# هانی پات

## وزارت ارتباطات و فناوري اطلاعات

**اداره كل ارتباطات و فناوري اطلاعات استان كرمانشاه**

**منبع : http://certcc.ir  مركز مديريت امداد و هماهنگي عمليات رخدادهاي رايانه اي( مركز ماهر )**

# هانی پات‌ها

حسگر و سنسورهای گردآوری کننده بدافزارها با جمع آوری اطلاعات کم حجم ولی بسیار با اهمیت می توانند استراتژی های حملات سایبری را شناسایی نمایند لذا داشتن اطلاعات بیشتر در مورد روش های متداول حملات سایبری می تواند به رفتارشناسی مهاجمین منتج گردد .

توانمند و امن سازی ورودی های شبکه های سازمانی یکی از مهمترین اقداماتی است که مدیران فناوری اطلاعات سازمانها آنرا بصورت جدی در دستورکار خود قرار داده اند و هر روزه بدنبال آموختن و بکارگیری متدولوژی های جدید روز هستند تا بتوانند درگاههای شبکه خود را از آماج حملات سایبری مصون دارند در این میان حسگر و سنسورهای گردآوری کننده بدافزارها می توانند بانك اطلاعاتی بسیار مفیدی باشند تا با برقراری ارتباط بین اجزای اطلاعاتی این پایگاه، بانکهای دانش مفیدی در میان سازمانها پدید آید و نهایتا کاهش احتمال حملات و یا خسارات احتمالی را برای دستگاه ها محقق سازند .

## Honeypot چیست؟

هانی پات یك تکنولوژی تقریبا جدید و شدیدا پویا هستند. همین ماهیت پویا باعث می‌شود که به راحتی نتوان آنها را تعریف کرد .
Honeypotها به خودی خود یك راه حل به شمار نرفته و هیچ مشکل امنیتی خاصی را حل نمی‌کنند، بلکه ابزارهای بسیار انعطاف پذیری هستند که کارهای مختلفی برای امنیت اطلاعات انجام می‌دهند.
این تکنولوژی با تکنولوژیهایی مانند فایروالها و سیستمهای تشخیص نفوذ (IDS) متفاوت است، چرا که این تکنولوژیها مسائل امنیتی خاصی را حل کرده و به همین دلیل راحتتر تعریف می‌شوند. فایروالها یك تکنولوژی پیشگیرانه به شمار می آیند، آنها از ورود مهاجمان به شبکه یا سیستم کامپیوتر جلوگیری می‌کنند .IDS ها یك تکنولوژی تشخیصی هستند. هدف آنها این است که فعالیتهای غیر مجاز یا خرابکارانه را شناسایی کرده و درباره آنها به متخصصان امنیت هشدار دهند. تعریف Honeypot ها کار سخت تری است، چرا که آنها ممکن است در پیشگیری، تشخیص، جمع آوری اطلاعات، و کارهای دیگری مورد استفاده قرار گیرند. شاید بتوان یك Honeypot را به این صورت تعریف کرد:
Honeypot»یك سیستم اطلاعاتی است که ارزش آن به استفاده غیر مجاز و ممنوع دیگران از آن است«.
این تعریف به وسیله اعضای لیست ایمیل Honeypot انجام شده است. لیست ایمیل Honeypot یك فروم متشکل از بیش از ۵۰۰۰ متخصص امنیت است .از آنجاییکه Honeypot ها در اشکال و اندازه های مختلفی وجود دارند، ارائه تعریف جامعی از آن کار بسیار سختی است. تعریف یك Honeypot نشان دهنده نحوه کار آن و یا حتی هدف آن نیست. این تعریف صرفا ناظر به نحوه ارزش گذاری یك Honeypotاست. به عبارت ساده تر، Honeypotها یك تکنولوژی هستند که ارزش آنها به تعامل مجرمان با آنها بستگی دارد. تمامی Honeypotها بر اساس یك ایده کار می‌کنند: هیچکس نباید از آنها استفاده کند و یا با آنها تعامل برقرار نماید، هر تعاملی با Honeypot غیر مجاز شمرده شده و نشانه ای از یك حرکت خرابکارانه به شمار می‌رود.
یك Honeypot سیستمی است که در شبکه سازمان قرار می‌گیرد، اما برای کاربران آن شبکه هیچ کاربردی ندارد و در حقیقت هیچ یك از اعضای سازمان حق برقراری هیچگونه ارتباطی با این سیستم را ندارند. این سیستم دارای یك سری ضعفهای امنیتی است. از آنجاییکه مهاجمان برای نفوذ به یك شبکه همیشه به دنبال سیستمهای دارای ضعف می‌گردند، این سیستم توجه آنها را به خود جلب می‌کند. و با توجه به اینکه هیچکس حق ارتباط با این سیستم را ندارد، پس هر تلاشی برای برقراری ارتباط با این سیستم، یك تلاش خرابکارانه از سوی مهاجمان محسوب می‌شود. در حقیقت این سیستم نوعی دام است که مهاجمان را فریب داده و به سوی خود جلب می‌کند و به این ترتیب علاوه بر امکان نظارت و کنترل کار مهاجمان، این فرصت را نیز به سازمان می‌دهد که فرد مهاجم را از سیستمهای اصلی شبکه خود دور نگه دارند.
یك Honeypot هیچ سرویس واقعی ارائه نمی‌دهد. هر تعاملی که انجام گیرد، هر تلاشی که برای ورود به این سیستم صورت گیرد، یا هر

فایل داده ای که روی یك Honeypot مورد دسترسی قرار گیرد، با احتمال بسیار زیاد نشانه ای از یك فعالیت خرابکارانه و غیر مجاز است. برای مثال، یك سیستم Honeypot می‌تواند روی یك شبکه داخلی به کار گرفته شود. این Honeypot از هیچ ارزش خاصی برخوردار نیست و هیچکس در درون سازمان نیازی به استفاده از آن نداشته و نباید از آن استفاده کند. این سیستم می‌تواند به ظاهر یك فایل سرور، یك وب سرور، یا حتی یك ایستگاه کاری معمولی باشد. اگر کسی با این سیستم ارتباط برقرار نماید، با احتمال زیاد در حال انجام یك فعالیت غیر مجاز یا خرابکارانه است.

در حقیقت، یك Honeypot حتی لازم نیست که حتما یك کامپیوتر باشد .این سیستم می‌تواند هر نوع نهاد دیجیتالی باشد (معمولا از آن به Honeytokenیاد می‌شود) که هیچ ارزش واقعی ندارد. برای مثال، یك بیمارستان می‌تواند یك مجموعه نادرست از رکوردهای اطلاعاتی بیماران ایجاد نماید. از آنجاییکه این رکوردها Honeypot هستند، هیچکس نباید به آنها دسترسی پیدا کرده یا با آنها تعامل برقرار کند. این رکوردها می‌توانند در داخل پایگاه داده بیماران این بیمارستان به عنوان یك جزء Honeypot قرار گیرند. اگر یك کارمند یا یك فرد مهاجم برای دسترسی به این رکوردها تلاش نماید، می‌تواند به عنوان نشانه ای از یك فعالیت غیر مجاز به شمار رود، چرا که هیچکس نباید از این رکوردها استفاده کند. اگر شخصی یا چیزی به این رکوردها دسترسی پیدا کند، یك پیغام هشدار صادر می‌شود. این ایده ساده پشت Honeypotهاست که آنها را ارزشمند می‌کند.

دو یا چند Honeypot که در یك شبکه قرار گرفته باشند، یك Honeynet را تشکیل می‌دهند. نوعا در شبکه های بزرگتر و متنوعتر که یك Honeypot به تنهایی برای نظارت بر شبکه کافی نیست، از Honeynet استفاده می‌کنند Honeynet .ها معمولا به عنوان بخشی از یك سیستم بزرگ تشخیص نفوذ پیاده سازی می‌شوند .در حقیقت Honeynet یك شبکه از Honeypot های با تعامل بالاست که طوری تنظیم شده است که تمامی فعالیتها و تعاملها با این شبکه، کنترل و ثبت می‌شود.

مزایای استفاده از Honeypot

- Honeypotها صرفا مجموعه های کوچکی از داده ها را جمع آوری می‌کنند Honeypot .ها فقط زمانی که کسی یا چیزی با آنها ارتباط برقرار کند داده ها را جمع آوری می‌نمایند، در نتیجه صرفا مجموعه های بسیار کوچکی از داده ها را جمع می-کنند، که البته این داده ها بسیار ارزشمندند .سازمانهایی که هزاران پیغام هشدار را در هر روز ثبت می‌کنند، با استفاده از Honeypotها ممکن است فقط صد پیغام هشدار را ثبت نمایند. این موضوع باعث می‌شود که مدیریت و تحلیل داده های جمع آوری شده توسط Honeypot ها بسیار ساده تر باشد .
- Honeypotها موارد خطاهای تشخیص اشتباه را کاهش می‌دهند .یکی از مهمترین چالشهای اغلب سیستمهای تشخیصی این است که پیغامهای هشدار دهنده خطای زیادی تولید کرده و در موارد زیادی، این پیغامهای هشدار دهنده واقعا نشان دهنده وقوع هیچ خطری نیستند. یعنی در حالی یك رویداد را تهدید تشخیص می‌دهند که در حقیقت تهدیدی در کار نیست. هر چه احتمال این تشخیص اشتباه بیشتر باشد، تکنولوژی تشخیص دهنده بی فایده تر می‌شود Honeypot .ها به طور قابل توجهی درصد این تشخیصهای اشتباه را کاهش می‌دهند، چرا که تقریبا هر فعالیت مرتبط با Honeypot ها به طور پیش فرض غیر مجاز تعریف شده است. به همین دلیل Honeypot ها در تشخیص حملات بسیار موثرند .
- Honeypotها می‌توانند حملات ناشناخته را تشخیص دهند .چالش دیگری که در تکنولوژیهای تشخیصی معمول وجود دارد این است که آنها معمولا حملات ناشناخته را تشخیص نمی‌دهند. این یك تفاوت بسیار حیاتی و مهم بین Honeypot ها و تکنولوژیهای امنیت کامپیوتری معمولی است که بر اساس امضاهای شناخته شده یا داده های آماری تشخیص می‌دهند.

تکنولوژیهای تشخیصی مبتنی بر امضا، در تعریف به این معنا هستند که ابتدا باید هر حمله ای حداقل یك بار انجام شده و امضای آن شناسایی گردد و سپس با استفاده از آن امضا، در موارد بعدی شناخته شود. تشخیص مبتنی بر داده های آماری نیز از خطاهای آماری رنج می‌برد Honeypot .ها طوری طراحی شده اند که حملات جدید را نیز شناسایی و کشف می‌کنند. چرا که هر فعالیتی در ارتباط با Honeypot ها غیر معمول شناخته شده و در نتیجه حملات جدید را نیز معرفی می‌کند .

- Honeypotها فعالیتهای رمز شده را نیز کشف می‌کنند .حتی اگر یك حمله رمز شده باشد، Honeypotها می‌توانند این فعالیت را کشف کنند. به تدریج که تعداد بیشتری از سازمانها از پروتکلهای رمزگذاری مانندSSH ، IPsec، و SSL استفاده

می‌کنند، این مساله بیشتر خود را نشان می‌دهد Honeypot .ها می‌توانند این کار را انجام دهند، چرا که حملات رمز شده با Honeypotبه عنوان یك نقطه انتهایی ارتباط، تعامل برقرار می‌کنند و این فعالیت توسط Honeypot رمز گشایی می‌شود .

- Honeypotبا IPv6 کار می‌کند .اغلب Honeypot ها صرف نظر از پروتکل IP از جملهIPv6 ، در هر محیط IP کار می‌کنند IPv6 .یك استاندارد جدید پروتکل اینترنت (IP) است که بسیاری از سازمانها در بسیاری از کشورها از آن استفاده می-کنند. بسیاری از تکنولوژیهای فعلی مانند فایروالها و سنسورهای سیستم تشخیص نفوذ به خوبی با IPv6 سازگار نشده اند .
- Honeypotها بسیار انعطاف پذیرند Honeypot .ها بسیار انعطاف پذیرند و می‌توانند در محیطهای مختلفی مورد استفاده قرار گیرند. همین قابلیت انعطاف Honeypot هاست که به آنها اجازه می‌دهد کاری را انجام دهند که تعداد بسیار کمی از تکنولوژیها می‌توانند انجام دهند: جمع آوری اطلاعات ارزشمند به خصوص بر علیه حملات داخلی .
- Honeypotها به حداقل منابع نیاز دارند .حتی در بزرگترین شبکه ها، Honeypotها به حداقل منابع احتیاج دارند. یك کامپیوتر پنتیوم قدیمی و ساده می‌تواند میلیونها آدرس IP یا یك شبکه OC-12 را نظارت نماید.

معایب استفاده از Honeypot

Honeypotها نیز مانند هر تکنولوژی دیگری معایبی دارند. آنها برای این طراحی نشده اند که جای هیچ تکنولوژی خاصی را بگیرند .

- Honeypotها دارای یك محدوده دید کوچك و محدود هستند Honeypot .ها فقط همان کسانی را می‌بینند که با آنها به تعامل می‌پردازند. در نتیجه حملات بر علیه سایر سیستمها و یا تعاملات انجام شده با سایر سیستمها را مشاهده نمی‌کنند. این نکته در عین حال که یك مزیت است، یك عیب نیز به شمار می‌رود. یك Honeypot به شما نمی‌گوید که سیستم دیگری مورد سوء استفاده قرار گرفته است، مگر اینکه سیستمی که مورد سوء استفاده قرار گرفته با خود Honeypot تعاملی برقرار نماید. برای برطرف کردن این عیب راههای زیادی وجود دارد که از طریق آنها می‌توانید فعالیت مهاجمان را به سمت Honeypot ها تغییر مسیر دهید. از این میان می‌توان به Honeytoken ها و تغییر مسیر اشاره کرد .
- ریسك هر زمان که شما یك تکنولوژی جدید را به کار می‌گیرید، آن تکنولوژی ریسکهای مخصوص به خود را نیز به همراه دارد، مثلا این ریسك که یك مهاجم بر این سیستم غلبه کرده و از آن به عنوان ابزاری برای حملات بر علیه اهداف داخلی و خارجی استفاده نماید. حتی سیستمهای تشخیص نفوذ که هیچ پشته IP به آنها تخصیص داده نشده است نیز می‌توانند در معرض خطر قرار داشته باشند Honeypot .ها نیز در این مورد استثناء نیستند Honeypot .های مختلف سطوح خطر متفاوتی دارند. راههای مختلفی نیز برای کاهش این خطرات وجود دارد. از میان انواع Honeypot ها، هانی نتها بیشترین سطح خطر را دارا هستند .

## انواع Honeypot

در این مقاله پس از معرفی انواع Honeypot ، به ذکر یك مثال از هر نوع خواهیم پرداخت.
برای درك بهتر Honeypot ها، می‌توانیم آنها را به دو گروه با تعامل (Interaction ) کم و با تعامل زیاد تقسیم کنیم. منظور از interaction، میزان فعالیت و تعاملی است که یك فرد مهاجم اجازه دارد با آن Honeypot انجام دهد. هر چه این میزان فعالیت و تعامل بیشتر باشد، فرد مهاجم کارهای بیشتری می‌تواند انجام دهد و در نتیجه شما می‌توانید راجع به وی و فعالیتش اطلاعات بیشتری بدست آورید. البته با افزایش این فعالیت و تعامل، میزان ریسك نیز افزایش می یابد Honeypot .های با تعامل کم اجازه انجام حجم کمی از تعاملات را صادر می‌کنند، در حالیکه Honeypot های با تعامل زیاد حجم زیادی از تعاملات را اجازه می‌دهند.

## Honeypotهای با تعامل کم

Honeypotهای با تعامل کم، با شبیه سازی سیستمها و سرویسها کار می‌کنند و فعالیتهای مهاجمان نیز صرفا شامل همان چیزهایی می‌شود که سرویسهای شبیه سازی شده اجازه می‌دهند. برای مثال، Honeypot BackOfficer Friendly یك نمونه Honeypot بسیار ساده است که هفت سرویس مختلف را شبیه سازی می‌کند. مهاجمان در مورد کارهایی که با Honeypot مبتنی بر سرویسهای شبیه سازی شده می‌توانند انجام دهند بسیار محدود هستند. در بیشترین حالت، مهاجمان می‌توانند به این Honeypot ها وصل شده و دستورات اولیه کمی را انجام دهند.

استفاده از Honeypot های با تعامل کم ساده تر است، چرا که آنها معمولا از پیش با گزینه های مختلفی برای administrator تنظیم شده اند. فقط کافی است شما انتخاب کرده و کلیك کنید و بلافاصله یك Honeypot را با سیستم عامل، سرویسها و رفتار مورد نظر خود در اختیار داشته باشید. از جمله این Honeypot ها می‌توان به Specter اشاره کرد که برای اجرای تحت ویندوز طراحی شده است. این Honeypotمی‌تواند تا ۱۳ سیستم عامل مختلف را شبیه سازی کرده و ۱٤ سرویس مختلف را نظارت نماید. واسطهای کاربری باعث می‌شوند که استفاده از این Honeypot ها بسیار ساده باشد، فقط کافی است روی سرویسهایی که می‌خواهید تحت نظارت قرار گیرند کلیك کرده و نحوه رفتار Honeypot را تعیین نمایید.

Honeypotهای با تعامل کم همچنین از خطر کمتری برخوردارند، چرا که سرویسهای شبیه سازی شده، کارهایی را که هکر می‌تواند انجام دهد محدود می‌کنند. هیچ سیستم عامل حقیقی برای لود کردن toolkit ها توسط مهاجم وجود ندارد، و هیچ سرویسی که واقعا بتوان به آن نفوذ کرد نیز موجود نیست.

اما این سرویسها حجم محدودی از اطلاعات را می‌توانند جمع آوری نمایند، چرا که هکرها در کار با آنها محدود هستند .همچنین این سرویسها در مواجهه با رفتارهای شناخته شده و حملات مورد انتظار بهتر کار می‌کنند. زمانی که هکرها کاری ناشناخته یا غیر منتظره را انجام می‌دهند، این Honeypot ها در درك فعالیت هکر، پاسخگویی مناسب، یا ثبت فعالیت با مشکل روبرو می‌شوند. به عنوان مثالهایی از Honeypotهای با تعامل کم می‌توان بهHoneyd ،Specter ، و KFSensor اشاره کرد. برای درك بهتر نحوه کار Honeypot های با تعامل کم، نگاه کوتاهی به Honeyd می اندازیم.

مثالی از Honeypot های با تعامل کمHoneyd :

Honeydیك Honeypot متن باز است که اولین بار در آوریل 2002 توسط «نیلز پرووس» عرضه شد Honeyd .به عنوان یك راه حل متن باز، رایگان بوده و اجازه دسترسی کامل کاربران به کد منبع خود را فراهم می آورد. این Honeypot که برای سیستمهای یونیکس طراحی شده است، می‌تواند در سیستمهای ویندوز نیز مورد استفاده قرار گیرد. البته در این حالت بسیاری از ویژگیهای مورد استفاده در سیستمهای یونیکس را از دست می‌دهد Honeyd .یك Honeypot با تعامل کم است که نرم افزار آن را روی یك کامپیوتر نصب می‌کنید. سپس این نرم افزار صدها سیستم عامل و سرویس مختلف را شبیه سازی می‌کند. با ویرایش فایل تنظیمات، شما تعیین می‌کنید که کدام آدرسهای IP توسط Honeyd کنترل گردند، انواع سیستم عاملهایی که شبیه سازی می‌شوند کدامها باشند، و کدام سرویسها شبیه سازی گردند.

برای مثال شما می‌توانید به Honeyd بگویید که هسته یك سیستم Linux 2.4.10 را با یك سرور FTP که به پورت ۲۱ گوش می‌دهد شبیه سازی نماید. اگر مهاجمان به این Honeypot مراجعه کنند، بر این باور خواهند بود که در حال تعامل با یك سیستم لینوکس هستند. اگر مهاجمان به سرویس FTP متصل شوند، تصور خواهند کرد که با یك سرویس واقعی FTP در تماس هستند. اسکریپت شبیه سازی شده از بسیاری نظرها کاملا شبیه یك سرویس FTP واقعی رفتار کرده و در عین حال، تمامی فعالیتهای فرد مهاجم را ثبت می‌کند. البته این اسکریپت چیزی بیش از یك برنامه نیست که منتظر یك ورودی مشخص از مهاجم می‌ماند و خروجی از پیش تعیین شده ای را تولید می‌کند. اگر فرد مهاجم کاری انجام دهد که اسکریپت شبیه سازی شده برای آن برنامه ریزی نشده باشد، این اسکریپت صرفا یك پیغام خطا برخواهد گرداند.

Honeydدارای ویژگیهایی است که برای Honeypot های با تعامل کم معمول نیست. این Honeypot نه تنها شبیه سازی سیستم عامل را به وسیله تغییر رفتار سرویسها انجام می دهد، بلکه سیستم عاملها را در سطح پشته IP نیز شبیه سازی می‌کند. اگر یك فرد مهاجم از روشهای فعال fingerprinting مانند ابزارهای امنیتی اسکن Nmap و Xprobe استفاده کند، Honeydدر سطح پشته IP به عنوان هر سیستم عاملی که بخواهید به شما پاسخ می‌دهد. به علاوه بر خلاف اغلب Honeypot های با تعامل کم، Honeydمی‌تواند میلیونها آدرس IP را کنترل نماید Honeyd .این کار را با کنترل کردن آدرسهای IP کامپیوترهایی که این Honeypot روی آنها نصب شده است انجام نمی‌دهد، بلکه تمامی آدرسهای IP بلا استفاده روی شبکه شما را کنترل می‌کند. زمانیکه Honeyd یك تلاش را برای اتصال به یکی از آدرسهای IP بلا استفاده تشخیص می‌دهد، آن تماس را قطع کرده، به طور پویا خود را به جای آن قربانی جا زده، و سپس با فرد مهاجم به تعامل می‌پردازد. این قابلیت به طور قابل توجهی شانس تعامل Honeyd با یك مهاجم را بالا می‌برد.

## Honeypotهای با تعامل زیاد

Honeypotهای با تعامل زیاد با Honeypot های با تعامل کم تفاوت بسیاری دارند، چرا که آنها کل سیستم عامل و برنامه ها را به طور حقیقی برای تعامل با مهاجمان فراهم می آورند Honeypot .های با تعامل زیاد چیزی را شبیه سازی نمی‌کنند، بلکه کامپیوترهایی واقعی هستند که برنامه هایی واقعی دارند که آماده نفوذ توسط مهاجمان هستند. مزایای استفاده از این دسته از Honeypot ها بسیار قابل توجه است. آنها برای این طراحی شده اند که حجم زیادی از اطلاعات را به دست آورند. این Honeypot ها نه تنها می‌توانند مهاجمانی را که به یك سیستم متصل می‌شوند شناسایی نمایند، بلکه به مهاجمان اجازه می‌دهند که به این سرویسها نفوذ کرده و به سیستم عامل دسترسی پیدا کنند. در نتیجه شما قادر خواهید بود rootkit های این مهاجمان را که به این سیستمها آپلود می‌شوند به دست آورده، در حالی-که مهاجمان با این سیستم در حال تعامل هستند ضربات کلید آنها را تحلیل نموده، و زمانیکه با سایر مهاجمان در حال ارتباط هستند آنها را کنترل کنید. در نتیجه می‌توانید حرکات، میزان مهارت، سازمان، و سایر اطلاعات ارزشمند را راجع به این مهاجمان به دست آورید.
همچنین از آنجایی که Honeypot های با تعامل زیاد شبیه سازی انجام نمی‌دهند، طوری طراحی شده اند که رفتارهای جدید، ناشناخته یا غیر منتظره را شناسایی کنند. این دسته از Honeypot ها بارها و بارها ثابت کرده اند که قابلیت کشف فعالیتهای جدید، از پروتکلهای IP غیر استاندارد مورد استفاده برای کانالهای دستورات پنهانی گرفته تا تونل زدن IPv6 در محیط IPv4 برای پنهان کردن ارتباطات را دارا هستند. البته برای به دست آوردن این قابلیتها باید بهای آن را نیز پرداخت .اولا Honeypot های با تعامل زیاد ریسك بالایی دارند. از آنجایی که مهاجمان با سیستم عاملهای واقعی روبرو می‌شوند، این Honeypot ها می‌توانند برای حمله کردن و ضربه زدن به سایر سیستمهایی که Honeypot نیستند مورد استفاده قرار گیرند. ثانیا Honeypot های با تعامل زیاد پیچیده هستند. این بار به همین سادگی نیست که یك نرم افزار نصب کنید و پس از آن یك Honeypot داشته باشید. بلکه شما باید سیستمهای واقعی را برای تعامل با مهاجمان ساخته و تنظیم نمایید. همچنین با تلاش برای کم کردن خطر مهاجمانی که از Honeypot شما استفاده می‌کنند، این پیچیدگی بیشتر نیز خواهد شد.
دو مثال از Honeypot های با تعامل زیاد عبارتند از Symantec Decoy Server و Honeynet ها. برای ارائه دید بهتری از Honeypotهای با تعامل زیاد، در ادامه به توضیح Decoy Server خواهیم پرداخت.

مثالی از Honeypot های با تعامل زیادSymantec Decoy Server :

Decoy Serverیك Honeypot تجاری است که توسط Symantec تولید شده و به فروش می‌رسد. این سیستم به عنوان یك Honeypotکه با تعامل زیاد است، سیستم عاملها و یا سرویسها را شبیه سازی نمی‌کند، بلکه سیستمهای حقیقی و برنامه های حقیقی را برای برقراری تعامل با مهاجمان ایجاد می‌کند. در حال حاضر Decoy Server صرفا روی سیستم عامل Solaris کار می‌کند. این برنامه ، نرم افزاری است که روی یك سیستم Solaris نصب می‌شود. سپس این نرم افزار سیستم میزبان موجود را در اختیار گرفته و تا چهار «قفس» یکتا ایجاد می‌کند، که هر قفس یك Honeypot است. هر قفس یك سیستم عامل جدا و سیستم فایل مخصوص به خود را داراست. مهاجمان درست مانند سیستم عاملهای واقعی با این قفسها ارتباط برقرار می‌کنند. چیزی که مهاجمان درك نمی‌کنند این است که هر

فعالیت و هر ضربه صفحه کلید آنها توسط Honeypot ثبت و ضبط می‌شود.

### Honeypotهای با تعامل کم در مقایسه با Honeypot های با تعامل زیاد

- در هنگام انتخاب Honeypot توجه داشته باشید که هیچ یك از این دو نوع از دیگری بهتر نیستند. بلکه هر یك دارای مزایا و معایبی بوده و برای کاری بهتر می‌باشند.
  مزایا و معایب Honeypot های با تعامل کم و Honeypot های با تعامل زیاد را می‌توان به شرح زیر بیان کرد :
  Honeypotهای با تعامل کم (شبیه سازی کننده سیستم عاملها و سرویسها(
- پیاده سازی و به کار گیری آسان: معمولا به سادگی نصب یك نرم افزار روی یك کامپیوتر است
- ریسك کم: سرویسهای شبیه سازی شده کارهایی که مهاجمان می‌توانند یا نمی‌توانند انجام دهند را کنترل می‌کنند .
- جمع آوری اطلاعات محدود: از آنجاییکه در این دسته از Honeypot ها مهاجمان مجاز به تعامل در حد محدودی هستند، اطلاعات محدودی نیز می‌توان راجع به آنها بدست آورد.
  Honeypotهای با تعامل زیاد (بدون شبیه سازی، با استفاده از سیستم عاملها و سرویسهای حقیقی(
- نصب و به کار گیری آنها می‌تواند سخت باشد (نسخه های تجاری ساده ترند )
- ریسك بالا. این موضوع که مهاجمان با سیستم عاملهای واقعی روبرو می‌شوند که می‌توانند با آن به تعامل بپردازند مزایا و معایب خاص خود را داراست .

سازمانهای مختلف، اهداف متفاوتی دارند و به همین دلیل از Honeypot های مختلفی نیز استفاده می‌کنند. یك روال معمول این است که سازمانهای تجاری مانند بانکها، خرده فروشان، و تولید کننده ها، Honeypotهای با تعامل کم را به علت ریسك پایین، به کار گیری آسان، و نگهداری ساده، ترجیح می‌دهند .استفاده از Honeypot های با تعامل زیاد نیز در میان سازمانهایی که به قابلیتهای منحصر به فرد راه حلهای با تعامل زیاد و مدیریت ریسك احتیاج دارند معمول تر است. از جمله این سازمانها می‌توان به سازمانهای نظامی، دولتی، و آموزشی اشاره کرد.

## کاربردهای Honeypot ها

در این مقاله قصد داریم کاربردهای Honeypot ها را به شما معرفی کنیم.

### Honeypotهای با تعامل زیاد

اکنون شما می‌دانید که Honeypot ها ابزارهایی بسیار انعطاف پذیرند که می‌توانند برای اهداف مختلفی مورد استفاده قرار گیرند. شما می‌توانید از آنها به عنوان ابزارهایی در انبار مهمات امنیتی خود به هر نحوی که مناسب نیازهای شماست استفاده کنید. به طور کلی می‌توان Honeypot ها را از لحاظ ارزش کاربردی در دو دسته «تجاری» و «تحقیقاتی» دسته بندی کرد. معمولا Honeypot های با تعامل کم برای اهداف تجاری مورد استفاده قرار می‌گیرند، درحالیکه Honeypot های با تعامل زیاد برای مقاصد تحقیقاتی استفاده می‌شوند. به هر حال هر یك از انواع Honeypot می‌توانند برای هر یك از اهداف فوق مورد استفاده قرار گیرند و هیچ یك از این اهداف، برتر از دیگری نیستند. زمانی که Honeypot ها برای اهداف تجاری مورد استفاده قرار می‌گیرند، می‌توانند از سازمانها به سه روش

محافظت نمایند: جلوگیری از حملات، تشخیص حملات، و پاسخگویی به حملات. اما زمانیك ه برای اهداف تحقیقاتی مورد استفاده قرار می‌گیرند، اطلاعات را جمع آوری می‌کنند. این اطلاعات ارزش های مختلفی برای سازمانهای گوناگون دارند. برخی سازمانها ممکن است بخواهند راهکارهای مهاجم را مطالعه کنند، در حالیکه ممکن است برخی دیگر به هشدارها و پیشگیری های زودهنگام علاقه مند باشند.

## جلوگیری از حملات

Honeypotها می‌توانند به روشهای مختلف از بروز حملات جلوگیری کنند. برای مثال Honeypot ها می‌توانند از حملات خودکار مانند حملاتی که به وسیله کرمها آغاز می‌شوند پیشگیری نمایند. این حملات مبتنی بر ابزارهایی هستند که به صورت تصادفی کل شبکه را اسکن کرده و به دنبال سیستمهای آسیب پذیر می‌گردند. اگر این سیستمها پیدا شوند، این ابزارهای خودکار به آن سیستم حمله کرده و کنترل آن را به دست می‌گیرند Honeypot.ها با کند کردن پروسه اسکن و حتی توقف آن به دفاع در برابر چنین حملاتی کمك می‌کنند. این Honeypotها که به نام Honeypot» های چسبناك» معروفند، فضای IP بدون استفاده را کنترل می‌کنند .زمانی که این Honeypot ها با یك فعالیت اسکن روبرو می‌شوند، شروع به تعامل کرده و سرعت کار مهاجم را کند می‌کنند. آنها این کار را با انواع مختلف ترفندهای TCPمانند استفاده از پنجره با اندازه صفر انجام می‌دهند. یك مثال از Honeypot های چسبناك، La Brea Tar pitاست .
Honeypotهای چسبناك معمولا از دسته با تعامل کم هستند. حتی می‌توان آنها را Honeypot بدون تعامل دانست، چرا که مهاجم را کند و متوقف می‌سازند.

شما می‌توانید با استفاده از Honeypot ها از شبکه خود در برابر حملات انسانی غیر خودکار نیز محافظت نمایید. این ایده مبتنی بر فریب یا تهدید است .در این روش شما مهاجمان را گیج کرده و زمان و منابع آنها را تلف می‌کنید. به طور همزمان سازمان شما قادر است که فعالیت مهاجم را تشخیص داده و در نتیجه برای پاسخگویی و متوقف کردن آن فعالیت زمان کافی در اختیار دارد. این موضوع حتی می-تواند یك گام نیز فراتر رود. اگر مهاجمان بدانند که سازمان شما از Honeypot استفاده می‌کند ولی ندانند که کدام سیستمها Honeypot هستند، ممکن است به طور کلی از حمله کردن به شبکه شما صرفنظر کنند. در این صورت Honeypot یك عامل تهدید برای مهاجمان به شمار رفته است. یك نمونه از Honeypot هایی که برای این کار طراحی شده اند، Deception Toolkit است.

## تشخیص حملات

یك راه دیگر که Honeypot ها با استفاده از آن از سازمان شما محافظت می‌کنند، تشخیص حملات است. از آنجایی که تشخیص، یك اشکال و یا نقص امنیتی را مشخص می‌کند، حائز اهمیت است. صرفنظر از این که یك سازمان تا چه اندازه امن باشد، همواره اشکالات و نقایص امنیتی وجود دارند. چرا که حداقل نیروی انسانی در پروسه امنیت درگیرند و خطاهای انسانی همیشه دردسر سازند. با تشخیص حملات، شما می‌توانید به سرعت به آنها دسترسی پیدا کرده، و خرابی آنها را متوقف ساخته یا کم نمایید.

ثابت شده است که تشخیص کار بسیار سختی است .تکنولوژیهایی مانند سنسورهای سیستم تشخیص نفوذ و لاگهای سیستمها، به دلایل مختلف چندان موثر نیستند. این تکنولوژیها داده های بسیار زیادی تولید کرده و درصد خطای تشخیص مثبت نادرست آن بسیار بالاست. همچنین این تکنولوژیها قادر به تشخیص حملات جدید نیستند و نمی‌توانند در محیطهای رمز شده یا IPv6 کار کنند. به طور معمول Honeypot های با تعامل کم، بهترین راه حل برای تشخیص هستند. چرا که به کار گرفتن و نگهداری این Honeypot ها ساده تر بوده و در مقایسه با Honeypotهای با تعامل بالا، ریسك کمتری دارند.

## پاسخگویی به حملات

Honeypotها با پاسخگویی به حملات نیز می‌توانند به سازمانها کمك کنند. زمانی که يك سازمان يك مشكل امنیتی را تشخیص می‌دهد، چگونه باید به آن پاسخ دهد؟ این مساله معمولا می‌تواند یکی از چالش برانگیزترین مسائل يك سازمان باشد. معمولا اطلاعات کمی درباره اینکه مهاجمان چه کسانی هستند، چگونه به آنجا آمده اند، و یا اینکه چقدر تخریب ایجاد کرده اند وجود دارد. در این شرایط، داشتن اطلاعات دقیق در مورد فعالیت های مهاجمان بسیار حیاتی است. دو مساله با پاسخگویی به رویداد آمیخته شده است. اول اینکه بسیاری از سیستم هایی که معمولا مورد سوء استفاده قرار می‌گیرند نمی‌توانند برای تحلیل شدن از شبکه خارج گردند. سیستم های تجاری، مانند میل سرور يك سازمان، به حدی مهم هستند که حتی اگر این سیستم هك شود، ممکن است متخصصان امنیت نتوانند سیستم را از شبکه خارج کنند و برای تحلیل آن بحث نمایند. به جای این کار، آنها مجبورند به تحلیل سیستم زنده در حالی که هنوز سرویسهای تجاری را ارائه می‌کند، بپردازند. این موضوع باعث می‌شود که تحلیل اتفاقی که رخ داده، میزان خسارت به بار آمده، و تشخیص نفوذ مهاجم به سیستم های دیگر سخت باشد.

مشکل دیگر این است که حتی اگر سیستم از شبکه خارج گردد، به حدی آلودگی داده وجود دارد که تشخیص اینکه فرد مهاجم چه کاری انجام داده است بسیار سخت است. منظور از آلودگی داده، داده های بسیار زیاد در مورد فعالیت های گوناگون(مانند ورود کاربران، خواندن حسابهای ایمیل، فایلهای نوشته شده در پایگاه داده، و مسائلی از این قبیل) است که باعث می‌شود تشخیص فعالیت های معمول روزانه از فعالیتهای فرد مهاجم سخت باشد.

Honeypotها برای هر دوی این مشکلات راه حل دارند. آنها می‌توانند به سرعت و سهولت از شبکه خارج گردند تا يك تحلیل کامل بدون تاثیر بر کارهای روزانه انجام گیرد. همچنین از آنجایی که این سیستم ها فقط فعالیت های خرابکارانه یا تایید نشده را ثبت می‌کنند، کار تحلیل بسیار ساده تر خواهد بود و داده های بسیار کمتری باید بررسی شوند. ارزش Honeypot ها به این است که آنها قادرند به سرعت اطلاعات عمیق و پرفایده را در اختیار سازمان قرار دهند تا بتواند به يك رویداد پاسخ دهد Honeypot .های با تعامل بالا بهترین گزینه برای پاسخگویی است. برای پاسخگویی به نفوذگران، شما باید دانش عمیقی در مورد کاری که آنها انجام داده اند، شیوه نفوذ، و ابزارهای مورد استفاده آنها داشته باشید. برای به دست آوردن این نوع داده ها، شما احتیاج به Honeypot های با تعامل بالا دارید.

## استفاده از Honeypot ها برای مقاصد تحقیقاتی

همانطور که پیش از این اشاره شد، Honeypotها می‌توانند برای مقاصد تحقیقاتی نیز مورد استفاده قرار گیرند. به این ترتیب اطلاعات ارزشمندی در مورد تهدیدات به دست می آید که تکنولوژیهای دیگر کمتر قادر به جمع آوری آن هستند. یکی از بزرگترین مشکلات متخصصان امنیت، کمبود اطلاعات یا آگاهی در مورد حملات مجازی است. زمانی که شما دشمن را نمی‌شناسید، چگونه می‌خواهید در برابر او دیوار دفاعی تشکیل دهید؟ Honeypot های تحقیقاتی این مشکل را با جمع آوری اطلاعاتی در مورد تهدیدات حل می‌کنند. سپس سازمانها می‌توانند از این اطلاعات برای مقاصد مختلفی مانند تحلیل، شناسایی ابزارها و روشهای جدید، شناسایی مهاجمان و جوامع آنها، هشدارهای اولیه و جلوگیری، و یا درك انگیزه های مهاجمان استفاده کنند.

اکنون شما باید درك بهتری از چیستی Honeypot ها، نحوه استفاده از آنها، تواناییها و مزایا و معایب آنها به دست آورده باشید .

# مکانیزم‌های جمع آوری اطلاعات در Honeypot ها

در این مقاله مکانیزم‌های مختلف جمع آوری اطلاعات در Honeypot ها را مورد بررسی قرار خواهیم داد.
جمع آوری اطلاعات در سیستمی که صرفا به این منظور طراحی شده است که مورد سوء استفاده مهاجمان و هکرها قرار گیرد، باید به صورتی باشد که علاوه بر اینکه تحلیل جدی فعالیت‌ها را ممکن می‌سازد، در عین حال مزاحم کار هکرها نیز نگردد. در شبکه هایی که از Honeypot به منظور تشخیص و تحلیل حملات و تهدیدات استفاده می‌کنند، داده‌ها می‌توانند در سه نقطه مختلف جمع آوری شوند که هریك مزایا و معایب خود را داراست. بر این اساس، سه مکانیزم مختلف برای جمع آوری اطلاعات در Honeypot ها تعریف می‌شود:

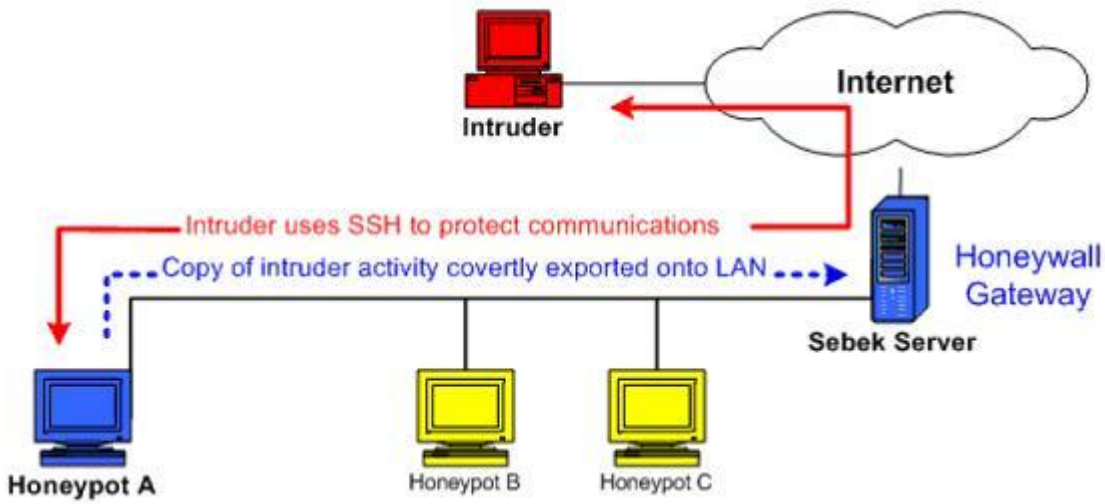
## ۱- مبتنی بر میزبان

داده هایی که بر روی میزبانی که مورد سوء استفاده قرار گرفته است جمع آوری می‌شوند، بیشترین پتانسیل را برای ثبت ارتباطات ورودی و خروجی، دستورات وارد شده بر روی میزبان از طریق خط دستور، و پردازه های در حال اجرا دارا هستند. متاسفانه این روش بیشترین خطر را نیز به همراه دارد. چرا که فرد نفوذگر معمولا به دنبال لاگ‌ها و یا ابزارهای امنیتی می‌گردد و سعی می‌کند آنها را غیرفعال نماید تا بتواند حضور خود را پنهان کند. به این ترتیب، جمع آوری داده ها می‌تواند توسط فرد هکر متوقف شده و یا دستخوش تغییر گردد، به طوری که نتایج به دست آمده را کاملا مغشوش نماید. به عنوان مثال‌هایی از ابزارهای مورد استفاده برای ثبت فعالیت بر روی یك Honeypot می‌توان به موارد زیر اشاره کرد:

- لاگ‌های سیستمی سیستم عامل (که نوعا اولین هدف یك نفوذگر است)
- سیستم‌های تشخیص نفوذ با قابلیت جمع آوری بسته مانند Snort
- ابزارهای جمع آوری و تحلیل بسته ها مانند Ethernal

## ۲- مبتنی بر شبکه

یك راه حل امن‌تر و در عین حال پیچیده تر برای جمع آوری داده ها این است که Honeypot، داده ها را به صورت پنهانی جمع آوری کرده و برای تحلیل بیشتر برای یك سرور دیگر ارسال نماید. این راه حل به ما اجازه می‌دهد که داده های جمع آوری شده توسط Honeypot را بر روی سیستم دیگری آرشیو کنیم. فرض بر این است که این سرور در برابر حملات مهاجمان ایمن شده است، چرا که ممکن است فرد نفوذگر متوجه جریان اطلاعات به بیرون از Honeypot شده و سعی کند مکانیزم جمع آوری و ارسال اطلاعات را متوقف نماید. با استفاده از ابزارهایی مانند Sebek، می‌توانیم سرویس جمع آوری داده را بر روی Honeypot پنهان کنیم و داده ها را از طریق یك ارتباط UDP به یك سرور دیگر ارسال کرده و بر روی آن ذخیره نماییم. Sebek فعالیت فرد نفوذگر را ضبط کرده و به صورت پنهانی آن را به یك سرور در داخل شبکه یا یك سرور در هر جایی بر روی اینترنت ارسال می‌کند. این موضوع در شکل زیر نمایش داده شده است.




جمع آوری اطلاعات مبتنی بر شبکه با استفاده از Sebek

### ۳- مبتنی بر مسیریاب/ دروازه (gateway)

آخرین روش معمول مورد استفاده برای جمع آوری داده ها در سطح gateway، مسیریاب یا فایروال شبکه است. از آنجاییکه یك gateway تمامی داده ها را بین میزبان‌های یك شبکه و اینترنت منتقل می‌کند، این فرصت را برای ما ایجاد می‌کند که از این طریق، تمامی ارتباطات و داده هایی را که از اینترنت به Honeypot های ما منتقل می‌شوند، ثبت نماییم. این مساله دارای خطر بیشتری نسبت به راه حل Sebekاست که در قسمت قبل توضیح داده شد. چرا که یك gateway معمولا در شبکه پنهان نیست و در نتیجه خود نیز به هدف حملات مهاجمان تبدیل می‌شود. به علاوه، این روش بیشتر وابسته به سخت افزار است، چرا که شما به سروری احتیاج دارید که در نقش یك gateway عمل کند. در عین حال، بسیاری از gateway هایی که در مقیاس کوچك یا خانگی طراحی می‌شوند، قابلیت‌های عمده ای برای ثبت اطلاعات ندارند و نمی‌توانند در این نقش مورد استفاده قرار گیرند.
بدون تکنیك‌های قوی جمع آوری داده، اعتبار اطلاعات جمع آوری شده از سیستم‌های میزبان به شدت کاهش می یابد و از آنجاییکه یکی از اهداف اصلی این اطلاعات شناخت مهاجمان است، اعتبار این اطلاعات نیز از اهمیت بسیار زیادی برخوردار است.

## مکانیزم‌های تحلیل اطلاعات در Honeypot ها

در این مقاله مکانیزم‌های مختلف تحلیل اطلاعات در Honeypot ها را مورد بررسی قرار خواهیم داد.
Honeypot ها در کشف فعالیت‌های هکرهای کلاه سیاه بسیار موثر عمل می‌کنند. پتانسیل حقیقی یك Honeypot فقط زمانی کاملا به کار گرفته می‌شود که داده های مربوط به این فعالیت‌ها به اطلاعات ارزشمندی تبدیل شوند. برای این منظور، باید یك روال برای جمع آوری این داده ها و ایجاد ارتباط بین آنها و ابزارها، تاکتیك‌ها و انگیزه های هکرهای کلاه سیاه وجود داشته باشد. چنین روالی تحلیل داده ها نامیده می‌شود. این روال یکی از پر چالش ترین و زمانبرترین بخش‌های کار است. در ادامه این مطلب، برخی از روش‌ها و تکنیك‌های موفق مورد استفاده برای این کار توضیح داده خواهند شد.

## ۱- لاگ های فایروال

فایروال‌ها می‌توانند در تحلیل ارتباطات ورودی و خروجی Honeypot مفید باشند. می‌دانیم که هر ترافیك شبکه ای که از Honeypot خارج شده و یا به آن وارد می‌شود، باید تحت عنوان ترافیك مشکوك یا خرابکار برچسب بخورد. تجزیه ترافیك ثبت شده از طریق فایروال و استخراج اطلاعات سودمند از آن، می‌تواند کاری خسته کننده باشد. بسته به نوع فایروالی که برای پروژه هانی‌نت مورد استفاده قرار می-دهید، برخی فایروال‌ها امکان ارسال پیغام هشدار از طریق ایمیل را در موارد ارتباطات مشکوك فراهم می آورند، که این کار می‌تواند حجم داده‌هایی را که باید تجزیه کنید کاهش دهد. برای مثال، شما می‌توانید فایروال خود را طوری پیکربندی کنید که پیغام هشداری را در زمان ایجاد یك ارتباط FTP از راه دور صادر نماید. چرا که این نوع ارتباطات معمولا نشان دهنده این هستند که Honeypot شما مورد سوء استفاده قرار گرفته و فرد مهاجم در حال تلاش برای ایجاد ارتباط FTP است.

## ۲- IDS

سیستم‌های تشخیص نفوذ مانند Snort، یك سری اطلاعات اصلی در اختیار کاربران خود قرار داده و نیز بسته به کنسول مورد استفاده کاربر، قابلیت گروه بندی هشدارهای مشابه، گروه بندی انواع ترافیك شبکه، و گروه بندی وقایع به ترتیب زمانی و یا حتی شناسایی یك گروه از وقایع به عنوان یك هشدار واحد را دارا هستند.

سه دسته اطلاعات اصلی که یك IDS به کاربر خود ارائه می‌دهد به این شرح هستند: یك IDS زمانی که فعالیت مشکوکی توسط یك امضاء شناسایی شده باشد پیغام هشدار صادر می‌کند، بسته‌های فعالیت مشکوك ذخیره شده را جمع آوری می‌کند، و در نهایت نشست‌های ASCII یا داده‌های ASCII کشف شده در payload بسته را ثبت می‌کند.

یك نکته مهم که باید در هنگام تحلیل اطلاعات به دست آمده از لاگ‌های Snort به آن توجه کرد این است که باید لاگ‌های Snort را با لاگ‌های فایروال مقایسه کرد تا به این وسیله، لایه ای از اطمینان به نتایج کار افزوده گردد. معمولا زمانی که یك فرد مهاجم Honeypot ما را هدف قرار می‌دهد، سعی در ایجاد یك ارتباط از راه دور می‌کند که به سادگی قابل شناسایی است.

یك ابزار مفید که می‌تواند برای جمع آوری ترافیك IRC مورد استفاده قرار گیرد، ابزاری به نام privmsg.pl است. این ابزار که اطلاعات حساس را به سرعت و به طور موثر از نشست‌های چت IRC استخراج می‌کند، توسط Max Vision توسعه داده شده است. IRC یا Internet Relay Chat اغلب برای ارتباط بین هکرها در زمان نفوذ مورد استفاده قرار می‌گیرد، بنابراین شما باید به طور جدی هر ترافیك IRC را که به Honeypot شما وارد شده یا از آن خارج می‌شود، ثبت کنید.

## ۳- لاگ های سیستم

بسته به نوع سیستم عامل مورد استفاده در Honeypot، تمامی فعالیت‌های سیستمی بر روی Honeypot شما به صورت محلی در یك فایل syslog (لاگ سیستمی) ثبت می‌شود. سیستم‌هایی مانند یونیکس، نسخه هایی از ویندوز مایکروسافت، و برخی سیستم عامل‌های دیگر، قابلیت ثبت تمامی فعالیت‌های سیستمی را که از طریق سیستم دیگری و از راه دور بر روی سیستم محلی انجام می‌شود دارا هستند. این قابلیت برای فهمیدن چگونگی دسترسی یك مهاجم به Honeypot، منبع حمله، انواع فعالیت سیستمی که می‌تواند مشکوك باشد مانند reboot ها، سرویس‌های متوقف شده یا آغاز شده، و حساب‌های غیرفعال شده یا ایجاد شده، بسیار مفید است. همچنین از آنجایی که این فعالیت سیستمی از راه دور ثبت می‌شود، ما می‌توانیم لاگ‌های سیستمی Honeypot را با لاگ‌های سرور دیگر مقایسه کنیم تا در صورتی که فرد مهاجم فایل‌های لاگ سیستمی موجود بر روی سیستم Honeypot محلی را حذف یا دستکاری کرده باشد، متوجه این موضوع شویم. همچنین این اطلاعات می‌تواند با اطلاعات ثبت شده در فایروال یا IDS نیز مقایسه گردد.

## ٤- جرم شناسی سیستم قربانی

جرم شناسی (Forensics) تکنیك دیگری است که به ما اجازه می‌دهد تحلیل دقیق‌تری بر روی یك سیستم Honeypot انجام دهیم. ما می‌توانیم روال‌ها، فایل‌ها یا حتی ابزارهایی را که هکرهای کلاه سیاه ممکن است برای سوء استفاده از یك سیستم مورد استفاده قرار داده باشند، بازیابی کنیم. این کار به ما اجازه می‌دهد فعالیت مهاجم را بازسازی کرده یا حتی فعالیت خرابکارانه ای را که سایر روش‌های تحلیلی نتوانسته اند کشف کنند، کشف کرده و معرفی نماییم. برای انجام جرم شناسی بر روی یك سیستم Honeypot، باید کپی‌هایی از تصویر سیستم عامل را به عنوان ابزار مقایسه در آغاز روال بازیابی در اختیار داشته باشیم. یك راه معمول برای ساختن کپی‌های بایت به بایتاز سیستم عامل Honeypot، استفاده از یك ابزار خط دستور معمولی به نام NetCat است. کپی کردن تصویر Honeypot ابتدا به وسیله

ایجاد يك نمونه از NetCat كه بر روی يك سيستم مورد اعتماد گوش نشسته است انجام می‌شود. برای مثال، دستور nc –l –p 5000 > Honeypot.hda1.dd، پورت شماره 5000 را برای گوش دادن بر روی سيستم مورد اعتماد باز می‌كند. سپس هر چيزی كه به اين پورت ارسال می‌شود در فايل Honeypot.hda1.dd ثبت می‌گردد. زمانی كه سيستم مورد اعتماد در حال گوش دادن است، شما می‌توانيد با دستور nc –w 3 5000 < partition/trusted_system/ يك پارتيشن را از سيستمی كه مورد سوء استفاده قرار گرفته كپی كنيد و آن را به سيستم مورد اعتماد ارسال نماييد.

### ۵- جرم شناسی پيشرفته سيستم قربانی

همانطور كه قبلا هم اشاره شد، بازيابی داده‌ها يك بخش حساس و بسيار مهم از تحليل فعاليت يك Honeypot است. اگر اين Honeypot توسط يك مهاجم مورد سوء استفاده قرار گرفته باشد، آنگاه احتمال زيادی وجود دارد كه وی برخی اطلاعات حساس را كه در صورت بازيابی مهم باشند، پاك كرده باشد. هكرها اغلب سعی می‌كنند با حذف فايل‌هايی كه برای دسترسی ايجاد شده اند يا فايل‌هايی كه نشان دهنده مجرم بودن آنهاست، ردپای خود را بعد از سوء استفاده از يك سيستم پاك نمايند. بنابراين داشتن يك روش برای بازيابی فايل‌های حذف شده بسيار مهم است. ابزاری به نام icat اين قابليت را دارد كه اين فايل‌های حذف شده را بازيابی كند. همچنين يك گزينه پيشرفته به نام unrm، يك پارتيشن خاص را دريافت كرده و تمامی فضای حذف شده از آن پارتيشن را برای تحليل‌های بعدی باز می‌گرداند.

## گام‌های راه اندازی و به كارگيری يك Honeypot

. در اين مقاله گام‌های راه اندازی و به كار گيری Honeypot ها را مورد بررسی قرار خواهيم داد.

به كار گيری يك Honeypot فيزيكی می‌تواند بسيار زمان‌بر و گران تمام شود، چرا كه سيستم عامل‌های مختلف ممكن است به سخت افزارهای خاصی نياز داشته باشند. به علاوه، هر Honeypot به سيستم فيزيكی خاص خود و حجم زيادی از تنظيمات پيكربندی احتياج دارد. در ادامه، گام‌های عمومی برای به كار گيری يك Honeypot اوليه را بيان می‌كنيم. اين گام‌ها، تا حدی به انواع دستگاه‌های شبكه، ابزارها و برنامه های نرم‌افزاری كه در اختيار ما است، بستگی دارد.

### ۱- انتخاب سخت افزار برای ميزبان

نخستين گام برای راه اندازی يك Honeypot، پيدا كردن كامپيوتری است كه شما می‌خواهيد آن را در معرض حملات هكرها و سوء استفاده قرار دهيد و بايد از هر داده ارزشمندی خالی شده باشد. اين سيستم، می‌تواند هر كامپيوتری باشد كه قادر به اجرای نرم‌افزار جمع آوری و كنترل داده ها باشد.

### ۲- نصب سيستم عامل

گام بعدی شامل ايجاد تغييرات لازم بر روی سيستم عامل فعلی، يا نصب يك سيستم عامل جديد بر روی كامپيوتر انتخاب شده است. نصب كردن يك سيستم عامل جديد، به شما امكان می‌دهد كه به بهترين شكل در مورد آسيب پذيری‌هايی كه مايليد بر روی سيستم وجود داشته باشد، تصميم گيری نماييد.

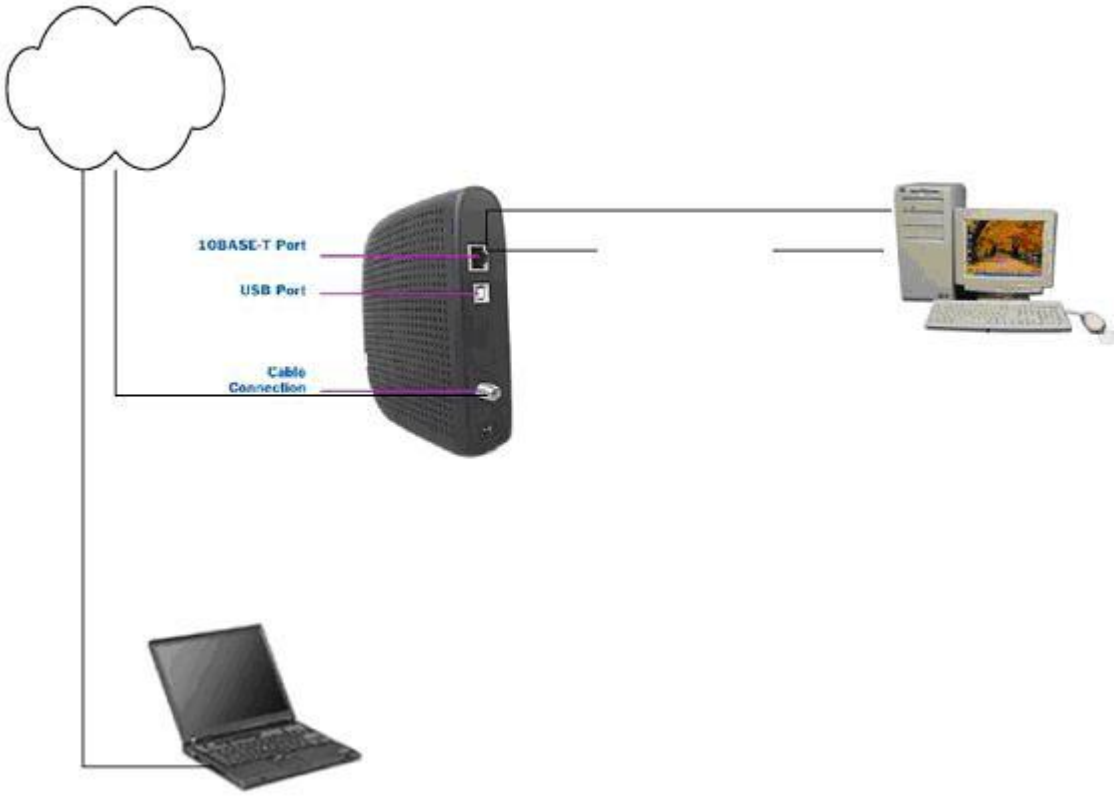
اگر تصميم گرفته ايد كه سيستم عامل فعلی را بر روی Honeypot خود نگه داريد، بايد از خطرات سوء استفاده مهاجمان از اين سيستم به عنوان يك Honeypot آگاه باشيد. برای مثال، ممكن است اطلاعات حساسی در مورد خود شما يا شخص ديگری بر روی اين سيستم وجود داشته باشد. اين اطلاعات می‌توانند در طول مدت استفاده از اين سيستم به عنوان Honeypot خراب شده، حذف شده و يا به سرقت روند. اگر قصد داريد پيكربندی سيستم عامل فعلی را نگه داريد، بهتر است تنظيمات جديدی را برای جلب ترافيك مشكوك به آن اضافه كنيد. برخی روال‌های معمول برای جذابتر كردن يك Honeypot عبارتند از باز كردن پورت‌های آسيب پذير شناخته شده، راه اندازی سرويس-

های آسیب پذیر شناخته شده، ایجاد درایوهای اشتراکی شبکه، استفاده از کلمات عبور و نام‌های کاربری ضعیف، و غیر فعال کردن نرم افزارهای آنتی ویروس و فایروال.

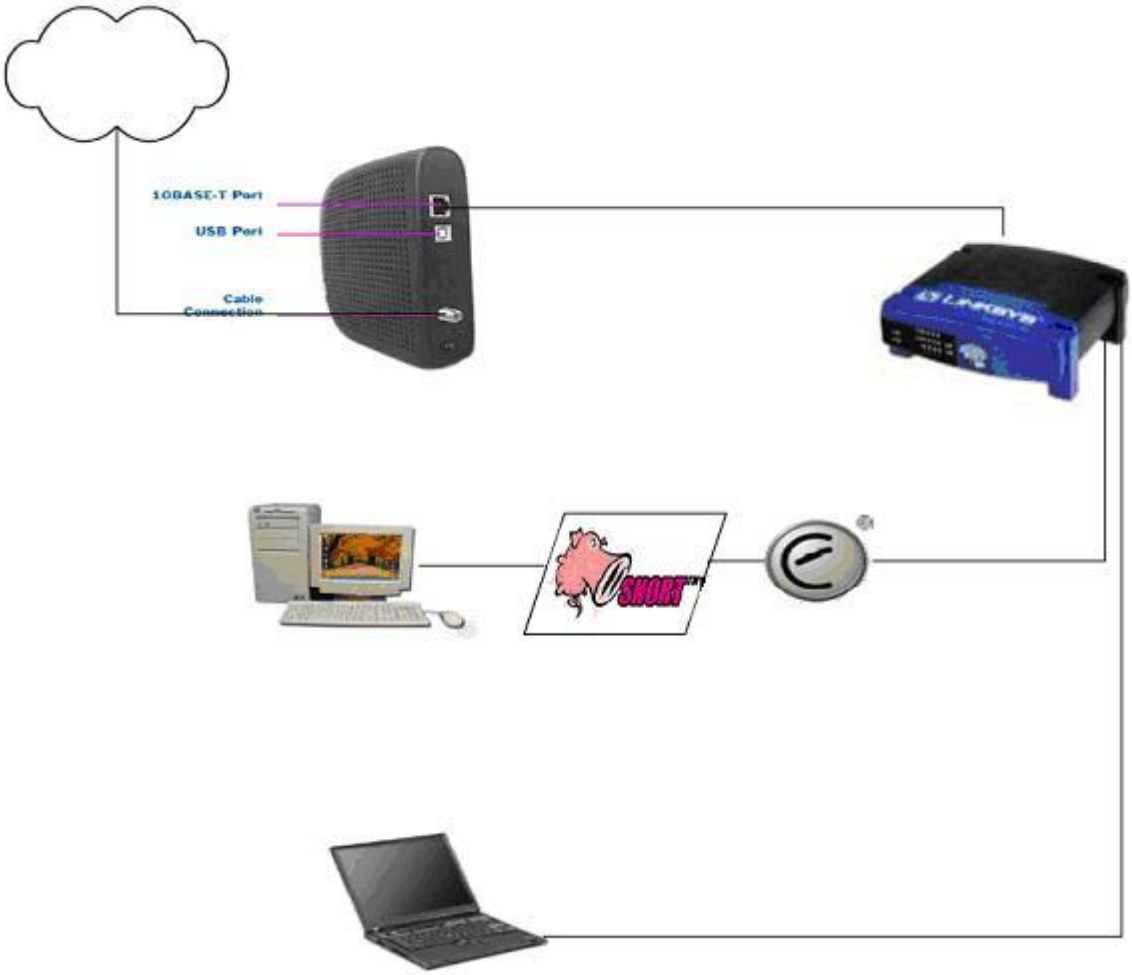
اگر تصمیم گرفته اید هارد را فرمت کرده و از ابتدا به نصب يك سيستم عامل جديد بپردازيد، انعطاف پذیری و تعداد گزینه ها برای تنظیم Honeypot افزایش می یابد. دیگر لازم نیست در مورد افشای اطلاعات حساسی که از قبل بر روی هارد میزبان وجود داشته است، نگران باشید. اگر تصمیم دارید این مسیر را طی کنید، ممکن است به برخی از ابزارهای معمول احتیاج داشته باشید. از جمله این ابزارها، يك ابزار پاك كردن ديسك مانند WIPE، يك ديسك راه انداز برای ایجاد پارتیشن‌ها و پارتیشن بندی مجدد هارد ديسك، ديسك‌های نصب سيستم عامل، و هر نرم‌افزار یا برنامه دیگری است که می‌خواهید بر روی این سیستم وجود داشته باشد. به خاطر داشته باشید که سایر بسته های نرم‌افزاری ممکن است حاوی آسیب‌پذیری‌هایی باشند که برای فرد نفوذگر مفید باشند.

## ۳- معماری شبکه

گام سوم شامل مشخص کردن معماری استراتژيك شبکه است. این شبکه باید طوری طراحی شده باشد که جمع آوری و ثبت داده‌ها برای تحلیل، و نیز جلوگیری از دسترسی به سایر سیستم‌های موجود بر روی LAN، به بهترین شکل ممکن باشد. شما باید اجزای شبکه خود را به شکل استراتژيك به یکدیگر متصل کنید تا بتوانید به خوبی در مورد بخش‌هایی از شبکه که ترافيك نفوذگر حق ورود به آن را داراست و بخش‌هایی از شبکه که باید از دسترس فرد نفوذگر مصون بماند، تصمیم گیری نمایید. این کار را باید با تعیین انواع اجزای شبکه (مانند فایروال‌ها، سیستم‌های تشخیص نفوذ، سایر سیستم‌های محلی، مودم‌های کابلی یا DSL و میزبان جمع آوری کننده داده ها) انجام دهید. در زیر، دو نمونه معماری شبکه مورد استفاده در به کارگیری Honeypot را مشاهده می‌کنید.

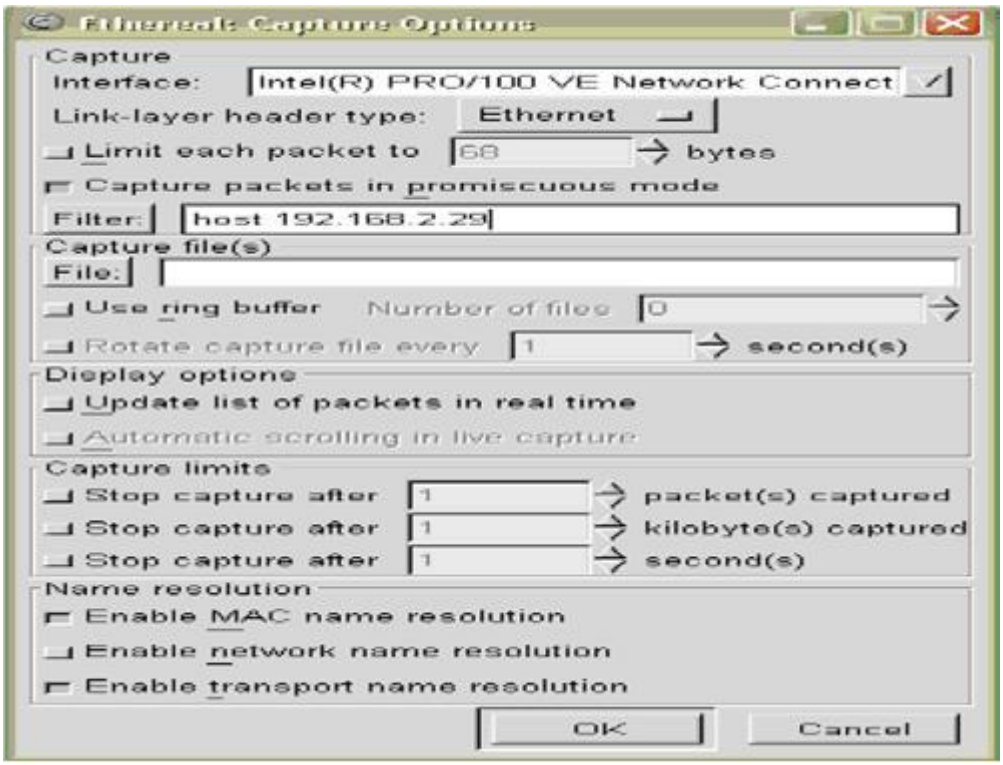



دو نمونه معماری شبکه مورد استفاده در به کار گیری Honeypot




## ٤- هشدارها و تشخیص نفوذ

چهارمین گام، مشخص کردن این است که چگونه می‌خواهید هشدارها را در زمانی که Honeypot با فعالیت‌های خرابکارانه ای مانند اسکن کردن پورت‌ها، اتصال به اشتراك شبکه، یا سایر ترافیك‌های خرابکار روبرو شده است، بررسی کرده، ثبت و دریافت نمایید و در نهایت فعالیت Honeypot را کنترل کنید. Snort و Ethereal برنامه های رایگانی هستند که از طریق اینترنت قابل دسترسی هستند. نصب Ethereal بسیار ساده است، اما نصب Snort ممکن است برای برخی افراد کمی سخت باشد. برای تحلیل کامل ترافیك، نصب کل بسته گزارش‌گیری Snort/ACID توصیه می‌شود. کل این بسته را می‌توان از سایت www.winSnort.com دانلود کرد. پیکربندی Ethereal برای نظارت بر ترافیك ورودی و خروجی شبکه به Honeypot، کار ساده ای است. شکل زیر نشان دهنده این است که چگونه می‌توانید یك فیلتر ساده را در Ethereal برای کنترل یك میزبان پیکربندی نمایید.




پیکربندی Snort برای کنترل ترافیك ورودی و خروجی شبکه به Honeypot، در مقایسه با پیکربندی مجموعه قوانین Snort ساده است. توجه داشته باشید که پیکربندی این سیستم تشخیص نفوذ بدون اطلاع از گزینه های قوانین Snort نباید انجام شود. Snort مجموع بزرگی از قوانین دارد که شما می‌توانید آنها را تغییر داده، اضافه یا حذف نمایید و به این ترتیب حجم خطاهای تشخیص اشتباه را کاهش دهید.

## مکانیزمهای تحلیل اطلاعات در Honeypot ها

در این مقاله مکانیزم‌های مختلف تحلیل اطلاعات در Honeypot ها را مورد بررسی قرار خواهیم داد.

Honeypot ها در کشف فعالیت‌های هکرهای کلاه سیاه بسیار موثر عمل می‌کنند. پتانسیل حقیقی یك Honeypot فقط زمانی کاملا به کار گرفته می‌شود که داده های مربوط به این فعالیت‌ها به اطلاعات ارزشمندی تبدیل شوند. برای این منظور، باید یك روال برای جمع آوری این داده ها و ایجاد ارتباط بین آنها و ابزارها، تاکتیك‌ها و انگیزه های هکرهای کلاه سیاه وجود داشته باشد. چنین روالی تحلیل داده ها نامیده می‌شود. این روال یکی از پر چالش ترین و زمانبرترین بخش‌های کار است. در ادامه این مطلب، برخی از روش‌ها و تکنیك‌های موفق مورد استفاده برای این کار توضیح داده خواهند شد.

### ۱- لاگ های فایروال

فایروال‌ها می‌توانند در تحلیل ارتباطات ورودی و خروجی Honeypot مفید باشند. می‌دانیم که هر ترافیك شبکه ای که از Honeypot خارج شده و یا به آن وارد می‌شود، باید تحت عنوان ترافیك مشکوك یا خرابکار برچسب بخورد. تجزیه ترافیك ثبت شده از طریق فایروال و استخراج اطلاعات سودمند از آن، می‌تواند کاری خسته کننده باشد. بسته به نوع فایروالی که برای پروژه هانی‌نت مورد استفاده قرار می-دهید، برخی فایروال‌ها امکان ارسال پیغام هشدار از طریق ایمیل را در موارد ارتباطات مشکوك فراهم می آورند، که این کار می‌تواند حجم داده‌هایی را که باید تجزیه کنید کاهش دهد. برای مثال، شما می‌توانید فایروال خود را طوری پیکربندی کنید که پیغام هشداری را در زمان ایجاد یك ارتباط FTP از راه دور صادر نماید. چرا که این نوع ارتباطات معمولا نشان دهنده این هستند که Honeypot شما مورد سوء استفاده قرار گرفته و فرد مهاجم در حال تلاش برای ایجاد ارتباط FTP است.

## ۲- IDS

سیستم‌های تشخیص نفوذ مانند Snort، یك سری اطلاعات اصلی در اختیار کاربران خود قرار داده و نیز بسته به کنسول مورد استفاده کاربر، قابلیت گروه بندی هشدارهای مشابه، گروه بندی انواع ترافیك شبکه، و گروه بندی وقایع به ترتیب زمانی و یا حتی شناسایی یك گروه از وقایع به عنوان یك هشدار واحد را دارا هستند.

سه دسته اطلاعات اصلی که یك IDS به کاربر خود ارائه می‌دهد به این شرح هستند: یك IDS زمانی که فعالیت مشکوکی توسط یك امضاء شناسایی شده باشد پیغام هشدار صادر می‌کند، بسته‌های فعالیت مشکوك ذخیره شده را جمع آوری می‌کند، و در نهایت نشست‌های ASCII یا داده‌های ASCII کشف شده در payload بسته را ثبت می‌کند.

یك نکته مهم که باید در هنگام تحلیل اطلاعات به دست آمده از لاگ‌های Snort به آن توجه کرد این است که باید لاگ‌های Snort را با لاگ‌های فایروال مقایسه کرد تا به این وسیله، لایه ای از اطمینان به نتایج کار افزوده گردد. معمولا زمانی که یك فرد مهاجم Honeypot ما را هدف قرار می‌دهد، سعی در ایجاد یك ارتباط از راه دور می‌کند که به سادگی قابل شناسایی است.

یك ابزار مفید که می‌تواند برای جمع آوری ترافیك IRC مورد استفاده قرار گیرد، ابزاری به نام privmsg.pl است. این ابزار که اطلاعات حساس را به سرعت و به طور موثر از نشست‌های چت IRC استخراج می‌کند، توسط Max Vision توسعه داده شده است.

IRC یا Internet Relay Chat اغلب برای ارتباط بین هکرها در زمان نفوذ مورد استفاده قرار می‌گیرد، بنابراین شما باید به طور جدی هر ترافیك IRC را که به Honeypot شما وارد شده یا از آن خارج می‌شود، ثبت کنید.

## ۳- لاگ های سیستم

بسته به نوع سیستم عامل مورد استفاده در Honeypot، تمامی فعالیت‌های سیستمی بر روی Honeypot شما به صورت محلی در یك فایل syslog (لاگ سیستمی) ثبت می‌شود. سیستم‌هایی مانند یونیکس، نسخه هایی از ویندوز مایکروسافت، و برخی سیستم عامل‌های دیگر، قابلیت ثبت تمامی فعالیت‌های سیستمی را که از طریق سیستم دیگری و از راه دور بر روی سیستم محلی انجام می‌شود دارا هستند. این قابلیت برای فهمیدن چگونگی دسترسی یك مهاجم به Honeypot، منبع حمله، انواع فعالیت سیستمی که می‌تواند مشکوك باشد مانند reboot ها، سرویس‌های متوقف شده یا آغاز شده، و حساب‌های غیرفعال شده یا ایجاد شده، بسیار مفید است. همچنین از آنجایی که این فعالیت سیستمی از راه دور ثبت می‌شود، ما می‌توانیم لاگ‌های سیستمی Honeypot را با لاگ‌های سرور دیگر مقایسه کنیم تا در صورتی که فرد مهاجم فایل‌های لاگ سیستمی موجود بر روی سیستم Honeypot محلی را حذف یا دستکاری کرده باشد، متوجه این موضوع شویم. همچنین این اطلاعات می‌تواند با اطلاعات ثبت شده در فایروال یا IDS نیز مقایسه گردد.

## ٤- جرم شناسی سیستم قربانی

جرم شناسی (Forensics) تکنیك دیگری است که به ما اجازه می‌دهد تحلیل دقیق‌تری بر روی یك سیستم Honeypot انجام دهیم. ما می‌توانیم روال‌ها، فایل‌ها یا حتی ابزارهایی را که هکرهای کلاه سیاه ممکن است برای سوء استفاده از یك سیستم مورد استفاده قرار داده باشند، بازیابی کنیم. این کار به ما اجازه می‌دهد فعالیت مهاجم را بازسازی کرده یا حتی فعالیت خرابکارانه ای را که سایر روش‌های تحلیلی نتوانسته اند کشف کنند، کشف کرده و معرفی نماییم. برای انجام جرم شناسی بر روی یك سیستم Honeypot، باید کپی‌هایی از تصویر سیستم عامل را به عنوان ابزار مقایسه در آغاز روال بازیابی در اختیار داشته باشیم. یك راه معمول برای ساختن کپی‌های بایت به بایتاز سیستم عامل Honeypot، استفاده از یك ابزار خط دستور معمولی به نام NetCat است. کپی کردن تصویر Honeypot ابتدا به وسیله ایجاد یك نمونه از NetCat که بر روی یك سیستم مورد اعتماد گوش نشسته است انجام می‌شود. برای مثال، دستور nc –l –p 5000 > Honeypot.hda1.dd، پورت شماره 5000 را برای گوش دادن بر روی سیستم مورد اعتماد باز می‌کند. سپس هر چیزی که به این پورت ارسال می‌شود در فایل Honeypot.hda1.dd ثبت می‌گردد. زمانی که سیستم مورد اعتماد در حال گوش دادن است، شما می‌توانید با دستور nc –w 3 5000 trusted_system /partition/ یك پارتیشن را از سیستمی که مورد سوء استفاده قرار گرفته کپی کنید و آن را به سیستم مورد اعتماد ارسال نمایید.

## ٥- جرم شناسی پیشرفته سیستم قربانی

همانطور که قبلا هم اشاره شد، بازیابی داده‌ها یك بخش حساس و بسیار مهم از تحلیل فعالیت یك Honeypot است. اگر این Honeypot توسط یك مهاجم مورد سوء استفاده قرار گرفته باشد، آنگاه احتمال زیادی وجود دارد که وی برخی اطلاعات حساس را که در صورت

بازیابی مهم باشند، پاك کرده باشد. هکرها اغلب سعی می‌کنند با حذف فایل‌هایی که برای دسترسی ایجاد شده اند یا فایل‌هایی که نشان دهنده مجرم بودن آنهاست، ردپای خود را بعد از سوء استفاده از یك سیستم پاك نمایند. بنابراین داشتن یك روش برای بازیابی فایل‌های حذف شده بسیار مهم است. ابزاری به نام icat این قابلیت را دارد که این فایل‌های حذف شده را بازیابی کند. همچنین یك گزینه پیشرفته به نام unrm، یك پارتیشن خاص را دریافت کرده و تمامی فضای حذف شده از آن پارتیشن را برای تحلیل‌های بعدی باز می‌گرداند.

## مکانیزمهای جمع آوری اطلاعات در Honeypot ها

در این مقاله مکانیزم‌های مختلف جمع آوری اطلاعات در Honeypot ها را مورد بررسی قرار خواهیم داد.
جمع آوری اطلاعات در سیستمی که صرفا به این منظور طراحی شده است که مورد سوء استفاده مهاجمان و هکرها قرار گیرد، باید به صورتی باشد که علاوه بر اینکه تحلیل جدی فعالیت‌ها را ممکن می‌سازد، در عین حال مزاحم کار هکرها نیز نگردد. در شبکه هایی که از Honeypot به منظور تشخیص و تحلیل حملات و تهدیدات استفاده می‌کنند، داده‌ها می‌توانند در سه نقطه مختلف جمع آوری شوند که هریك مزایا و معایب خود را داراست. بر این اساس، سه مکانیزم مختلف برای جمع آوری اطلاعات در Honeypot ها تعریف می‌شود:

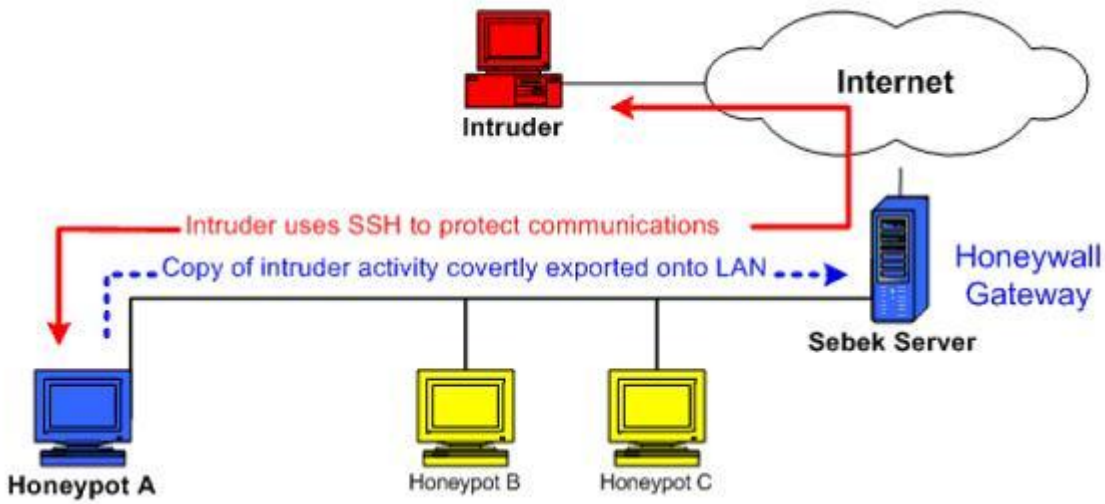
### ۱- مبتنی بر میزبان

داده هایی که بر روی میزبانی که مورد سوء استفاده قرار گرفته است جمع آوری می‌شوند، بیشترین پتانسیل را برای ثبت ارتباطات ورودی و خروجی، دستورات وارد شده بر روی میزبان از طریق خط دستور، و پردازه های در حال اجرا دارا هستند. متاسفانه این روش بیشترین خطر را نیز به همراه دارد. چرا که فرد نفوذگر معمولا به دنبال لاگ‌ها و یا ابزارهای امنیتی می‌گردد و سعی می‌کند آنها را غیرفعال نماید تا بتواند حضور خود را پنهان کند. به این ترتیب، جمع آوری داده ها می‌تواند توسط فرد هکر متوقف شده و یا دستخوش تغییر گردد، به طوری که نتایج به دست آمده را کاملا مغشوش نماید. به عنوان مثال‌هایی از ابزارهای مورد استفاده برای ثبت فعالیت بر روی یك Honeypot می‌توان به موارد زیر اشاره کرد:

- لاگ‌های سیستمی سیستم عامل (که نوعا اولین هدف یك نفوذگر است)
- سیستم‌های تشخیص نفوذ با قابلیت جمع آوری بسته مانند Snort
- ابزارهای جمع آوری و تحلیل بسته ها مانند Ethernal

### ۲- مبتنی بر شبکه

یك راه حل امن‌تر و در عین حال پیچیده تر برای جمع آوری داده ها این است که Honeypot، داده ها را به صورت پنهانی جمع آوری کرده و برای تحلیل بیشتر برای یك سرور دیگر ارسال نماید. این راه حل به ما اجازه می‌دهد که داده های جمع آوری شده توسط Honeypot را بر روی سیستم دیگری آرشیو کنیم. فرض بر این است که این سرور در برابر حملات مهاجمان ایمن شده است، چرا که ممکن است فرد نفوذگر متوجه جریان اطلاعات به بیرون از Honeypot شده و سعی کند مکانیزم جمع آوری و ارسال اطلاعات را متوقف نماید. با استفاده از ابزارهایی مانند Sebek، می‌توانیم سرویس جمع آوری داده را بر روی Honeypot پنهان کنیم و داده ها را از طریق یك ارتباط UDP به یك سرور دیگر ارسال کرده و بر روی آن ذخیره نماییم. Sebek فعالیت فرد نفوذگر را ضبط کرده و به صورت پنهانی آن را به یك سرور در داخل شبکه یا یك سرور در هر جایی بر روی اینترنت ارسال می‌کند. این موضوع در شکل زیر نمایش داده شده است.




جمع آوری اطلاعات مبتنی بر شبکه با استفاده از Sebek

### ۳- مبتنی بر مسیریاب/ دروازه (gateway)

آخرین روش معمول مورد استفاده برای جمع آوری داده ها در سطح gateway، مسیریاب یا فایروال شبکه است. از آنجاییکه یك gateway تمامی داده ها را بین میزبان‌های یك شبکه و اینترنت منتقل می‌کند، این فرصت را برای ما ایجاد می‌کند که از این طریق، تمامی ارتباطات و داده هایی را که از اینترنت به Honeypot های ما منتقل می‌شوند، ثبت نماییم. این مساله دارای خطر بیشتری نسبت به راه حل Sebekاست که در قسمت قبل توضیح داده شد. چرا که یك gateway معمولا در شبکه پنهان نیست و در نتیجه خود نیز به هدف حملات مهاجمان تبدیل می‌شود. به علاوه، این روش بیشتر وابسته به سخت افزار است، چرا که شما به سروری احتیاج دارید که در نقش یك gateway عمل کند. در عین حال، بسیاری از gateway هایی که در مقیاس کوچك یا خانگی طراحی می‌شوند، قابلیت‌های عمده ای برای ثبت اطلاعات ندارند و نمی‌توانند در این نقش مورد استفاده قرار گیرند.
بدون تکنیك‌های قوی جمع آوری داده، اعتبار اطلاعات جمع آوری شده از سیستم‌های میزبان به شدت کاهش می یابد و از آنجاییکه یکی از اهداف اصلی این اطلاعات شناخت مهاجمان است، اعتبار این اطلاعات نیز از اهمیت بسیار زیادی برخوردار است.