بسم الله الرحمن الرحیم

جلوگیری از حملات بوسیله سیستم های تشخیص نفوذ و هانی پات ها

نویسندگان:

مهندس عباس مسلمانی

دکتر محبوبه شمسی

(عضو هیئت علمی دانشگاه صنعتی قم)

ویراستار

آتوسا مهران فر

انتشارات علمی و فرهنگی پزشکی اهواز

زمستان ۹۵

سرشناسه : مسلمانی، عباس، ۱۳٦٤ -
عنوان و نام پدیدآور : جلوگیری از حملات بوسیله سیستم‌های تشخیص نفوذ و هانی‌پات‌ها/نویسندگان عباس مسلمانی، محبوبه شمسی؛ ویراستار آتوسا مهران‌فر.
مشخصات نشر : اهواز : انتشارات علوم و فنون پزشکی اهواز، ۱۳۹۵.
مشخصات ظاهری : ۱۳۸ ص.
شابک : 978-600-7937-88-4
وضعیت فهرست نویسی : فیپا
یادداشت : کتابنامه : ص.۱۰۷.
موضوع : نرم‌افزار بدافزار
موضوع : Malware (Computer software)
موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع : Computer networks -- Security measures
موضوع : ویروس‌های کامپیوتر
موضوع : Computer virus
شناسه افزوده : [illegible]، محبوبه، ۱۳۵۷-
شناسه افزوده : [illegible]، آتوسا، ۱۳۶۰-، ویراستار
رده بندی کنگره : [illegible]TK
رده بندی دیویی : ۰۰۵/۸
شماره کتابشناسی ملی : ٤٤٩١٠٦٧

نویسندگان: مهندس عباس مسلمانی، دکتر محبوبه شمسی
انتشارات: علوم و فنون پزشکی اهواز
ویراستار: مهندس آتوسا مهران فر
قیمت: ۲۵۰۰۰ تومان
نوبت چاپ: اول ۱۳۹۵
تیراژ: ۱۰۰۰ نسخه
آدرس انتشارات: اهواز-امانیه- خیابان سقراط غربی جنب مجتمع تصادفات دادگستری- کوچه خاکسار- پلاک ۱۲۰

اخطار!

تلفن تماس: ۳۳۳۳۳۸۶۵-۳۳۳۶۲۸۹۳-۰۶۱
دورنگار: ۳۳۳۶۴۵۶۸-۰۶۱
نشانی اینترنتی: www.parsinbook.ir
پست الکترونیکی: olomofonon.pezeshki@gmail.com

مقدمه

یکی از کلیدی‌ترین مفاهیم دنیای فناوری اطلاعات، موضوع امنیت اطلاعات است. امنیت اطلاعات شامل مباحث مختلف محرمانگی، جامعیت و دسترسی به منابع می‌باشد. درحالی‌که به کمک الگوریتم‌های پیشرفته می‌توان محرمانگی و جامعیت اطلاعات را تضمین نمود، دسترسی به اطلاعات همواره در معرض چالش‌های متعددی قرار دارند. از قطع سرویس به دلیل خرابی سخت‌افزار شبکه تا ازدحام درخواست‌ها، دلایل متعددی را می‌توان یافت که سبب قطع شدن دسترسی به اطلاعات گردند. قطع سرویس به هر دلیلی که باشد، در شرکت‌ها و سازمان‌های بزرگ می‌تواند هزینه‌های سنگین چند هزار دلاری تا چند میلیون دلاری را برای این شرکت‌ها و سازمان‌ها در پی داشته باشد.

حملات انکار سرویس یا انکار سرویس نوعی حمله می‌باشند که هدف آن، از کار انداختن سیستم هدف با هدر دادن منابع آن است. این حمله به‌گونه‌ای منابع سیستم را مورد تهدید قرار می‌دهد که سرویس‌دهنده قادر به پاسخگویی به کاربران قانونی خود نمی‌باشد. در واقع یک حمله انکار سرویس شمار زیادی از اتصالات ورودی را درون سرور تولید نموده و باعث مصرف میزان زیادی از پهنای باند شبکه، تحمیل بار اضافی به شبکه، از کار انداختن سرویس‌های حیاتی سیستم و هدر دادن منابع سیستم می‌شود . به‌عنوان‌مثال حملات Smurf از روش Spoofing یا جعل آدرس مبدأ استفاده می‌کنند و همچنین حملات UDP Flood که مبتنی بر پروتکل UDP می‌باشند و حملاتی با نام SYN Flood که مبتنی بر پروتکل TCP می‌باشند ، به‌عنوان شایع‌ترین نوع از حملات انکار سرویس بشمار می‌روند.

تشخیص نفوذ عبارت است از تحلیل بی‌درنگ داده‌های شبکه به منظور تشخیص و ثبت و اخطار به هنگام بروز حملات و یا اقدامات مخرب امنیتی.در عمل انواع مختلفی از روش‌های تشخیص حمله وجود دارد که با توجه با انواع مختلف اقدامات درون شبکه قادر هستند اقدامات مخرب و نفوذی را کشف کنند.در عین این سیستم‌ها از بخش‌های مختلفی تشکیل شده‌اند و به طرق مختلفی این اجزا می‌توانند در کنار هم قرار گیرنده عملکرد خاصی را ایجاد کنند. سیستم‌های تشخیص نفوذ به‌عنوان یکی از راه‌کارهای برقراری امنیت در شبکه‌های کامپیوتری مورداستفاده قرار می‌گیرند. به‌عبارت‌دیگر این سیستم‌ها یکی از فناوری‌های مورداستفاده برای برقراری امنیت هستند و از گذشته سیستم‌های دیگری به‌صورت مکمل در کنار این سیستم‌ها برای برقراری امنیت استفاده می‌شدند که هرکدام جایگاه خاصی در برقراری امنیت دارند.

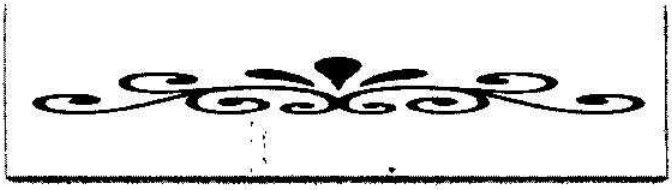
فناوری هانی پات یک تکنولوژی تقریباً جدید و شدیداً پویا می‌باشد. همین ماهیت پویا باعث می‌شود که به‌راحتی نتوان آن‌ها را تعریف کرد هانی پات ها به‌خودی‌خود یک راه‌حل به شمار نرفته و هیچ مشکل امنیتی خاصی را حل نمی‌کنند، بلکه ابزارهای بسیار انعطاف‌پذیری هستند که کارهای مختلفی

برای امنیت اطلاعات انجام می‌دهند.این تکنولوژی با فنّاوری‌هایی مانند فایروال‌ها و سیستم‌های تشخیص نفوذ متفاوت است، چراکه این فنّاوری‌ها مسائل امنیتی خاصی را حل کرده و به همین دلیل راحت‌تر تعریف می‌شوند. فایروال‌ها یک تکنولوژی پیشگیرانه به شمار می‌آیند، آن‌ها از ورود مهاجمان به شبکه یا سیستم کامپیوتر جلوگیری می‌کنند سیستم‌های تشخیص نفوذها یک تکنولوژی تشخیصی هستند. هدف آن‌ها این است که فعالیت‌های غیرمجاز یا خرابکارانه را شناسایی کرده و درباره آن‌ها به متخصصان امنیت هشدار دهند. تعریف هانی پات‌ها کار سخت‌تری است، چراکه آن‌ها ممکن است در پیشگیری، تشخیص، جمع‌آوری اطلاعات، و کارهای دیگری مورداستفاده قرار گیرند. شاید بتوان یک هانی پات را به این صورت تعریف کرد: هانی پات یک سیستم اطلاعاتی است که ارزش آن به استفاده غیرمجاز و ممنوع دیگران از آن است.

با توجه به جایگاه هانی پات در تشخیص زودهنگام حملات، در این کتاب ابتدا یک ارزیابی و پیشنهاد برای محل قرارگرفتن سرویس‌دهنده هانی پات ارائه شد. این پیشنهاد مشتمل بر قرار گرفتن هانی پات در نزدیک‌ترین بخش به شبکه به‌منظور تسهیل روئیت آن توسط مهاجمان احتمالی و جذب راحت‌تر آن‌ها به سمت هانی پات، می‌باشد. برخلاف تصور رایج، قرار گرفتن هانی پات در مسیر ترافیک‌های عمومی و در پشت فایروال‌ها، به دلیل تفکیک ترافیک و کاهش قابلیت مشاهده آن توسط مهاجمان، مطلوب نمی‌باشد.

ازآنجاکه هانی پات باید به شکلی رفتار کند که از یک‌سو کمترین فشار محاسباتی برای تشخیص حملات را به سرویس‌دهنده وارد بنماید و از سوی دیگر باید در مسیر تشخیص سرعت عمل به خرج دهد، برخلاف روش‌های پیچیده رایج تشخیص حملات مبتنی بر سرویس در سیستم‌های اجتناب از نفوذ در این کتاب از روش درختان تصمیم‌گیری استفاده شده است. درختان تصمیم‌گیری علاوه بر قابلیت کشف مناسب، ازنظر پیاده‌سازی نیز بسیار سبک هستند.

همچنین به‌منظور تسهیل بیش‌ازپیش فرآیند ایجاد و تصمیم‌گیری درختان تصمیم‌گیری، قبل از اقدام برای ساخت درختان، یک مرحله تفکیک ویژگی‌های در دسترس و مبتنی‌بر ویژگی‌های مطلوب و ویژگی‌های نامطلوب و افزونه، برروی مجموعه داده‌های آموزش پیشنهاد شده است. به‌این‌ترتیب هزینه ساخت درختان (از نظر زمان و مقدار حافظه موردنیاز) کاهش چشمگیری پیدا خواهد نمود.



فهرست مطالب