المقالات العلمية

Penetration Test

الكاتب: زايد حمد

تنبيه:
تعتبر هذه المقالة مشاركة من كاتبها في زيادة التوعية والمحتوى الخاص بأمن المعلومات، وقد راجعها مراجع واحد على الأقل، ولا يتحمل مركز التميز لأمن المعلومات أي تبعات لهذه المقالة، ولا أي معلومات تطرح في هذه المقالة ولا يضمن دقة المعلومة وصحتها.

تعريف:

يقصد بالـ Penetration Test : هي عملية إثبات أن نظام ما غير امن، وذلك بمحاولة اختراقه والوصول لمعلومات لا ينبغي الوصول لها والإطلاع عليها إلا من قبل من يحق له . وتعتبر هذه العملية قانونية إذا ما تم توقيع عقد بين الطرفين وفيه يتم تحديد نوع الـ Penetration Test ومدته وبدايته ونهايته واختيار التطبيقات أو الأنظمة التي سوف يجرى عليها الاختبار.

أهمية Penetration Test:

في عصر المعلومات واتجاه جميع المؤسسات والجهات الحكومية والخاصة إلى العالم الرقمي والبيئة المعلوماتية واعتماد الكثير على الخوادم التطبيقات الانترنت، وقيام جميع أعمال تلك المؤسسات أو المنظمات في عملها على التقنية، أصبح بقاء هذه الخدمة لاستمرارية العمل واجبه وضرورية لتلك المنظمات والمؤسسات، ومن هنا انطلقت خدمه الـ Penetration Test كأحد الخدمات المساهمة لتقييم المخاطر ومحاولة لوضع تقرير نهائي يوضح ثغرات وعيوب النظام أو التطبيق وتصنيف خطورة هذه الثغرات، مما يعطي لمدير نظام المؤسسة أو المنظمة تفاصيل لكيفية سد هذه الثغرات وتجنب حدوث أي اختراق أو سرقة بيانات مهمة بالنسبة لهم لا قدر الله.

أنواع Penetration Test:

اختبار الاختراق يشمل كل ما يتعلق بالحاسب الآلي وشبكة الانترنت والشبكة السلكية واللاسلكية بما فيها البلوتوث. وحتى الموظفين أنفسهم يجرى عليهم الاختبار دون علمهم وهذا يسمى Social Engineering .

وتحديد نوع اختبار الاختراق المبدئي يكون بطلب من صاحب النظام المراد تقييمه، فهناك اختبار اختراق داخلي Internal وخارجي External وبعدها يتم تحديد نوع الهجوم إما يكون Black Box أو White Box

مبدئيا يحدد اختبار الاختراق أولا بكونه داخلي أو خارجي.

External Penetration Test:

محاولة اختراق الشبكة أو النظام من الخارج، أي لا يكون المخترق داخل الشبكة المراد اختراقها وهو الأقرب للواقع

Internal Penetration Test:

يقوم المخترق بإجراء الاختبار من داخل الشبكة المعنية، ويأتي مكملاً لاختبار الاختراق الخارجي، لان اخطر هجمات الاختراق غالبا ما تأتي من الداخل.

Black Box Penetration Test:

وتعني أن المختبر أو المخترق لا يملك أي معلومات عن الهدف أو الأهداف المراد اختراقها، عدا عنوان الموقع أو الشبكة، فلا يعلم عن أي شيء يخص النظام أو الشبكة أو إعداداته أو موظفيه، وهذا النوع اقرب للواقع، فهو يحاكي عملية اختراق فعلية. ولهذا يكون الاختبار أكثر قيمة بالنسبة لصاحب العمل، لأنه يعتمد بشكل أساسي اكتش اف عيوب النظام وثغراته الواضحة للإطراف الخارجية.

White Box Penetration Test:

يقوم المختبر في هذا النوع بمعرفه تفاصيل عن النظام المرد اختراقه، وتفاصيل الشبكة وكيفية بنائها، وإعدادات النظام وإصداره، يكون المخترق ملم بمعظم تفاصيل النظام وعليها يبدأ صياغة سينا ريو الاختراق، مع أن هذا النوع غير محبب من اغلب مدراء الأنظمة، ولكن يكون ذا أهمية اكبر في حالات خاصة . على سبيل المثال خدمة حفظ ملفات تقدمها جهة ما لموظفيها، ولا يمكن لأي شخص الدخول إلا باستخدام كلمة مرور ومعرف، هنا يكون المخترق كجزء من النظام بمنحه حق الدخو ل، وهدف العملية معرفه ماذا سيحدث إذا ما حصل احد المخترقين معلومات الدخول لأي موظف له الحق بالدخول على الخادم.

وقد يشمل اختبار الاختراق:

- الشبكات والبلوتوث
- خوادم الانترنت (السيرفرات) وجميع خدماته FTP, SSH
- أنظمة الحاسب الآلي
- الراوترات
- تطبيقات الانترنت مثل php,asp
- الأشخاص ومن يملك علاقة بالنظام أو الشبكة social engineering

بعد عملية الـ Penetration Test يعطى صاحب النظام الذي اجري عليه الاختبار تقرير نهائي يوضح فيه الثغرات التي تمكن المخترق من الوصول إليها ونبذه عامه عن عيوب الشبكة والأخطار المحتمل مواجهتها، لتفادي حدوث اختراق أو عطل يسبب ضياع معلومات لا قدر الله.

© CoEIA
الكاتب: زايد حمد