تست نفوذ چیست و چگونه انجام می‌شود؟

شرکت رهاکو

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

فهرست

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

تعداد حملات سایبری بسیار زیاد شده است و هر روز هم به تعداد آن‌ها اضافه می‌شود. وجود چنین مسائلی باعث می‌شود تا کسب و کارها برای امنیت سایت خود از تست نفوذ استفاده کنند. این تست یک شبیه سازی از هک اخلاقی است که به منظور تایید اثر بخشی کنترل‌های امنیتی در یک محیط خاص انجام می‌شود و آسیب و حملات احتمالی را مشخص می‌کند. هک اخلاقی در زیرساخت شرکت یا پرسنل همان سازمان به منظور تست امنیت انجام می‌شود. این فرآیند با استفاده از تکنیک‌های مختلف حمله به امنیت اطلاعات سازمان‌ها را شبیه سازی می‌کند. در ادامه با تست نفوذ بیشتر آشنا می‌شوید.

تست نفوذ چیست؟

تست نفوذ (Penetration Testing) به فرآیند هک اخلاقی گفته می‌شود که شامل ارزیابی برنامه یا زیرساخت یک سازمان در برابر انواع مختلف تهدیدات می‌شود. این تست کمک می‌کند تا از آسیب پذیری‌های مختلف سیستم جلوگیری شود و دلایل احتمالی این آسیب پذیری‌ها مانند تنظیمات نادرست و طراحی ضعیف تشخیص داده شود. تست نفوذ که به عنوان تست قلم نیز شناخته می‌شود، یک حمله سایبری شبیه سازی شده علیه سیستم کامپیوتری برای بررسی آسیب پذیری‌های آن است. در رابطه با امنیت برنامه‌های تحت وب، از این تست معمولا برای تقویت فایروال برنامه وب (WAF) استفاده می‌شود.

تست قلم معمولا انواع حملات تهدید کننده وبسایت‌ها را شبیه سازی می‌کند تا مطمئن شود سیستم از سطح امنیت بالایی برخوردار است. با این تست می‌توان بررسی کرد که آیا سیستم به اندازه کافی قوی است که بتواند در برابر حملات مقاومت کند یا خیر. یک پن تستر استاندارد می‌تواند تا حد زیادی حامی کسب و کارها باشد و حملات احتمالی را شناسایی کند تا ایمنی سایت را در برابر حملات تضمین کند. در واقع تسترهای نفوذ همانند هکرهایی هستند که در جبهه‌ی شما میجنگد.

تفاوت تست نفوذ دستی و خودکار

پن تستر به صورت دستی

- به منظور دستیابی به نتایج بهتر، به تلاش بیشتری برای تست آسیب پذیری‌ها نیاز داریم.
- انجام این تست به صورت دستی زمان بیشتری می‌برد.
- وقتی یک حمله یا روش سو استفاده جدید ایجاد می‌شود، بسیاری از ابزارهای خودکار برای مقابله با این حملات باید منتظر اپدیت باشند. این در در صورتی است که انسان‌ها می‌توانند تکنیک جدید را به سرعت یاد گرفته و آن را پیاده سازی کنند.
- تعداد نتایج کاذب در تست دستی در مقایسه با تست خودکار کمتر است.

پن تستر خودکار

- ابزارهای خودکار بدون دخالت انسان استفاده می‌شوند، در حالی که تست دستی برای تمام موارد قابل انجام نیست.
- ابزارهای خودکار سریع‌تر عمل می‌کنند که طبیعتا به زمان کمتری نیاز دارد و فرایند را با سرعت بالاتری انجام می‌دهد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

- این روش بهترین راه برای انجام تست با آمار بالاست.
- در تست نفوذ خودکار، تعداد نتایج کاذب بیشتر است.

انواع مختلف پن تست

پن تستر شبکه

در تست شبکه ابتدا ساختار فیزیکی سیستم به منظور شناسایی خطرات موجود در شبکه سازمان بررسی می‌شود. در این روش شخص انجام دهنده تست (penetration tester) آزمایش‌ها و تست‌هایی را در شبکه سازمان انجام می‌دهد تا نقایص و ایرادها را در طراحی و عملکرد شبکه مورد نظر پیدا کند. تست گیرنده تمام اجزای مختلف سازمان که شامل رایانه‌ها، مودم‌ها و remote access devices می‌شود را بررسی می‌کند تا حملات احتمالی را تشخیص دهد.

پن تستر فیزیکی

تست فیزیکی به منظور شبیه سازی‌های دنیای واقعی انجام می‌شود. فرد انجام دهنده تست به عنوان یک مهاجم سایبری عمل می‌کند و سعی دارد سد فیزیکی امنیت را بشکند. این تست برای تشخیص آسیب پذیری‌های موجود در کنترل‌های فیزیکی مانند دوربین‌های امنیتی و سنسورها انجام می‌شود.

پن تستر برنامه وب

تستر برنامه وب برای بررسی حملات احتمالی و نقاط ضعف برنامه‌های مبتنی بر وب انجام می‌شود. این روش برای مسائل امنیتی استفاده می‌شود که ممکن است به دلیل توسعه غیر ایمن ناشی از طراحی یا کد رخ دهد. همچنین این تست برای شناسایی حملات احتمالی در وب سایت‌ها و برنامه‌ها استفاده می‌شود.

پن تستر شبکه بی سیم

این نوع تست برای بررسی ارتباط بین تمام دستگاه‌ها مانند: تبلت‌ها، لپ‌تاپ‌ها، رایانه‌ها و گوشی‌های هوشمند انجام می‌شود. از این روش به منظور جلوگیری از هرگونه نشت داده که ممکن است هنگام به اشتراک گذاری اطلاعات از یک دستگاه به دستگاه دیگر از طریق شبکه Wi-Fi رخ دهد، استفاده می‌شود.

چه کسی تست نفوذ را انجام می‌دهد؟

یکی از بزرگ‌ترین موانع برای محقق شدن امنیت سایبری، استفاده از افراد واجد شرایط و مجرب در این زمینه است. پن تسترها یا متخصصان تست نفوذ حیاتی‌ترین بخش این فرایند می‌باشند. انجام تست‌های پیچیده، کاوش عمیق در انواع سیستم‌ها و اجرای تمرین‌هایی شامل زنجیره حملات متعدد، به مهارت متخصصان تست نفوذ نیاز دارد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

سازمان‌ها می‌توانند با استفاده هوشمندانه از منابعی که به آسانی در دسترس است، یک برنامه تست نفوذ قوی را برای خود طراحی نمایند. تمام مراحل این تست به متخصص نیاز ندارد و افرادی که دانش کمتری در این زمینه دارند نیز می‌توانند از این ابزارها استفاده کنند. درست است که این ابزارها در تست‌های ساده کاربرد دارند، اما مهم است که این تست به طور منظم انجام شود.

ابزارهای پن تست شامل چیست؟

معمولا نفوذگران برای انجام حملات خود از ابزارهای مخصوصی بهره می‌گیرند. همین امر در مورد آزمون گیرنده‌های نفوذ هم صادق است. ابزارهای این تست صرفا برای تقویت و کمک به انسان مورد استفاده قرار می‌گیرند اما در جایگاه یک جایگزین برای انسان قرار ندارند. این ابزارها به پن تسترها کمک می‌کنند تا بیشتر تمرکز کنند. افراد متخصص در این عملیات باید انتخاب کنند که چه ابزاری بیشتر از سایر ابزارها به پن تستر کمک خواهد کرد. ابزارهای تست نفود معمولا عملکردهای متفاوتی را ارائه می‌دهند. برخی از آن‌ها به صورت open source در دسترس قرار می‌گیرند و برخی دیگر اهداف تجاری دارند. این ابزارها توسط هکر واقعی مورد استفاده قرار می‌گیرند، این باعث می‌شود که امکان تکرار دقیق حملات برای تست گیرنده فراهم شود. برخی دیگر از ابزارها نیازهای یک هکر قانونمند را برطرف می‌نمایند و بر اهداف آزمون امنیتی بیشتر تاکید می‌کند.

نتیجه گیری

تست نفوذ یک فرایند تست موثر است که با کمک به کشف مسائل امنیتی مهم سیستم، آسیب پذیری‌های موجود در زیر ساخت فناوری اطلاعات را نیز بررسی می‌کند. با افزایش تهدیدات سایبری، ایمن نگه داشتن زیر ساخت‌های فناوری اطلاعات در برابر هرگونه تهدید و آسیب پذیری احتمالی برای شرکت‌ها به یک ضرورت تبدیل شده است. بنابراین،با حملات سایبری که در دنیای دیجیتال امروزی در حال وقوع است، تست نفوذ یک امر بسیار مهم تلقی می‌شود.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net