۱ مقدمه

تست نفوذ یا ارزیابی امنیتی روشی است که توسط آن قادر خواهیم بود تا آسیب‌پذیری‌های موجود در شبکه، وب سایت و بانک‌های اطلاعاتی خود را شناسایی کرده و پیش از آنکه نفوذگران واقعی به سیستم وارد شوند، امنیت شبکه خود را افزایش دهیم. این روش با استفاده از ارزیابی جنبه‌های مختلف امنیتی کمک می‌کند تا با کاهش دادن ریسک‌های امنیتی موجود در شبکه، سیستم‌عامل‌ها، بانک‌های اطلاعاتی و برنامه‌های کاربردی، احتمال نفوذ غیرمجاز به شبکه را کاهش دهیم.

هدف از انجام تست نفوذ، یافتن آسیب‌پذیری در یک یا چند مورد از زمینه‌های زیر می‌باشد:

- امنیت تجهیزات فعال شبکه
- امنیت سیستم‌عامل‌ها
- امنیت سرویس‌های شبکه و بانک‌های اطلاعاتی
- امنیت برنامه‌های کاربردی تحت شبکه و وب

تست نفوذ را می‌توان از دیدگاه‌های متفاوتی بررسی نمود. براساس میزان اطلاعاتی که در اختیار تیم نفوذ است، می‌توان سه دسته White Box، Black Box و Gray Box را در نظر گرفت و از دیدگاه مکان انجام تست نفوذ به Internal و External تقسیم نمود.

۱-۱ رویکرد Black-Box ، Gray-Box و White-Box

تست نفوذ به روش‌های متفاوتی قابل انجام است. بیشترین تفاوت میان این روش‌ها، در میزان اطلاعات مرتبط با جزییات 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 سه دسته Black-Box، White - Box و Gray-Box تقسیم نمود.

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

از سوی دیگر در تست White-Box 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 شبیه سازی می‌کند که ممکن است در اثر افشای اطلاعات محرمانه از شبکه داخلی یا حضور نفوذگر در داخل سازمان بوجود آید. تست White-Box دارای گستردگی وسیعی می‌باشد و محدوده آن شامل بررسی شبکه محلی تا جستجوی کامل منبع نرم افزارهای کاربردی به منظور کشف آسیب‌پذیری‌هایی که تا کنون از دید برنامه نویسان مخفی مانده است، می‌باشد.

روش های متنوع دیگری نیز وجود دارد که در واقع مابین دو روش ذکر شده در بالا قرار می‌گیرند که معمولاً از آنها به تست های Gray-Box تعبیر می‌شود.

۱-۲ تست نفوذ External و Internal

تست External به انواع تست‌هایی اطلاق می‌شود که در خارج از محدوده سازمانی که قرار است مورد تست نفوذ قرار بگیرد، انجام می‌شود و تست‌های Internal در حوزه مکانی آن سازمان و در میان افرادی که آن سازمان فعالیت می‌کنند انجام می‌شود.

نوع اول در واقع سناریویی را بررسی می‌کند که مهاجم با دسترسی داشتن به منابع مورد نیاز خود، از جمله آدرس های IP که از سازمان مورد نظر در اختیار دارد و یا با در اختیار داشتن کد منبع نرم افزارهایی که در سازمان استفاده می‌شوند و در اینترنت موجود می باشند اقدام به پویش و کشف آسیب‌پذیری نماید.

در نوع دوم سناریویی بررسی می‌شود که مهاجم به هر طریق ممکن موفق به ورود به سازمان مورد نظر شده و با جمع آوری داده های مورد نظر اقدام به حمله می‌کند. با ورود به محدوده مکانی یک سازمان مهاجم می تواند سناریوهای مختلفی را پیاده سازی نماید. برای نمونه با استفاده از شبکه بی‌سیم داخلی و بررسی داده‌های به اشتراک گذاشته شده که می تواند اطلاعات کارمندان باشد، حدس زدن کلمات عبور اصلی برای مهاجم ساده‌تر خواهد شد.