تست امنیت

این نوشتار به هیچ منبع و مرجعی استناد نمی‌کند.

بیشتر بدانید

این مقاله نیازمند ویکی‌سازی است. لطفاً با توجه به راهنمای ویرایش و شیوه‌نامه، محتوای آن را بهبود بخشید.

بیشتر بدانید

تست امنیت فرایندی است که به منظور کشف و شناسایی نقص‌هایی در سیستم‌های امنیتی و با هدف مراقبت از داده‌ها و حفظ عملکرد در یک سیستم اطلاعاتی به کار می‌رود. به منظور محدودیت‌های منطقی که در تست امنیت وجود دارد، گذراندن تست امنیت به معنای عدم وجود نقص و یا برآورده ساختن ملزومات امنیتی نیست.

ملزومات امنیتی معمول شامل فاکتورهایی مانند محرمانگی، یکپارچگی، احراز هویت، دسترس‌پذیری، مجوز دسترسی و عدم انکار می‌باشند. آن دسته از ملزومات امنیتی که توسط سیستم پیاده‌سازی شده‌اند مورد تست و بررسی قرار می‌گیرند. تست امنیت به عنوان یک اصطلاح معانی متفاوتی دارد که می‌تواند به روش‌های مختلف کامل گردد. به‌همین علت رده‌بندی امنیت به ما در درک معانی و رویکردهای متفاوت این حوزه کمک می‌کند.

محرمانگی

- محرمانگی یک اقدام امنیتی می‌باشد که از افشای اطلاعات در برابر اشخاصی غیر از گیرنده مورد نظر جلوگیری می‌کند. این روش به تنهایی نمی‌تواند به‌طور کامل امنیت سیستم اطلاعاتی را تضمین کند.

یکپارچگی

یکپارچگی اطلاعات به مراقبت از اطلاعات در مقابل تحریف آن‌ها توسط شخص غیرمجاز اطلاق می‌شود.

- روشی است که به دریافت‌کننده اجازه بررسی و تعیین درستی اطلاعات دریافتی توسط سیستم را می‌دهد.

- در روش‌هایی که یکپارچگی را میسر میکنند اغلب از روش‌های دیگری مانند محرمانگی نیز استفاده می‌کنند. روش‌های محرمانگی به جای رمز کردن تمام اطلاعات مخابره شده، تنها اطلاعاتی را اضافه می‌کند که در سمت گیرنده با آن اطلاعات امکان بررسی درستی اطلاعات میسر می‌شود.
- این روش برای بررسی درستی اطلاعات ارسال شده از یک برنامه به یک برنامه دیگر و عدم وجود تغییر در آن اطلاعات استفاده می‌شود.

احراز هویت

احراز هویت می‌تواند شامل تأیید هویت فرد، ردیابی مبدأ یک محصول تولیدشده، اطمینان از مطابقت محصول با برچسب و بسته‌بندی آن و یا کسب اطمینان از قابل اعتماد بودن یک برنامه کامپیوتری باشد.

مجوز دسترسی

- فرآیند تعیین اجازه دریافت یک سرویس و یا اجرای یک عملیات به یک درخواست کننده.
- کنترل دسترسی یک مثال از احراز هویت می‌باشد.

دسترس‌پذیری

- اطمینان از اینکه اطلاعات و سرویس‌های ارتباطی در صورت اعلام نیاز، آماده استفاده می‌باشند.
- اطلاعات برای افرادی که هویتشان تصدیق شده، باید در صورت اعلام نیاز در دسترس باشد.

عدم انکارپذیری

- با توجه به امنیت دیجیتال، عدم انکارپذیری به معنای کسب اطمینان از اینکه پیام ارسال شده توسط فرستنده و گیرنده‌ای که ادعا می‌کنند پیام را ارسال و دریافت کرده‌اند، ارسال و دریافت شده‌است.

رده‌بندی تست امنیت

اصطلاحات رایج برای میسر ساختن تست امنیت:

- **کشف:** هدف این مرحله شناسایی سیستم در محدوده و خدمات مورد استفاده آن می‌باشد. هدف این مرحله کشف آسیب‌پذیری‌ها نیست اما بررسی نسخه برنامه‌های سیستم می‌تواند نسخه‌های منسوخ شده نرم‌افزار و یا سفت افزار را مشخص و در نتیجه آسیب‌پذیری‌های بالقوه را نمایان کند.
- **اسکن آسیب‌پذیری:** پس از مرحله کشف، اسکن آسیب‌پذیری به دنبال مسائل امنیتی شناخته‌شده می‌گردد. این موضوع توسط ابزارها و به صورت خودکار انجام می‌شود. این ابزارها آسیب‌پذیری‌های شناخته شده را با شرایط مطابقت می‌دهند و در نتیجه آن سطح ریسک را گزارش می‌دهند. سطح ریسک گزارش شده توسط صاحب سیستم قابل تغییر

نخواهدبود. در این اسکن می‌توان فردی را مسئول اسکن معرفی کرد و در نتیجه این اسکن می‌تواند اسکن همراه با اختیار باشد که در یک سیستم بار کمتری را به شبکه اعمال کرده و در نهایت می‌تواند خطاهایی را که به اشتباه معرفی شده‌اند(مثبت غلط) را از بین ببرد.

- **ارزیابی آسیب‌پذیری:** این ارزیابی از کشف و اسکن آسیب‌پذیری برای مشخص کردن آسیب‌پذیری امنیتی استفاده کرده و آن‌ها را در محیط تست قرار می‌هد. یک مثال از این اسکن می‌تواند از بین بردن خطاهای به اشتباه گزارش‌شدهٔ رایج و تصمیم برای گزارش سطح ریسک باشد. هر دو مورد ذکر شده برای بهبود درک توسط کسب و کار می‌باشد.
- **ارزیابی امنیتی:** ارزیابی امنیتی بعد از ارزیابی آسیب‌پذیری و با اعمال تأیید دستی برای اعلام گزارش انجام می‌شود. این تأیید شامل استفاده از آسیب‌پذیری‌ها برای ایجاد دسترسی بیشتر می‌باشد. تأییدها می‌تواند به فرم دسترسی مجاز به یک سیستم برای تأیید تنظیمات آن سیستم، برررسی لاگ‌ها، پاسخ‌های سیستم، پیام‌های خطا، کدها و غیره باشند. یک ارزیابی امنیتی سطح گسترده‌ایی از سیستم را تحت آزمون و بررسی قرار می‌دهد و عمیقاً به یک آسیب‌پذیری و تبعات آن می‌پردازد.
- **تست نفوذپذیری:** تست نفوذپذیری یک حمله را که ممکن است توسط مهاجم انجام شود را شبیه‌سازی می‌کند. این مرحله با توجه به مراحل قبل انجام شده و با توجه به آسیب‌پذیری‌های موجود، دسترسی‌های جدیدی را پیدا می‌کند. با این رویکرد می‌توان توانایی مهاجم برای دسترسی به امکانات محرمانه، تأثیر بر یکپارچگی اطلاعات و یا تأثیر بر دسترس‌پذیری یک سرویس را درک کرد. هر تست به طریقی انجام می‌شود که بتواند به تست‌کننده اجازه دهد تا از توانایی حل مسئله خویش استفاده کرده و با استفاده از علم خود از شبکه، آسیب‌پذیری‌هایی را پیدا کند که با ابزارهای موجود به‌طور خودکار یافت نمی‌شود. تفاوت این رویکرد با ارزیابی امنیت در این می‌باشد که در ارزیابی امنیت، بررسی در سطح گسترده‌تری انجام می‌شود اما در ارزیابی نفوذپذیری حملات عمیقاً بررسی می‌شوند.
- **ممیزی امنیتی:** ممیزی امنیتی یک نگاه کلی و جامع بر روی فرایندها و سیستم‌های امنیتی یک سازمان دارد. این رویکرد به بررسی و ثبت فعالیت‌ها برای ارزیابی روش‌ها و ابزار کنترلی مورد استفاده در سامانه برای تضمین انطباق آن‌ها با خط مشی‌های تدوین شده و ارائه پیشنهاد دربارهٔ تغییرات لازم در ابزارها، خط مشی‌ها و یا روال‌های کنترلی می‌پردازد. لازم به‌ذکر است که در بررسی‌های جزئی‌تر، این رویکرد می‌تواند از هریک از رویکردهایی که پیشتر در مورد آن‌ها بحث شد(ارزیابی آسیب‌پذیری، ارزیابی امنیتی، تست نفوذپذیری) استفاده کند.
- **مرور امنیتی:** تأییدی است که یک صنعت و یا استانداردهای امنیت داخلی بر روی اجزای سیستم و یا محصول اعمال می‌کنند. مرور امنیتی معمولاً با مستندات طراحی و یا دیاگرام‌های معماری و یا مرور کد کامل می‌شوند. این مرحله از هیچ یک از رویکردهای ارزیابی آسیب‌پذیری، ارزیابی امنیتی، تست نفوذپذیری و ممیزی امنیتی استفاده نمی‌کند.

جستارهای وابسته

- واژه‌نامه تضمین اطلاعات ملی

منابع

آخرین ویرایش ۱ سال پیش **توسط Hooman Mallahzadeh انجام شده**