✓کارنیل، بزرگترین شبکه موفقیت ایرانیان می باشد، که افرادی زیادی توانسته اند با آن به موفقیت برسند، فاطمه رتبه ۱۱ کنکور کارشناسی، محمد حسین رتبه۶۸ کنکور کارشناسی، سپیده رتبه ۳ کنکور ارشد، مریم و همسرش راه اندازی تولیدی مانتو، امیر راه اندازی فروشگاه اینترنتی،کیوان پیوستن به تیم تراکتور سازی تبریز، میلاد پیوستن به تیم صبا، مهسا تحصیل در ایتالیا، و..... این موارد گوشه از افرادی بودند که با کارنیل به موفقیت رسیده اند، شما هم می توانید موفقیت خود را با کارنیل شروع کنید.

برای پیوستن به تیم کارنیلی های موفق روی لینک زیر کلیک کنید.

www.karnil.com

همچنین برای ورود به کانال تلگرام کارنیل روی لینک زیر کلیک کنید.

https://telegram.me/karnil

مجموعه مقالاتی
پیرامون

هانی پات و هانی نت

به اهتمام
عباس عظیمی

تقدیم به همه تولید کنندگان ایرانی
که کارایی و کیفیت دغدغه همیشگی آنهاست.

فهرست مقالات

امیدواریم توی سازمان شما هیچ کارمند شیطونی وجود نداشته باشه،
اما خدای ناخواسته اگر یکی پیدا شد، با درایت شما اینطوری پیش خودش فکر کنه:

اشتباه کردم. من کی هستم که بخوام حال بچه‌های انفورماتیک سازمان رو بگیرم؟!
البته شاید خیلی هم مقصر نباشم، آخه این روزا همه از امنیت و هک صحبت می کنن و خودش کلی محرکه تا آدم وقت های بیکاریش رو پشت کامپیوتر اداره یه جورایی پر کنه. می دونم، می دونم. این دلیل نمیشه که بخوام کارتابل بقیه رو مطالعه کنم، یا از این نرم افزارهای کوفتی برای اسکن امنیتی سرورها استفاده کنم.
خودمونیم، خوب شد کسی نبود اون موقعیت رو ببینه که بادی به غَب غَب انداختم و با یه تُپُر درشت به مدیر انفورماتیک سازمان گفتم: "برید به جای گیر دادن و بستن DVDها و USBها یه کم به امنیت سرورهاتون رسیدگی کنید. این همه پورت باز خنده داره!!!"
آخ آخ، بد جوری غافلگیرم کرد و بد ضد حالی بود که گفت: "عزیزم تو با هانی پات ما سر کار بودی، همه فعالیت های ضد امنیتی به همراه گزارشات و مستندات مربوطه روی میز رئیس حراسته. برو خوش باش."
انگار یه سطل آب یخ ریختن روم. یخهاش هم هنوز آب نشده بود، سرم درد می کنه. دارم دیونه می شم.

1

هانی پات چیست؟

Honeypot ها یک تکنولوژی تقریبا جدید و شدیداً پویا هستند. همین ماهیت پویا باعث می شود که به راحتی نتوان آنها را تعریف کرد. Honeypot ها به خودی خود یک راه حل به شمار نرفته و هیچ مشکل امنیتی خاصی را حل نمی کنند، بلکه ابزارهای بسیار انعطاف پذیری هستند که کارهای مختلفی برای امنیت اطلاعات انجام می دهند و تأثیر شگرفی بر امنیت سازمان می گذارند.

این فن آوری با تکنولوژیهایی مانند فایروالها و سیستمهای تشخیص نفوذ (IDS) متفاوت است، چرا که آنها مسائل امنیتی خاصی را حل کرده و به همین دلیل راحت تر تعریف می شوند. فایروالها یک تکنولوژی پیشگیرانه به شمار می آیند، آنها از ورود مهاجمان به شبکه یا سیستم های کامپیوتری جلوگیری می کنند. IDS ها یک 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 کار سخت تری است، چرا که آنها در پیشگیری، تشخیص، جمع آوری اطلاعات و کارهای دیگری مورد استفاده قرار می گیرند، اما حالت دفاعی ندارند و به عبارتی کار امنیتی نمی کنند اما بر امنیت شبکه به شدت تأثیر می گذارند.

شاید بتوان یک Honeypot را با عناوین زیر توصیف کرد:

- یک هانی پات با هویتی نفوذ پذیر به وظایف خود می پردازد.
- هانی پات یک ابزار امنیتی است و نقشی ضروری در امنیت سازمانها، بسیار بیش تر از Firewall و IPS ایفاء می کند.

- Honeypot یک سیستم اطلاعاتی است که ارزش آن به استفاده غیر مجاز و ممنوع دیگران از آن است.

این تعاریف به وسیله اعضای لیست ایمیل Honeypot انجام شده است. لیست ایمیل Honeypot یک انجمن 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 یک Honeypot نشان دهنده نحوه کار آن و یا حتی هدف آن نیست. این تعریف صرفاً ناظر به نحوه ارزش گذاری یک Honeypot است. به عبارت ساده تر، Honeypot ها تکنولوژی هستند که ارزش آنها به تعامل مجرمان با آنها بستگی دارد. تمامی Honeypot ها بر اساس یک ایده کار می کنند:

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 یک حرکت خرابکارانه به شمار می رود.

یک Honeypot سیستمی است که در شبکه سازمان قرار می گیرد، اما برای کاربران آن شبکه هیچ کاربردی ندارد و در حقیقت هیچ یک از اعضای سازمان حق برقراری هیچگونه ارتباطی با این سیستم را ندارند. این سیستم دارای یک سری ضعفهای امنیتی عمدی است. از آنجاییکه مهاجمان برای نفوذ به یک شبکه همیشه به دنبال سیستمهای دارای ضعف می گردند، این سیستم توجه آنها را به خود جلب می کند و با توجه به اینکه هیچکس حق ارتباط با این سیستم را ندارد، پس هر تلاشی برای برقراری ارتباط با این سیستم، یک تلاش خرابکارانه از سوی مهاجمان محسوب می شود. در حقیقت این سیستم نوعی دام است که مهاجمان را فریب داده و به سوی خود جلب می کند و به این ترتیب علاوه بر امکان نظارت و کنترل کار مهاجمان، این فرصت را نیز به سازمان می دهد که فرد مهاجم را شناسایی کند و از سیستمهای اصلی شبکه خود دور نگه دارند.

یک Honeypot هیچ سرویس واقعی ارائه نمی دهد. هر تعاملی که انجام گیرد، هر تلاشی که برای ورود به این سیستم صورت گیرد، یا هر فایل داده ای که روی یک Honeypot مورد دسترسی قرار گیرد، با احتمال بسیار زیاد نشانه ای از یک فعالیت خرابکارانه و غیر مجاز است. برای مثال، یک سیستم Honeypot می تواند روی یک شبکه داخلی به کار گرفته شود. این Honeypot از هیچ ارزش خاصی برخوردار نیست و هیچکس در درون سازمان نیازی به استفاده از آن ندارد و نباید از آن استفاده کند. این سیستم می تواند به ظاهر یک فایل سرور، یک وب سرور، یا حتی یک ایستگاه کاری معمولی باشد. اگر کسی با این سیستم ارتباط برقرار نماید، به احتمال زیاد در حال انجام یک فعالیت غیر مجاز یا خرابکارانه است.

در حقیقت، یک Honeypot حتی لازم نیست که حتماً یک کامپیوتر باشد. این سیستم می تواند هر نوع نهاد دیجیتالی باشد (معمولاً از آن به عنوان Honeytoken یاد می شود) که هیچ ارزش واقعی ندارد. برای مثال، یک بیمارستان می تواند مجموعه ای نادرست از رکوردهای اطلاعاتی بیماران ایجاد نماید. از آنجا که این رکوردها Honeypot هستند، هیچکس نباید به آنها دسترسی پیدا کرده و یا با آنها تعامل برقرار کند. این رکوردها می توانند در داخل پایگاه داده بیماران این بیمارستان به عنوان یک جزء Honeypot قرار گیرند. اگر یک کارمند یا یک فرد مهاجم برای دسترسی به این رکوردها تلاش نمود، می توان اقدام وی را به عنوان نشانه ای از یک فعالیت غیر مجاز تلقی کرد، چرا که هیچکس نباید از این رکوردها استفاده کند. اگر شخصی یا چیزی به این رکوردها دسترسی پیدا کند، یک پیغام هشدار صادر می شود. این ایده ی ساده پشت Honeypot هاست که آنها را ارزشمند می کند.

دو یا چند Honeypot که در یک شبکه قرار گرفته باشند، یک HoneyNET را تشکیل می دهند. نوعاً در شبکه های بزرگتر و متنوع تر که یک Honeypot به تنهایی برای نظارت بر شبکه کافی نیست، از HoneyNet استفاده می کنند. HoneyNet ها معمولا به عنوان بخشی از یک سیستم بزرگ تشخیص نفوذ پیاده سازی می شوند. در حقیقت HoneyNet یک شبکه از Honeypot های با تعامل بالاست که طوری تنظیم شده است که تمامی فعالیتها و تعاملها با این شبکه، کنترل و ثبت می شود.

مزایای استفاده از Honeypot

- Honeypot ها صرفا مجموعه های کوچکی از داده ها را جمع آوری می کنند. Honeypot ها فقط زمانی که کسی یا چیزی با آنها ارتباط برقرار کند داده ها را جمع آوری می نمایند، 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 می کنند، با استفاده از Honeypot ها ممکن است فقط صد پیغام هشدار را ثبت نمایند. این موضوع باعث می شود که مدیریت و تحلیل داده های جمع آوری شده توسط Honeypot ها بسیار ساده تر باشد.

- Honeypot ها موارد خطاهای تشخیص اشتباه را کاهش می دهند. 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 یک رویداد را تهدید تشخیص می دهند که در حقیقت تهدیدی در کار نیست. هر چه احتمال این تشخیص اشتباه بیشتر باشد، تکنولوژی تشخیص دهنده بی فایده تر می شود. Honeypot ها به طور قابل توجهی درصد این تشخیصهای اشتباه را کاهش می دهند، 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.

- Honeypot ها می توانند حملات ناشناخته را تشخیص دهند. چالش دیگری که در تکنولوژیهای تشخیصی معمول وجود دارد این است که آنها معمولا حملات ناشناخته را تشخیص نمی دهند. این یک 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 می دهند. تکنولوژیهای تشخیصی مبتنی بر امضا، در تعریف به این معنا هستند که ابتدا باید هر حمله ای

حداقل یک 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 می برد. Honeypot ها طوری طراحی شده اند که حملات جدید را نیز شناسایی و کشف می کنند. چرا که هر فعالیتی در ارتباط با Honeypot ها غیر معمول شناخته شده و در نتیجه حملات جدید را نیز معرفی می کند.

- هانی پات ها فعالیتهای رمز شده را نیز کشف می کنند. حتی اگر یک حمله رمز شده باشد، Honeypot ها می توانند این فعالیت را کشف کنند. به تدریج که تعداد بیشتری از سازمانها از پروتکلهای رمزگذاری مانند SSH، IPsec و SSL استفاده می کنند، این مساله بیشتر خود را نشان می دهد. Honeypot ها می توانند این کار را انجام دهند، چرا که حملات رمز شده با Honeypot به عنوان یک نقطه انتهایی ارتباط، تعامل برقرار می کنند و این فعالیت توسط Honeypot رمز گشایی می شود.

- Honeypot با IPv6 کار می کند. اغلب Honeypot ها صرف نظر از پروتکل IP از جمله IPv6، در هر محیط IP کار می کنند. IPv6 یک 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.

- Honeypot ها بسیار انعطاف پذیرند. Honeypot ها بسیار انعطاف پذیرند و می توانند در محیطهای مختلفی مورد استفاده قرار گیرند. همین قابلیت انعطاف پذیر Honeypot هاست که به آنها اجازه می دهد کاری را انجام دهند که تعداد بسیار کمی از تکنولوژیها می توانند انجام دهند: جمع آوری اطلاعات ارزشمند به خصوص بر علیه حملات داخلی.

- Honeypot ها به حداقل منابع نیاز دارند. حتی در بزرگترین شبکه ها، Honeypot ها به حداقل منابع احتیاج دارند. یک کامپیوتر پنتیوم قدیمی و ساده می تواند میلیونها آدرس IP یا یک شبکه بسیار بزرگ را نظارت نماید.

منبع: www.certcc.ir

انواع هانی پات

در مقاله ***هانی پات چیست؟*** به تعریف سیستمهای Honeypot، مزایا و معایب این سیستمها پرداختیم. در این مقاله پس از معرفی انواع Honeypot، به ذکر یک مثال از هر نوع خواهیم پرداخت.

برای درک بهتر هانی پات 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 یک 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 ریسک نیز افزایش می یابد. هانی پات 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 می دهند.

Low Interaction – LinT

هانی پات های با تعامل کم

Honeypot های 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 یک 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 هانی پات های با تعامل کم ساده تر است، چرا که آنها معمولاً از پیش با گزینه های مختلفی برای Administrator تنظیم شده اند. فقط کافی است شما انتخاب کرده و کلیک کنید و بلافاصله یک 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 Honeypot می‌تواند تا ۱۳ سیستم عامل مختلف را شبیه سازی کرده و ۱۴ سرویس مختلف را نظارت نماید. واسط های کاربری باعث می‌شوند که استفاده از این Honeypot ها بسیار ساده باشد، فقط کافی است روی سرویسهایی که می‌خواهید تحت نظارت قرار گیرند کلیک کرده و نحوه رفتار Honeypot را تعیین نمایید. هانی پات های 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 واقعاً 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 درک فعالیت هکر، پاسخگویی مناسب، یا ثبت فعالیت با مشکل روبرو می‌شوند.

به عنوان مثالهایی از هانی پات های با تعامل کم می‌توان به HoneyD، Specter، و KFSensor اشاره کرد. برای درک بهتر نحوه کار Honeypot های با تعامل کم، نگاه کوتاهی به HoneyD می اندازیم.

HoneyD – مثالی از Honeypot های با تعامل کم:

HoneyD یک هانی پات متن باز است که اولین بار در آوریل ۲۰۰۲ توسط **نیلز پرووس** عرضه شد. HoneyD به عنوان یک 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.
HoneyDیک Honeypot با تعامل کم است که نرم افزار آن را روی یک 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 یک سیستم Linux 2.4.10 را با یک سرور FTP که به پورت ۲۱ گوش می‌دهد شبیه سازی نماید. اگر مهاجمان به این هانی پات مراجعه کنند، بر این باور خواهند بود که در حال تعامل با یک سیستم لینوکس هستند. اگر مهاجمان به سرویس FTP متصل شوند، تصور خواهند کرد که با یک سرویس واقعی FTP در تماس هستند. اسکریپت شبیه سازی شده از بسیاری نظرها کاملاً شبیه یک سرویس FTP واقعی رفتار کرده و در عین حال، تمامی فعالیتهای فرد مهاجم را ثبت می‌کند. البته این اسکریپت چیزی بیش از یک برنامه نیست که منتظر یک 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 یک پیغام خطا باز می گرداند.

HoneyD دارای 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 یک فرد مهاجم از روشهای فعال fingerprinting مانند ابزارهای امنیتی اسکن Nmap و Xprobe استفاده کند، HoneyD در سطح پشته IP به عنوان هر سیستم عاملی که بخواهید پاسخ می‌دهد.

بر خلاف اغلب هانی پات های با تعامل کم، HoneyD می‌تواند 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 یک 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 HoneyDبا یک مهاجم را بالا می‌برد.

High Interaction - HinT

هانی پات های با تعامل زیاد

Honeypot های 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 کامپیوترها و سیستم عامل هایی واقعی هستند که برنامه هایی واقعی دارند که آماده نفوذ توسط مهاجمان هستند. مزایای استفاده از این دسته از هانی پات 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 یک 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 آورید و در حالی‌که 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. اولاً هانی پات های با تعامل زیاد ریسک 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. ثانیاً Honeypot های با تعامل زیاد پیچیده هستند. این بار به همین سادگی نیست که یک نرم افزار نصب کنید و پس از آن یک 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 Decoy Server و Honeynet ها. برای ارائه دید بهتری از Honeypot های با تعامل زیاد، در ادامه به توضیح Decoy Server خواهیم پرداخت.

Decoy Server – مثالی از Honeypot های با تعامل زیاد:

Decoy Server یک Honeypot تجاری است که توسط Symantec تولید شده و به فروش می‌رسد. این سیستم به عنوان یک Honeypot که 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 صرفاً روی سیستم

عامل Solaris کار می‌کند. این برنامه، نرم افزاری است که روی یک 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 یک Honeypot است. هر قفس یک 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 درک نمی‌کنند این است که هر فعالیت و هر ضربه صفحه کلید آنها توسط Honeypot ثبت و ضبط می‌شود.

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

در هنگام انتخاب Honeypot توجه داشته باشید که هیچ یک از این دو نوع از دیگری بهتر نیستند. بلکه هر یک 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:

Honeypot های با تعامل کم (شبیه سازی کننده سیستم عاملها و سرویسها)

- پیاده سازی و به کار گیری آسان: معمولاً به سادگی نصب یک نرم افزار روی یک کامپیوتر است.
- ریسک کم: سرویس های 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.

Honeypot های با تعامل زیاد

(بدون شبیه سازی، با استفاده از سیستم عاملها و سرویس های حقیقی)

- نصب و به کار گیری آنها می‌تواند سخت باشد (نسخه های تجاری ساده ترند)
- ریسک 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 هانی پات های مختلفی نیز استفاده می‌کنند. یک روال معمول این است که سازمانهای تجاری مانند بانکها، خرده فروشان، و تولید کننده ها، Honeypot های با تعامل کم را به علت ریسک 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 ریسک احتیاج دارند معمول تر است.

Medium Interaction - MinT

هانی پات هایی با سطح تعامل میانه

به منظور پوشش خلأ موجود بین هانی پات های LinT و HinT، هانی پات هایی با عنوان MinT ارائه شدند. در این نوع از هانی پات ها که توسط گروه امنیتی کمین پـاد با نام **کیمن پاد** و تحت لیسانس شرکت .vaya co طراحی و تولید شده است، فاصله بین ۲ نوع اول پوشش داده شده و هانی پات علاوه بر آنکه در حالت LinT فعالیت می کند، در وضعیتی کامل به ایجاد تعامل با هکر و بدافزار ها می پردازد. بعبارتی دیگر هانی پات هایی با سطح عملکرد میانه، معماری و ساختاری مشابه هانی پات های LinT دارند اما رفتاری مشابه هانی پات های HinT را ارائه می دهند و امروزه این نوع از هانی پات ها جزء پر کاربردترین هانی پات ها قلمداد می شوند.

منبع: www.certcc.ir

3

کاربردهای هانی پات ها

پیش از این در دو مقاله به معرفی Honeypot ها، مزایا و معایب این سیستمهای امنیتی، و انواع آنها پرداختیم. در این مقاله قصد داریم کاربردهای Honeypot ها را به شما معرفی کنیم.

هانی پات های 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 یک از انواع Honeypot می‌تواند برای هر یک از اهداف فوق مورد استفاده قرار گیرند و هیچ یک از این اهداف، برتر از دیگری نیستند. زمانی که هانی پات 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 زمانیکه 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 زود هنگام علاقه مند باشند.

جلوگیری از حملات

هانی پات ها می‌توانند به روشهای مختلف از بروز حملات جلوگیری کنند. برای مثال هانی پات 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 آنها را به دست می‌گیرند. Honeypot ها با کند کردن پروسه اسکن و حتی توقف آن به دفاع در برابر چنین حملاتی کمک می‌کنند. این Honeypot ها که به نام **هانی پات های چسبناک** معروفند، فضایIP بدون استفاده را کنترل می‌کنند. زمانی که این هانی پات ها با یک 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.

یک مثال از هانی پات های چسبناک، LaBrea Tarpit است. هانی پات های چسبناک معمولا از دسته با تعامل کم هستند. حتی می‌توان آنها را هانی پات 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 داشته باشد. این موضوع حتی می‌تواند یک گام نیز فراتر رود. اگر مهاجمان بدانند که سازمان شما از هانی پات استفاده می‌کند ولی ندانند که کدام سیستم ها هانی پات هستند، ممکن است به طور کلی از حمله کردن به شبکه شما صرف نظر کنند. در این صورت Honeypot یک عامل تهدید برای مهاجمان به شمار رفته است. یک نمونه از Honeypot هایی که برای این کار طراحی شده اند، Deception Toolkit است.

تشخیص حملات

یک راه دیگر که هانی پات ها با استفاده از آن از سازمان شما محافظت می‌کنند، تشخیص حملات است. از آنجایی که تشخیص، یک اشکال و یا نقص امنیتی را مشخص می‌کند، حائز اهمیت است. صرف نظر از این که یک 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 نادرست آن بسیار بالاست. همچنین این تکنولوژیها قادر به تشخیص حملات جدید نیستند و نمی‌توانند در محیطهای رمز شده یا IPv6کار کنند. به طور معمول هانی پات های با تعامل کم، بهترین راه حل برای تشخیص هستند. چرا که به کار گرفتن و نگهداری این هانی پات ها ساده تر بوده و در مقایسه با هانی پات های با تعامل بالا، ریسک کمتری دارند.

پاسخگویی به حملات

Honeypot ها با پاسخگویی به حملات نیز می‌توانند به سازمانها کمک کنند. زمانی که یک سازمان یک مشکل امنیتی را تشخیص می‌دهد، چگونه باید به آن پاسخ دهد؟ این مسأله معمولاً می‌تواند یکی از چالش برانگیزترین مسائل یک سازمان باشد. معمولاً 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 مسأله با پاسخگویی به رویداد آمیخته شده است. اول اینکه بسیاری از سیستم هایی که معمولاً مورد سوء استفاده قرار می‌گیرند، نمی توانند برای تحلیل شدن از شبکه خارج گردند. سیستم های تجاری، مانند Mail Server یک سازمان، به حدی مهم هستند که حتی اگر این سیستم هک 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.

هانی پات ها برای هر دوی این مشکلات راه حل دارند. آنها می‌توانند به سرعت و سهولت از شبکه خارج گردند تا یک تحلیل کامل بدون تأثیر بر کارهای روزانه انجام گیرد. همچنین از آنجایی که این سیستم ها فقط فعالیت های خرابکارانه یا تأیید نشده را ثبت می‌کنند، کار تحلیل بسیار ساده تر خواهد بود و داده های بسیار کمتری باید بررسی شوند. ارزش هانی پات ها به این است که آنها قادرند به سرعت اطلاعات عمیق و پرفایده را در اختیار سازمان قرار دهند تا بتواند به یک 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، Honeypot ها 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؟ هانی پات 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 درک انگیزه های مهاجمان استفاده کنند.

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

منبع: www.certcc.ir

۴

مکانیزم های جمع آوری اطلاعات در هانی پات ها

پیش از این در سه مقاله ***هانی پات چیست؟***، ***انواع هانی پات*** و ***کاربردهای هانی پات ها***، به معرفی اجمالی هانی پات ها و کاربردهای این سیستم‌ها پرداختیم. در این مقاله مکانیزم های مختلف جمع آوری اطلاعات در Honeypot ها را مورد بررسی قرار خواهیم داد.

جمع آوری اطلاعات در سیستمی که صرفاً 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 هریک مزایا و معایب خود را داراست. بر این اساس، سه مکانیزم مختلف برای جمع آوری اطلاعات در Honeypot ها تعریف می‌شود:

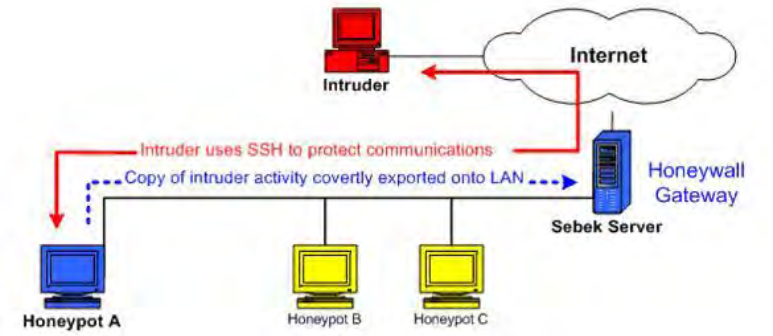
۱- مبتنی بر میزبان

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. متأسفانه این روش بیشترین خطر را نیز به همراه دارد. چرا که فرد نفوذگر معمولاً 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 کاملاً مغشوش نماید. به عنوان مثال‌هایی از ابزارهای مورد استفاده برای ثبت فعالیت بر روی یک Honeypot می‌توان به موارد زیر اشاره کرد:

- لاگ‌های سیستمی سیستم عامل (که نوعاً اولین هدف یک 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

یک راه حل امن‌تر و در عین حال پیچیده تر برای جمع آوری داده ها این است که هانی پات، داده ها را به صورت پنهانی جمع آوری کرده و برای تحلیل بیشتر برای یک سرور دیگر ارسال نماید. این راه حل به ما اجازه می‌دهد که داده های جمع آوری شده توسط هانی پات 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 یک ارتباط UDP به یک سرور دیگر ارسال کرده و بر روی آن ذخیره نماییم. Sebek فعالیت فرد نفوذگر را ضبط کرده و به صورت پنهانی آن را به یک سرور در داخل شبکه یا یک 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 یک Gateway تمامی داده ها را بین میزبان‌های یک 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 هانی پات های ما منتقل می‌شوند، ثبت نماییم. این مسأله دارای خطر بیشتری نسبت به راه حل Sebek است که در قسمت قبل توضیح داده شد. چرا که یک 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 یک Gateway عمل کند. در عین حال، بسیاری از Gateway هایی که در مقیاس کوچک یا خانگی طراحی می‌شوند، قابلیت‌های عمده ای برای ثبت اطلاعات ندارند و نمی‌توانند در این نقش مورد استفاده قرار گیرند.

بدون تکنیک‌های 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.

منبع: www.certcc.ir

5

مکانیزمهای تحلیل اطلاعات در هانی پات ها

پیش از این در چهار مقاله ***هانی پات چیست؟***، ***انواع هانی پات***، ***کاربردهای هانی پات ها*** و ***مکانیزم‌های جمع آوری اطلاعات در هانی پات ها*** به معرفی اجمالی هانی پات ها، کاربردهای این سیستم ها و روش‌های جمع آوری اطلاعات در این سیستم ها پرداختیم. در این مقاله مکانیزم‌های مختلف تحلیل اطلاعات در Honeypot ها را مورد بررسی قرار خواهیم داد.

هانی پات ها در کشف فعالیت‌های هکرهای کلاه سیاه بسیار موثر عمل می‌کنند. پتانسیل حقیقی یک هانی پات فقط زمانی کاملا به کار گرفته می‌شود که داده های مربوط به این فعالیت‌ها به اطلاعات ارزشمندی تبدیل شوند. برای این منظور، باید یک روال برای جمع آوری این داده ها و ایجاد ارتباط بین آنها و ابزارها، تکنیک ها 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 تکنیک‌های 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 ترافیک شبکه ای که از هانی پات خارج شده و یا به آن وارد می‌شود، باید تحت عنوان ترافیک مشکوک یا خرابکار برچسب بخورد. تجزیه ترافیک 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 می‌دهید، برخی فایروال‌ها امکان ارسال پیغام هشدار از

طریق ایمیل را در موارد ارتباطات مشکوک 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 یک 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، یک 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 ترافیک شبکه، و گروه بندی وقایع به ترتیب زمانی و یا حتی شناسایی یک گروه از وقایع به عنوان یک هشدار واحد را دارا هستند.

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

یک 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. معمولاً زمانی که یک فرد مهاجم هانی پات ما را هدف قرار می‌دهد، سعی در ایجاد یک ارتباط از راه دور می‌کند که به سادگی قابل شناسایی است.

یک ابزار مفید که می‌تواند برای جمع آوری ترافیک IRC مورد استفاده قرار گیرد، ابزاری به نام privmsg.pl است. این ابزار که اطلاعات حساس را به سرعت و به طور مؤثر 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 ترافیک 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 یک 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 یک مهاجم به هانی پات، منبع حمله، انواع فعالیت سیستمی که می‌تواند مشکوک 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.

۴- جرم شناسی سیستم قربانی

جرم شناسی (Forensics) تکنیک دیگری است که به ما اجازه می‌دهد تحلیل دقیق‌تری بر روی یک سیستم هانی پات انجام دهیم. ما می‌توانیم روال‌ها، فایل‌ها یا حتی ابزارهایی را که هکرهای کلاه سیاه ممکن است برای سوء استفاده از یک 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 یک سیستم Honeypot، باید کپی‌هایی از

تصویر سیستم عامل را به عنوان ابزار مقایسه در آغاز روال بازیابی در اختیار داشته باشیم. یک راه معمول برای ساختن کپی‌های بایت به بایت از سیستم عامل هانی پات، استفاده از یک ابزار خط دستور معمولی به نام NetCat است. کپی کردن تصویر هانی پات ابتدا به وسیله ایجاد یک نمونه از NetCat که بر روی یک سیستم مورد اعتماد گوش نشسته است انجام می‌شود.

۵- جرم شناسی پیشرفته سیستم قربانی

همانطور که قبلا هم اشاره شد، بازیابی داده‌ها یک بخش حساس و بسیار مهم از تحلیل فعالیت یک هانی پات است. اگر این Honeypot توسط یک مهاجم مورد سوء استفاده قرار گرفته باشد، آنگاه احتمال زیادی وجود دارد که وی برخی اطلاعات حساس را که در صورت بازیابی مهم باشند، پاک 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 یک سیستم پاک نمایند. بنابراین داشتن یک 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 یک گزینه پیشرفته به نام unrm، یک پارتیشن خاص را دریافت کرده و تمامی فضای حذف شده از آن پارتیشن را برای تحلیل‌های بعدی باز می‌گرداند.

منبع: www.certcc.ir

6

گامهای راه اندازی و به کارگیری یک هانی پات

قبل از پیاده سازی هانی پات خود به این مهم دقت فرمایید که تمامی ارزش یک هانی پات به گزارشات و هشدار هایی است که از وقوع رخدادهای متعدد در اختیار شما قرار می دهد. بنابراین علاوه بر پیاده سازی سیستم برای شبیه سازی و فریب دادن هکر ها و بدافزارها، به کارآمد بودن گزارشات و هشدار هایی که آن سیستم برای شما فراهم می کند نیز توجه داشته باشید.

۱- انتخاب سخت افزار برای میزبان

نخستین گام برای راه اندازی یک هانی پات، پیدا کردن کامپیوتری است که شما می‌خواهید آن را در معرض حملات هکرها و سوء استفاده قرار دهید و باید از هر داده ارزشمندی خالی شده باشد. این سیستم، می‌تواند هر کامپیوتری باشد که قادر به اجرای نرم‌افزار جمع آوری و کنترل داده ها باشد.

۲- نصب سیستم عامل

گام بعدی شامل ایجاد تغییرات لازم بر روی سیستم عامل فعلی، یا نصب یک سیستم عامل جدید بر روی کامپیوتر انتخاب شده است. نصب کردن یک سیستم عامل جدید، به شما امکان می‌دهد که به بهترین شکل در مورد آسیب پذیری‌هایی که مایلید بر روی سیستم وجود داشته باشد، تصمیم گیری نمایید.

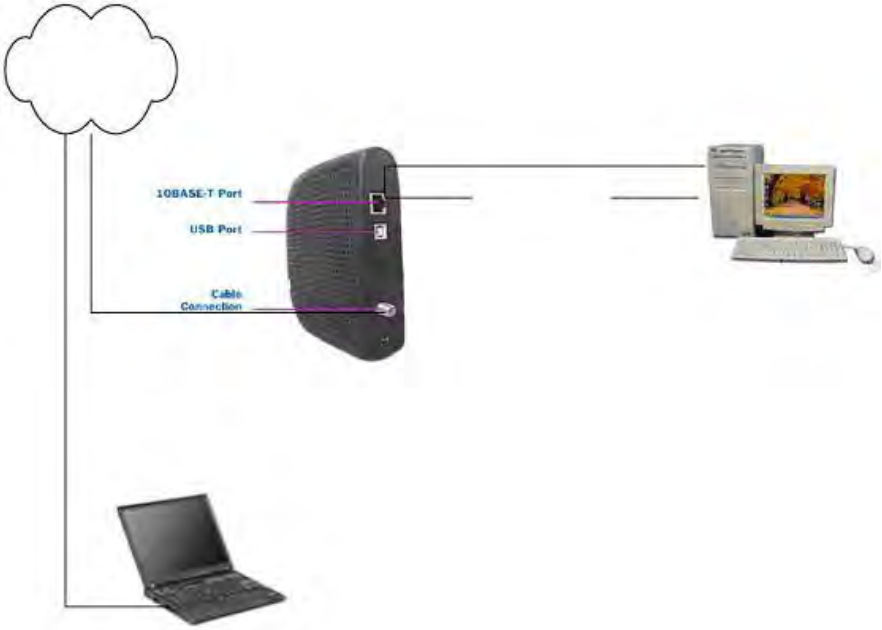
اگر تصمیم گرفته اید که سیستم عامل فعلی را بر روی هانی پات خود نگه دارید، باید از خطرات سوء استفاده مهاجمان از این سیستم به عنوان یک هانی پات آگاه باشید. برای مثال، ممکن است اطلاعات حساسی در مورد خود شما یا شخص دیگری بر روی این سیستم وجود داشته باشد. این اطلاعات می‌توانند در طول مدت استفاده از این سیستم به عنوان Honeypot خراب شده، حذف شده و یا به سرقت روند. اگر قصد دارید پیکربندی سیستم عامل فعلی را نگه دارید، بهتر است تنظیمات جدیدی را برای جلب ترافیک مشکوک به آن اضافه کنید. برخی روال‌های معمول برای جذابتر کردن یک Honeypot عبارتند از باز کردن پورت‌های آسیب پذیر شناخته شده، راه اندازی سرویس‌های 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 یک سیستم عامل جدید بپردازید، انعطاف پذیری و تعداد گزینه ها برای تنظیم هانی پات 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، یک ابزار پاک کردن دیسک مانند WIPE، یک دیسک راه انداز برای ایجاد پارتیشن‌ها و پارتیشن بندی مجدد هارد دیسک، دیسک‌های نصب سیستم عامل و هر نرم افزار 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.

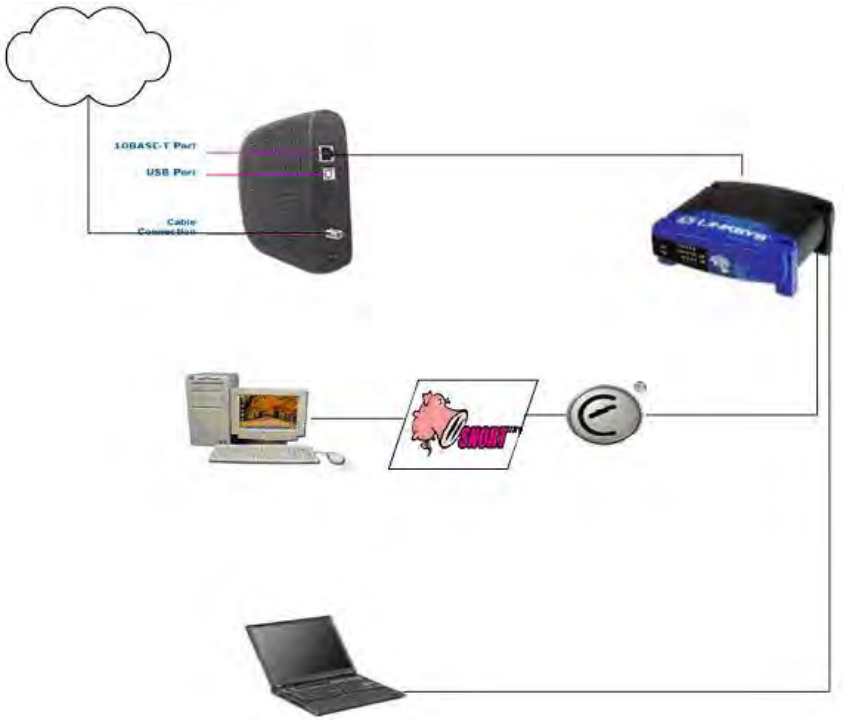
۳- معماری شبکه

گام سوم شامل مشخص کردن معماری استراتژیک 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 استراتژیک به یکدیگر متصل کنید تا بتوانید به خوبی در مورد بخش‌هایی از شبکه که ترافیک 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 هانی پات را مشاهده می‌کنید.

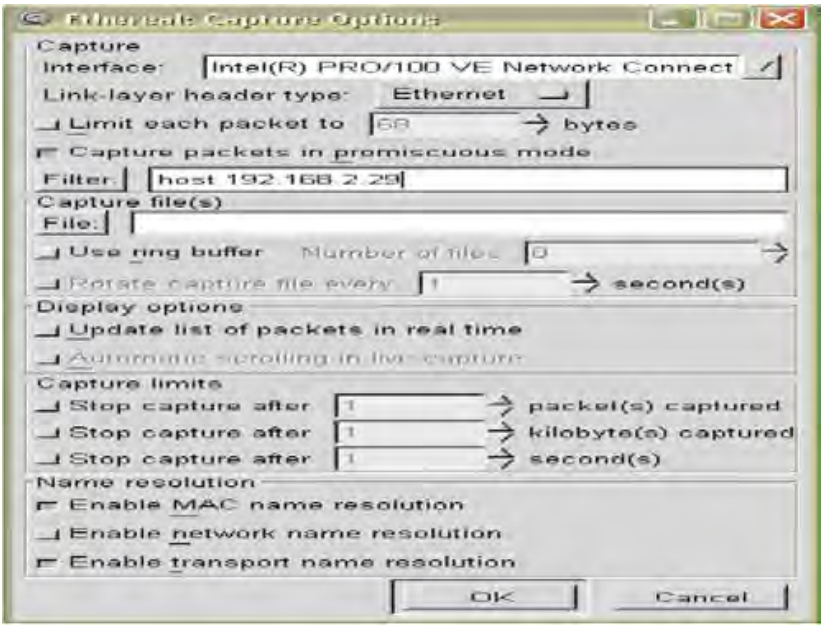


دو نمونه معماری شبکه مورد استفاده در به کار گیری Honeypot



۴- 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 اشتراک شبکه، یا سایر ترافیک‌های خرابکار روبرو شده است، بررسی کرده، ثبت و دریافت نمایید و در نهایت فعالیت هانی پات 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.



پیکربندی Snort برای کنترل ترافیک ورودی و خروجی شبکه به هانی پات، 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.

منبع: www.certcc.ir

اعتراف می‌کنم من یک هکر هستم. اگر تعریف از خودباشه از نوع قدرتمند و کارکشته!

یه هانی‌پات باعث لو رفتنم شد. مثل تله می‌مونه! ما هکرها به هانی‌پات می‌گیم: "آخر دسر" توی CEH و سایت‌های هک و امنیت کلی راجع به این تکنولوژی منحصر به فرد امنیتی خونده بودم، اما نتونستم دورش بزنم!

هانی‌پات یه ابزار امنیتی متفاوت و جدید که اگر به درستی انتخاب و تنظیم شده باشه، تشخیص اون غیرممکن یا خیلی خیلی سخت و طاقت فرساست.

آخه یکی نیست به خودش بگه، هکر بدبخت چطوری باید بتونه یه هانی‌پات رو از سیستم‌های واقعی تشخیص بده!؟ اگر هم تشخیص بدیم، تازه می‌فهمیم طرف خیلی حالیشه و باید هرچه سریعتر فرار کنیم.

واسه ما Firewall و IPS مصنوعی هم پیاده‌سازی کردن!

لعنت به این تکنولوژی ایمن!!!

هکر کلاه سیاه

7

آیا هانی پات ها و هانی نت ها موثر هستند؟

سخن مترجم

طی مدتی که با هانی پات های گوناگون سروکار داشتم به این نتیجه رسیدم که HoneyD بعنوان یکی از پرمصرف ترین آنها مورد توجه قرار گرفته است. این گستردگی به اندازه ای است که نمی توان متخصصی را یافت که با هانی پات ها سرو کار داشته اما بعنوان اولین یا دومین گزینه به سراغ HoneyD نرفته باشد. این ابزار در زبان انگلیسی با عنوان هانی دی تلفظ می شود، اما در کشور عزیزمان با عنوان هانید بین برخی از کاربران رایج است. HoneyD از سال ۲۰۰۵ به روز رسانی چشم گیری نداشته و در بعضی موارد نقص هایی از قبیل مبتنی بودن بر Command و باگ هایی در عملکرد به چشم می خورد، اما همه این نقایص نتوانسته از جذابیت این ابزار برای شروع تجربه هانی پاتی بکاهد.

اوایل سال ۱۳۸۹ شمسی در اثنای فاز مطالعاتی محصول کمین پـاد و به منظور ارائه مقاله ای برای بررسی تأثیر هانی پات ها، از آنجا که HoneyD بعنوان ابزاری برجسته، گستره وسیعی از کاربران دنیا را متوجه خود ساخته بود، مناسب دیدم تا مفید بودن یا نبودن هانی پات ها را در شرایطی که از HoneyD استفاده شده است مورد بررسی و مطالعه قرار دهم. در حین بررسی و جستجو به مقاله ای ارزشمند از دانشگاه Edith Cowan استرالیای غربی برخوردم و بعد از مطالعه، برای درک نقش مؤثر هانی پات ها ترجمه و ارائه نسخه فارسی آنرا ارزشمند یافتم.

این ترجمه از پروژه تحقیقاتی و کاملاً عملیاتی "آیا HoneyD مفید است یا خیر؟" برگرفته شده است. پروژه مذکور منجر به نشر مقاله ای ارزشمند توسط دانشکده علوم کامپیوتری دانشگاه Edith Cowan گردیده است و بنده به منظور درک بهتر مطلب با کمی دخل و تصرف و به روش ترجمه های مفهومی، نسخه فارسی آنرا تقدیم خوانندگان گرامی می نمایم.

عباس عظیمی

آیا هانی پات ها و هانی نت ها موثر هستند؟

چکیده:

هانی پات ها برای فریب دادن، به دام انداختن و نظارت بر فعالیت مهاجمان طراحی شده اند و برای این منظور از شیوه هایی مانند نقاب، تقلید، طعمه، عکس العمل های جعلی و ساختگی، بسته بندی مجدد و ... بهره می گیرند.

مقاله حاضر روشی برای استفاده از تأثیر فریفتن در بهبود و اثر بخشی هانی پات ها ارائه می نماید. در این تحقیق برای یک موسسه قانونی توسط HoneyD (یک هانی پات معروف) یک شبکه فریبنده پیاده سازی می شود و با رویکرد یادگیری تجربی در مراحل مختلف مورد تهاجم قرار می گیرد و سپس بهبود می یابد. به منظور تعیین اثر بخشی هانی نت ایجاد شده، داده های جمع آوری شده در طول مانور با استفاده از شیوه های مختلف مورد بررسی قرار می گیرند. نتایج حاکی از آنست که مهاجمان کاملاً فریب خورده و باور کرده اند که با یک شبکه واقعی مواجه شده اند.

کلمات کلیدی:

هانی پات، فریب، HoneyD

مقدمه:

فریب دادن شیوه عملکرد و مفهوم پایه هانی پات هاست. این ابزارها با فراهم کردن مکانیزم های دفاعی و فریبنده می توانند مهاجمان را به این باور مبهم برسانند که با یک سیستم فعال و واقعی دست و پنجه نرم می کنند. همچنین به کارگیری صحیح، نظارت و تحلیل گزارشات و داده های گردآوری شده توسط متخصصین هانی پات، کمک شایانی به افزایش درک

متخصصین امنیت سیستم نموده و باعث می شود تصویری واضح تر از روش های حمله و ابزارهایی که هکر ها و بدافزارها مورد استفاده قرار می دهند را داشته باشند.

هانی پات ها برای به دام انداختن هکر ها و بدافزارها و رمز گشایی شیوه حمله آنها به کار گرفته می شوند. (Brenton, n.d; Klug, 2000; Spitzer, 2002)

این پژوهش به منظور بهبود توانایی دفاعی هانی نت ها اهمیت داشته و مورد توجه قرار گرفته است. (هانی نت ها، هانی پات هایی با تعامل بالا هستند که تشکیل شبکه ای منسجم و مرتبط را می دهند.) این پژوهش در دانشگاهها، سازمان های دولتی و موسسات آموزشی که قادرند داده های حاصل از این تحقیق را بعنوان یک بسته راهبردی برای ادامه و توسعه تحقیقات کامپیوتری و امنیتی مورد استفاده قرار دهند، اهمیت ویژه ای دارد و نتایج آن افراد، متخصصین و سازمان ها را قادر می سازد تا حملات متعدد و ناشناخته را بشناسند و درک صحیحی از شیوه عملیاتی مهاجمین بدست آورند.

HoneyD – یک هانی پات متن باز

HoneyD در آوریل ۲۰۰۲ توسط نیلز پرووز از دانشگاه میشیگان ایجاد شده و توسعه یافته است. این ابزار دوست داشتنی یک هانی پات متن باز(Open Source) می باشد و برای اجرا شدن بر روی سیستم عامل های مبتنی بر لینوکس و یونیکس طراحی شده است. این در حالی است که دیگر توسعه دهندگان نسخه ای را برای سیستم عامل ویندوز ارائه نموده اند که در آن ویرایش HoneyD عملکرد برخی از قابلیت های خود را از دست داده است. HoneyD می تواند رفتار بیش از ۴۰۰ نوع سیستم عامل و دستگاه IP Base را تقلید و شبیه سازی کند و به طور بالقوه توانایی ایجاد شبکه ای با بیش از هزاران کامپیوتر را داراست.

برخلاف Specter (یک نوع هانی پات)، HoneyD به خوبی سیستم عامل را در سطح پشته IP نیز شبیه سازی می کند. این بدان معنی است که در هنگامی که یک مهاجم به منظور آگاهی از سیستم های روشن و سیستم هایی که IP فعال دارند، سعی می کند IP های شبکه

را توسط ابزاری نظیر NMAP مورد اسکن قرار دهد و عملیات Net Scan / IP Probing را به انجام برساند، هم سرویس و هم پشته IP رفتاری مشابه سیستم عامل تعیین شده را شبیه سازی می کنند.

HoneyD با نظارت بر آدرس های IP که بلااستفاده بوده و به هیچ دستگاهی اختصاص نیافته کار می کند و در درجه ی اول برای تشخیص حملات استفاده می شود و نمی تواند فقط به صورت پویا با مهاجمان تعامل کند.

روش تحقیق:

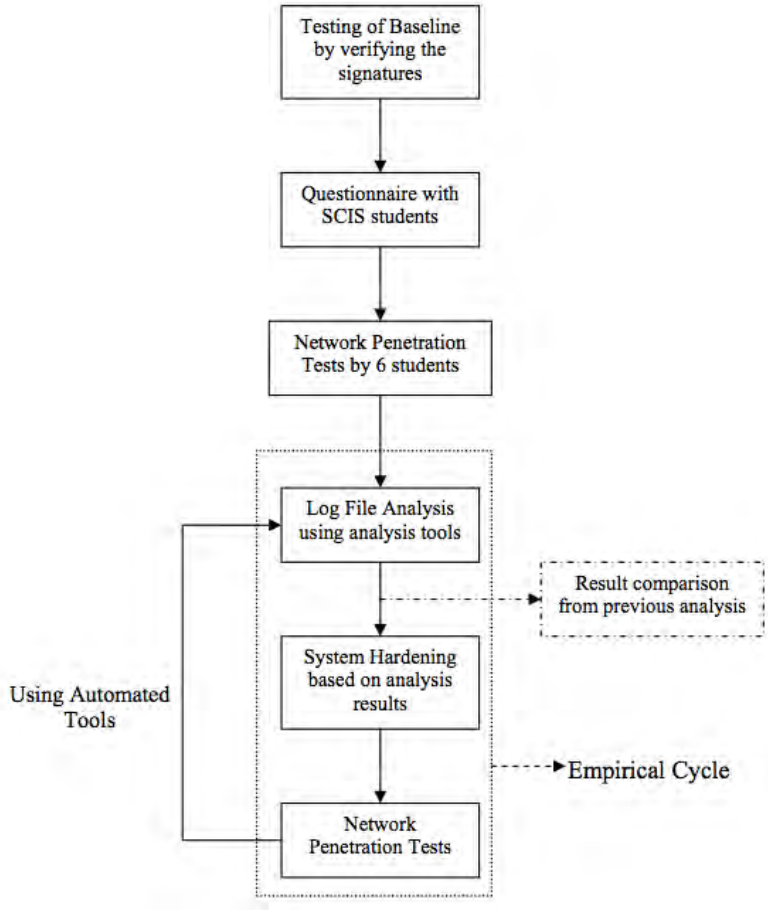
روند پژوهش به مراحل مختلف تقسیم شده است که در آن نتایج حاصل از هر مرحله به مرحله قبل بستگی دارد. شکل شماره یک مراحل فرآیند تحقیقات را نشان می دهد.

مرحله ۱- تایید امضاء

در مرحله اولیه این تحقیق، یک سیستم با استفاده ازHoneyD، (که یک Honeypot منبع باز Open Source است) ایجاد شد. HoneyD با لیستی از امضاءها (در حدود بیش از ۴۰۰ مورد) ارائه شده است که می تواند برای پیکربندی Honeynet استفاده شود. اما ممکن است که امضاءهای ارائه شده با HoneyD قطعاً نتواند به صورت موفقیت آمیزی مورد استفاده قرار گیرد. بنابراین قبل از اجرای Honeypot برای جمع آوری داده ها، نیاز به تأیید این امضاءها با استفاده از HoneyD وجود دارد، پس هر امضای منحصر به فردی در فایل پیکربندی HoneyD اجرا می شد و Nmap (ابزار اسکن شبکه) (فئودور ۱۹۹۸) برای تست آنها مورد استفاده قرار می گرفت. همه ی امضاهای موفق (نزدیک به ۵۰٪ از کل امضا) به طور جداگانه در فهرست قرار داده می شدند و پس از آن برای پایه Honeypot مورد استفاده قرار می گرفتند. هنگامی که امضاء های پایه بدست آمد، محقق مرحله بعد پژوهش را آغاز می کند.

مرحله ۲- پرسشنامه

شرکت کنندگان منتخب می بایست حملاتی به سیستمی که بر روی آن HoneyD نصب شده بود برای تست اثر بخشی انجام می دادند. برای انتخاب شرکت کنندگان، از پرسشنامه که یک نوع روش بررسی است استفاده شد. پرسشنامه از پیش تعیین شده ای با ۲۰ سوال مرتبط با امنیت کامپوتر آماده گردید.



شکل(۱) چارچوب تئوری: مراحلی از روند پژوهش

هدف اصلی این پرسشنامه انتخاب شرکت کنندگانی برای تست نفوذ به شبکه بود. پرسشنامه میان دانشجویانی از دانشکده علوم کامپیوتر و اطلاعات (SCIS) دانشگاه Edith Cowan، Perth، توزیع شد. این دانشجویان در مرحله ی اول انتخاب شدند، چرا که دانشجویان نمونه ای از دانشکده علوم کامپیوتر و با دانش کامپیوتری بالایی بودند. دانشجویانی که پرسشنامه را پاسخ می دادند از ماهیت واقعی پروژه آگاه نبودند و تنها درباره ی مانور هک مطلع شده بودند و به آنها گفته شده بود که مانور فقط برای تعیین مهارت های هک آنهاست. لازم است بدانید تأثیر شرکت کنندگان تا زمانی که تست نفوذ شبکه انجام گرفت ناشناخته بود.

مرحله ۳- تست نفوذ شبکه توسط دانشجویان منتخب

شرکت کنندگان فوق، تست نفوذ شبکه بر روی Honeynet پیکربندی شده انجام دادند. این تست ها به منظور کاوش در شبکه برای یافتن نقاط ضعف ها و آسیب پذیری ها بود. همان طور که قبلاً ذکر شد، این شرکت کنندگان از Honeynet واقعی در ساختار شبکه مطلع نبودند. به این شرکت کنندگان اجازه استفاده از لپ تاپ شخصی خود و برنامه های مورد نیازشان برای تست شبکه داده شده بود. این امکان برای دانشجویان فرصتی فراهم می ساخت تا از ابزار های مطلوبشان برای انجام مانور استفاده کنند. زمانی که مانور نفوذ شبکه توسط شرکت کنندگان کامل شد، آنها به طور داوطلبانه گزارش های ناشناس خود را به محقق ارائه دادند. این گزارش ها نظرات آنها در مورد معماری شبکه و یافته هایشان در طول مانور را مشخص می کرد.

مرحله ۴- تجزیه و تحلیل فایل های Log

Log های تولید شده در طول مانور نفوذ به شبکه، به طور کاملاً ایمن روی یک سرور ذخیره شدند و همچنین اقدامات بکاپ گیری مناسبی مانند ذخیره سازی بر روی دیسک های فشرده و بکاپ گیری از دیتابیس بر روی سیستم های دور، اتخاذ شدند. ابزار های تجزیه و تحلیل

مختلفی با دقت کافی به منظور تجزیه و تحلیل کردن این فایل های Log مورد استفاده قرار گرفتند. ابزارهایی مانند:

- **ACID** (کنسول تجزیه و تحلیل از نفوذ به پایگاه داده) (Danyliw, n.d)
ACID در درجه اول برای انجام آنالیز آماری از فایل های Log مورد استفاده قرار گرفت. این ابزار به دسته بندی هشدار های امنیتی تولید شده توسط شرکت کنندگان طی تست نفوذ به شبکه کمک کرد.

- **Ethereal and Tcpdump**
آنالیز Log شامل مطالعه عمیقی از بسته های مخربی که به سیستم وارد می شدند نیز بود. ساختارها و تهدیدات بالقوه آنها بدقت تجزیه و تحلیل می شدند و بسته های مخرب نیز با استفاده از ابزارهای آنالیز بسته Ethereal و Tcpdump آنالیز می شدند. Ethereal به طور عمده به دلیل توانایی های زیر مورد استفاده قرار گرفت:
  - بررسی داده از یک شبکه موجود (Live Network) یا از یک فایل موجود بر روی دیسک
  - مشاهده جریان بازسازی شده از لایه TCP session
  - قابل استفاده برای ماشین های ویندوز و Unix
  - تشریح ۲۸۰ پروتکل
  - روشن و رنگی کردن اطلاعات خلاصه از بسته انتخابی
  - ذخیره تمام قسمت های رد یابی شده شبکه بر روی دیسک
  - Ethereal به محقق امکان تولید آمار سلسله مراتبی از پروتکل ها را می دهد. با استفاده از Ethereal محقق قادر خواهد بود هر بسته منحصر بفرد را به طور جداگانه آنالیز کند.

- **نوت بوک تحلیل گر ۶:**

نوت بوک تحلیل گر ۶ یک ابزار آنالیز تجاری بود که به ایجاد نمودار تصویری از ترافیک ثبت شده شبکه در فایل های Log کمک می کرد. این نمودار تصویری به تفسیر اطلاعات پیچیده که انجام آن به صورت دستی غیر ممکن بود کمک می کرد. نتایج بدست آمده توسط تحلیل گر به آسانی قابل درک و در دسترس بود.

همچنین تعدادی از فایل های Log به صورت دستی آنالیز شدند. در طی آنالیز، تکرار انواع مختلف حمله و تأثیرشان بر روی شبکه شناسایی شدند. این ابزار ها به جهت اینکه نرم افزار های رایگان (به جز تحلیل گر) و Open Source و در دسترسی در اینترنت هستند انتخاب شدند. این انتخاب انعطاف پذیری مناسبی در پیکربندیشان براساس نیاز فراهم می کرد.
با ترکیب جمعی از نتایج بدست آمده از ابزارهای آنالیز، نقاط ضعف مختلفی در پیکر بندی شبکه شناسایی شدند. این نقاط ضعف با مشاهده الگوهای داده در فایل های Log و همچنین بوسیله ی بررسی ابزار ها و برنامه های مورد استفاده توسط شرکت کنندگان برای حمله به شبکه مشخص شد. اطلاعات در مورد این ابزارها و برنامه ها در Log ها گرفته شده بود. از آنالیز دقیق Log ها و بسته های ردیابی شده، مشخص شد که تعدادی خطای پیکربندی در ایجاد Honeynet با استفاده از HoneyD وجود داشته و همچنین سرویس هایی یافت شدند که مستعد حمله بوده ولی به درستی پیکر بندی نشده بودند. چنین نقاط ضعفی با استفاده از ابزار های مختلف آنالیز که در بالا توضیح داده شد مشخص شدند.

مرحله ۵- مستحکم سازی سیستم

بر اساس نتایج بدست آمده از آنالیز مراحل قبل، پیکر بندی شبکه و سیستم برای انجام تست های بیشتر و جمع آوری داده بهبود یافت.

مستحکم سازی سیستم به وسیله بهبود فایل پیکر بندی Honeynet و با استفاده از امضاهای دقیق تر و همچنین با بهبود فایل های پیکربندی سرویس های شبیه سازی بر روی انواع پورت ها انجام گرفت.

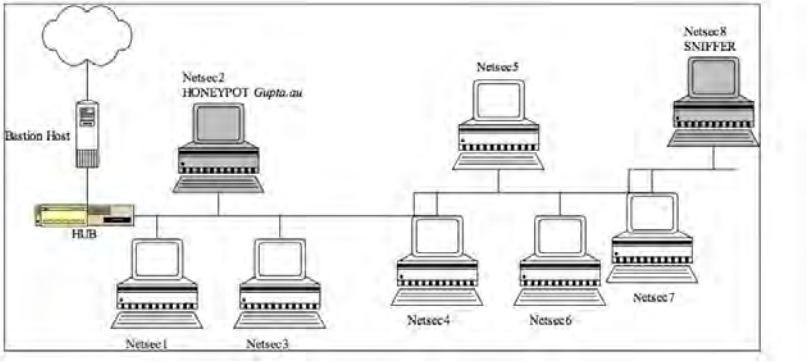
مرحله ۶- تست نفوذ شبکه با استفاده از ابزارها

بعد از اینکه مستحکم سازی شبکه و سیستم کامل شد، تست های نفوذ دیگری به شبکه با استفاده از برخی ابزارهای امنیتی اتوماتیک که در اینترنت قابل دسترس هستند انجام شد. این ابزار ها به طور عمده به دلیل رایگان بودن مورد استفاده قرار گرفتند و توسط خود محقق با استفاده از ابزار های مختلف هک، برای تعیین اینکه آیا رفتار شبکه پس از مستحکم سازی سیستم بر اساس نقاط ضعف مشخص شده در آنالیز قبلی بهبود یافته یا خیر انجام شدند. بعد از اتمام تست، گام های مراحل ۴ و ۵ و ۶ بصورت تجربی ادامه پیدا کردند تا مشخص شود که آیا سطح فریب Honeynet بهبود یافته است یا خیر. نتایج بدست آمده از آنالیز هر مرحله با نتایج مرحله قبل مقایسه می شدند. مقایسه نتایج به تعیین سطح فریب کمک می کرد. این کار با مطالعه تکنیک های مختلف و موفق هک، که در فایل های Log تعریف شده بودند مشخص می شد. گام های مراحل ۴ و ۵ و ۶ تا جایی ادامه یافت که به شرکت کنندگان برای تعیین حفره های امنیتی در شبکه حداقل شانس را بدهد.

با ادامه بهبود در Honetynet، می توان در نظر گرفت که سطح موفقی از فریب به دست آمد که به طور مؤثر قادر به فریب و گمراه کردن شرکت کنندگان بود.

گسترش Honeypot:

از آنجایی که این یک تجربه آزمایشگاهی بسته، برای اهداف محقق بود از این رو یک Honeypot برای جمع آوری اطلاعات حمله در محیط آزمایشگاهی کافی بود. شکل ۲، ساختار شبکه آزمایشگاهی با وجود Honeypot و یک Sniffer به منظور جمع آوری داده را نشان می دهد.



شکل (۲) *ساختار شبکه آزمایشگاهی*

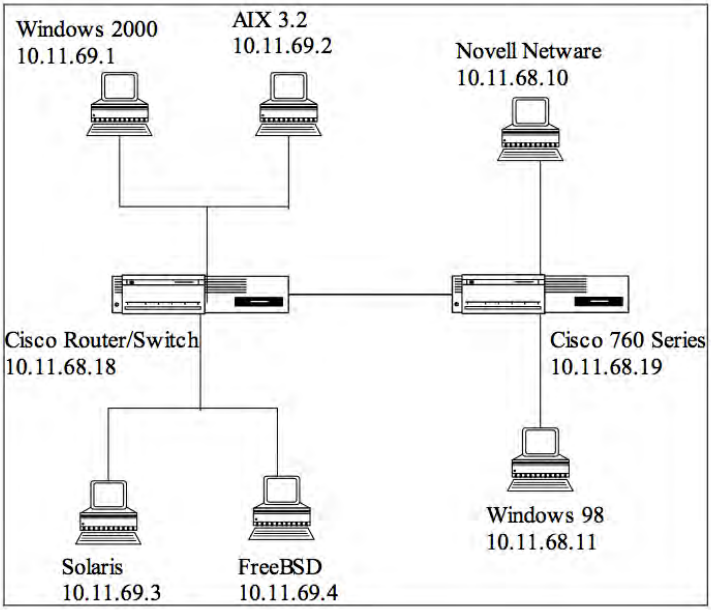
در شبکه فوق، ۸ میزبان (با نامهای NetSec 1....8) که به یک هاب متصل شده اند وجود داشت. برای این کار از یک هاب استفاده شد. زیرا ما را قادر می ساخت تا تمام ترافیک شبکه sniff شود چراکه تمام پورت ها بر روی دامنه برخورد (Domain Collision) مشابه بودند، در حالی که بر روی سوئیچ، از آنجایی که هر پورت بر روی یک دامنه برخورد متفات می باشد، Sniffing امکان پذیر نمی باشد. هاب به میزبان پایه وصل شده بود که به اینترنت اتصال داشت. این میزبان به عنوان یک سرور برای شبکه و همچنین بعنوان یک فایروال برای محافظت شبکه از حملات خارجی عمل می کرد.

میزبان Netsec2 برای استقرار یک هانی پات HoneyD، Gupta.au و Netsec8 برای نصب یک Snort Sniffer به منظور جمع آوری اطلاعات حمله بر روی شبکه مورد استفاده قرار می گرفت. Gupta.au شامل یک Red Hat Linux 7.3 که بر روی کامپیوتری با پیکربندی زیر در حال اجرا است، می باشد:

CPU	Pentium 3, 450MHz
Memory	256Mb
Hard disk	6 GB
Operating System	RedHat Linux 7.3
Installed Softwares	HoneyD 0.4, Syslog-ng

جدول (۱) *پیکربندی سیستم honeypot*

در پیکربندی فوق، فقط از یک کارت شبکه برای پیاده سازی Honeynet استفاده شده است. هانی پات HoneyD با یک آدرس IP بلااستفاده برای ایجاد یک شبکه Honeynet مجازی پیکربندی شده است. شکل ۳ ساختار شبکه مجازی ایجاد شده با هانی پات HoneyD را نشان می دهد.



شکل (۳) *هانی نت مجازی*

HoneyD دارای قابلیت ایجاد آدرس IP و سرویس های مجازی است. دو شبکه داخلی ایجاد شد (10.11.68.0.24,10.11.0/24) که هر دو با استفاده از روتر های Cisco به یکدیگر متصل شده اند. جدول ۲ آدرس های IP و سرویس های اختصاص داده شده بر روی شبکه مجازی HoneyD را به طور خلاصه نشان می دهد:

IP Addresses	Signatures	Services
10.11.69.1	Windows 2000 Professional, Build 2218	Http – port 80
10.11.69.2	AIX 3.2	Http – port 80
10.11.69.3	Solaris 2.3 – 2.4	Http – port 80
10.11.69.4	FreeBSD 3.2 – 4.0	Http – port 80
10.11.68.10	Novell Netware 3.12 or 386 TCP/IP	Http – port 80
10.11.68.11	Windows 98	Http – port 80
10.11.68.18	Cisco Router/Switch with IOS 11.2	Http – port 80
10.11.68.19	Cisco 760 Series (non IOS) or IBM Stackable Hub	Http – port 80
Default	Windows 98	Http – port 80 Netbios – port 139

جدول (۲) *خلاصه ایی از آدرس های IPاختصاص داده شده بر روی شبکه*

شبکه 10.11.69.0/24، در حال اجرای یک سرور ویندوزی بر روی آدرس 10.11.69.2 می باشد. مشخصات این سرور به شرح زیر است:
Windows 2000 ProfessionalServer به همین ترتیب Aix 3.2 Server بر روی سرور 10.11.69.2، Solaris 2.3-2.4 بر روی سرور 10.11.69.4، Free BSD 3.2-4.0 بر روی سرور 10.11.69.4 و Windows 98 (بعنوان پیش فرض) بر روی بقیه میزبانهای باقیمانده از شبکه 10.11.69.0/24 می باشد.

میزبان ها با آدرس 10.11.69.1 تا 10.11.69.4 فقط در حال اجرای سرویس Http (پورت 80) با یک اسکریپت پیش فرض (با نام فایل web.sh) می باشند. سرویس HTTP به دلیل جذاب بودن برای هکر ها بر روی شبکه شبیه سازی شده است. تمام میزبان های باقیمانده ی دیگر از شبکه 10.11.69.0/24 در حال اجرای ویندوز ۹۸ به عنوان پیش فرض با سرویس های باز بر روی پورت 80 (HTTP) و پورت 139 (Net-Bios) هستند. ویندوز ۹۸ به دلیل

نزدیک بودن به معماری شبکه شرکت ها بعنوان یک سیستم عامل پیش فرض بر روی شبکه شبیه سازی شد.

شبکه 10.11.69.0/24 به شبکه 10.11.69.0/24 با استفاده از Cisco Router / Switch with IOS 11.2 با آدرس IP10.11.68.18 متصل شده که خود آن نیز به Cisco سری 760 دیگر Cisco 160 Service (Non IOS) یا IBM Stackable Hub با آدرس 10.11.68.19 متصل می باشد.

شبکه 10.11.69.0/24، Novell Network 3.12 یا سرور 386 TCP/IP با آدرس 10.11.68.10، ویندوز ۹۸ با آدرس 10.11.68.11 را اجرا می کرد. همچنین ویندوز ۹۸ بعنوان پیش فرض بر روی بقیه Client های شبکه اجرا می شد.

این ساختار شبکه کامل بر روی Redhat Linux 7.3 با استفاده از Honeyd 0.4 پیکربندی شده بود.

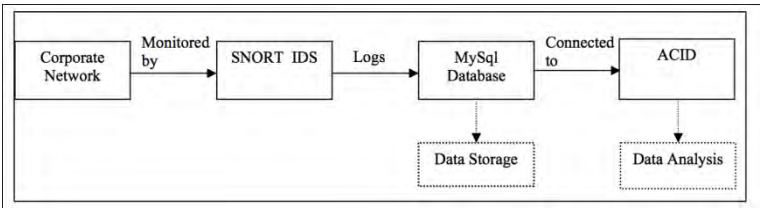
جمع آوری داده ها و ذخیره سازی آنها به صورت ایمن از جنبه های اصلی یک Honeynet می باشد. لذا یک ماشین جداگانه برای Sniffing و ذخیره سازی داده راه اندازی شد. این ماشین شامل یک Redhat Linux 7.3 در حال اجرا بر روی سیستمی با پیکربندی زیر می باشد:

CPU	Pentium 3, 450MHz
Memory	256Mb
Hard disk	6 GB
Operating System	RedHat Linux 7.3
Installed Softwares	MySql, ACID, Apache, Webmin, Snort, Syslog-ng

جدول (۳) *مشخصات ماشین جمع آوری داده*

Snort IDS بعنوان یک Sniffer برای جمع آوری اطلاعات درباره ی همه ترافیک ورودی و خروجی بر روی شبکه مورد استفاده قرار گرفت.

از آنجا که Snort نیز دارای قابلیت اتصال از طریق پایگاه داده Mysql می باشد. داده های جمع آوری شده به وسیله Snort به پایگاه داده MYSql انتقال داده شد. داده های جمع آوری شده در پایگاه داده بوسیله ACID (کنترل و آنالیز نفوذ به پایگاه داده) استفاده شدند. این داده ها برای فعال کردن یک آنالیز کامل با ایجاد نمودار ها و جداول با استفاده از داده های ذخیره شده در پایگاه داده با استفاده از Snort مورد استفاده قرار گرفتند.



شکل (۴) *معماری ماشین جمع آوری داده*

مجموعه دیگری از داده ها با استفاده از Syslog-ng ثبت شدند. این داده ها بر روی ماشین دیگری به صورت ریموت نیز ذخیره می شدند اگر ماشین جمع آوری داده به خطر بیافتد، مجموعه ی دیگری از داده ها بعنوان Backup در دسترس خواهند بود. Webmin برای مدیریت Honeypot از راه دور مورد استفاده قرار می گرفت. از آنجا که محقق بیشتر به ابزارها و برنامه ها یا اسکریپت هایی که توسط مهاجمان در طی مانور نفوذ به شبکه استفاده می شود علاقه مند است، بنابراین جمع آوری اطلاعات سخت افزاری ماشین های مهاجمان برای هدف این تحقیق غیر مرتبط می باشد.

اولین نتایج تست در Honeyd 0.4 A :

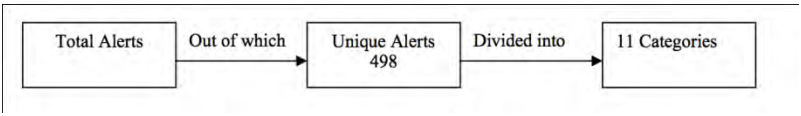
در طول فاز اولیه تست، از گروهی از شرکت کنندگان درخواست شد تا شبکه ی طراحی شده را بررسی کنند (10.11.68.0/24 و 10.11.69.0/24، شکل ۳).

همه ی شرکت کنندگان منتخب لپ تاپ های خود را همراه داشتند و برای انجام این مانور، از ابزار و برنامه های مورد نظرشان استفاده کردند. این مرحله تست بین محدوده زمانی[11:00:28] 17.02.2003 تا [17:58:01] 18-02-2003 به طول انجامید. حملات

مختلفی توسط شرکت کنندگان انجام شد که میزان قابل توجهی از داده را در ماشین های نظارت بر شبکه تولید می کردند. همچنین تعدادی از شرکت کنندگان بازخورد و گزارش هایی را ارائه کردند که به آنالیز داده ها کمک می کرد.

بخش1.01- تجزیه و تحلیل ACID:

از تست اولیه Snort IDS، ۱۹۵۱ هشدار در پایگاه داده SQL وارد و ثبت شد. فرمت پایگاه داده SQL تایید کرد که 498 هشدار منحصر به فرد ایجاد شده است که در ۱۱ دسته ی مختلف تقسیم می شوند.



این ۱۱ دسته در زیر آورده شده است:

Classification	Total Alerts	Signatures
Unclassified	1032 (5%)	285
Misc-activity	494 (3%)	3
Bad-unknown	5764 (30%)	2
Attempted-recon	8369 (43%)	79
Web-application activity	2957 (15%)	90
Web-application attack	748 (4%)	30
Misc-attack	7 (0%)	1
Attempted-dos	56 (0%)	5
Protocol-command-decode	16 (0%)	1
Attempted users	3 (0%)	1
Successful admin	5 (0%)	1

جدول (۴) *۱۱ دسته از انواع مختلف حملات*

از جدول فوق واضح است که شرکت کنندگان انواع مختلفی از حملات را انجام داده اند. به نظر می رسد که شرکت کنندگان بیشتر بر آسیب پذیری های مبتنی بر وب تمایل دارند. همچنین

تعداد زیادی پورت اسکن بر روی میزبان های مختلف وجود داشت. شواهدی نیز وجود داشت که نشان می داد شرکت کنندگان سعی در انجام چند حمله DDOS بر روی شبکه داشتند. تعدادی از مهاجمان نیز سعی در انجام حمله Flood به میزبانها با تعداد زیادی از درخواست های SNMP برای انجام حملات Dos بر روی سرور ها داشتند. از آنالیز داده ها، به نظر می رسد که شرکت کنندگان بیشتر تمایل به انجام حملات مبتنی بر DOS و یا بهره برداری از آسیب پذیری های مبتنی بر وب داشتند. ۵ مورد از شایع ترین آنها در جدول ۵ نشان داده شده است:

Signature	Classification	Total
ICMP redirect host	Bad-unknown	5743 (30%)
SNMP request udp	Attempted-recon	1639 (8%)
SCAN Squid Proxy attempt	Attempted-recon	1412 (7%)
SCAN Proxy (8080) attempt	Attempted-recon	940 (5%)
WEB-IIS scripts access	Web-application activity	775 (4%)

جدول (۵) *شایع ترین هشدارها*

آسیب پذیری در پردازش درخواست SNMPV1 از تعداد زیادی نسخه SNMP به مهاجمان از راه دور امکان می داد که بتوانند موفق به انجام DoS یا کسب دسترسی از طریق پیام های ۱)Get Request، ۲)Get Next Request و ۳)Set Request شوند.

این نشان می دهد که شرکت کنندگان سعی در حمله Flood به میزبان ها و سرور ها با درخواست های SNMP داشتند که این عمل آنها را برای پاسخ دادن به درخواست های دیگری که بوسیله انواع میزبانها و سرورهای دیگر ارسال می شود غیر قابل دسترس می کند. همچنین به نظر می رسد که شرکت کنندگان در تلاش برای بدست آوردن دسترسی به میزبان ها و سرورها اقدام به ارسال در خواست های SNMP به کلاینت های مختلف در شبکه کردند. اگر درخواست توسط Client خاصی پذیرفته شود، به آنها دسترسی کامل روی سرور یا میزبان خاص داده خواهد شد.

همچنین تعداد زیادی عملیات اسکن پورت بر روی میزبان های مختلف وجود داشت. این شماره پورت می تواند جزئیات بیشتری را براساس وقوع کل هشدارها و هشدارهای منحصر به فرد بر روی آنها ارائه دهد.

Port Type	Occurrences	Unique Alerts
80 /tcp	5421	195
161 /tcp	2465	4
3128 /tcp	1412	1
8080 /tcp	943	3
1080 /tcp	519	1
162 /tcp	517	3
1 /tcp	345	3
0 /udp	295	5
22 /tcp	256	10
/udp	112	1
7001 /udp	93	1
10080 /udp	81	1
10081 /udp	73	1
31337 /udp	68	1
1014 /tcp	67	7

جدول (۶) *لیستی از شماره های پورت مقصد با هشدار های مکرر*

بخش 1.02 تجزیه و تحلیل Ethereal:

یک لاگ فایل مربوط به Tcpdump با نام 1045547976 Tcpdump log طی اولین مرحله آزمایش تولید شد، که با استفاده از Ethereal Packet Sniffer تجزیه و تحلیل گردید. با توجه به آمار سلسله مراتبی پروتکل، تولید شده توسط Ethereal، 8717 بسته در فایل لاگ Tcpdump گزارش شد که نزدیک به ۴۵٪ بسته های ICMP و ۳۷,۲۶% بسته های TCP وجود داشت. پس از تجزیه و تحلیل بیشتر فایل Log، مشخص شد که برخی بسته ها بر روی از پورتها خاصی بیشتر تکرار شدند. این نتایج به شرح زیر می باشند:

- وقوع مکرر بسته های TCP SYN از پورت 1060 به Webcache

- بسته هایی با برچسب ACK، FIN، PSH و URG به TCPmux
- بسته های ACK به پورت 22 از SSH

در پی دریافت رابطه داده ها با استفاده از ACID بر روی پورت 22 از SSH مشخص شد که از مجموع ۲۵۶ هشدار بر روی این پورت، ۱۰ هشدار منحصر به فرد وجود دارد که می تواند به شرح زیر بیشتر موشکافی شود:

۴ هشدار: Portscans
۱ هشدار: NMAP Fingerprint (Stateful) detection (تشخیص اثر انگشت NMAP)
۱ هشدار: Stealth Activity (FIN Scan)
۱ هشدار: Stealth Activity (Null Scan)
۱ هشدار: Stealth Activity (Vecna Scan)
۱ هشدار: Scan Nmap TCP که نشان می دهد یک کاربر از راه دور با استفاده از ابزار پورت اسکن NMAP به بررسی سرور پرداخته و یک NMAP TCP ping برای تعیین اینکه آیا میزبان در دسترس است یا خیر ارسال کرده است.

- بسته های SYN در پورت 705 برای DNM

در مجموع ۶۲ هشدار بر روی پورت 105 وجود داشت که تنها یک هشدار منحصر به فرد بود و آن حمله درخواستAgent X/TCP (cVE:CAN-2002-0012) SNMP بود.

- بسته های SYN در پورت 162 برای Solaris. که یک پورت اتصال برای سیستم سولاریس است. از مجموع ۱۰۴ هشدار SNMP تنها یک هشدار منحصر به فرد وجود داشت. این هشدار SNMP TRAP بود که بطور عمده برای ایجاد حملات DOS استفاده می شود. (CRE: CAN-2002-0013)

- چند پیغام خطا نیز وجود داشت.

خطا: پیغام هدر (Header) نمی تواند تجزیه شود: نوعی اشتباه در آن مورد.

- چند بسته UDP در TFTP که اطلاعاتش ناشناخته بود نیز وجود داشت.

از داده های جمع آوری شده فوق به نظر می رسد که شرکت کنندگان در تلاش برای ایجاد ارتباط TCP با میزبان های مختلف از طریق تعدادی از شماره پورت ها هستند.

تلاش هایی برای دسترسی به Web Cache انجام شده بود که در صورت موفقیت می توانست اطلاعات مربوط به وب سایت ها یا اطلاعاتی در مورد هریک از سرویس های مبتنی بر وب را به مهاجمان بدهد. با استفاده از این اطلاعات، مهاجمان ممکن است قادر به انجام چند حمله Brute Force بر روی شبکه شود. همچنین تلاش هایی برای بهره برداری از سرویس SSH نیز وجود داشت. به نظر می رسد که شرکت کنندگان تلاش داشتند داده های منتقل شده بین میزبان ها در شبکه را ثبت کنند.

همچنین تلاش هایی برای بهره برداری از سرویس های SNMP وجود داشت که عمدتاً به منظور انجام حملات DoS بر روی میزبان های مختلف انجام می شد.

بخش 1.03 بازخورد شرکت کنندگان

در پایان مانور نفوذ به شبکه، از شرکت کنندگان درخواست شد به طور داوطلبانه درباره ی تجارب خود در زمان کاوش و بررسی شبکه بازخوردشان را ارائه دهند. اظهارات آنها در زیر خلاصه شده است:

شرکت کننده ۱: یک شبکه ساده با اکثریت میزبان بر روی سیستم عامل ویندوز. ساختار شبکه گیج کننده به نظر می رسید چراکه ترافیک شبکه با استفاده از یک Gateway به سمت دیگری هدایت می شد، بنابراین هیچ دسترسی مستقیم به روتر وجود نداشت.

شرکت کننده ۲: یک شبکه بزرگ با تعداد زیادی از میزبان ها اما اکثر میزبان ها (که من اسکن کردم) بر روی ویندوز 98 بودند. به نظر می رسد سازمان فاقد پشتیبانی جهت ارتقاء

سیستم عامل به آخرین سیستم عامل موجود است. چرا که از ویندوز 98 امن تر و قابل اعتمادتر هم وجود دارد. هیچ دسترسی به FTP و Telnet وجود نداشت.

شرکت کننده ۳: معماری شبکه ساده و با استفاده از ویندوز 98 بعنوان سیستم عامل اصلی بر روی میزبان های مختلف به نظر می رسید. بر روی سرور AIX پورت 25 مستعد SPAM (هرزنامه) بود. نتوانستم جزئیات زیادی در مورد سرویس های مختلف دیگر بر روی میزبان های دیگر پیدا کنم. پورت باز ویندوز 98 میزبان ها، فقط در حال اجرای سرویس http بودند در حالی که چند میزبان دیگر SSH و NetBIOS هم به چشم می خورد.

نتایج آزمایش دوم بر روی HONEYD 0.5:

بعد از اولین مرحله تست، تعدادی حفره های امنیتی و هشدار که بطور بالقوه شناسایی شد وجود داشتند. همچنین بر اساس بازخورد دریافتی از هکرها در مورد معماری شبکه، مشخص شد که شبکه موجود یک شبکه با تعامل بسیار پائین است که به شرکت کنندگان فرصت زیادی را برای تعامل نمی دهد. از دیدگاه هکرها، شبکه موجود یک شبکه بسیار امن با تعامل در سطح محدود بود. بنابراین، پیکر بندی شبکه براساس تجزیه و تحلیل داده های قبلی بهبود یافت. تغییرات زیر قبل از آغازتست مرحله دوم انجام شد:

HoneyD 0.4a به HoneyD 0.5 ارتقاء یافت. این ارتقاء انجام شد، زیرا آخرین نسخه Honeyd تعدادی ویژگی اضافی مانند تسهیلات Logging جداگانه داشت و همچنین قادر به استفاده از ابزار انگشت نگاری Xprobe برای امضاء اثر انگشت بود.

- Arpd 0.1 به Arpd 0.2 ارتقاء یافت.
- فایل پیکر بندی Honeyd اصلاح شد. تغییرات زیر در فایل پیکربندی ایجاد شدند:
- تغییر آدرس IP از 10.X.X.X به 192.168.X.X
- میزبان "Windows 2000 Professional, Build 2128" با

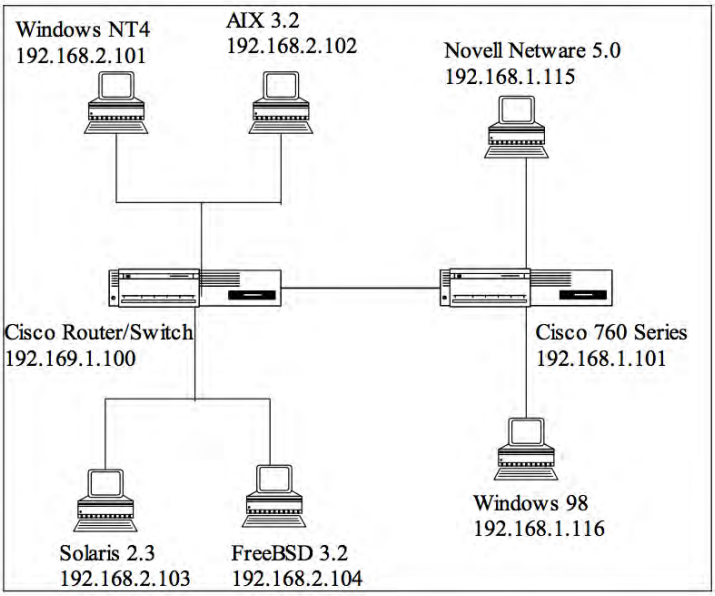
"Windows NT4.5 Server SP5-SP6" جایگزین شد. این کار عمدتاً به منظور ارائه یک معماری شبکه از نوع سرور، که قبلاً وجود نداشت انجام شد. علاوه بر این، اسکریپ Perl که شبیه ساز سرور IIS بود بر روی پورت 80، http اجرا شد. همچنین پورت های مختلف بر روی این میزبان خاص باز گذاشته شدند، مانند پورت های 139,137 از پروتکل TCP و پورت های 137,135 از پرتکل UDP. این پورتها به وسیله ی Net-Bios برای اتصال به شبکه برای سرویس های ورودی- خروجی بر روی سرورها استفاده می شوند.

- بر روی میزبان "AIX 3.2"، پورت ۲۵ مسدود شد. این استاندارد توسط سازمان های مختلف و ISP ها برای بستن پورت ۲۵ که برای ارسال ایمیل است اجرا می شود. این کار به کاهش میزان SPAM ها کمک می کند. این معماری شبکه بهبود یافته شبیه به شبکه یک شرکت می باشد. همچنین پورت ۲۱ برای FTP با یک اسکریپت Sell بر روی پورت باز سرور اجرا شد. این اسکریپت Log ناشناسی را بر روی سرور FTP با دسترسی محدود بعنوان مهمان فراهم می کرد. FTP یک سرویس جذاب برای مهاجمان است زیرا با استفاده از FTP آنها امکان Upload برنامه ها و ابزارهایشان را از مکان هایی از راه دور بر روی شبکه دارند.

- هم روتر و هم سوئیچ های Cisco قابلیت اتصال Telnet داشتند. بر روی پورت Telnet, 23 ، یک اسکریپت "Router- Telnet. Pl" اجرا شد که دسترسی Telnet به روتر را فراهم می کرد. این امر دسترسی کنسولی به روتر را با استفاده از Telnet برای مهاجمان ایجاد می کرد.

- "Novell Netware 3.12 or 386 TCP/IP" با آخرین امضا از "Novell Netware 5.0 SP5" جایگزین شد.

تغییرات ذکر شده در بالا ظاهر واقع گرایانه تر به شبکه می داد و با توجه به حضور فریب به حذف هر نوع سوءظن که می توانست در ذهن شرکت کنندگان در حال کاوش و حمله به شبکه به وجود آید کمک می کرد.



شکل (۵) معماری بهبود یافته Honeynet

جدول ۷، در زیر خلاصه آدرس های IP اختصاص داده شده و سرویس های جدید و بهبود یافته شبکه مجازی HoneyD را نشان می دهد.

IP Addresses	Signatures	Services
192.168.2.101	Windows NT 4.0 Server SP5-SP6	TCP – port 80, 137, 139 UDP - port 135, 137
192.168.2.102	AIX 3.2	TCP – port 21, 80
192.168.2.103	Solaris 2.3 – 2.4	TCP – port 80
192.168.2.104	FreeBSD 3.2 – 4.0	TCP – port 80
192.168.1.100	Cisco IOS 11.3 – 12.0(11)	TCP – port 23
192.168.1.101	Cisco Router/Switch with IOS 11.2	TCP – port 23
192.168.1.115	Novell Netware 5.0 SP5	TCP – port 80
192.168.1.116	Windows 98	TCP – port 80
Default	Windows 98	TCP – port 80, 22, 139

جدول (۷) خلاصه ایی از آدرس های IP اختصاص داده بر روی شبکه شرکت ها

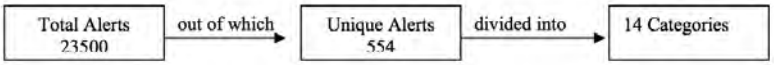
سرویس Telnet فقط بر روی روترهای Cisco (192.168.1.100-101) در دسترس قرار گرفت. از آنجا که روترهای Cisco به وسیله کنسول Telnet در دسترس هستند. این کار فرصتی را برای شرکت کنندگان جهت بهره برداری از سرویس Telnet برای بدست آوردن دسترسی به روترها فراهم می کرد. به طور پیش فرض پورت 22 برای SSH برای برقراری ارتباط بین میزبان ها سرورهای دیگر به شیوه ای امن، روی سیستم های ویندوز 98 باز بود. به طور عمده دلیل تصمیم محقق برای باز گذاشتن پورت 22 بر روی شبکه این حقیقت بود که ممکن است شرکت کنندگان سعی در Sniff داده های رمزگذاری شده (مانند کلمات عبور) برای برقراری ارتباط بین میزبان های مختلف و سرورهای شبکه داشته باشند.

بخش 1.04 نتایج تست دوم:

در طول مراحل تست دوم، از گروهی از دانشجویان در خواست شد تا به بررسی شبکه بهبود یافته (192.168.2.0/24 و 192.168.1.0.24 ، شکل ۶) با استفاده از HoneyD 0.5 بپردازند. این مرحله تست بین محدوده زمانی {00:54:26}21-03-2003 تا {12.21.55}22-03-2003 انجام شد. مکانیزم های مختلفی توسط دانشجویان برای تولید میزان قابل توجهی از داده ها آزموده شد.

تجزیه تحلیل ACID

از تست اولیه Snort IDS، 23500 هشدار ثبت شد، که ۵۵۴ هشدار منحصر به فرد وجود داشت که به ۱۴ دسته مختلف تقسیم می شوند.



این ۱۴ دسته در زیر آورده شده است:

Classification	Total Alerts	Signatures
Unclassified	1486 (6%)	266
Bad-unknown	9466(40%)	5
Attempted-recon	5615 (24%)	89
Web-application activity	3914 (17%)	112
Web-application attack	2641 (11%)	60
Misc-activity	125 (1%)	2
Misc-attack	14 (0%)	1
Attempted-dos	106 (0%)	6
Protocol-command-decode	23 (0%)	1
Attempted users	21 (0%)	2
Successful admin	44(0%)	1
Attempted-admin	20 (0%)	3
Unknown	5 (0%)	1
Rpc-portmap-decode	20 (0%)	4

از نتایج فوق، به نظر می رسد که شرکت کنندگان روش های مختلف حمله را برای نفوذ به شبکه انجام داده اند. شبیه به تست قبلی، تعداد زیادی پورت اسکن و همچنین حملات مبتنی بر وب با استفاده از اسکریپت های CGI و IIS وجود داشت. موارد کمی از تلاش برای Login از راه دور نیز وجود داشت.

شواهد نشان می دهد که شرکت کنندگان در تلاش برای بدست آوردن دسترسی Root در برخی از میزبان های شبکه بودند. یک رویداد ثبت شده نشان می داد که یک Query به RPCbind/Portmap بر روی ماشین Solaris فرستاده شد، که اطلاعات پورت برای سرویس RPC با استفاده از فهرست RPC را درخواست داشت. بسیاری از این حملات بسیار شبیه به آنچه که در تست قبلی انجام شد، بودند. بنابر بحث بالا ۵ مورد از شایع ترین هشدارها به صورت زیر هستند:

Signature	Classification	Total
ICMP redirect host	Bad-unknown	8451 (36%)
SNMP request udp	Attempted-recon	2756 (12%)
WEB-MISC Cisco IOS HTTP configuration attempt	Web-application attack	1270 (5%)
MISC Tiny Fragments	Bad-unknown	960 (4%)
STEALTH ACTIVITY (XMAS scan detection)	Unclassified	736 (3%)

جدول (۹) :۵ هشدارشایع تر

حمله تغییر مسیر میزبان ICMP حدود ۳۶٪ از تعداد کل هشدارها (مثلاً ۲۳۵۰۰) را تشکیل می داد. این نوع از حمله قادر به از کار انداختن یا قفل کردن ماشین میزبان می باشد.

هشدار دیگری که اغلب رخ می داد (حدود 12%) SNMP Request UDP بود که زیر گروه تلاش های بازسازی، طبقه بندی شده است. همچنین تعدادی حمله بر روی برنامه های تحت وب روی Cisco IOS وجود داشت.

Port Type	Occurrences	Unique Alerts
80 /tcp	8633	255
161 /tcp	2950	5
/tcp	960	1
162 /tcp	250	3
10080 /udp	114	1
177/udp	114	1
7001 /udp	114	1
10081 /udp	114	1
31337 /udp	96	1
22 /tcp	84	26
1 /tcp	62	4
69/tcp	47	2
800/udp	39	1
3128/tcp	33	1
8080/tcp	24	1

جدول (۱۰) لیستی از شماره پورت مقصد با هشدارهای مکرر

بخش 1.05 یافته هایی از فایل های Log

از مطالعه ی فایل Log، مشخص شد که بسیاری از شرکت کنندگان از Nessus (http://www.nessus.org) بعنوان ابزار اسکن شبکه برای شناسایی آسیب پذیری آن استفاده کرده بودند. یافته های مربوط به آسیب پذیری های نشان می دهد که بسیاری از آنها سعی در انجام حمله Brute Force داشتند. کاوش های مختلفی نیز برای بهره برداری از آسیب پذیری ها در پورتها و سرویس های مبتنی بر وب وجود داشت. اسکریپت های مختلف CGI و Perl برای ورود به سرویس های مبتنی بر وب استفاده شده بودند.

تلاش های مختلفی برای بهره برداری از آسیب پذیرهای SSH با استفاده از Nessus و Putty-Release-0.53b وجود داشت. Putty یک نرم افزار رایگان SSH، Telnet و Rlogin بر روی سیستم های ویندوز ۳۲ بیتی می باشد.

بخش 1.06 تجزیه و تحلیل Ethereal

دو فایل لاگ Tcpdump تولید شده در طول مراحل تست دوم وجود داشت.
Tcpdump.log.1048208266[Created on 21/03/03] و
Tcpdump.log.1048298249[Created on 22/03/03] که با استفاده از Ethereak Packet Sniffer تجزیه و تحلیل شدند. با توجه به آمار سلسله مراتب پروتکل ایجاد شده توسط Ethereal در فایل Tcpdump.log.1048208266، 22146 بسته که نزدیک به ۳۷,۷۸ ٪ آن ICMP و ۴۵,۹۰٪ بسته ها TCP بودند، وجود داشت. اکثر بسته های TCP، بسته های HTTP بودند. یعنی ۳۶,۶۵٪ از کل بسته های TCP. همچنین شواهدی از وجود Remote shell و بسته های پروتکل Rlogin وجود داشت. حدود ۱۶,۳۳٪ از کل بسته ها، شامل بسته های UDP هستندکه از آن ها ۱۳,۴۸٪ بسته های SNMP بودند. در تجزیه و تحلیل بیشتر از فایل Log مشخص شد که برخی از بسته ها روی برخی از پورت ها بیشتر تکرار شده اند. این نتایج در زیر فهرست شده اند:

- تلاش برای Login از راه دور بعنوان root از آدرس 172.16.253.253 (مهاجم یا آدرس منبع) به 192.168.1.1 (آدرس مقصد)

- Query های مربوط به TFTP از آدرس 172.16.253.253 به 192.168.1.1 وجود داشت. همچنین یک درخواست Read از TFTP برای فایل /etc/passwd ارسال شد.

- ارسال مکرر بسته هایی از TCP FIN، PSH و URG از پورت 42778 از آدرس 172.16.253.253 به پورت های مختلف 192.168.1.1

بر اساس آمار سلسله مراتب پروتکل تولید شده توسط Ethereal در فایل Tcpdump.log.1048298249، 746 بسته وجود داشت که نزدیک به 14.61٪ از بسته های ICMP و 76.94٪ از بسته های TCP بودند. اکثر بسته های TCP از نوع HTTP بودند. یعنی 69.71٪ از کل بسته های TCP. همچنین شواهدی از بسته های Shell و پروتکل Rlogin از راه دور در این فایل Log وجود داشت. حدود 8.45٪ از کل بسته ها شامل بسته های UDP می باشند. در تجزیه و تحلیل بیشتر از فایلLog، مشخص شد که برخی از بسته ها روی برخی از پورتها بیشتر تکرار شدند. این نتایج در زیر فهرست شده اند:

- شواهدی از استفاده برنامه Portmap نسخه ۲ با روال Dump از مبدأ (Source) با آدرس 172.16.1.120 به سمت آدرس مقصد 192.168.1.1 وجود دارد. این بسته ها از منبعی با پورت 624 به سمت پورت SunRPC (پورت 111) فرستاده شده اند.

- تعداد کمی بسته UDP از آدرس 172.16.0.1 با پورت nfsd به سمت 172.16.1.120 پورت 800 با حجم بالایی از داده وجود داشت (حدود ۴۲۱۶ بایت)

- همچنین چند بسته از صفحات زرد رمز عبور (YPPASSWORD) از برنامه نسخه ۳۲۸۰۳ با استفاده از فراخوانی روال از راه دور (RPC) نسخه ۲ وجود داشت.

- تلاش برای Login از راه دور به عنوان root از 172.16.1.120 (مهاجم یا آدرس مبدأ) به 192.168.1.1 (آدرس مقصد) انجام شد.

- Query های مربوط به TFTP از آدرس 172.16.1.120 به آدرس 192.168.1.1 وجود داشت. همچنین یک درخواست Read از TFTP برای فایل /etc/passwd وجود داشت.

بخش 1.07 باز خورد شرکت کنندگان:

شبیه به مانور نفوذ قبلی، از شرکت کنندگان خواسته شد به طور داوطلبانه نظرات شخصی خود را در مورد شبکه و یافته هایشان ارائه دهند. بازخورد رسیده از دو شرکت کننده در زیر آمده است:

شرکت کننده ۱: با توجه به ردیابی بسته ها با استفاده از traceroute و ping، به نظر می رسد هدف، شبکه ای بزرگ با تعداد زیادی از میزبان ها و چند سرور باشد. تعداد زیادی از درخواست های آدرس MAC در شبکه وجود دارد. از نتایج traceroute به نظر می رسد که میزبان 192.168.1.1 به Subnet متصل شده است. بنابراین، من به طور عمده میزبان 192.168.1.1 را هدف حملات قرار دادم. به نظر می رسد که این میزبان در موقعیت خوبی به عنوان یک روتر قرار دارد. همچنین برخی از مسیر های NFS در subnet را به اشتراک گذاشته است. پس از کاوش عمیق بر روی میزبان 192.168.1.1 اوضاع کمی گیج کننده شد. به نظر می رسید که دو میزبان در همان آدرس 192.168.1.1 وجود دارد و زمانی که در حال کاوش شبکه بودم شدیداً مرا سردگم می کرد و به نحوی شرایط پیچیده ای ایجاد کرده

بود. من همچنین یک روتر Cisco که در معرض خطر حمله DoS بود را در شبکه کشف کردم.

شرکت کننده ۲: تعداد زیادی از میزبان ها با سیستم عامل 98 که در حال اجرای سرور SSH بودند را مشاهده کردم. به نظر می رسید که یک SSH آسیب پذیر بر روی شبکه در حال اجرا بود. نقطه ورود به شبکه روتر Cisco با آدرس 192.168.1.100 بود. اما وقتی که تعدادی traceroute را در میزبان های مختلف دیگر انجام دادم، به نظر می رسید بیش از 192.168.1.1 را ردیابی می کند. به نظر می رسید که 192.168.1.1 به عنوان یک ماشین Gateway که ترافیک شبکه را به subnet هدایت میکرد عمل می کند. به طور کلی این شبکه یک شبکه بزرگ با آسیب پذیری های محدود به نظر می رسد.

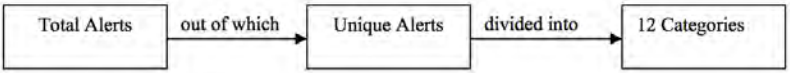
نتایج تست سوم با استفاده از HoneyD 0.5

بعد از مراحل تست دوم چند حفره ی امنیتی و هشدار که به طور بالقوه شناسایی شدند وجود داشت. بر اساس بازخورد دریافتی از شرکت کنندگان در مورد معماری شبکه، مشخص شد که دفاع شبکه به صورت محلی به خوبی انجام شده و فرصت زیادی به یک نفوذگر (مهاجم) برای انجام کاربر روی شبکه ارائه نشده است. بنابراین اشتباه نیست فرض کنیم که فریب ایجاد شده در گمراه کردن و گول زدن شرکت کنندگان موفق بوده است. از آنجا که آنها باور داشتند با یک شبکه سازمانی مواجه شده اند. یک نکته مهم که توسط یکی از شرکت کنندگان اشاره شد آن بود که او به درستی متوجه شده بر روی ویندوز 98 مایکروسافت IIS v.5 در حال اجرا است که این امر ممکن نیست. بنابراین تنها تغییر ایجاد شده در فایل پیکربندی، تغییر اسکریپت در سیستم عامل ویندوز 98 برای مایکروسافت IIS v.4 بود.

بخش 1.08 نتایج آزمون سوم

در طول مرحله تست سوم، از یک گروه از شرکت کنندگان خواسته شد به بررسی شبکه با طراحی بهبود یافته (192.168.1.0/24 و 192.168.2.0/24) با استفاده از HoneyD 5.0 بپردازند. این مرحله آزمون بین محدوده زمانی[14:09:16] 26-05-2003 تا [18:14:50] 27-05-2003 انجام شد. مکانیزم های مختلف توسط شرکت کنندگان به کار گرفته شد که میزان قابل توجهی داده در فایل های Log تولید می کرد.

از تست اولیه Snort IDS، ۱۹۰۳۶هشدار ثبت شد، که در آن میان ۴۵۳ هشدار منحصر به فرد وجود داشت که به ۱۲ دسته مختلف تقسیم شدند.



این ۱۲ دسته در جدول ۱۱ نشان داده شده است.

Classification	Total Alerts	Signatures
Unclassified	342 (2%)	211
Bad-unknown	11737(62%)	4
Attempted-recon	4814 (25%)	81
Web-application activity	1299 (7%)	104
Web-application attack	664 (3%)	40
Misc-activity	151 (1%)	3
Misc-attack	1 (0%)	1
Attempted-dos	15 (0%)	5
Protocol-command-decode	3 (0%)	1
Successful admin	6(0%)	1
Attempted-user	1 (0%)	1
Rpc-portmap-decode	3 (0%)	1

جدول (۱۱) *دسته بندی هشدار های جمع آوری شده در ۱۲ گروه*

شبیه به آزمون قبلی، میزان زیادی عملیات اسکن پورت و همچنین حملات مبتنی بر وب با استفاده از اسکریپت های CGI و تلاش هایی برای دسترسی به IIS وجود داشت.

در جدول صفحه قبل می توان دید که ۱۰۴ امضاء تحت Web-Application-Activity و ۴۰ امضاء تحت Web-Application-Attack می باشند. بسیاری از این حملات بسیار شبیه به حملات قبلی انجام شده در ۲ مانور آخر نفوذ به شبکه بودند. تعداد زیادی بسته UDP به میزبان 192.168.1.28 سرریز شده بودند. این کار عمدتاً برای انجام یک حمله DoS بر روی میزبان انجام می شود و باعث از کار افتادن آن میزبان در پاسخ به درخواست های شبکه می گردد. یک نکته مهم دیگر که در داده های بالا باید به آن توجه داشت این است که ۶۲٪ از مجموع هشدارها تحت Bad-Unknown دسته بندی شده اند. این بدان معنی است که بسیاری از حملات انجام شده درخواست ICMP از بسته های بزرگ UDP جهت انجام حمله DoS بوده اند. ۵ مورد از شایع ترین هشدارها در جدول ۱۲ نشان داده شده است.

Signature	Classification	Total
ICMP redirect host	Bad-unknown	6478 (34%)
MISC large UDP packets	Bad-unknown	5242 (28%)
Scan Squid Proxy Attempt	Attempted-recon	1061 (6%)
Scan Proxy (8080) attempt	Attempted-recon	730 (4%)
SNMP request udp	Attempted-recon	690 (4%)

جدول (۱۲) ۵ مورد از شایع ترین هشدارها

حمله میزبان ICMP Redirect حدود ۳۴٪ از تعداد کل هشدارها را تشکیل می دهد. این نوع از حمله قادر است ماشین میزبان را از کار انداخته یا آن را قفل کند. هشدار شایع دیگری که رخ داده است، Misc Large UDP Packets بود که این هشدار نیز تحت عنوان Bad-Unknown دسته بندی شده است.

این رویداد نشان می دهد که یک بسته UDP غیر عادی و بسیار بزرگ به سرور شما فرستاده شده است. این بسته ممکن است باعث DoS و یا استفاده از یک کانال پنهان را نشان دهد. از آنجایی که این رویداد توسط یک بسته UDP ایجاد شده، آدرس IP مبدأ (Source) به راحتی می تواند جعل شود. همچنین، گفته شده است که با توجه به ماهیت این رویداد مهاجم به

طور معمول نیاز به ترافیک پاسخ ندارد. بنابراین، در اکثر موارد این رویداد باید همراه با سایر داده ها قبل از اقدام به حمله تجزیه و تحلیل شود.

سه هشدار دیگر در گروه Attempted-Recon (تلاش- بازسازی) دسته بندی شدند. از مقایسه نتایج بدست آمده در جداول ۱۱ و ۱۲ می توان گفت که اکثریت ترافیک شبکه در گروه Bad-Unknown وAttempted-Recon دسته بندی شده اند.

همچنین تعداد زیادی از عملیات اسکن پورت در شبکه به چشم می خورد. نتایج بررسی آن می تواند جزئیات بیشتری از وقوع هشدارها و هشدارهای منحصر به فرد ارائه دهدکه در جدول ۱۳ ارائه شده است.

Port Type	Occurrences	Unique Alerts
80 /tcp	7777	217
161 /tcp	1375	4
3128 /tcp	1062	2
8080 /tcp	731	2
1080 /tcp	463	1
162 /tcp	407	3
705 /tcp	169	1
0 /udp	139	7
137 /udp	81	77
177 /udp	18	1
10080 /udp	17	1
10081 /udp	16	1
7001 /udp	16	1
22 /tcp	14	8
69 /udp	13	2

جدول (۱۳) فهرستی از شماره های پورت مقصد با هشدارهای مکرر

بخش 1.09 یافته هایی از فایل های Log

از مطالعه فایل Log، مشخص شد که اکثر شرکت کنندگان Nessus

(http://www.nessus.org) را بعنوان ابزار اسکن شبکه برای شناسایی آسیب پذیری ها در شبکه استفاده کرده اند. در یافته های آسیب پذیریها مشخص شد که اکثر آنها سعی در انجام حمله Brute Force در شبکه هدف را داشته اند. بررسی های متعددی نیز برای بهره برداری از آسیب پذیری ها در سرویس ها و پورت های تحت وب انجام شده بود. شواهد نشان می دهد که شرکت کنندگان تلاش کردند تا برای کسب دسترسی به :c:\>drive به ماشین های مختلفی متصل شوند.

participants tried to connect few machines to gain access to *C:\>* drive:

```
GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c: HTTP/1.0
GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:+/s HTTP/1.0
:
:
:
http://192.168.1.28/scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:+/s
http://192.168.0.1/scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:+/s
http://192.168.1.28/scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:+/s
GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:+/s HTTP/1.0
GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:wwwroot+/s HTTP/1.0
GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:wwwroot+/s HTTP/1.0
```

فایل Log فوق نشان می دهد که شرکت کنندگان در تلاش برای دسترسی به سیستم فایل سرور IIS از طریق دستورات مبتنی برکنسول بودند. این حمله اگر موفق می شد، می توانست دسترسی کامل به Web-Server را برای شرکت کنندگان فراهم کند. در نتیجه این امر در سازش با Web Server، شرکت کنندگان می توانستند تمام سرویس های Web- Based (مبتنی بروب) را متوقف یا غیر فعال کنند که ممکن بود تاثیر زیادی در شبکه داشته باشد.

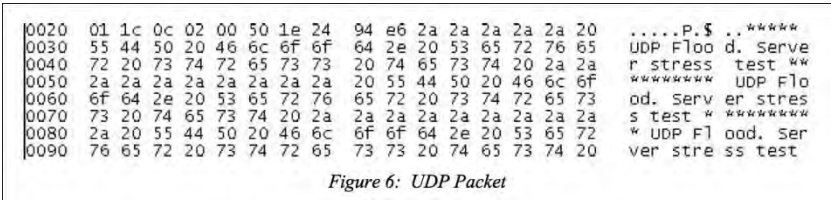
بخش 1.10 تجزیه و تحلیل Ethereal

دو فایل Log مربوط به Tcpdump در طول مرحله تست سوم تولید شدند:
tcpdump.log.1053944062 و tcpdump.log.1054023963 که با استفاده از Ethereal Packet Sniffer تجزیه و تحلیل شدند. براساس آمار سلسله مراتب پروتکل تولید شده در فایل tcpdump.log.1053944062، ۱۴۴۱۹ بسته وجود داشت که از آن

میان، حدود 30.52% بسته های ICMP و25.36% بسته های TCP بودند. اکثر بسته های TCP از نوع HTTP بودند که 12.03% از کل بسته های TCP را شامل می شوند. حدود 44.13% از کل بسته ها شامل بسته های UDP بودند که از آن میان حدود 37.10% بسته های داده بودند. این نشان می دهد که میزان زیادی از داده در شبکه از نوع UDP در برخی از پورتها سر ریز شده اند.

در تجزیه و تحلیل بیشتر فایل Log، مشخص شد که برخی از بسته ها در برخی از پورتها بیشتر تکرار شده اند. این نتایج در زیر فهرست شده اند:

- مقدار زیادی از بسته های داده UDP با میزبان 192.168.1.28 از منبع با شماره پورت 3074 به پورت 80 (پورت HTTP) منتقل شدند.



```
0020  01 1c 0c 02 00 50 1e 24  94 e6 2a 2a 2a 2a 2a 20   .....P.$ ..*****
0030  55 44 50 20 46 6c 6f 6f  64 2e 20 53 65 72 76 65   UDP Floo d. Serve
0040  72 20 73 74 72 65 73 73  20 74 65 73 74 20 2a 2a   r stress  test **
0050  2a 2a 2a 2a 2a 2a 2a 2a  20 55 44 50 20 46 6c 6f   ********  UDP Flo
0060  6f 64 2e 20 53 65 72 76  65 72 20 73 74 72 65 73   od. Serv er stres
0070  73 20 74 65 73 74 20 2a  2a 2a 2a 2a 2a 2a 2a 2a   s test * ********
0080  2a 20 55 44 50 20 46 6c  6f 6f 64 2e 20 53 65 72   * UDP Fl ood. Ser
0090  76 65 72 20 73 74 72 65  73 73 20 74 65 73 74 20   ver stre ss test
```

Figure 6: UDP Packet

شکل (۶) *بسته UDP*

این عمل منجر به تأخیر جریان ترافیک شبکه در این میزبان خاص می شود که بعنوان تخریب کامل عملکرد جریان ترافیک بر روی کل شبکه تلقی می شود. همانطور که قبلاً ذکر شد، Ethereal بسته ای را ردیابی و ثبت کرده است که نشان می دهد مهاجم یک دستور اسکریپ برای بازیابی اطلاعات مربوط به سطح دایرکتوری را اجرا کرده است:

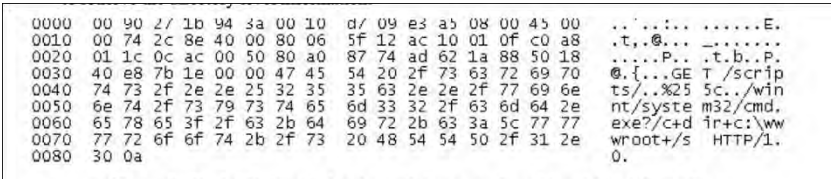


Figure 7: Packet Captured showing script command used to retrieve information

شکل (۷) *بسته ثبت شده نشان دهنده اسکریپ مورد استفاده برای بازیابی اطلاعات است*

براساس آمار سلسله مراتب پروتکل تولید شده در فایل tcpdump.log.1054023963، ۴۰۸۲ بسته وجود دارد که از آن حدود 49.73% بسته های ICMP بودند و 35.96٪ بسته ها TCP و اکثریت آنها از نوع HTTP بودند که 19.79% از کل بسته های TCP را شامل می شوند. حدود 14.31% از کل بسته ها شامل بسته های UDP هستند که از آن بین 12.47% بسته هایی از پروتکل SNMP بودند.

نتیجه گیری

هدف از این تحقیق ارتقاء سطح فریب ارائه شده به شرکت کنندگان در معماری شبکه Honeynet بود. مستحکم سازی هانی پات های فریبنده برای آزمایش اثر بخشی در روش های جمع آوری اطلاعات حمله با استفاده از روش یادگیری تجربی ضرورت داشت. مانور نفوذ به شبکه در سه نوبت مختلف انجام شد. داده های جمع آوری شده از هر مانور ابتدا تجزیه و تحلیل شدند و سپس پیکر بندی شبکه قبل از شروع مانور نفوذ بعدی به منظور جمع آوری داده ها بهبود می یافت. بعد از اتمام هر مانور، شرکت کنندگان بطور داوطلبانه بازخوردشان را از جزئیات درک خود از شبکه طراحی شده ارائه دادند. این روند در تعیین بهبود سطح فریب ارائه شده به شرکت کنندگان که به وضوح برای آنها ناشناخته بود کمک می کرد.

از داده های جمع آوری شده از اولین مانور نفوذ به شبکه مشخص شده که 50% از ترافیک شبکه، ترافیک TCP بوده است. درحالی که UDP و ICMP به ترتیب 18% و 32% را تشکیل می دهند. اکثر حمله ها در پروتکل های مبتنی بر TCP/IP بودند برای مثال، در

HTTP پورت 80 یا 8080 برای حمله مبتنی بر وب هدف قرار گرفتند. حملات مبتنی بر وب زیاد دیگری نیز در شبکه انجام شدند که برجسته ترین آنها Proxy Scan و حملات مبتنی بر دسترسی اسکریپت WEB-IIS بودند.

از آنجا که از بازخورد کلی شرکت کنندگان مشخص شد که آنها معماری شبکه را شبکه ای ساده که فاقد سرویس های FTP یا Telnet برای ارائه هر گونه دسترسی از راه دور پنداشته بودند، بنابراین معماری شبکه برای شبیه سازی چنین سرویس هایی بهبود یافت. پس از آنکه شبکه پس از اصلاح اسکرپیت پیکر بندی و ارتقاء HoneyD با آخرین نسخه بهبود یافت، دور دوم نفوذ انجام شد. مشخص شد که ترافیک TCP برروی شبکه با 5% کاهش به 45% رسیده است. که این نشان می دهد که Honeypot مستحکم تر از تنظیمات قبلی شده و پیکربندی آن اجازه ترافیک TCP/IP کمتر و قانونی تر را می دهد. همچنین یک کاهش جزئی در ترافیک بیش از حد UDP وجود داشت. اما ترافیک ICMP از4% به 38% افزایش یافت. از آنجا که شواهدی مبنی بر تلاش برای Login از راه دور در شبکه وجود داشت، می توان در نظر گرفت که اجرای سرویس های شبیه سازی شده دسترسی از راه دور مانند FTP و Telnet نیز موفقیت آمیز بود. شواهدی نیز از استفاده از ابزارهای مختلف مانند Putty–Release–0.53b (SSH-Client) وجود داشت.

از باز خورد کلی شرکت کنندگان نیر مشخص شد آنها اعتقاد دارند شبکه هدف به جز چند ریسک امنیتی کوچک فرصت های زیادی به آنها برای حمله ارائه نکرده است. بنابر این در می یابیم شبکه به خوبی طراحی شده و به قدر کافی ایمن است.

در تست سوم نفوذ به شبکه، ترافیک TCP مقدار قابل توجهی کاهش داشت. از کل ترافیک شبکه، TCP فقط 29% از ترافیک را تشکیل می داد که 16% کاهش یافته است در حالی که ترافیک UDP از 20% به 37% افزایش یافته است. در تجزیه و تحلیل این نتایج مشخص شد که این بار شرکت کنندگان در تلاش برای راه اندازی حمله DoS (Denial of service) با

استفاده از یک تروجان به نام UDP Flooder با میزان زیادی از بسته های UDP بوده اند. تغییرات بسیاری در ترافیک ICMP وجود نداشت.

شرکت کنندگان همچنین در تلاش برای اتصال به سرور شبیه ساز مایکروسافت IIS با استفاده از دستورات اسکریپت GET بودند. این تلاش ها نشان می دهد که شرکت کنندگان باور داشته اند که یک شبکه واقعی با سرویس های واقعی را بررسی کرده اند. بنابراین، باور اینکه فریب شبکه ایجاد شده با استفاده از HoneyD یک تلاش موفق بوده و قادر به ارائه بسیاری از حقایق و نتایج جالب در بهبود فریب بوده سخت نیست.

پیکر بندی و پیاد سازی یک Honeynet کار بسیار وقت گیر و پر مخاطره است. یک اشتباه کوچک در پیکر بندی و پیاده سازی یک Honeynet ممکن است باعث نگرانی جدی در شبکه شود. همه داده ها باید به دقت تجزیه و تحلیل شده و مکانیزم پشتیبان گیری (Backup) مناسب در جای خود انجام شود. بنابراین، یک Honeynet باید با هدایت و نظارت مناسب پیکر بندی شود.

هانی نت پیکر بندی شده در این پژوهش را می توان بعنوان یک هانی نت موفق در نظر گرفت زیرا که می توانست شرکت کنندگان را گمراه کرده، اطلاعات جاسوسی و حملات را جمع آوری کند و داده های مناسبی را برای تحلیل در اختیار کارشناسان قرار دهد.

گردآوری و ترجمه: عباس عظیمی

با تشکر از خانم ها کبری بدرلو و مریم ثقفی

منابع:

www.ecu.edu.au
www.kaminpod.com
www.vaya.ir

Head Office: +9821 88 35 39 55
Support Center: +9821 442 311 47
R&D Unit: +98281 335 96 70
www.vaya.ir info@vaya.ir