امنیت شبکه لایه بندی شده (قسمت دوم)

گردآوری شده توسط جامعه گیک‌های کامپیوتر

در این . به اولین لایه که لایه پیرامون است، اشاره شدقسمت قبلیدر قسمت به لایه امنیت شبکه می‌پردازیم.

امنیت شبکه :سطح دو

امنیت شبکه

داخلی شما **LAN**و **WAN**سطح شبکه در مدل امنیت لایه بندی شده به شبکه داخلی شما ممکن است شامل چند کامپیوتر و سرور و یا .اشاره دارد شاید پیچیده‌تر یعنی شامل اتصالات نقطه به نقطه به دفترهای کار دور باشد. بیشتر شبکه‌های امروزی در ورای پیرامون، باز هستند؛ یعنی هنگامی که داخل این قضیه به .شبکه قرار دارید، می‌توانید به راحتی در میان شبکه حرکت کنید خصوص برای سازمان‌های کوچک تا متوسط صدق می‌کند که به این ترتیب این شبکه‌ها برای هکرها و افراد بداندیش دیگر به اهدافی وسوسه انگیز مبدل تکنولوژی‌های ذیل امنیت را درسطح شبکه برقرار می‌کنند .می‌شوند:

سیستم های جلوگیری) IPS - (سیستم های تشخیص نفوذ) IDS (از نفوذ

ترافیک گذرنده در شبکه شما را با جزییات بیشتر **IPS**و **IDS**تکنولوژی‌های مشابه سیستم‌های آنتی ویروس، ابزارهای .نسبت به فایروال تحلیل می‌کنند ترافیک را تحلیل و هر بسته اطلاعات را با پایگاه داده‌ای از IPSو IDS هنگامی که حملات تشخیص .مشخصات حملات شناخته شده مقایسه می‌کنند را ITمسؤولین IDSابزارهای .داده می‌شوند، این ابزار وارد عمل می‌شوند یک گام جلوتر می‌روند و به IPSاز وقوع یک حمله مطلع می‌سازند؛ ابزارهای صورت خودکار ترافیک آسیب رسان را مسدود می‌کنند.

ها درIPSدر حقیقت، بیشتر .ها مشخصات مشترک زیادی دارندIPSها و IDS تفاوت کلیدی بین این تکنولوژی‌ها از نام آن‌ها .دارند IDSهسته خود یک

تنها ترافیک آسیب رسان را تشخیص IDSامحصولات د. استنباط می‌شو از ورود چنین ترافیکی به شبکه شما IPSامی‌دهند، در حالیکه محصولات جلوگیری می‌کنند.

لایه های امنیت شبکه

مدیریت آسیب پذیری

سیستم‌های مدیریت آسیب پذیری دو عملکرد مرتبط را انجام می‌دهند:

1. شبکه را برای آسیب پذیری‌ها پیمایش می‌کنند.
2. روند مرمت آسیب پذیری یافته شده را مدیریت می‌کنند.

اما این .در گذشته، این تکنولوژی تخمین آسیب پذیری نامیده می‌شد تکنولوژی اصلاح شده است، تا جایی که بیشتر سیستم‌های موجود، عملی سیستم‌های .بیش از تخمین آسیب پذیری ابزار شبکه را انجام می‌دهند مدیریت آسیب پذیری ابزار موجود در شبکه را برای یافتن رخنه‌ها و آسیب پذیری‌هایی که می‌توانند توسط هکرها و ترافیک آسیب رسان مورد بهره آن‌ها معمولاً پایگاه داده‌ای از قوانینی را .برداری قرار گیرند، پیمایش می‌کنند نگهداری می‌کنند که آسیب پذیری‌های شناخته شده برای گستره‌ای از ابزارها .و برنامه‌های شبکه را مشخص می‌کنند

در طول یک پیمایش، سیستم هر ابزار یا برنامه‌ای را با به کارگیری قوانین همچنان که از نامش برمی‌آید، سیستم مدیریت آسیب .مناسب می‌آزماید لازم به .پذیری شامل ویژگی‌هایی است که روند بازسازی را مدیریت می‌کند ذکر است که میزان و توانایی این ویژگی‌ها در میان محصولات مختلف، فرق .می‌کند

> ***تکنولوژی Shielded Virtual Machines چیست؟ datacenter security***

تابعیت امنیتی کاربر انتهایی

روش‌های تابعیت امنیتی کاربر انتهایی به این طریق از شبکه محافظت می‌کنند که تضمین می‌کنند کاربران انتهایی استانداردهای امنیتی تعریف شده این .را قبل از اینکه اجازه دسترسی به شبکه داشته باشند، رعایت کرده‌اند عمل جلوی حمله به شبکه از داخل خود شبکه را از طریق سیستم‌های ناامن

روش‌های امنیت نقاط انتهایی .می‌گیرد RASو VPNکارمندان و ابزارهای براساس آزمایش‌هایی که روی سیستم‌هایی که قصد اتصال دارند انجام هدف آن‌ها از این تست‌ها معمولا .می‌دهند، اجازه دسترسی می‌دهند:

1. برای بررسی نرم افزار مورد نیاز، مانند سرویس پک‌ها، آنتی ویروس‌های ...به روز شده و
2. کاربردهای ممنوع مانند اشتراک فایل و نرم افزارهای جاسوسی است.

امنیت در شبکه

تأیید هویت -کنترل دسترسی

کنترل دسترسی نیازمند تأیید هویت کاربرانی است که به شبکه شما هم کاربران و هم ابزارها باید با ابزار کنترل دسترسی در .دسترسی دارند سطح شبکه کنترل شوند.

کنترل دسترسی شبکه

> ***در این سلسله مباحث، به کنترل دسترسی و تأیید هویت در سطوح شبکه، میزبان، نرم افزار و دیتا در میان .چارچوب امنیتی لایه بندی شده می‌پردازیم طرح‌های کنترل دسترسی بین لایه‌های مختلف معمولاً .همپوشانی قابل توجهی وجود دارد تراکنش‌های تأیید هویت در مقابل دید کاربر اتفاق اما به خاطر داشته باشید که کنترل .میفتد دسترسی و تأیید هویت مراحل پیچیده‌ای هستند که برای ایجاد بیشترین میزان امنیت در شبکه، باید به .دقت مدیریت شوند***

مزایا و معایب

و مدیریت آسیب پذیری تحلیل‌های پیچیده‌ای روی IPS، IDSتکنولوژی‌های در حالی که فایروال به .تهدیدها و آسیب پذیری‌های شبکه انجام می‌دهند تجزیه و IDSو IPSترافیک، برپایه مقصد نهایی آن اجازه عبور می‌دهد، ابزار تحلیل عمیق تری را برعهده دارند، بنابراین سطح بالاتری از محافظت را ارایه با این تکنولوژی‌های پیشرفته، حملاتی که داخل ترافیک قانونی شبکه .می‌دهند

وجود دارند و می‌توانند از فایروال عبور کنند، مشخص خواهند شد و قبل از آسیب رسانی به آن‌ها خاتمه داده خواهند شد.

سیستم‌های مدیریت آسیب پذیری روند بررسی آسیب پذیری‌های شبکه شما را به صورت خودکار استخراج می‌کنند. انجام چنین بررسی‌هایی به صورت دستی با تناوب مورد نیاز برای تضمین امنیت، تا حدود زیادی غیرعملی خواهد بود. به علاوه، شبکه ساختار پویایی دارد و ابزار جدید، ارتقا دادن نرم افزارها و وصله‌ها، و افزودن و کاستن از کاربران، همگی می‌توانند آسیب پذیری‌های جدید را پدید آورند. ابزار تخمین آسیب پذیری به شما اجازه می‌دهند که شبکه را مرتب و کامل برای جستجوی آسیب پذیری‌های جدید پیمایش کنید.

روش‌های تابعیت امنیتی کاربر انتهایی به سازمان‌ها سطح بالایی از کنترل بر روی ابزاری را می‌دهد که به صورت سنتی کنترل کمی بر روی آن‌ها وجود داشته است. هکرها به صورت روز افزون به دنبال بهره برداری از نقاط انتهایی برای داخل شدن به شبکه هستند، پدیده‌های اخیر چون Mydoom، برنامه‌های امنیتی کاربران. گواهی بر این ادعا هستند Sobigو Sasser انتهایی، این درهای پشتی خطرناک به شبکه را می‌بندند.

آسیب های شبکه

تمایل به تولید تعداد زیادی علایم هشدار غلط دارند، که به عنوان هاIDS ممکن است که یک IDSدر حالیکه. شوندنیز شناخته می false positives حمله را کشف و به اطلاع شما برساند، این اطلاعات می‌تواند زیر انبوهی از هشدارهای غلط یا دیتای کم ارزش مدفون شود. ممکن است به IDSمدیران سرعت حساسیت خود را نسبت به اطلاعات تولید شده توسط سیستم از باید بصورت پیوسته بررسی شود IDSابرای تأثیرگذاری بالا، یک. دست بدهند و برای الگوهای مورد استفاده و آسیب پذیری‌های کشف شده در محیط شما تنظیم گردد.

سطح. چنین نگهداری معمولاً میزان بالایی از منابع اجرایی را مصرف می‌کند ها می‌تواند به میزان زیادی در میان محصولات، متفاوتIPSخودکار بودن در بسیاری از آن‌ها باید با دقت پیکربندی و مدیریت شوند تا مشخصات باشد. تأثیرات. الگوهای ترافیک شبکه‌ای را که در آن نصب شده‌اند منعکس کنند جانبی احتمالی در سیستم‌هایی که بهینه نشده‌اند، مسدود کردن تقاضای کاربران قانونی و قفل کردن منابع شبکه معتبر را شامل می‌شود.

بسیاری از روش‌های امنیتی کاربران انتهایی، نیاز به نصب یک عامل در هر این عمل می‌تواند مقدار قابل توجهی بار کاری اجرایی به. نقطه انتهایی دارد نصب و نگهداری اضافه کند تکنولوژی‌های کنترل دسترسی ممکن است برای مثال، بعضی ممکن است با تمام ابزار. محدودیت‌های فنی داشته باشند موجود در شبکه شما کار نکنند، بنابراین ممکن است به چند سیستم برای همچنین، چندین فروشنده سیستم‌های کنترل. ایجاد پوشش نیاز داشته باشید

دسترسی را به بازار عرضه می‌کنند و عملکرد می‌تواند بین محصولات مختلف متفاوت باشد.

چنین .پیاده سازی یک سیستم یکپارچه در یک شبکه ممکن است دشوار باشد عمل نامنظم و از هم گسسته ای، به عبارت دیگر رویکرد چند محصولی ممکن است در واقع آسیب پذیری‌های بیشتری را در شبکه شما به وجود آورد .

نویسنده: ریحانه غفوریان