

بسم الله الرحمن الرحيم

**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



استاد ارشد علمی و فن پژوهشگر

ژانویه ۱۵۰۰

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 دلار تا چند میلیون دلار 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 بر ارزش 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. به‌عنوان مثال حملات Smurf از روش Spoofing یا جعل آدرس مبدأ استفاده می‌کنند و همچنین حملات UDP Flood 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 شده به‌طور تشخیص و ثبت و اخطار به هنگام بروز حملات و یا اقدامات مخرب امنیتی. در عمل انواع تشخیصی از روش‌های تشخیص حمله وجود دارد که با توجه با انواع مختلف اقدامات درون شبکه قادر به تشخیص اقدامات مخرب و نفوذی را کشف کنند. در عین این سیستم‌ها از بخش‌های مختلفی تشکیل شده‌اند و به‌طریق 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 مورد استفاده قرار می‌گیرند. به‌عبارت دیگر این سیستم‌ها یکی از فناوری‌های مورد استفاده 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.

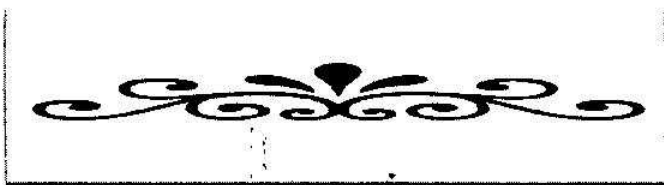
فناوری‌های پات یک تکنولوژی تقریباً جدید و شدیداً پویا می‌باشد. همین ماهیت پویا باعث می‌شود که به‌راحتی نتوان آن‌ها را تعریف کرد. هانی پات‌ها به‌خودی‌خود یک راه‌حل به شمار نرفته و هیچ مشکل امنیتی خاصی را حل نمی‌کنند، بلکه ابزارهای بسیار انعطاف‌پذیری هستند که کارهای مختلفی

برای امنیت اطلاعات انجام می‌دهند. این تکنولوژی با فناوری‌هایی مانند فایروال‌ها و سیستم‌های تشخیص نفوذ متفاوت است، چراکه این فناوری‌ها 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 هانی‌پات‌ها کار سخت‌تری است، چراکه آن‌ها ممکن است در پیشگیری، تشخیص، جمع‌آوری اطلاعات، و کارهای دیگری مورد استفاده 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 متنوع دیگران از آن است.

با توجه به جایگاه هانی پات در تشخیص زودهنگام حملات، در این کتاب ابتدا یک ارزیابی و پیشنهاد برای محل قرار گرفتن سوبس‌دهنده هانی پات ارائه شد. این پیشنهاد مشتمل بر قرار گرفتن هانی پات در نزدیک‌ترین بخش به شبکه به منظور تسهیل رویت 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 دریاچه، به دلیل تفکیک ترافیک و کاهش قابلیت مشاهده آن توسط مهاجمان، مطلوب نمی‌باشد.

از آنجاکه هانی پات باید به شکلی رفتار کند که از یک سو 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، کار سرویس در سیستم‌های اجتناب از نفوذ در این کتاب از روش درختان تصمیم‌گیری استفاده شده است. درختان تصمیم‌گیری علاوه بر قابلیت کشف مناسب، از نظر پیاده‌سازی نیز بسیار سبک هستند.

همچنین به منظور تسهیل بیش‌ازپیش فرآیند ایجاد و تصمیم‌گیری درختان تصمیم‌گیری، قبل از اقد برای ساخت درختان، یک مرحله تفکیک ویژگی‌های در دسترس و ارزیابی ویژگی‌های مطلوب و ویژگی‌های نامطلوب و افزونه، بر روی مجموعه داده‌های آموزش پیشنهاد شده است. به این ترتیب هزینه ساخت درختان (از نظر زمان و مقدار حافظه مورد نیاز) کاهش چشمگیری پیدا خواهد نمود.



فهرست مطالب

فصل ۱: مروری بر افزارها.....	۱۳
۱-۱- سیر تکاملی پیروسیهای رایانه‌ای.....	۱۴
۱-۲- بدافزار چیست؟.....	۱۵
۱-۳- کرم.....	۱۶
۱-۴- ویروس.....	۱۷
۱-۵- تروجان.....	۱۹
۱-۶- تروجان دسترسی از راه دور.....	۱۹
۱-۷- روتکیت.....	۲۰
۱-۸- حملات DOS.....	۲۰
۱-۹- بررسی بسته‌های TCP و چگونگی برقراری ارتباط تحت پروتکل TCP/IP.....	۲۱
۱-۹-۱- بررسی اجزای داخل یک بسته TCP.....	۲۱
۱-۹-۲- بررسی عملکرد پروتکل TCP.....	۲۱
۱-۱۰- بررسی برخی از انواع حملات DOS.....	۲۲
۱-۱۰-۱- حمله Smurf.....	۲۲
۱-۱۰-۲- حمله UDP Flood.....	۲۳
۱-۱۰-۳- حمله SYN Flood.....	۲۳
۱-۱۱- حملات DDOS.....	۲۴
۱-۱۱-۱- انواع حملات DDOS.....	۲۵
۱-۱۱-۲- حملات Trinoo.....	۲۵
۱-۱۱-۳- حملات TFN/TFN2K.....	۲۷
۱-۱۲- حملات Stacheldraht.....	۲۸

۲۹	فصل دوم مروری بر سیستم های تشخیص نفوذ
۳۰	۱-۱۳- مروری بر سیستمهای تشخیص نفوذ
۳۰	۱-۱۴- انواع حملات شبکه
۳۰	۱-۱۴-۱- انواع حملات شبکههای با توجه به طریقه حمله
۳۲	۱-۱۴-۲- انواع حملات شبکههای با توجه به حمله کننده
۳۲	۱-۱۵- مکملهای سیستمهای تشخیص نفوذ در برقراری امنیت
۳۳	۱-۱۵-۱- دیواره آتش
۳۴	۱-۱۶- ساروکارهای رمزنگاری و تأیید هویت
۳۵	۱-۱۶-۱- سیستمهای کنترل دسترسی
۳۵	۱-۱۷- انواع سیستمهای تشخیص نفوذ
۳۵	۱-۱۷-۱- سیستمهای تشخیص نفوذ مبتنی بر میزبان
۳۷	۱-۱۷-۲- سیستمهای تشخیص نفوذ مبتنی بر شبکه
۳۷	۱-۱۷-۳- اجزای تشکیل دهنده سیستمهای تشخیص نفوذ مبتنی بر شبکه
۳۸	۱-۱۸- معماری شبکههای و جایگزینی - سگرها
۳۸	۱-۱۸-۱- حالت بر خط
۴۰	۱-۱۸-۲- سیستمهای توزیع شده
۴۴	۱-۱۸-۳- روشهای مبتنی بر امضا
۴۵	۱-۱۸-۴- روشهای تشخیص حمله مبتنی بر ناهنجاری
۴۸	۱-۱۸-۵- روشهای مبتنی بر تحلیل حالت پروتکل ارتباطی
۵۰	۱-۱۹- تکنولوژیهای سیستمهای تشخیص نفوذ
۵۰	۱-۱۹-۱- اجزای سامانههای تشخیص نفوذ
۵۱	۱-۱۹-۲- ساختار و همبندی اجزای سیستم تشخیص نفوذ
۵۱	۱-۱۹-۳- عملکرد امنیتی سیستمهای تشخیص نفوذ
۵۴	۱-۱۹-۴- قابلیتهای مدیریتی ابزارهای تشخیص نفوذ
۵۸	۱-۱۹-۵- ویژگیهای ابزار تشخیص نفوذ ایدئال
۵۹	۱-۱۹-۶- دقت بالا، نرخ تشخیص بالا و کم بودن هشدارهای نادرست
۵۹	۱-۱۹-۷- نحوه واکنش و ایجاد هشدار و کار با IDSهای دیگر
۶۰	۱-۱۹-۸- قابلیتهای پیکربندی و تنظیمات فاز نصب و سازگاری با شرایط سیستم
۶۱	۱-۱۹-۹- امکان اعمال سیاست امنیتی در نسخه امنیتی یا با استفاده از قوانین کارآمد

- ۱۹-۱۰- مقیاس پذیری و توزیع پذیری ۶۱
- ۱۹-۱۱- اجرای مداوم و تحمل پذیری خطا ۶۲
- ۱۹-۱۲- قابلیت تشخیص حملات دیده نشده ۶۲
- ۱۹-۱۳- بهرهوری و عملکرد مناسب ۶۲
- ۱۹-۱۴- کار با حداقل سربار و امکان بررسی عملکرد و بهرهوری ابزار تشخیص نفوذ ۶۴

فصل سوم: چرا هانی پات ها ۶۵

- ۲۰-۱- چرا هانی پات ها امنیت شبکه را بهبود می بخشد؟ ۶۶
- ۲۱-۱- مفاهیم، معماری و اصطلاحات مربوط به هانی پات ۶۷
- ۲۲-۱- کلاه سیاه ها و کلاه سفیدها ۶۷
- ۲۳-۱- تاریخچه هانی پات ۶۸
- ۲۴-۱- انواع هانی پات ۶۹
- ۲۵-۱- تولید هانی پات ۷۰
- ۲۶-۱- پژوهش در هانی پات ۷۲
- ۲۷-۱- هانی نت ها ۷۲
- ۲۸-۱- سطوح تعاملی ۷۴
- ۲۸-۱-۱- هانی پات های با تعامل پایین ۷۴
- ۲۸-۲-۱- هانی پات های با تعامل میانی ۷۵
- ۲۸-۳-۱- هانی پات های با تعامل بالا ۷۵
- ۲۹-۱- حملات مستقیم ۷۶
- ۳۰-۱- مقولات امنیتی ۷۷
- ۳۱-۱- پیشگیری ۷۷
- ۳۲-۱- تشخیص ۷۸
- ۳۳-۱- پاسخ (واکنش) ۷۹
- ۳۴-۱- آدرس های IP مخفی ۷۹
- ۳۵-۱- Backscatter ها ۸۰

فصل چهارم: هانی پاتها در حوزه کاربردی ۸۱

- ۳۶-۱- سناریوی اول- محیط حفاظت نشده ۸۲
- ۳۷-۱- سناریوی دوم- محیط های حفاظت شده ۸۳
- ۳۸-۱- سناریوی سوم- آدرس های عمومی ۸۴

۸۶	۳۹-۱- سناریوی چهارم- آدرس خصوصی
۸۷	۴۰-۱- سناریوی پنجم- ارزیابی ریسک
۸۸	۴۱-۱- سناریوی ششم- هانی پات ها خارج از Box
۹۳	۴۲-۱- سناریوی هفتم- دانش - آموزش
۹۵	فصل پنجم: روش اجرای تحقیق
۹۷	۴۳-۱- مقدمه
۹۷	۴۴-۱- طرح کلی روش پیشنهادی
۹۹	۴۵-۱- تعیین محل هانی پات در شبکه
۱۰۲	۴۶-۱- انتخاب ویژگیهای مطلوب
۱۰۴	۴۷-۱- درخت تصمیم گیری
۱۰۴	۴۷-۱- مزایا و معایب درختان تصمیم گیری
۱۰۶	۴۷-۲- ایجاد یک درخت تصمیم گیری
۱۰۸	۴۷-۳- چالش صرف حافظه و توان پردازشی درختان تصمیم گیری
۱۱۰	۴۸-۱- نتیجه گیری
۱۰۹	فصل ششم: تجزیه و تحلیل یافته ها
۱۱۲	۴۹-۱- مقدمه
۱۱۲	۵۰-۱- مشخصات مجموعه داده مورد استفاده در ارزیابی
۱۱۴	۵۱-۱- انتخاب محل نصب سرویس دهنده هانی پات و تکنیک ترافیک آن در مجموعه داده
۱۱۶	۵۲-۱- انتخاب ویژگیهای مطلوب در مجموعه داده
۱۱۸	۵۳-۱- ایجاد درختان تصمیم گیری
۱۲۳	۵۴-۱- ارزیابی مقدار دقت درختان مختلف
۱۲۸	۵۵-۱- نتیجه گیری
۱۲۷	فصل هفتم: بحث و نتیجه گیری
۱۳۰	۵۶-۱- جمع بندی و نتیجه گیری
۱۳۲	۵۷-۱- کارهای آتی پیشنهادی
۱۳۱	مراجع