

معرفی محصول

محصول مدیریت آسیب پذیری شبکه با استفاده از اسکنر مستمر شبکه از منظر آسیب پذیری و جستجوی دارایی/سرویس/تجهیز را می‌توان به عنوان یک مدل ارزیابی مداوم شبکه دانست که عملیات جمع آوری، تست و ارزیابی پیوسته را به صورت خودکار در شبکه اعمال می‌نماید. سامانه قادر به جمع آوری اطلاعات از بخش‌های مختلف شبکه بوده و میتواند از زوایای مختلف پویش شبکه را انجام دهد که این امر با استفاده از سنسورهای سامانه در کلیه نقاط شبکه با دسترسی‌های گوناگون امکان پذیر می‌گردد. با فراهم آوردن داشبورد مرکزی برای کلیه سنسورهای مستقر در شبکه، کلیه اطلاعات مورد نیاز در داشبورد مرکزی ارائه می‌شود.

خدمات محصول

پس از پیاده‌سازی سامانه در سازمان، خدمات زیر توسط سامانه قابل ارائه می‌باشد:

- کشف آسیب‌پذیری‌های انواع دارایی‌ها شامل سوئیچ‌ها، فایرووال‌ها، سیستم عامل‌ها، مجازی‌سازی، نرم‌افزارها و درایورها و پیکربندی بندی ناصحیح به صورت مستمر
- ارائه گزارشات دقیق و مدیریتی از آسیب‌پذیرهای کشف شده
- پویش زمانبندی شده و خودکار آسیب‌پذیری‌های شبکه
- امکان نصب چندین سنسور و نمایش مرکز خروجی‌ها از طریق کنسول مرکزی
- شناسایی و تفکیک آسیب‌پذیری‌ها بر اساس نوع و اهمیت متناسب با هر دارایی
- بروزرسانی سامانه به صورت آفلاین
- ارائه راهکار در خصوص رفع و یا کاهش مخاطرات آسیب‌پذیری‌های کشف شده
- ارائه توضیح به تفکیک هر آسیب‌پذیری کشف شده
- ارائه تاریخ انتشار آسیب‌پذیری کشف شده
- ارائه CVE ID و همچنین CVSS یا درجه اهمیت متناسب با هر آسیب‌پذیری
- ارائه زمان کشف و گزارش بر طرف‌سازی آسیب‌پذیری‌های کشف شده
- اعلام Exploitable بودن آسیب‌پذیری‌های کشف شده
- ارائه API جهت استفاده در نرم‌افزارها و سامانه‌ها
- قابلیت گزارش‌گیری با فرمتهای مختلف از قبیل (...PDF, TXT, XML, EXCEL)
- نمایش تاریخچه پویش‌های صورت گرفته به تفکیک کلیه تجهیزات
- ایجاد تاریخچه‌ای از اطلاعات سازمان بصورت روزانه که امکان رجوع به آن در آینده وجود خواهد داشت.
- مقایسه وضعیت آسیب‌پذیری‌های فعلی شبکه با وضعیتهای قبلی
- استفاده از داده‌های جمع آوری شده بصورت بلند مدت به منظور اهداف فارنزیکی
- ایجاد آگاهی وضعیت سایبری از شبکه شامل دارایی‌ها، سرویسها، آسیب‌پذیری‌ها و ...





AVIN

سامانه مدیریت آسیب پذیری – VMS

با توجه به پویا بدون شبکه های کامپیوتری و تغییرات دائمی در این شبکه ها، پویش مستمر اطلاعات و آسیب پذیریها در زیرشبکه ها بصورت همزمان نیازمند نیروی انسانی کافی و انجام عملیات تکراری بصورت مدام می باشد. لذا با استفاده از این ماژول عملیات جمع آوری، نیست و ارزیابی پیوسته امکان پذیر شده و پوشش تمامی زیرشبکه از طریق نصب سنسورهای این سامانه در نقاط مختلف شبکه مقدور خواهد شد. نمونه ای از شماتیک سنسور سامانه در شکل زیر نمایش داده شده است.



ویژگی‌های اصلی سامانه

- اسکنر NESSUS به عنوان نرم افزار
 - عدم وجود محدودیت در ابعاد شبکه تحت پوشش
 - اولویت‌بندی خودکار آسیب‌پذیری‌های کشف شده بر اساس استاندارد CVSS
 - کمترین خطای مثبت کاذب در شناسایی آسیب‌پذیری‌ها
 - پیاده‌سازی به صورت مایکروسرویس
 - ارائه CVE Bank بروز و یویشن برخط و بلادرنگ آنها بر روی دارایی‌ها



تهران، اقدسیه، بلوار ارتش، مجتمع شمیران ستر، طبقه ۶، واحد ۶۰۲

٨-٢١٥١٢٢٣٠٢١٢١