بهبود امنیت شبکه با هانی‌پات

ترجمه و تالیف

دکتر مجید مقدادی

(عضو هیات علمی دانشگاه زنجان)

انور پوراحمد

سرشناسه
عنوان و نام پدیدآور
مشخصات نشر
مشخصات ظاهری
شابک
وضعیت فهرست نویسی
موضوع
موضوع
موضوع
موضوع
موضوع
شناسه افزوده
رده بندی کنگره
رده بندی دیویی
شماره کتابشناسی ملی

مقدادی، مجید، ۱۳۴۴.
بهبود امنیت شبکه با هانی‌پات / تالیف مجید مقدادی، انور پوراحمد.
تهران: انتشارات دانشگاهی کیان، ۱۳۹۳.
۱۲۸ص.: مصور، جدول، نمودار.
۹۷۸-۶۰۰-۳۰۷-۰۵۳-۰
فیپا
کامپیوترها — ایمنی اطلاعات.
هکرها.
فایروال (ایمن‌سازی کامپیوترها).
شبکه‌های کامپیوتری — تدابیر ایمنی.
ارتباطات بی سیم — تدابیر ایمنی.
پوراحمد، انور، ۱۳۶۹.
۱۳۹۳ ۲۷م۷/۱۲۵/QA۷۶۹
۰۰۵/۸
۳۶۱۵۰۸۵

نشردانشگاهی کیان
Kian Publication

نام کتاب	: بهبود امنیت شبکه با هانی‌پات
ناشر	: دانشگاهی کیان
مولفان	: مجید مقدادی و انور پوراحمد
ویراستار	: مرضیه امانت
ناظر چاپ	: پیمان عمرانی
چاپ اول	:۱۳۹۳
تیراژ	: ۲۰۰
چاپ و صحافی	: گنج شایگان
قیمت	: ۸۵۰۰ تومان
شابک	: ۹۷۸-۶۰۰-۳۰۷-۰۵۳-۰
ISBN	: 978-600-307-053-0

مرکز پخش:
تهران، خیابان انقلاب، خیابان ۱۲ فروردین، کوچه‌ی نوروز، پلاک ۲۷، طبقه‌ی اول
۶۶۴۱۱۷۱۵ – ۶۶۴۰۶۸۳۴ – ۶۶۴۱۶۴۴۶

خرید آنلاین از طریق وب‌سایت www.kianpub.com
SMS ۳۰۰۰۲۲۱۴۴۱

سخنی با خوانندگان

«سپس، به کاتبان و نویسندگانت بنگر و بهترین آن‌ها را بر کارهای خود بگمار... کاتبان و نویسندگانی برگزین که قدر خود را بشناسند، چون کسی که به قدر خود شناخت ندارد، دیگران را هم نمی‌شناسد.»

«برگرفته از نامه‌ی ۵۳ نهج‌البلاغه به مالک‌اشتر»

اگرچه نوشتن و پرداختن زکات علم از توصیه‌های اکید بزرگان و گواه بر کرامت اهل دانش است، اما امروزه پرداختن به انگیزه‌ها و اهداف نوشتن بیشتر جلوه می‌کند. بی‌شک این‌که چه کسی می‌نویسد مهم نیست، اما این‌که چرا و به چه پشتوانه‌ای می‌نویسد، درخور تأمل است. ما معتقدیم که چاپ روزافزون کتاب‌های به اصطلاح «زرد» که خالی از هرگونه نوآوری و بی‌توجه به استانداردهای چاپ کتاب و نیازهای مخاطبان است، حاصل تفکر بازاری مستولی بر جامعه‌ی نشر است. بی‌پرده آن‌که عنوان پر زرق و برق، دستاویز قرار دادن مضمون‌های نو با هدف فروش بالا و طویل کردن سیاهه‌ی سابقه‌ی علمی، نمی‌تواند دلیل محکمی برای چاپ و نشر کتابی باشد که خواننده‌ی مشتاق با صرف هزینه‌های نه چندان کم آن را تهیه می‌کند؛ به امید آن که چیزی از آن بیاموزد.

باید پذیرفت که انگیزه‌ی نوشتن کم از محتوای نوشته نیست و بین این دو رابطه‌ای مستقیم برقرار است. اگر انگیزه از نوشتن، تولید دانش باشد، بی‌شک نویسنده از قلم بی‌محتوا وکم‌عمق پرهیز می‌کند و اگر دغدغه‌ی دانش و فرهنگ زخم‌خورده در میان باشد، ناشر تنها به عنوان پرطمطراق بسنده نمی‌کند.

و چقدر امروزه، فرهنگ و دانش این مرز بوم که گرفتار آفت بی‌انگیزگی و زخم هوس است، نیازمند ناشران و نویسندگانی است که نیت‌شان کمک به رشد دانش و ارتقای فرهنگ جامعه است و به راستی که التیامی بر این درد نیست مگر نویسندگانی که قدر خود و دیگران را می‌دانند و خوب می‌فهمند که کتاب، ابزار سودجویی‌های مغرضانه نیست و می‌کوشند تا خود را از هرگونه شهوت نام و رسم و ثروت تهی کنند.

انتشارات دانشگاهی کیان خود را بری از عیب و خطا نمی‌داند، اما همواره بیش از پیش می‌کوشیم تا در راستای تولید علم و نشر کتاب‌های پرمحتوا، دست نویسندگانی که انگیزه‌ی پاک دارند را فشرده و در کنارشان باشیم و از خداوند متعال می‌خواهیم که در این مسیر صعب و پرخطر در سایه‌ی لطف و عنایت خود از آن‌چه به عهده‌ی ما نهاده شده، سربلند و پیروز برآییم.

انتشارات دانشگاهی کیان

تقدیم و تشکر

سپاس و ستایش خدای جل‌وجلاله که آثار قدرت او بر چهره روز روشن، تابان است و انوار حکمت او در دل شب تار، درخشان. آفریدگاری که خویشتن را به ما شناساند و درهای علم را بر ما گشود و عمر و فرصتی عطا فرمود تا بدان، بنده ضعیف خویش را در طریق علم و معرفت بیازماید.

تقدیم به پدر بزرگوار و مادر مهربانم

آن دو فرشته‌ای که از خواسته‌هایشان گذشتند، سختی‌ها را به جان خریدند و خود را سپر بلای مشکلات و ناملایمات کردند تا من به جایگاهی که اکنون در آن ایستاده‌ام، برسم.

انور پوراحمد

مقدمه‌ی مولفان

با توجه به کمبود منابع فارسی مطالعاتی در رابطه با امنیت شبکه به روشی نوین، بر آن شدیم که همراه با ارایه کتابی در این راستا، شما را تاحدودی با فناوری جدیدی که در حال حاضر در بسیاری از مراکز، بانک‌ها، دانشگاه‌ها و شرکت‌ها، که جهت مقابله با هک و نفوذ مورد استفاده قرار می‌گیرد، آشنا سازیم.

به جهت گسترده شدن اینترنت و فراگیر شدن آن در تمام نقاط جهان، لزوم برقراری امنیت نیز یکی از پارامترهای اساسی است و باید مورد توجه قرار گیرد، چرا که در غیراین‌صورت فاجعه‌های جبران‌ناپذیری به بار خواهند آمد. هانی‌پات یکی از فناوری‌هایی است که برای تامین امنیت سیستم‌ها و جلوگیری از نقوذ هکرها طراحی و توسعه داده شده است.

برای بسیاری از افراد هنوز هم واژه هانی‌نت و هانی‌پات مبهم بوده و حتی بسیاری از فارغ‌التحصیلان رشته‌های مرتبط نیز اطلاعی از آن ندارند. در این کتاب علاوه بر معرفی اجمالی هانی‌پات و هانی‌نت، نحوه پیاده‌سازی و همچنین پیکربندی صحیح آن آموزش داده شده و واژگان تخصصی این حوزه مطرح گردیده است.

با توجه به اینکه مطالب این کتاب تا حدودی تخصصی است، شاید برای افراد مبتدی زیاد مناسب نباشد که در شروع کار این کتاب را مطالعه نمایند؛ زیرا خواننده باید دانش عمومی از شبکه، لایه‌های آن و نحوه کار آن داشته باشد. البته باتوجه به اینکه سعی شده متن کتاب تا حد امکان ساده و روان باشد، مبتدیان می‌توانند با مطالعه‌ای جزیی در رابطه با شبکه‌های رایانه‌ای، به مطالعه این کتاب بپردازند.

در فصل اول ابتدا پیش‌نیازها آمده‌اند و سعی شده خواننده با واژگان و اصطلاح‌های اولیه آشنا شود و دلیل استفاده از هانی‌پات را درک نماید. در فصل دوم به معرفی مفاهیم و معماری هانی‌پات پرداخته شده است. در فصل سوم هر یک از سناریوهای هانی‌پات به تفصیل شرح داده شده‌اند. در فصل چهارم روش شروع کار عملی آمده است. کریستین دورینگ آزمایش‌های خود را در آزمایشگاه دانشگاه محل تحصیل خود، یعنی FHD به انجام رسانده و مراحل کار و روند آن نیز براساس آزمایش‌های وی تدارک دیده شده است. در فصل پنجم نحوه ثبت داده‌ها، آنالیز داده‌ها، توضیح برخی از انواع حملات و موارد دیگر آمده و در نهایت در فصل ششم خلاصه‌ای از مطالب

کتاب و جمع‌بندی آن‌ها ارایه شـــده اســـت. همچنین در انتهای کتاب، قسمت ضمایم، فرم‌ها و نمونه آزمایش‌هایی برای کار عملی و ثبت نتایج آمده است.

در انتهـــا از جناب آقای مهندس امیرحســـین حاجوی به جهت کمک‌های شـــایانی که در امر ترجمه و تالیف این کتاب داشـــته‌اند، نهایت تشـــکر و قدردانی را دارم. از خوانندگان گرامی تقاضا می‌شـــود ایرادهای احتمالی کتاب را به آدرس apco_pourahmad@yahoo.com ایمیل نمایید. هرگونه پیشنهاد، انتقاد یا نظر خود را نیز با این ایمیل مطرح نمایید.

مجید مقدادی
انور پوراحمد

فهرست مطالب

فصل اول ـ چرا هانی‌پات‌ها امنیت شبکه را بهبود می‌بخشند؟

فصل دوم ـ مفاهیم، معماری و اصطلاحات مربوط به هانی‌پات

۲-۱. کلاه‌سفیدها و کلاه‌سیاه‌ها ۱۳
۲-۲. تاریخچه هانی‌پات ۱٤
۲-۳. انواع هانی‌پات ۱۵
۲-٤. سطوح تعاملی ۲۰
۲-۵. انواع حملات ۲۱
۲-٦. مقوله‌های امنیتی ۲۲
۲-۷. آدرس‌های IP مخفی ۲٤

فصل سوم ـ هانی‌پات در حوزه کاربردی

۳-۱. سناریوی اول- محیط حفاظت‌نشده ۲۸
۳-۲. سناریوی دوم- محیط حفاظت‌شده ۲۹
۳-۳. سناریوی سوم- آدرس‌های عمومی ۲۹
۳-٤. سناریوی چهارم- آدرس‌های محرمانه ۳۰
۳-۵. سناریوی پنجم- ارزیابی ریسک ۳۱
۳-٦. سناریوی ششم- هانی‌پات‌ها، خارج از box ۳۲
۳-۷. سناریوی هفتم- دانش/ آموزش ۳۷

فصل چهارم ـ برنامه‌ریزی هانی‌پات در FHD

٤-۱. آنالیز محیط ٤۱
٤-۲. ارزیابی راه‌حل‌های سابق ٤۱
٤-۳. برنامه‌ریزی تجربی هانی‌پات ٤۳
٤-٤. پیاده‌سازی Honeywall (دیواره عسلی) ٤۸
٤-۵. انتخاب طعمه ۵۰

فصل پنجم ـ اجرا و مشاهده آزمایش‌ها

۵-۱. نیازمندی‌ها برای برپایی شبکه‌ای ایمن ۵۱
۵-۲. حملات اینترنتی ۵۸
۵-۳. تجزیه‌وتحلیل وقایع ثبت‌شده در حالت کلی ٦٦
۵-٤. آنالیز داده‌ها مطابق با Roo_Die و Roo_Mue ۷۵

فصل ششم ـ خلاصه

٦-۱. بهبود هانی‌پات ۸۱
٦-۲. نتیجه ۸۲
٦-۳. پیشنهاداتی برای ادامه کارهای آتی ۸۲

ضمایم

مراجع

فصل اول

چرا هانی‌پات‌ها امنیت شبکه را بهبود می‌بخشند؟

هانی‌پات‌ها باعث بروز تغییری شـــگرف برای هکرها و متخصصان امنیت رایانه شدند. با وجود آن که یک رایانه تا حد امکان باید ایمن باشـــد، در حوزه هانی‌پات‌ها، حفره‌های امنیتی با هدف خاصی بازنگه‌داشته می‌شوند. به‌عبارت دیگر، هانی‌پات‌ها به هکرها و دیگر تهدیدات خوش‌آمد می‌گویند.

هدف یک هانی‌پات تشخیص و یادگیری الگوها و رخنه‌ها از روی حملات و در نهایت استفاده از این اطلاعات برای بهبود امنیت شـــبکه می‌باشد. فرد مدیر شبکه، نخستین بار اطلاعاتی در رابطه با حملات سابق به‌دست می‌آورد. حفره‌های امنیتی کشف‌نشده را می‌توان به‌وسیله اطلاعاتی که از هانی‌پات به‌دست آمده، حفاظت نمود.

در دانشنامه ویکیپدیا، هانی‌پات این‌گونه تعریف شده است:

«هانی‌پات‌ها مجموعه‌ای از حفره‌ها یا تله‌ها هســـتند که به‌صورت غیرمجاز از اطلاعات سیســـتم‌ها استفاده می‌کنند».

هانی‌پات رایانه‌ای متصل به شـــبکه اســـت. این رایانه می‌تواند برای تشـــخیص آسیب‌پذیری سیستم‌عامل یا شبکه، مورد استفاده قرار گیرد. بسته به نوع راه‌اندازی، حفره‌های امنیتی را در حالت کلی یا حالاتی خاص می‌توان مورد بررســـی قرار داد. همچنین، می‌توان برای مشـــاهده فعالیت‌های فردی که به هانی‌پات دسترســـی پیدا کرده، اســـتفاده نمود. هانی‌پات‌ها ابزاری منحصربه‌فرد جهت یادگیری در رابطه با تدابیری که هکرها به‌کار می‌برند، هستند.

تاکنون تکنیک‌های دیده‌بانی[1] شـــبکه، از دســـتگاه‌هایی منفعل اســـتفاده می‌کردند؛ از این قبیل می‌توان به سیستم کشف و ردیابی نفوذ[2] یا IDS اشاره کرد. در IDS ترافیک شبکه برای ارتباط‌هایی مبتنـــی بر الگوها، تجزیه و تحلیل می‌شـــدند. این تکنیک‌ها می‌تواننـــد عبارت‌هایی خاص در بازدهی بسته‌ها یا مجموعه‌ای از بسته‌ها باشند. اگرچه امکان وجود پیام‌های مثبت کاذب وجود دارد، که به اقتضای عدم تطابق یک الگو یا حتی وخیم بودن آن، پیام منفی کاذب، در حملات واقعی می‌باشد. در هانی‌پات هر بسته در ابتدا مشکوک است. دلیلی که برای این مورد وجود دارد، سناریوی هانی‌پات اســـت، هانی‌پات روی هیچ‌گونه سیستم تولیدی ثبت نشده است. سیستم‌های تولیدی معین، نباید از وجود هانی‌پات مطلع باشند. همچنین هانی‌پات نباید هیچ‌گونه داده حقیقی تولیدشده را در دسترس قرار دهد. این تضمین می‌نماید که هانی‌پات به واســـطه یک وســـیله قابل اعتماد متصل نشده است. بنابراین هر وسیله‌ای برای ایجاد یک اتصال با هانی‌پات یا وسیله‌ای که به‌صورت اشتباه پیکربندی شده یا منبع حملات، مورد استفاده قرار می‌گیرد. این مورد باعث سادگی در تشخیص حملات روی هانی‌پات‌ها می‌شود (به مطلب ۳-۶-۵ مراجعه کنید [فصل سوم، مبحث ۶-۵، صفحه ۳۶، هشدار]).

1. Monitoring
2. Intrusion Detection Systems

فصل دوم

مفاهیم، معماری و اصطلاحات مربوط به هانی‌پات

در این فصل مفاهیم، معماری و اصطلاح‌های مربوط به هانی‌پات آمده است. به‌وسیله این موارد امکان‌پذیری پیاده‌سازی انواع هانی‌پات و هدف استفاده از آن را توصیف می‌کنند. به‌علاوه عبارت‌ها و اصطلاح‌های معینی همراه با توضیح کامل، جهت به‌دست آوردن درک عمیق‌تر در رابطه با اهداف موجود در مفاهیم هانی‌پات، آمده است.

۲-۱. کلاه‌سیاه‌ها و کلاه‌سفیدها

در مبحث امنیت رایانه، کلاه‌سیاه هکری ماهر(خبره)، فردی است که از توانایی خود در جهت بهره بردن به‌صورت غیرقانونی و غیرمجاز استفاده می‌کند. آنها برخی اوقات از دیدگاه اقتصادی برانگیخته می‌شوند، یا ممکن است نماینده یک انحراف سیاسی باشند. به‌طورکامل، برخی اوقات این فعالیت ناشی از کنجکاوی است [Wikip 05]. اصطلاح "کلاه‌سیاه" از فیلم‌های قدیمی غربی گرفته شده که در آنها یاغیان و قانون‌شکنان با کلاه سیاه و قهرمانان و دلاوران را با کلاه سفید نشان می‌دادند.

کلاه‌سفیدها از لحاظ اخلاقی نقطه مقابل سواستفاده از سیستم‌های رایانه‌ای هستند. یک کلاه‌سفید در حالت کلی روی ایمنی سیستم‌های IT متمرکز است، درحالی‌که یک کلاه‌سیاه تمایل به شکستن ایمنی آنها را دارد.

هر دو دسته کلاه‌سفیدها و کلاه‌سیاه‌ها، هکر به‌شمار می‌روند. به هر حال هردوی آنها متخصص رایانه‌ای هستند که به آنها "script kiddies" اطلاق می‌گردد. در واقع script kiddies را می‌توان به کلاه‌سیاه‌ها ارجاع داد، اما چنین ارجاعی، به نوعی می‌تواند تعریف کردن از چنین اشخاصی باشد.

آنها رفتارها و کردارهای خود، یا آسیب‌های کشف‌شده را در میان نمی‌گذارند. در عوض از ابزارهای منتشرشده به‌وسیله جامعه کلاه‌سیاه‌ها استفاده کرده و آسیب و زیانی تصادفی را ایجاد می‌کنند.

یک کرم، برنامه‌ای منحصربه‌فرد است که تلاش می‌کند در سطح شبکه به‌صورتی عادی همتاسازی (کپی‌برداری از خود) را انجام دهد. پس از آلوده شدن سیستم‌ها به کرم‌ها، آنها حتی دانلود شده و نرم‌افزار آنها به‌صورت خودکار جهت کنترل کامل روی شبکه نصب می‌شود. این‌گونه نرم‌افزارها، برخی اوقات Backdoor یا اسب تروا[1] نامیده می‌شوند. کرم‌ها می‌توانند از راه‌های گوناگونی منتشر شوند. یک پیوند (لینک) روی یک سایت، به‌صورت عادی می‌تواند کرم یا فایل ضمیمه‌شده به یک ایمیل باشد که حاوی کدهای مخرب باشد. متد انتشاری که در این نوشته به آن پرداخته شده است، آلودگی از طریق شبکه است. این متد، آسیب‌پذیری شناخته‌شده‌ای را در نرم‌افزار شبکه برای تزریق کد مربوط به کرم مورد بررسی قرار می‌دهد (به مطلب ۵-۳-۲ مراجعه کنید [مطالعه موردی: کرم گرفته‌شده (شناسایی یک کرم)، صفحه ۷۰]).

۲-۲. تاریخچه هانی‌پات

مفهوم هانی‌پات‌ها برای اولین بار توسط کلیفورد استول[2] در سال ۱۹۹۰ مطرح شد [Stoll 90]. کتابی که وی نوشت، مطلب جدیدی بر مبنای گزارشی (داستانی) واقعی بود که برای کلیفورد استول پیش آمده بود. وی رایانه‌ای را یافت که هک شده بود و تصمیم گرفت نحوه دسترسی فرد متجاوز به سیستم را کشف کند. برای پیگیری هکر و رسیدن به نقطه منشا ورود، کلیفورد استول محیطی جعلی هدفمند که فعالیت حمله‌کننده را نگهداری می‌کرد، ایجاد نمود. ایده وی به شکلی بود که در طول زمانی که حمله‌کننده در داخل اسناد مهیاشده، جست‌وجو می‌کرد، اتصال را پیگیری می‌نمود. کلیفورد استول نام دامی که ابداع کرده بود را هانی‌پات نگذاشت؛ وی تنها شبکه‌ای همراه با اسناد جعلی برای رد گم کردن فردی که نفوذ کرده بود، ابداع نمود. سپس از ابزارهایی جهت نمایش دادن منشا و پیگیری هکرها و یافتن اینکه آنها چگونه وارد سیستم می‌شوند، استفاده نمود.

1. Trojan Horse
2. Clifford Stoll

در سال ۱۹۹۹میلادی این ایده دوباره به‌وسیله پروژه هانی‌نت انتخاب شد، که مؤسس آن، لانس اسپیتزنر بود. در طول سال‌های پیاپی که پروژه هانی‌نت توسعه داده می‌شد، مقالاتی در رابطه با هانی‌پات‌ها و معرفی تکنیک‌هایی برای ایجاد هانی‌پات‌های کارا و مؤثر، ارایه شد. پروژه هانی‌نت تحقیقی سازمانی بود که جهت به‌دست آوردن سود و منفعت مالی نبود و وقف امنیت اطلاعات گردید.

کتاب "هانی‌پات‌ها، ردیابی هکرها" [Spitzner 02] که توسط لانس اسپیتزنر نوشته شد، یک کار استاندارد بود که مفاهیم و معماری هانی‌پات‌ها در آن آمده است. این کتاب منبعی دارای صلاحیت کافی است که تعاریف، اصطلاحات و نمادگذاری‌های مربوط به هانی‌پات را ارایه می‌دهد.

متأسفانه اطلاعاتی در رابطه با اینکه چه فردی اصطلاح "هانی‌پات" را کشف کرده، موجود نیست. در کتاب اسپیتزنر برخی راه‌حل‌های اولیه برای هانی‌پات آمده، اما در هیچ‌کدام آنها از نام هانی‌پات استفاده نشده است.

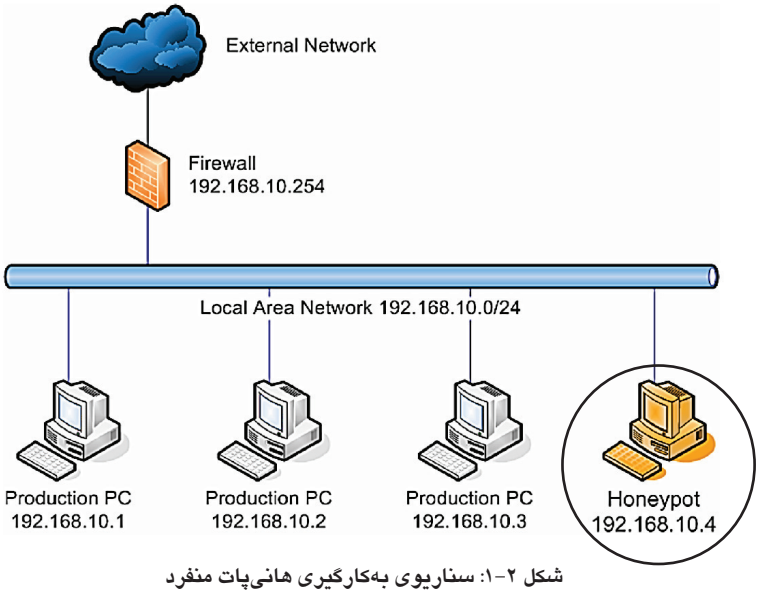
۲-۳. انواع هانی‌پات

جهت توصیف هانی‌پات‌ها با جزییات بیشتر، لازم است که انواع هانی‌پات‌ها را تعریف کنیم. همان‌طور که در ادامه مشاهده می‌کنید، نامی که برای نوع آنها انتخاب شده، هدف آنها را نیز بیان می‌کند، البته توصیف بسیار مناسب و کامل آنها را می‌توانید در منبع [Spitzner 02] مشاهده نمایید.

۲-۳-۱. ایده هانی‌پات

مفهوم هانی‌پات‌ها در حالت کلی، دریافت فعالیت‌های مخرب و مشکوک است که همراه با ماشینی آماده شده، ارایه می‌شود. این نوع رایانه تحت عنوان طعمه مورد استفاده قرار می‌گیرد. فردی که تصمیم دارد نفوذ کند، قصد دارد هانی‌پات را تشخیص داده و سعی در تخریب آن نماید. سپس نوع و هدف هانی‌پات، تعیین می‌کند که حمله‌کننده قادر به انجام چه اموری بوده است.

برخی اوقات هانی‌پات‌ها به‌صورت پیوسته (ترکیبی عطفی) با سیستم تشخیص نفوذ، ترکیب می‌شوند. در این حالت‌ها، هانی‌پات به‌عنوان هانی‌پات تولیدی (به مطلب ۲-۳-۲ [در صفحه ۱۶، تولید هانی‌پات] مراجعه کنید) به‌کار گرفته می‌شوند و تنها IDS را توسعه می‌دهند، اما در مفهوم هانی‌نت‌ها (به مطلب ۲-۳-٤ [در صفحه ۱۸، هانی‌نت‌ها] مراجعه کنید) هانی‌پات بخش عمده و حایز اهمیت است. در این حالت IDS جهت توسعه قابلیت‌های ثبت هانی‌پات‌ها نصب می‌شوند.



شکل ۲-۱: سناریوی به‌کارگیری هانی‌پات منفرد

آماده‌سازی متداول برای هانی‌پات، آرایش و به‌کارگیری در داخل سیستم تولیدی است. در شکل ۲-۱، هانی‌پات داخل دایره نمایش داده شده است. این هانی‌پات روی هیچ سروری یا دیگر سیستم‌های تولیدی ثبت و فعال نشده است. در این روش، هیچ فردی نباید درباره وجود هانی‌پات اطلاع داشته باشد. این مورد بسیار حایز اهمیت است، زیرا تنها داخل شبکه‌های پیکربندی شده وجود دارد. شخص می‌تواند فرض کند که هر بسته به هانی‌پات ارسال می‌شود و نیز می‌تواند در رابطه با حمله بدگمان باشد. درصورتی‌که بسته‌های پیکربندی‌نشده دریافت شوند، مقدار و تعداد اعلان‌های اشتباه افزایش یافته و مقدار هانی‌پات قطع شده و افت می‌کند.

۲-۳-۲. تولید هانی‌پات

به‌طورعمده هانی‌پات‌ها برای تشخیص و شناسایی به‌کار می‌روند (به مطلب ۲-۶-۲ [صفحه ۲۳، تشخیص] مراجعه کنید). هانی‌پات‌ها اغلب به‌عنوان سیستم تشخیص نفوذ برای انجام یک عملکرد (تابع) تشخیص پیشرفته، کار می‌کنند. درصورتی‌که توابع امنیتی آنها به اندازه کافی و به‌طور مناسب صورت پذیرد، آشکارسازی‌ها نیز راحت‌تر خواهد بود. اگر یک هانی‌پات مورد تجزیه‌وتحلیل یا مورد حمله قرار گیرد، مهاجم (حمله‌کننده[1]) باید راهی برای نفوذ به هانی‌پات بیابد. این راه می‌تواند راهی شناخته شده (راه‌هایی که هکرها آنها را می‌شناسند و در ابتدا سعی

1. Atacker

دارند آنها را مورد آزمایش قرار دهند) که بســتن و مســدود نمودن آن مشکل است و یا حفره‌های ناشناخته (حفره‌ای که به‌تازگی کشف شده و باید کنترل شود) باشد. با این وجود باید اقداماتی در جهت جلوگیری از نفوذ در برابر حملات واقعی صورت پذیرد. با کسب دانش و آگاهی در رابطه با هانی‌پات، تعیین و بستن حفره‌های امنیتی راحت‌تر و آسان‌تر خواهد بود.

ســرمایه‌گذاری روی هانی‌پات نسبت به دیواره آتش[1] توجیه‌پذیر است. در صورت عدم وجود هانی‌پات و وجود دیواره آتش، هیچ‌گونه شــواهدی مبنی بر حملات وجود نخواهد داشــت و در واقع فردی که عهده‌دار مدیریت شــبکه اســت، هیچ حمله‌ای را مشــاهده نخواهد کرد. از این‌رو آن فرد (به لحاظ اینکه متوجه هیچ‌گونه خطری نمی‌شود)، نیازی به سرمایه‌گذاری روی امنیت شبکه نخواهد دید. با وجود هانی‌پات روی شــبکه، مدارک و شــواهدی از حملات صورت‌گرفته موجود خواهد بود. این سیستم می‌تواند اطلاعات مربوط به آمار حملات جمع‌آوری‌شده در ماه را که رخ داده‌اند، ارایه کند.

حملاتی که ممکن است توسط کارمندان و کارکنان صورت پذیرد، حتی مهم‌تر هستند. به‌طور معمول به هر کارمند یک حساب روی شبکه همراه با دسترسی چند کاربر اختصاص داده می‌شود. در بســیاری از موارد، شبکه نسبت به شبکه خارجی (بیرون) بسته می‌باشد، اما در محدوده داخلی (شــبکه محلی[2]) باز است. بنابراین فردی که دارای دسترسی قانونی به شبکه داخلی است، می‌تواند یک تهدید غیرقابل شناسایی دربر داشته باشد. در هانی‌پات‌ها هرگونه فعالیت مشکوک ثبت و ضبط می‌گردد، البته درصورتی‌که فرد دارای نیت‌های مخرب باشد. به‌عنوان نمونه یک پوشه روی شبکه همراه با اسناد جعلی حساس می‌تواند مهیا شود. کارمند بدون هیچ‌گونه نیت بدی می‌تواند به فایل‌ها نگاه کند (درحالی‌که گمانه‌زنی در رابطه با کپی بودن آنها ندارد) و آنها را به‌عنوان یک خال ســیاه (هدف) ببیند.

یکــی از مزایای دیگر و یکی از مهم‌ترین دلایل، این اســت که هانی‌پات حملاتی را که توســط دیگــر سیســتم‌های امنیتــی شناســایی و ردیابی نمی‌شــوند را شناســایی و ردیابــی می‌کند. یک IDS (Intrusion Detecting System) بــه یــک پایگاه داده همراه با آپدیت حملات جدید شناخته‌شــده[3]، نیازمند است.

درصورتی‌که یک هکر کلاه‌ســیاه، آسیب‌پذیری ناشناخته‌ای بیابد، چه اتفاقی رخ می‌دهد؟ در بخش ۲-٦ توضیحات بیشتری در مورد اینکه یک هانی‌پات چگونه در تشخیص حملات می‌تواند به ما کمک کند، آمده است.

1. Firewall
2. Local Network
3. Signatures

۲-۳-۳. پژوهش در هانی‌پات

پژوهش، تحقیق و تفحص در هانی‌پات، در سناریوهای مختلفی مورد استفاده قرار می‌گیرد. پژوهش در هانی‌پات برای آموختن درباره تکنیک و تاکتیک‌های هکرهای کلاه‌سیاه، مورد استفاده قرار می‌گیرد و از آن به‌عنوان یک سازمان دیده‌بانی (پست دیده‌بانی) استفاده می‌شود تا ببینید که یک نفوذگر چگونه سیستم را به مخاطره می‌اندازد. در این رابطه، فرد مزاحم (نفوذگر) در سیستم می‌ماند و اسرار خود (اعم از نحوه نفوذ، IP خود و موارد دیگر) را فاش می‌کند.

اپراتور (کاربر سیستم) می‌تواند در مورد ابزارها و تاکتیک‌هایی که هکر کلاه‌سیاه به‌کار می‌برد، دانش کسب کند. هنگامی که امنیت یک سیستم به خطر می‌افتد، مدیران به‌طورمعمول سعی در یافتن ابزار مورد استفاده توسط مهاجم را دارند، اما هیچ‌گونه اطلاعاتی درباره تکنیک‌ها و ابزارهایی که استفاده کرده‌اند، وجود نخواهد داشت. هانی‌پات با دارا بودن بینشی[1] به جهان واقعی موجود روی شبکه، سعی دارد به چگونگی حمله به سیستم بپردازد و آن را مورد تجزیه و تحلیل قرار دهد.

۲-۳-۴. هانی‌نت‌ها

گسترش هانی‌پات‌ها باعث تولید مفهوم جدیدی به نام هانی‌نت می‌شود که شبکه‌ای حاوی هانی‌پات‌هاست. همان‌طور که در بخش ۲-۳-۱ بیان شد، استقرار هانی‌پات رده‌ای، هانی‌پاتی درونی در شبکه را تشکیل می‌دهد. در یک شبکه ممکن است بیش از یک هانی‌پات مستقر شود، اما با توجه به مفهوم فوق، راه‌حل‌های هریک از هانی‌پات‌ها به تنهایی جهت برخورد با حملات، چاره‌ساز است و به‌عنوان ماشینی منفرد با آن برخورد می‌شود.

برای برقراری یک هانی‌نت حداقل به دو دستگاه نیاز داریم؛ یک هانی‌پات و یک هانیوال[2] (دیواره عسلی!).

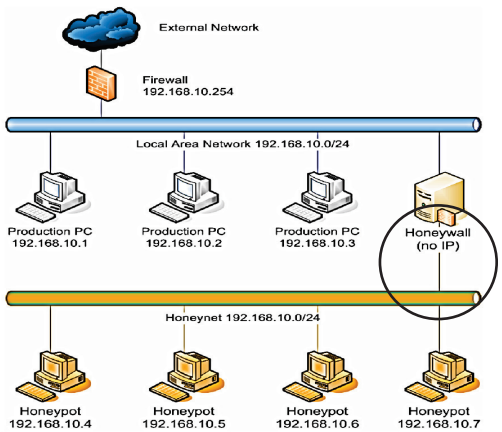
در این سناریو، مهاجم با هانی‌پاتی همراه با سیستم‌عامل واقعی مواجه می‌شود. این بدان معناست که وی می‌تواند به‌طور کامل به آن دسترسی داشته و آن را تکه و پاره[3] کرده و یا به آن آسیب برساند. از این طریق می‌تواند به راحتی به دیگر سیستم‌ها حمله کند و یا حمله‌ای به Denial-Of-Service انجام دهد. برای کاهش این ریسک، یک دیواره آتش در هانیوال پیکربندی می‌شود که اتصال‌های خروجی[4] شبکه را محدود می‌کند. به این طریق دسترسی به شبکه به‌طور کامل محدود شده است. همچنین هانیوال یک سیستم تشخیص نفوذ (IDS) به‌شمار می‌رود که روی بسته‌هایی که از هانی‌پات ارسال یا دریافت می‌شوند، نظارت می‌کند.

1. Insight
2. Honeywall
3. Mangle
4. Outbound Connections

در پروژه هانی‌نت دو نوع معماری هانی‌پات وجود دارد؛ Gen-I (یا نسل اول) و Gen-II (یا نسل دوم) [منبع Honeynet 04]. معماری نسل اول یا Gen-I اولین راه‌حل است و در آن امکان پنهان‌سازی خود (یعنی پنهان کردن وجود هانی‌پات) وجود ندارد. در این نوع از هانی‌پات، کشف اثر انگشت‌ها و موارد دیگر توسط کلاه‌سیاه‌های حرفه‌ای بسیار راحت است. علاوه بر این روی سیستم‌عامل هانی‌نت هیچ‌گونه حسگری وجود ندارد. این بدان معناست که ترافیک شبکه ثبت و ضبط می‌شود، اما اتفاق‌ها و رویدادها در سیستم میزبان به‌صورت مجزا، امنیت شبکه با هانی‌پات‌ها را کنترل نمی‌کند و نفوذگر[1] می‌تواند آنها را پاک کند و اثری از خود برجای نگذارد. دسترسی به هانی‌نت از طریق لایه سوم (layer-3) دیواره آتش مهیا می‌شود.

شبکه‌های نسل دوم یا Gen-II توسعه بیشتری پیدا کرده‌اند و تشخیص آنها بسیار سخت است. در این نوع شبکه‌ها، فعالیت‌ها در سمت میزبان (هاست) ثبت و ضبط می‌شوند و حتی درصورتی‌که نحوه اتصال مهاجم رمزگذاری[2] هم شده باشد، کلیدهای استفاده‌شده از صفحه‌کلید ثبت می‌شوند. در این نوع شبکه، مجوز دسترسی توسط لایه دوم دیواره آتش یا layer-2 مهیا می‌شود که شناسایی و دریافت اثر انگشت درحالی‌که آدرس IP نیز وجود ندارد، مشکل خواهد بود. شکل ۲-۲ نموداری شبکه‌ای از راه‌اندازی یک هانی‌نت همراه با چهار هانی‌پات را نشان می‌دهد.

هانیوال موجود در شکل داخل دایره به‌صورت bridge عمل می‌کند (لایه دوم شبکه [OSI 94]) که دارای تابعی یکسان با گزینه‌های اجراشده است. هانیوال، هانی‌نت را به‌طور منطقی به شبکه تولیدشده متصل می‌کند و اجازه می‌دهد در محدوده آدرس‌های یکسانی قرار گیرد.



شکل ۲-۲: پیاده‌سازی هانی‌نت

1. Intruder
2. Encrypt

۲-۴. سطوح تعاملی

در بخش‌های پیش، هانی‌پات‌ها توسط نقش خود در برنامه‌های کاربردی، توصیف و تشریح شدند. برای توصیف آنها با جزییات بیشتر، لازم است که سطوح تعاملی آنها را در مقابله با مهاجمان بیان کنیم.

۲-۴-۱. هانی‌پات‌های با تعامل پایین[1]

هانی‌پات با تعامل پایین سرویس‌های شبکه را تنها برای نقاطی که حمله‌کننده می‌تواند در آنها وارد شود، شبیه‌سازی می‌کند، اما عملیات خاصی انجام نمی‌دهد. در برخی موارد امکان دارد علامتی به مکان اولیه (منشا) ارسال شود، اما ادامه پیدا نخواهد کرد. هانی‌پات‌های با تعامل پایین تنها برای تشخیص و خدمت به هانی‌پات‌های تولیدی به‌کار گرفته می‌شوند.

در مقابل سیستم‌های IDS، هانی‌پات‌های با تعامل پایین، ورود به سیستم و حملات را تشخیص می‌دهند. علاوه بر این، در اینگونه هانی‌پات‌ها امکان پاسخ‌گویی به اقدام‌هایی که جهت ورود به سیستم انجام می‌پذیرد، وجود دارد درحالی‌که IDSها در اینگونه موارد منفعل باقی می‌مانند.

مهاجم (حمله‌کننده) تنها به سرویس شبیه‌سازی‌شده دسترسی پیدا خواهد کرد. به سیستم‌عاملی که در زیر سیستم قرار دارد، در هیچ حالتی دستیابی پیدا نخواهد شد. از این‌رو این محیط راه‌حلی بسیار امن خواهد بود که خطر بسیار کمی را برای محیطی که در آن نصب شده، دربر خواهد داشت.

۲-۴-۲. هانی‌پات‌های با تعامل میانی[2]

هانی‌پات‌های با تعامل میانی بیشتر از نوع پیشین برای شبیه‌سازی کامل سرویس‌ها یا آسیب‌پذیری‌های[3] خاص مستعد هستند. این بدان معناست که آنها می‌توانند رفتار سرور وب[4] IIS مایکروسافت را شبیه‌سازی کنند. هدف اصلی آنها تشخیص است و همچنین از آنها برای تولید هانی‌پات‌ها استفاده می‌شود.

درست مشابه هانی‌پات‌های با تعامل پایین، هانی‌پات‌های با تعامل میانی نیز به‌عنوان برنامه‌ای کاربردی روی سیستم‌عامل میزبان[5] نصب می‌شوند و در آنها تنها سرویس‌هایی که خاصیت Public (عمومی) دارند، شبیه‌سازی و ارایه می‌شود. اما سرویس‌های شبیه‌سازی‌شده در هانی‌پات‌های با تعامل میانی، قدرتمندتر هستند، بنابراین شانس گسیختگی یا شکست (مهاجم) بیشتر خواهد بود که استفاده از هانی‌پات‌های با تعامل میانی را با ریسک بالاتری همراه می‌کند.

1. Low interaction
2. Medium interaction
3. Vulnerabilities
4. Web Server
5. Host