



## ما هو اختبار الاختراق؟



اختبار الاختراق (penetration testing) هو اختبار مصرح يتم إجراؤه على الأنظمة أو الأجهزة لتقييم مستوى الأمان فيها. يستخدم مختبر الاختراق نفس الأدوات والتقنيات والعمليات التي يستخدمها المهاجمون لاكتشاف الثغرات ونقاط الضعف وتأثيرها لحماية الأنظمة والمؤسسات.

### فوائد اختبار الاختراق:

- البحث عن نقاط الضعف في الأنظمة
- تحديد قوة ومتانة الأوامر والإجراءات المتبعة
- إظهار المخاطر المحتملة
- دعم استمرارية العمل
- إتباع اللوائح والإجراءات وتدعيمها
- تقديم أمثلة كمية ونوعية للوضع الأمني الحالي وأولويات الميزانية للإدارة

### مراحل اختبار الاختراق:

#### ١- الاستطلاع (Reconnaissance)

في هذه المرحلة يقوم المختبر بجمع أكبر عدد ممكن من المعلومات عن الهدف المراد اختراقه. ويوجد العديد من المصادر والأدوات التي تسهل على المخترق عملية جمع المعلومات. تتضمن المصادر عمليات البحث على الإنترنت والهندسة الاجتماعية. تساعد هذه العملية المخترقين على تحديد نقاط الضعف والثغرات المحتملة.

#### ٢- المسح (Scanning)

يقوم مختبر الاختراق باستخدام العديد من الأدوات المتاحة لمسح الهدف والبحث عن نقاط الضعف المتاحة في الأنظمة المستخدمة. يمكن من خلال عملية المسح معرفة الخدمات المفتوحة على الأجهزة مثل (http) و (ftp) وغيرها ومعرفة أي منها يحتوي على ثغرة شائعة يمكن استغلالها.

### ٣- الوصول إلى النظام

من دوافع المخترقين الحصول على صلاحية للدخول إلى النظام للقيام بالعديد من العمليات منها السرقة، حذف أو تعديل المعلومات أو حتى تشويه سمعة الشركة. لذلك على المختبرين استغلال أفضل الأدوات والطرق التي تُمكنهم من الحصول على صلاحية الدخول للنظام.

### ٤- الحفاظ على صلاحية الدخول

بعد نجاح عملية الاختراق وتمكن المخترقين من الدخول إلى النظام يحاول المخترقون الحفاظ على دخولهم للنظام من خلال بعض الاستراتيجيات التي تساعدهم على ذلك مثل تثبيت باب خلفي (Backdoor) لتمكينهم من الدخول إلى النظام مرات أخرى.

### مجالات اختبار الاختراق:

يمكن القيام باختبارات الاختراق على العديد من الأنظمة والتقنيات لضمان حمايتها من هذه التقنيات:

- تطبيقات الويب
- تطبيقات الهاتف الذكي
- الشبكات
- السحابة الإلكترونية
- تقنيات إنترنت الأشياء (Internet of Things)
- أجهزة الهاتف والحواسب الشخصية



كما توجد منصات عديدة تسمح للمختبر الأخلاقي بالقيام باختبارات الاختراق لاكتشاف الثغرات البرمجية منها منصة مكافآت الثغرات (Bug Bounty) وهي الأشهر محلياً والمطلقة من الاتحاد السعودي للأمن السيبراني والدرنوز وهي المنصة الأولى على مستوى الشرق الأوسط. تهدف إلى توظيف مهارات وخبرات المختبرين في اكتشاف الثغرات البرمجية في مواقع ومنتجات الشركات المشاركة في المنصة.

أخيراً، تحرص العديد من المنظمات والجهات على حماية أنظمتها لذلك تقوم بالاستفادة من اختبارات الاختراق لتحديد نقاط الضعف والثغرات ومعالجتها لتفادي مخاطر الاختراق.

إعداد عضوة النادي: سارة البسام