Penetration Testing

H4ckm1nD.SecurityG33ks

- محتوى الكتاب

مقدمة توضيحية عن اختبار الأختراق Penetration Testing

تعريف :

هي عملية لمحاولة اثبات ان نظام ما او منظومة امنية ما ليست أمنة او بمعنى عام هي محاولة لاختراق منظومة امنية ما واستخراج بيانات غير مصرح له بعرضها او العبث والأطلاع على بيانات قبيل اتمام عملية ارسالها لوجهتها الصحيحة او ايقاف منظومة امنية ما والأطاحة بعملها وجعلها متوقفة عن العمل لفتره زمنية معينة

مفهوم اختبار الاختراق :

ان اختبار الاختراق لا يتم بشكل عشوائي بل يتم من خلال عقد مبرم بين المنظومة الامنية التي ترغب بالقيام بهذا الفحص الامني وبين المختبر من خلال عقد توضع فيه شروط معينة يتم تحديدها من خلال المنظومة والمختبر وتتم هذه الطريقة اما لمره واحدة او من خلال اشتراك شهري او اسبوعي
ليتم بعد ذلك تقديم تقرير كامل عن الموضع الامني لهذه المنظومة الامنية
وهنالك شروط كثيرة تدرج ضمن العقد ومن اهمها هية عدم الحاق اي ضرر مادي في المنظومة او تعديل على بيانات ما

اهمية اختبار الأختراق :

ان اختبار الاختراق هو من اهم المراحل التي تحافظ على الأستقرار الامني للمنظومة ويبقى المختبر الذي يعتبر ضليع ولديه خبرة في مجال الاختراق والحماية والشبكات والهندسة الاجتماعية هو الشخص الافضل للقيام بهذه العملية فهو الذي يعمل من اين تأكل الكتف

وعلى اطلاع دائم ومستمر بجديد الثغرات وعلى اطلاع كامل على الاساليب والطرق المتبعة في الاختراق

وبما ان عالم الشبكة والانترنت لا يعرف الانضباط فهذا الجانب مهم جدا للكثير من الشركات التجارية والامنية التي من الممكن ان تتعرض للتطفل والأضرار بأسمها وبعملائها فأكتشاف خلل امني قبيل وقوعه يجعل الضرر اقل ويحميه من هجوم مستقبلي قد يطيح بهذه المنظومة

عند البدأ في عملية اختبار الاختراق هنالك سلم هرمي يجب اتباعه دون التخلي عن اي نقطة فيه ليتم الاختبار بشكل صحيح

High-Level Assesment

القيام بعملية تقيم وفحص لسياسة المنظومة واسأليب عملها مواعيد عملها مفاهيم الموظفين وافكارهم
وهذا الجانب هو جانب نظري بحت ولكنه يعتبر الخطوة الاولى في الأختبار فهذا الجانب النظري يفيد جدا في مرحلة استخدام الهندسة الأجتماعية ويعتبر دراسة نظري عن ما يدور حول هذه المنظومة

Network Evaluation

هية عملية اختبار للشبكة المرتبطة في المنظومة تحليلها ومعرفة اسلوب ربطها مع المصادر المتخلفة ومعرفة اسلوب اتخاذ اجراءات الحماية المتبعة للخفاظ على الأمان ضمن الشبكة الواحدة
واسلوب منح التصاريح والصلاحيات بين اعضاء المنظومة

Low-Level Assesment

هنا يتم استخدام الجانب العملي لاستكمال المرحلة السابقة ليتم فحص الشبكة واستخراج اكبر قدر ممكن من البيانات والمصادر المستخدمة ضمن الشبكة الداخلية

Penetration Testing

وهنا تبدا مرحلة محاولة الاختراق الفعلية للمنظومة بشتى الوسائل المتبعة - ثغرات الويب – ثغرات الانظمة – الهندسة الاجتماعية ..الخ

وهنا تقسم المرحلة الى نوعين

BlackBox

يتم من خلال القيام بعملية الاختراق دون منح المختبر اي معلومات او اي بيانات تساعده في عمليءة الاختراق وتتم العملية من خلال جهد شخصي من المختبر ومستقل

White Box

يمنح فيها المخترق جميع البيانات التي يحتاجها للقيام بعمله

الخـاتمـه

في ما سبق تحدثنا ان الاختبار يتم على نوعين بلاك بوكس او وايت بوكس ويعتبر الخيار الاول هو الخيار المستخدم بشكل اكثر فهو اكثر فاعلية ومحاكات للواقعة
فعند تعرض المنظومة لمحاولة اختراق سيكون على سبيل الاختيار الأول فيتم بطريقة يجهل بها المتطفل اي معلومات مسبقة عن هذه المنظومة

يمنع في اختبار الأختراق

- استخدام برامج خبيثة وضارة قد تؤدي لأضرار
- يمنع تغير او تعديل في البيانات الخاصة قبل مراجعة اداة المنظومة لو تطلب الامر ذلك
- يمنع تقديم تقارير عشوائية دون تقديم دلائل واثباتات عن الوضع الامني

المـزيـد

http://en.wikipedia.org/wiki/Penetration_test

http://www.de-ice.net

rOckHuntEr
r0ck.hunt3r@gmail.com
http://h4ckm1nd.wordpress.com/

Gr33tz

L3zrGroup*SecurityGurus*Medo-Hacker*rOckMaster*BL4ckZ3rO*LinuxAc.Org*