تست نفوذپذیری

آزمون نفوذپذیری یا **آزمون نفوذ** (به انگلیسی: Penetration test) روشی برای تخمین میزان امنیت یک کامپیوتر (معمولاً سرور) یا یک شبکه است که با شبیه‌سازی حملات یک حمله‌کننده (هکر) صورت می‌گیرد. در این روش تمام سیستم و نرم‌افزارها و سرویس‌های نصب شده روی آن برای یافتن مشکلات امنیتی آزمایش می‌شوند و سپس اقدام به رفع مشکلات موجود می‌شود.

فرایند تست نفوذ

1. مشخص کردن دامنه (هدف، تارگت)
2. جمع‌آوری اطلاعات
3. ارزیابی آسیب‌پذیری
4. تست نفوذ
5. گزارش و ارائه راهکار

رویکرد تست نفوذ

تست نفوذ به روش‌های متفاوتی قابل انجام است. بیشترین تفاوت میان این روش‌ها، در میزان اطلاعات مرتبط با جزئیات پیاده‌سازی سیستم در حال تست می‌باشد که در اختیار تیم تست نفوذ قرار داده می‌شود. با توجه به این موضوع تست

نفوذ را می‌توان به چهار دسته White–Box , Covert,Black-Box و Gray-Box، تقسیم نمود.

Black-Box

تست Black-Box (جعبه سیاه) با فرض فقدان دانش قبلی از زیرساخت‌هایی است که قرار است مورد تست قرار گیرند. متخصصان باید پیش از آنالیز و بررسی، ابتدا مکان و گستره سیستم‌ها را به‌طور دقیق مشخص کنند. تست Black-Box در واقع شبیه‌سازی کردن حمله‌ای است که توسط نفوذگری انجام می‌شود که در ابتدا با سیستم آشنایی ندارد.

White-Box

تست White-Box (جعبه سفید یا تست شفاف) اطلاعات ضروری مانند معماری شبکه، کدهای منبع، اطلاعات آدرس IP و شاید حتی دسترسی به بعضی از کلمات عبور، در اختیار تیم ارزیابی امنیتی قرار می‌گیرد. تست White-Box حمله‌ای را شبیه‌سازی می‌کند که ممکن است در اثر افشای اطلاعات محرمانه از شبکه داخلی یا حضور نفوذگر در داخل سازمان به‌وجود آید. تست White-Box دارای گستردگی وسیعی می‌باشد و محدوده آن شامل بررسی شبکه محلی تا جستجوی کامل منبع نرم‌افزارهای کاربردی به منظور کشف آسیب‌پذیری‌هایی که تا کنون از دید برنامه نویسان مخفی مانده‌است، می‌باشد.

Gray-Box

روش‌های متنوع دیگری نیز وجود دارد که در واقع مابین دو روش ذکر شده در بالا قرار می‌گیرند که معمولاً از آنها به تست‌های Gray-Box (جعبه خاکستری) تعبیر می‌شود.

Covert

این نوع تست که به تست نفوذ double-blind نیز مشهور است اشاره به زمانی دارد که تقریباً هیچ‌کس از جمله افراد متخصص امنیت شبکه در شرکت مورد هدف اطلاعی از این حملهٔ کنترل شده ندارند. در این نوع تست نفوذ بسیار اهمیت دارد که متخصصین امنیت اجراکنندهٔ تست اطلاعاتی پایه‌ای دربارهٔ موضوع داشته باشند که از مشکلات قانونی جلوگیری شود.

تست نفوذ External و Internal

External

به انواع تست‌هایی اطلاق می‌شود که در خارج از محدوده سازمانی که قرار است مورد تست نفوذ قرار بگیرد، انجام می‌شود

در واقع سناریویی را بررسی می‌کند که مهاجم با دسترسی داشتن به منابع مورد نیاز خود، از جمله آدرس‌های IP که از سازمان مورد نظر در اختیار دارد یا با در اختیار داشتن کد منبع نرم‌افزارهایی که در سازمان استفاده می‌شوند و در اینترنت موجود می‌باشند اقدام به پویش و کشف آسیب‌پذیری نماید.

Internal

در حوزه مکانی آن سازمان و در میان افرادی که آن سازمان فعالیت می‌کنند انجام می‌شود.

سناریویی بررسی می‌شود که مهاجم به هر طریق ممکن موفق به ورود به سازمان مورد نظر شده و با جمع‌آوری داده‌های مورد نظر اقدام به حمله می‌کند. با ورود به محدوده مکانی یک سازمان مهاجم می‌تواند سناریوهای مختلفی را پیاده‌سازی نماید. برای نمونه با استفاده از شبکه بی‌سیم داخلی و بررسی داده‌های به اشتراک گذاشته شده که می‌تواند اطلاعات کارمندان باشد، حدس زدن کلمات عبور اصلی برای مهاجم ساده‌تر خواهد شد.

انواع تست نفوذ

1. تحلیل ریسک‌های امنیت
2. برنامه‌ریزی تست امنیت
3. طراحی و اجرای تست امنیت
4. تکنیک‌های جمع‌آوری اطلاعات یک برنامه کاربردی (عمدتاً وب سایتها)
5. تست مدیریت پیکربندی (Configuration Management)
6. تست منطق کاری (Business Logic)
7. تست مدیریت نشست (Session Management)
8. تست احراز هویت (Authentication)
9. تست کنترل دسترسی (Authorization)
10. تست‌های مربوط به اعتبارسنجی داده‌های ورودی (Injections, Buffer overflow)

تست نفوذ در ایران

با توجه به اهمیت دادن مسئولان و سران نظام به مسئله امنیت در ایران، امنیت در حوزه فناوری اطلاعات نیز از اهمیت ویژه‌ای برخوردار است. این مسئله سبب شده بر خلاف سایر حوزه‌های تضمین کیفیت و تست نرم‌افزار، برای این حوزه اهمیت خیلی زیادی قائل شوند. علاوه بر این، جذابیت مباحث هک و نفوذ سبب شده افراد زیادی به این موضوع علاقه پیدا کنند. به دلیل بومی نبودن تکنولوژی مربوط، دانش سطحی و نبود زیر ساخت‌های لازم، تعداد متخصصین و افراد خبره

در این موضوع بسیار اندک است، اما در چند سال اخیر گروه‌های تخصصی و فنی مجرب زیادی شروع به کار کرده‌اند که آینده روشنی را برای ایران در حوزه امنیت تداعی می‌کنند.

ارزیابی امنیتی سامانه‌ها و تست نفوذ

تست نفوذ یا آزمون نفوذپذیری (به انگلیسی: Penetration test) روشی برای تخمین میزان امنیت یک کامپیوتر (معمولاً سرور) یا یک شبکه یا یک سایت یا یک نرم‌افزار است که با شبیه‌سازی حملات یک حمله‌کننده (هکر) صورت می‌گیرد. در این روش تمام سیستم و نرم‌افزارها و سرویس‌های نصب شده روی آن برای یافتن مشکلات امنیتی آزمایش می‌شوند و سپس اقدام به رفع مشکلات موجود می‌شود. امروز بر روی سایت، نرم‌افزار، اپلیکیشن و شبکه اینترنت تست نفوذ انجام می‌گیرد. اولین اقدام برای اطمینان از امنیت یک سایت یا نرم‌افزار انجام تست نفوذ بر روی آن است.

منابع

- (فارسی) https://www.testnofoz.com/?p=1753

آخرین ویرایش ۲ ماه پیش **توسط GameO7er انجام شده**

ویکی‌پدیا