيلی وقت ها به شما كمک ميكند كه در تشخيص ظرف عسل راحت تر شويد

```
#include <stdio.h>

int main () {

unsigned char m[2+4], rpill[] = "\x0f\x01\x0d\x00\x00\x00\x00\xc3";

*((unsigned*)&rpill[3]) = (unsigned)m;

((void(*)())&rpill)();

printf ("idt base: %#x\n", *((unsigned*)&m[2]));

if (m[5]>0xd0) printf ("Inside Matrix!\n", m[5]);

else printf ("Not in Matrix.\n");

return 0;

}
```

در آخر بايد بگم كه علاوه بر همه تكنيك هاي موجود براي تشخيص يك هاني پات از سرور هاي اصلي باز هم تشخيص نهايي يك امر ذاتي خواهد بود ! و اين قدرت تشخيص هم با مطالعه روش هاي برخورد سيستم ها با درخواست ها ، نحوه مديريت سيستم ، راه نفوذ به سيستم ، محل قرار گيري سيستم و نامگذاري اون ، ترافيك ارسالي /دريافتي و ... بدست مياد .

امیدوارم که تونسته باشم شما رو تا حدی با این موجودات شیرینه فریب کار آشنا کرده باشم.

چند تا عکس از بهترین هکرهای دنیا

route – alisa دو هکر کلاه مشکی از گروه root

This boy is Black Hat- Defcon

Dr.Mudge & route

Author: Satanic Soulful
E-Mail: Satanic.Soulful@GMail.Com
Satanic_Soulful@Yahoo.Com
Developed In:Satanic Digital Network Security ™
Special TNX 2 :Hell Hacker – Mr.P Hacker – I loveu Mct Collector & X Hulk
Research By:5/-\t4N1C

For More Information Go to Http://Hack-er.cjb.net/

Life & Girl's Is No Matter's
The End.