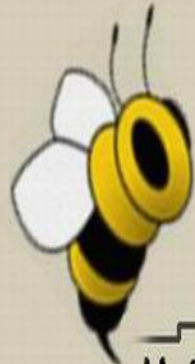


Honey Pot



H/-\ckel2

Author : Satanic Soulful

©All Rights Reserved For Satanic Team

©All Rights Reserved For PersianHacker's 2005-2006



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

ملاحظات:

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 مسوولیتی نسبت به استفاده نادرست از این مقاله را بر عهده نمی گیرند!

استفاده از مطالب این مقاله با ذکر نام نویسنده و همچنین گروه های 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 شدن و رو به هک کردن سرور کردن 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 شوند و خسارت های بسیار زیاد از نظر مالی و اعتباری به شرکت های کوچک و بزرگ زده می شود. حتی یک حمله کوچک گاهی بزرگترین خسارت ها رو وارد میگرد! بنابراین دانشمندان و برنامه نویسان چیره دست سریع دست به کار شدند 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 نتوانستند 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 و هم 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 کامپیوتری است 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 از قبیل آقا و ... مواظب باشند 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 است و مسلما

مسئول 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 متأسفانه باید بگویم قضیه به این سادگی ها هم نیست و هر تله ای موش نا به کار را به دام نمی اندازد. هکرها بزرگ تماماً دارای سواد بالایی می باشند و علم نفوذ به شبکه را نیز فوت آنبند. 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 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 يك ابزار قابل انعطافی می باشند که به شکلهای مختلفی قابل استفاده هستند.

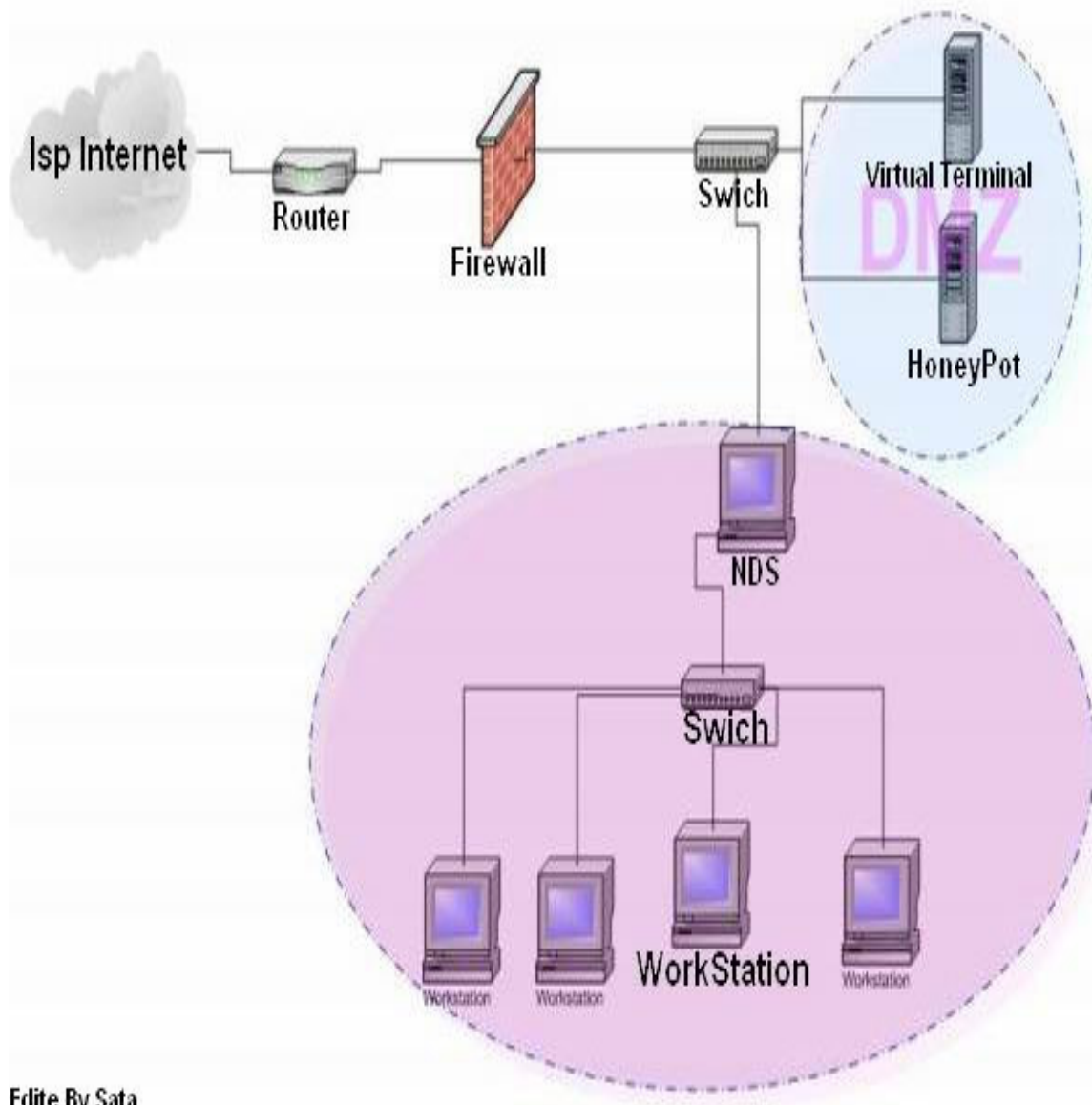
آنها هر کاری را می توانند انجام دهند از کشف حملات پنهانی در شبکه های IPv6 تا ضبط آخرین کارت اعتباری جعل شده! و همین انعطاف پذیرها باعث شده است که Honeypot ها ابزارهایی قوی به نظر برسند و از جهتی نیز غیر قابل تعریف و غیر قابل فهم!!

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

یک Honeypot يك منبع سیستم اطلاعاتی می 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

HoneyPot Net Positioning



Edite By Sata

البته این یک تعریف کلی می باشد که تمامی گونه های مختلف Honeypot ها را در نظر گرفته است. ما در ادامه مثالهایی 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 تقریباً تراکنش های بی مجوز و یا فعالیتهاي 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.

Honeypot چه کارهایی می تواند انجام دهد؟

با توجه به این که از یک Honeypot چه می خواهیم، Honeypot می تواند کارهای زیر را انجام دهد :

- فراهم کردن هشدارهایی در مورد حملات در حال انجام
- معطل کردن نفوذگر و دور نگه داشتن او از شبکه واقعی(نفوذگران پس از شناسایی شبکه، به طور معمول از ضعیفترین و آسیب پذیرترین سیستم در شبکه شروع می کنند. زمانی که آنها صرف کلنجر رفتن با این سیستم قلابی می کنند می تواند یک آسودگی خاطر برای بقیه ماشین ها ایجاد کند.)
- فراهم کردن امکان مونیترینگ بلادرنگ حملات صورت گرفته

- فراهم کردن اطلاعاتی در مورد جزئیات حمله (اطلاعاتی از قبیل این که نفوذگران چه کسانی هستند، چه می‌خواهند)
- فراهم کردن امکان ردیابی و پیگرد قانونی نفوذگر

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 يك حجم كوچكي از داده ها را جمع آوري مي كنند. به جاي اينكه ما در يك روز چندین گیگابایت اطلاعات را در فایلهاي ثبت رویدادها ذخیره کنیم توسط Honeypot فقط در حد چندین مگابایت باید ذخیره کنیم. به جاي تولید 10000 زنگ خطر در يك روز آنها فقط 1 زنگ خطر را تولید مي كنند. یادتان باشد که Honeypot ها فقط فعالیتهای ناچور را ثبت می کنند و هر ارتباطی با Honeypot می تواند يك 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 يك Honeypot آسانتر (و ارزانتر) از اطلاعات ثبت شده به صورت کلی می باشد.

2. ابزار و تاکتیکی جدید :

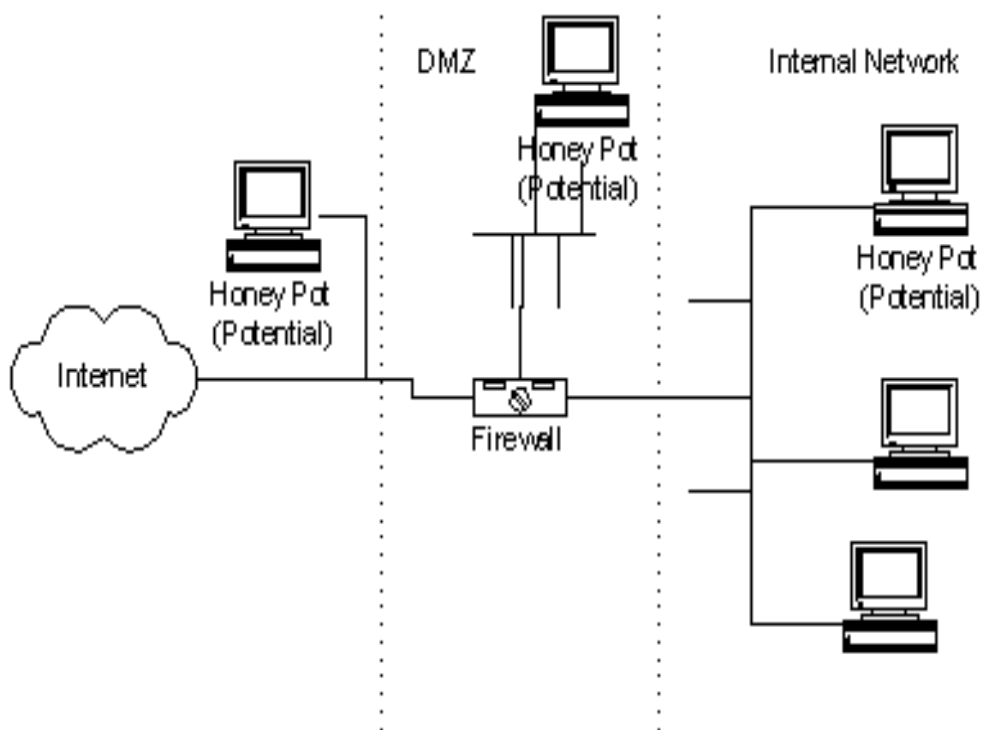
Honeypot برای این طراحی شده اند که هر چیزی که به سمت آنها جذب می شود را ذخیره کنند. با ابزارها و تاکتیکیهای جدیدی که قبلاً دیده نشده اند.

3. کمترین احتیاجات:

Honeypot ها به كمترين احتياجات نياز دارند زيرا كه آنها فقط فعاليتهاي ناجور را به ثبت مي رسانند. بنابر اين با يك پنتيوم قديمي و با 128 مگابايت RAM و يك شبكه با رنج B به راحتی 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 :

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

بلخره هر نقطه قوتی نقطه ضعیفی هم دارد!

1- محدودیت دید :

Honeypot ها فقط فعالیتهایی 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.

چگونگی و شیوه به کار بردن Honeypot ها می باشد که ارزش و فواید و مضرات آنها را مشخص می کند. در ادامه بیشتر روی آن بحث خواهد شد.

بد از چندی که ظرف های عسل پدید آمدند و روش موثری برای گمراه کردن نفوذکنندها و ردیابی آنها بودند این ظرف ها هم کم کم

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

در این بخش با انواع این ظرف های شیطان آشنا میشویم

انواع Honeypot ها :

Honeypot ها در اندازه و شکل های 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 هایشان 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 معمولاً 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 Spectator, Honeyd و KFSensor را نام برد. (در صفحات بعد با کی اف سنسور ... بیشتر آشنا می شویم)

2- Honeypot های پرواکنش :

Honeypot های پرواکنش متفانتند. آنها معمولاً 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 پرواکشن 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 پرواکشن 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 پرواکشن می تواند علاوه بر کارهای یک HoneyPot کم واکنش کارهای خیلی بیشتری را انجام دهد.

برای فهم بهتر اینکه HoneyPot کم واکنش و پرواکشن 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 می‌تواند در هر جایی که یک سرویس دهنده قادر است قرار بگیرد، واقع شود ولی مطمئناً برخی جاها بهتر از بقیه است.

یک Honeypot با توجه به سرویس‌های مورد استفاده می‌تواند در اینترنت یا اینترانت مورد استفاده قرار گیرد. اگر بخواهیم فعالیت‌های خرابکارانه اعضای ناراضی را در شبکه خصوصی کشف کنیم قرار دادن Honeypot در اینترانت مفید است. در اینترانت Honeypot پشت دیواره آتش قرار می‌گیرد.

در شبکه اینترنت یک Honeypot می‌تواند در یکی از محل‌های زیر قرار گیرد :

1- جلوی دیواره آتش

2- درون DMZ

شکل فوق قرار گرفتن Honeypot را در محل‌های گفته شده نشان می‌دهد.

هر کدام از این دو مزایا و معایبی دارد که به آن می‌پردازیم.

با قرار گرفتن Honeypot در جلوی دیواره آتش، خطر داشتن یک سیستم تحت سیطره نفوذگر در پشت دیواره آتش از بین می‌رود و هیچ خطر اضافی (منتج از نصب Honeypot) متوجه شبکه داخلی نمی‌شود.

یک Honeypot مقداری ترافیک ناخواسته مثل پویش درگاه یا الگوهای حمله را ایجاد و جذب می‌کند که با قرار دادن Honeypot

در بیرون از دیواره آتش چنین وقایعی توسط دیواره آتش ثبت نمی-شود و سیستم تشخیص نفوذ داخلی (که در حالت عادی در مواجهه با چنین رخدادهایی هشدار تولید می‌کند) پیغام هشدار تولید نمی‌کند.

عیب قرار گرفتن Honeypot جلوی دیواره آتش این است که نفوذگران داخلی به راحتی فریب نمی‌خورند، مخصوصاً اگر دیواره آتش ترافیک خروجی و در نتیجه ترافیک دریافتی Honeypot را محدود کند.

قرار گرفتن Honeypot درون یک DMZ یک راحل خوب به نظر می‌رسد به شرطی که امنیت دیگر سیستم‌های درون DMZ در برابر Honeypot برقرار شود. از آنجایی که فقط سرویس‌های مورد نیاز اجازه عبور از دیواره آتش را دارند، دسترسی کامل به اغلب DMZها ممکن نیست. به این دلیل و با توجه به این که تنظیم قوانین مرتبط روی دیواره آتش کاری زمانبر و مخاطره‌آمیز است، در چنین حالتی قرار دادن Honeypot جلوی دیواره آتش مورد توجه قرار می‌گیرد.

قرار دادن Honeypot پشت دیواره آتش، می‌تواند باعث بروز خطرات امنیتی جدیدی در شبکه داخلی شود، مخصوصاً اگر شبکه داخلی توسط دیواره‌های آتش اضافی در برابر Honeypot ایمن نشده باشد. توجه داشته باشید که اگر Honeypot را پشت یک دیواره آتش قرار می‌دهید، باید قوانین دیواره آتش را طوری تنظیم کنید که دسترسی از اینترنت مجاز باشد.

بزرگترین مشکل وقتی به وجود می‌آید که یک نفوذگر خارجی کنترل Honeypot داخلی را در اختیار می‌گیرد. در این صورت نفوذگر امکان دسترسی به شبکه داخلی را از طریق Honeypot به دست می‌آورد. زیرا این ترافیک، به عنوان ترافیک ورودی به Honeypot در نظر گرفته می‌شود و از آنجایی که ترافیک ورودی به Honeypot مجاز است، دیواره آتش جلوی عبور این ترافیک را

نمی‌گیرد. بنابراین ایمن کردن Honeypot داخلی ضروری است. دلیل اصلی قرار گرفتن Honeypot پشت دیواره آتش شناسایی نفوذگران داخلی است.

بهترین راه حل قرار دادن یک Honeypot درون DMZ به همراه یک دیواره آتش است. بسته به این که هدف شناسایی نفوذگران داخلی یا خارجی است، دیواره آتش می‌تواند به اینترنت یا اینترنت وصل شود.

در حقیقت شما می‌خواهید از طریق Honeypot یک مانور ترتیب دهید و به یک دشمن فرضی حمله کنید یا در مقابل یک دشمن فرضی بایستید. لذا شرایط را به صورت واقعی تنظیم کنید.

Trojan Horse-1

Backdoor-2

Intrusion Detection System-3

Social Engineering-4

Sniffer-5

DeMilitarized Zone-6

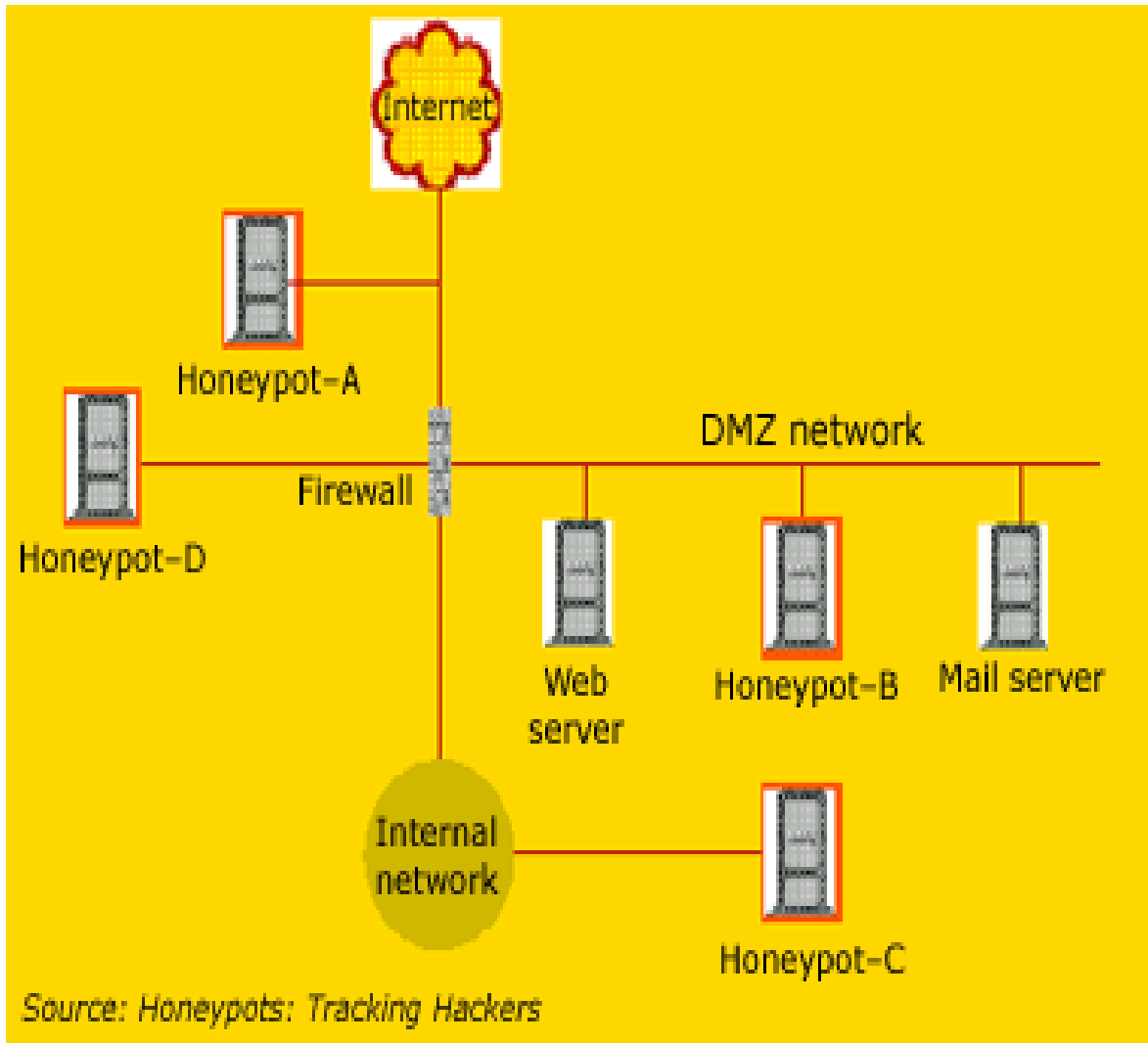


Figure 1. Honeypots can be deployed from a variety of locations. This diagram shows four different possible locations. The optimum location for deployment depends on an array of factors, such as the type of information the organization is interested in gathering, and the level of risk that organization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

Honeyd (یک Honeypot کم واکنش) :

Niels Honeyd یک Honeypot کم واکنش است که توسط 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 می‌کند و خودش را جای قربانی جا می‌زند.

به صورت پیش فرض Honeyd تمامی پورت‌ها TCP و یا UDP را زیر نظر گرفته و تمامی درخواست‌های آنها را ثبت می‌کند. همچنین برای زیر نظر گرفتن یک پورت خاص شما می‌توانید سرویس شبیه‌سازی شده مورد نظر را پیکربندی کنید مانند شبیه‌سازی یک سرور FTP که روی پروتکل TCP پورت 21 کار می‌کند. وقتی که نفوذگر با یک سرویس شبیه‌سازی شده ارتباط برقرار می‌کند تمامی فعالیت‌های او را با سرویس‌های شبیه‌سازی شده دیگر ثبت کرده و زیر نظر می‌گیرد. مثلاً در سرویس FTP شبیه‌سازی شده ما می‌توانیم نام کاربری و کلمه‌های رمزی که نفوذگر برای شکستن FTP سرور استفاده می‌کند و یا دستوراتی که صادر می‌کند را به دست آوریم و شاید حتی پی ببریم که او به دنبال چه چیزی می‌گردد و هویت او چیست!

همه اینها به سطحی از شبیه‌سازی بر می‌گردد که Honeypot در اختیار ما گذاشته است. بیشتر سرویس‌های شبیه‌سازی شده به یک صورت کار می‌کنند. آنها منتظر نوع خاصی از رفتارهای هستند و طبق راه‌هایی که قبلاً تعیین کرده‌اند به این رفتارهای واکنش نشان می‌دهند.

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 برنامه‌ها در این است که اگر نفوذگر دستوراتی را وارد کند که هیچ پاسخی برای آنها شبیه‌سازی 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.

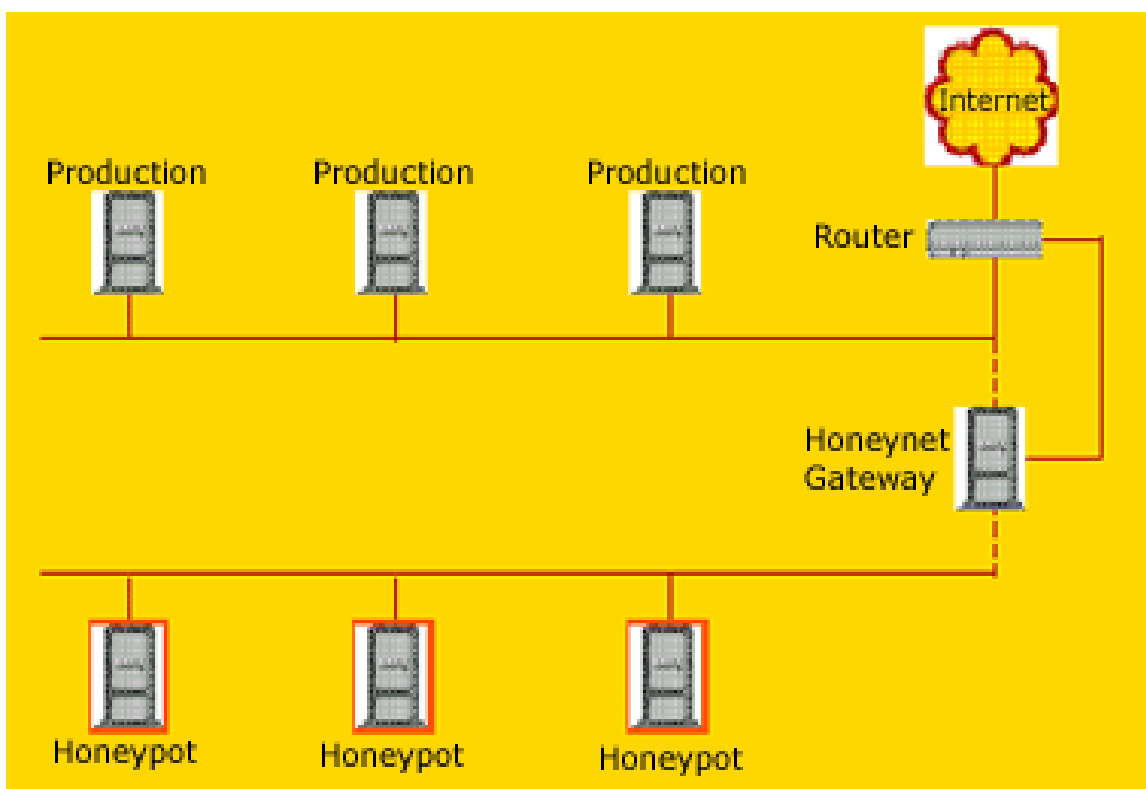


Figure 2. In this Honeynet (a research honeypot used to gather information), the Honeynet Gateway is a Layer 2 bridge that isolates the Honeynet from the rest of the production network. The bridge controls inbound and outbound traffic. Systems are placed in the Honeynet as intended targets for attackers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

The screenshot shows the KfSensor application window. The left sidebar displays a tree view of simulated services on port 127.0.0.1, including FTP Guild, SSH, Telnet, SMTP, DNS, IIS, POP3, sunrpc, ident, imap, HTTPS, WinSatan, NetSpy, Trojan, WinGate, Grokster, P2P file sharing, and MS SQL Server. The main pane shows a table of network events with columns for ID, Start Time, Protocol, Sensitivity, Name, Visitor, and Received data.

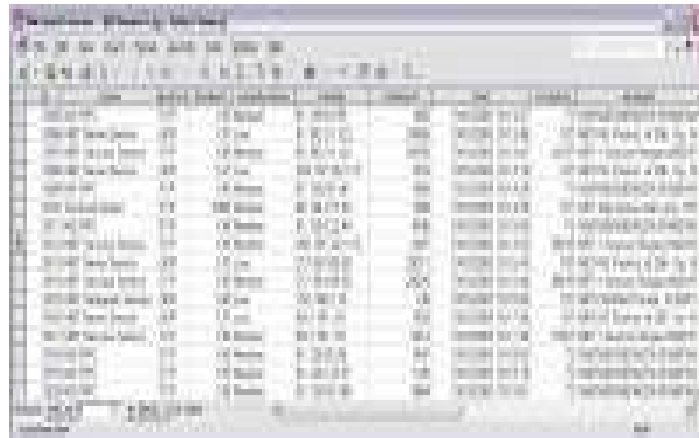
ID	Start Time	Pr...	Sens...	Name	Visitor	Received
4365	20:59:07.125	TCP	5900	VNC	pc1-mapp2-6-cust64...	RFB 003.003[0A]tm[1
4364	20:39:45.562	UDP	1434	MS SQL Server	1Cust68.tnt42.mia5.d...	[04 01 01 01 01 01 01
4363	20:36:59.234	TCP	80	IIS	IS~NEGAHDARI2	GET /default.ida?XXX
4362	19:53:52.421	TCP	25	SMTP	211.201.15.8	HELO 45xgl9b3rsi78s[
4361	19:05:55.625	TCP	1080	WinGate	www.vipondassociate...	[05 01 00]
4360	19:05:53.031	TCP	1080	WinGate	www.vipondassociate...	[04 01 01 A4 D1 A4 1.
4359	18:12:35.281	TCP	21	FTP Guild	p508E3E58.dip.t-diali...	USER anonymous[0D
4358	16:02:53.343	TCP	17300	Kuang 2, Trojan	12-230-64-180.client...	
4357	15:58:17.187	UDP	111	sunrpc	61.185.147.2	g[00]\$(A6 00 00 00 0
4356	15:15:01.015	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%252f.
4355	15:15:00.828	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%25%
4354	15:15:00.593	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%35
4353	15:15:00.375	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%35
4352	15:15:00.140	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%c1%
4351	15:14:59.921	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%c0%
4350	15:14:59.671	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%c0%
4349	15:14:59.437	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%c1%
4348	15:14:59.250	TCP	80	IIS	VICENTE-PL4D3RX	GET /msadc/..%255c.
4347	15:14:59.062	TCP	80	IIS	VICENTE-PL4D3RX	GET /_mem_bin/..%2!
4346	15:14:58.796	TCP	80	IIS	VICENTE-PL4D3RX	GET /_vti_bin/..%255

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!)

جایگاه Honeypot ها :

حال که آشنایی ابتدایی با هر دو نوع Honeypot داریم لازم است که ارزش و جایگاه آنها را در دنیای امنیتی بیان کنیم ، به خصوص در ادامه بیان خواهیم کرد که چگونه باید از Honeypot استفاده کنیم.

همانطور که قبلا اشاره کردیم دو دسته Honeypot داریم که برای اهداف و تحقیقات ما مورد مطالعه قرار می گیرند. وقتی از Honeypot ها به صورت محصولات تولید شده برای محافظت از سازمان ها استفاده می کنیم می توانند ما را در موارد مختلفی محافظت کنند از جمله می توان محافظت ، کشف و پاسخ مناسب به يك حمله را بیان کرد. وقتی آنها را در جهت امور تحقیقاتی به کار می بریم Honeypot ها اطلاعات لازم را برای ما جمع آوری می کنند. البته این اطلاعات برای سازمانهای مختلف فرق می کند. عده ای شاید بخواهند دشمنان بیرونی خود را شناسایی کنند ، یا کارمندان و خریداران خرابکار خود را بشناسند این سازمانها نیز می توانند از این دسته Honeypot ها استفاده کنند.

اگر بخواهیم به صورت کلی بیان کنیم Honeypot های کم واکنش به عنوان محصولات تولیدی به کار می روند در صورتیکه Honeypot های پرواکنش برای عملیاتی تحقیقاتی روی شبکه به کار گرفته می شوند. البته هر کدام از آنها می توانند در اهداف دیگر نیز به کار روند .

Honeypot های تولیداتی می توانند ما را در سه رده زیر کمک کنند:

- 1- پیشگیری (Prevention)
- 2- ردیابی یا کشف (Detection)
- 3- پاسخ (Response)

Honeypot ها از راه‌های مختلفی می‌توانند ما را از حملات حفظ کنند. ابتدا حملاتی که به صورت اتوماتیکی انجام می‌شود مثل کرم‌ها و یا Auto-router ها. این حملات به این صورت کار می‌کنند که نفوذگران با استفاده از بعضی از ابزارها یک رنجی از شبکه‌ها را پوشش کرده تا آسیب‌پذیری سرورهای موجود در این شبکه را پیدا کنند این ابزارها پس از پیدا کردن آسیب‌پذیریهای موجود، به این سیستم‌ها حمله می‌کنند. (مانند کرم ساسر که وقتی سیستمی را آلوده می‌کند به صورت اتوماتیک و به وسیله یک آدرس IP تصادفی، سیستم دیگری را نیز آلوده می‌کند). روشی که Honeypot ها برای محافظت شبکه ما از این گونه حملات استفاده می‌کنند این است که می‌توانند سرعت اینگونه حملات را کند کنند و یا حتی آنها را متوقف کنند! به این دسته از Honeypot ها Honeypot های چسبنده (Sticky) می‌گویند.

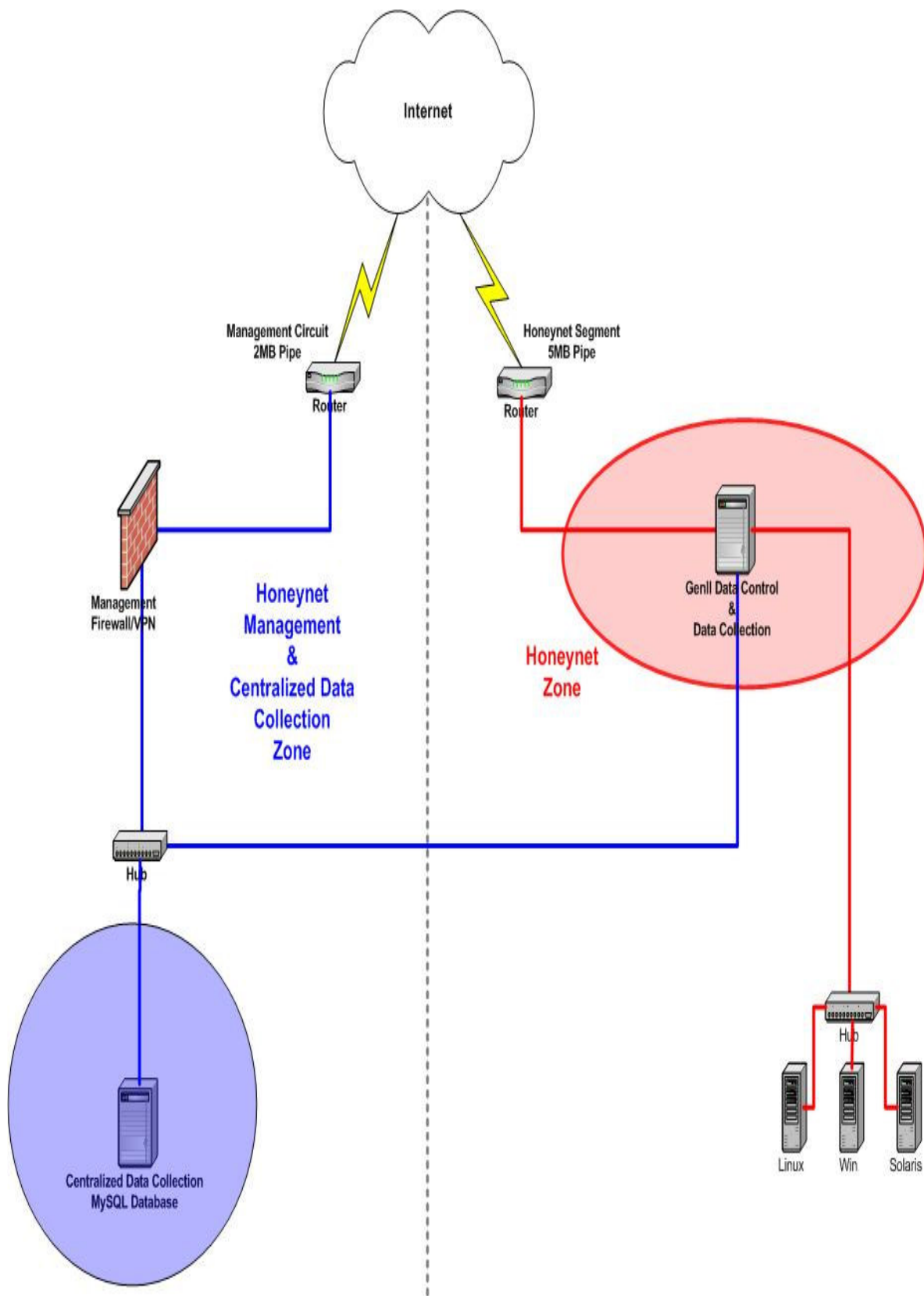
در این راه حل Honeypot ها، آن دسته از آدرس‌هایی را که در شبکه استفاده نمی‌شوند، در نظر می‌گیرند و به آنها واکنش نشان می‌دهند. یعنی هنگامیکه یک برنامه مخرب یا نفوذگر قصد پوشش رنجی از آدرس‌ها را دارد، Honeypot به آن دسته از آدرس‌هایی که در شبکه موجود نمی‌باشند واکنش نشان می‌دهد برای مثال با استفاده از پیغامهای TCP روند این گونه حملات را آهسته‌تر می‌کند.

(برای نمونه، با دادن پیغام پنجره صفر، نفوذگر را در یک گودال هل می‌دهد تا نتواند بسته‌های دیگر را ارسال کند) این امر برای آهسته کردن سرعت انتشار و یا محافظت در برابر کرم‌هایی که شبکه داخلی ما را مورد هجوم قرار می‌دهند بسیار مناسب است. LaBrea جزو این دسته از Honeypot ها می‌باشد. Honeypot های چسبنده اغلب به عنوان یک Honeypot کم واکنش شناخته می‌شوند.

(البته شما می توانید آنها را Honeypot های بدون واکنش بنامید زیرا که آنها فقط سرعت نفوذ یک نفوذگر را در شبکه کند می کنند)
Honeypot همچنین می توانند سازمان شما را از اشخاص نفوذگر محافظت کنند. البته این کار فقط حيله اي مي باشد که باعث تهدید و ارباب نفوذگر می شود. یعنی نفوذگر را گيج و دست پاچه کنیم تا بتوانیم از این طریق وقت او را به وسیله درگیر شدنش با Honeypot بگیریم. در ضمن سازمان شما می تواند با کشف فعالیتهای نفوذگر و داشتن زمان لازم برای پاسخ ، این گونه جملات را متوقف کند.

حتی می توان یک مرحله بالاتر رفت . اگر نفوذگر بداند که سازمان شما از Honeypot استفاده می کند ولی نداند که کدام سیستم Honeypot می باشد همیشه یک نگرانی در ذهن خود دارد که « آیا این یک سیستم حقیقی است یا در یک Honeypot گرفتار شده ام !! » و ممکن است همین نگرانی باعث شود که هیچگاه به فکر نفوذ در شبکه شما نیفتد.

بنابر این Honeypot می توانند نفوذگران را بترسانند. Deception Toolkit یکی از همین نوع Honeypot های کم واکنش می باشد. راه دومی که Honeypot ها به محافظت سازمانها کمک می کنند از طریق کشف یا ردیابی است. عمل کشف خیلی بحرانی می باشد که وظیفه اش شناسایی ناتوانی ها و از کار افتادگی های بخش پیشگیری می باشد. صرف نظر از اینکه امنیت یک سازمان به چه صورت می باشد معمولاً اتفاقی برای شبکه های آنها می افتد که باعث بعضی از شکست ها می گردد. صرف نظر از مشکلات و درگیری هایی که اشخاص برای کشف یک حمله انجام می دهند، وقتی یک حمله شناسایی شود می توان خیلی سریع به آن واکنش نشان داد و آن را متوقف کرد و یا حداقل اثر آن را کمتر کرد. متأسفانه کشف یک حمله بسیار کار مشکلی می باشد. تکنولوژی هایی مانند IDS ها و فایل های ثبت وقایع (log) از جهاتی بدون اثر می باشند.



آنها داده هاي فراواني را توليد مي کنند که خواندن تاممي آنها زمان فراواني را مي طلبد و بسياري از اين داده ها نيز بيهوده و به درد نخور مي باشند. همچنين آنها در کشف حملات جديد نيز ناتوان مي باشند. حتي نمي توانند با محيط هاي رمز شده و يا IPV6 کار کنند. Honeypot ها براي کشف و رديابي يك حمله نسبت به اين تکنولوژيهاي قديمي برتري دارند. Honeypot داده هاي کم و با قطع و يقين بيشتري جمع آوري مي کند که ارزش بسيار فراواني دارد. آنها حتي مي تواند حملات جديد و يا کدهاي چند شکلي را به راحتی کشف کنند و مي توانند در محيطهاي رمز شده و IPv6 نيز استفاده شوند.

براي اينکه اطلاعات بيشتري راجع به اين دسته از Honeypot کسب کنید مي توانيد مقاله [Honeypot: Simple, Cost Effective Detection](#) را مطالعه کنید. به هر جهت Honeypot هاي کم و اکنش بهترين راه حل براي کشف مي باشند. ساخت و نگهداري آنها آسان تر از Honeypot هاي پر و اکنش مي باشد و همچنين ريسک کم تري نسبت به آنها دارد.

سومين و آخرين راهي که honeypot ها سازمانهاي ما را محافظت مي کنند پاسخ (Response) است. هر زماني که يك سازمان يك خطا و مشکلي را در شبکه خود تشخيص داد حال چگونه بايد پاسخ دهد؟ همين موضوع مي تواند يکي از چالش هايي باشد که يك سازمان با آن مواجه مي باشد. معمولا اطلاعات کمي درباره اينکه نفونگر چه کسي است! و چه کاري مي خواهد انجام دهد!، وجود دارد. در اين وضعيت کوچکترين اطلاعات درباره فعاليت هاي نفونگر، مهم و حيالتي است.

معمولا در پاسخ مناسب به يك حمله دو تا مشکل وجود دارد؛ ابتدا اينکه ، بيشتري سيستم هايي که مورد هجوم قرار گرفته اند را نمي توان براي يك تجزيه و تحليل مناسب ، از کار انداخت . سيستم هاي توليداتي ، مانند سرور پست الکترونيکي براي يك سازمان بسيار مهم

و حیاتی می باشند و حتی اگر متوجه بشوند که سرور آنها هک شده است باز هم حاضر نیستند این سیستم ها را از کار بیاندازند تا تجزیه و تحلیل دقیقی روی آنها انجام شود و پاسخ مناسبی به آن داده شود. در عوض باید در هنگامی که این سیستم ها در حال کار می باشند آنها را بررسی کرد. همین امر باعث می شود که نتوان به درستی پی برد که چه اتفاق افتاده است و چه مقدار خسارت توسط هکر به سیستم وارد شده است و آیا نفوذگر به سیستم های دیگر وارد شده است؟ و یا می تواند وارد شود!؟

مشکل دیگر در اینجا می باشد که حتی اگر سیستم را نیز از کار بیاندازیم آنقدر داده در سیستم وجود دارد که نمی توان به درستی متوجه شد که کدامیک متعلق به نفوذگر است. در عوض Honeypot ها برای چنین کارهایی بسیار عالی می باشند، زیرا که آنها را می توان به آسانی از کار انداخت تا تجزیه و تحلیل کاملی روی آنها انجام گیرد بدون اینکه به روند کاری سازمان صدمه ای وارد شود. همچنین Honeypot ها تنها فعالیت های غیر قانونی و بد اندیشانه را در خود ذخیره می کنند و به همین دلیل است که تجزیه و تحلیل يك Honeypot هک شده بسیار آسان تر از يك سیستم واقعی می باشد. هر داده ای که در Honeypot ذخیره شده است مربوط به فعالیت های فرد نفوذگر می باشد و همین موضوع این امکان را به يك سازمان می دهد که خیلی راحت به اطلاعات مفیدی درباره نوع حمله و هویت نفوذگر پی برده و پاسخ سریع و موثری را به آن دهد. به صورت کلی Honeypot پرواکشن برای پاسخ بهترین گزینه می باشند. برای پاسخ به يك اخلاص ابتدا باید دانست که اخلاص گر قصد چه کاری را داشته است و چگونه توانسته است که اخلاص ایجاد کند، همچنین از چه ابزارهایی استفاده کرده است. پس برای این مرحله نیاز به Honeypot پرواکشن داریم.

آنچه که مسلم است ، Honeypot ها يك تکنولوژی جدید می باشند و هنوز راه فراوانی را باید بپیمایند تا به تکامل برسند. اما آنها برای

بسیاری از اهدافی که یک سازمان برای مسایل امنیتی نیاز دارد ، مناسب می باشند و ما را برای برای پیشگیری از یک نفوذ ، کشف نفوذ و پاسخ به آن کمک می کنند.

جدول زیر کاربرد هر کدام از Honeypot ها را با توجه به میزان تعامل آن با نفوذگر نشان می دهد:

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

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

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

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

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

ایستگاه کاری چیست؟

VMware

طراحی شده برای توسعه نرم افزار قدرتمند ماشین مجازی ،
دهندگان نرم افزارها و مدیران سیستم و کسانی است که می خواهند
در ساختار نرم افزاری شان تغییرات اساسی بدهند.
این نرم افزار با قدمت بیش از 5 سال و برنده شدن بیش از یک دو
جین جوایز بزرگ محصولات نرم افزاری ، توسعه دهندگان نرم
پیچیده ترین برنامه های تحت شبکه را که در افزار را قادر می کند،
اجرا می شوند Net ware یا Linux ویندوزهای مایکروسافت ،
، اجرا کنند desktop روی تنها یک رایانه

(Virtual Networking) نظیر: شبکه بندی مجازی خصیصه های ویژه ای
به Real time انجام تراکنشها به صورت زنده و (Networking
PXE) پشتیبانی از drag and drop اشتراک گذاری پوشه ها و
یک وسیله ضروری VMware بوت شده) از محیط اجرایی از پیش
است.

بگذریم به شما خواهد گفت که آیا سیستمی که کد روی اون اجرا

شده تحت VMware کار میکند یا خیر؟

از VMware خیلی وقت ها برای راه اندازی سرور های مجازی
یاهانی پات ها استفاده میشه...

این کد خیلی وقت ها به شما کمک میکند که در تشخیص ظرف عمل
راحت تر شوید

```

#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 باید بگم که علاوه بر همه تکنیک های موجود برای تشخیص يك هانی پات از سرور های اصلی باز هم تشخیص نهایی يك امر ذاتی خواهد بود ! و این قدرت تشخیص هم با مطالعه روش های برخورد سیستم ها با درخواست ها ، نحوه مدیریت سیستم ، راه نفوذ به سیستم ، محل قرار گیری سیستم و نامگذاری اون ، ترافیک ارسالی /دریافتی و ... بدست میاد .

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/-At4N1C
©©Copyright For : Satanic Team 2005-2006
For More Information Go to [Http://Hacker.cjb.net/](http://Hacker.cjb.net/)



SATANIC
DIGITAL NETWORK SECURITY
www.Hacker.cjb.net

©©All Right Reserved For Persian Hacker's™

Mr.PHacker_Ir

2005-2006 For More Information

Visit:[Http://PersianHacker.Net/](http://PersianHacker.Net/)



Persian Hackers

تمام حقوق مقاله مربوط به تیم های پرشین هکرز و جهنم شیطانی می باشد.

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