اشهر عشرة هجمات في الامن سيبراني

ثغرة الصفر zero day exploit
عبارة عن ثغرة يتم اكتشافها في تطبيق او نظام تشغيل وتكون هذه الثغرة غير مكتشفة من قبل المنُتج.

هجوم كلمة المرور
استغلال ثغرة امنية في النظام مع استخدام أدوات هجوم كلمة المرور التلقائية التي تساعد في تسريع عملية التخمين وفك كلمات المرور.

ثغرات XXS
ثغرة امنية في برامج الويب يقوم المهاجم بأدراج تعليمات ضاره في مواقع ويب موثوقة يتم تضمين البرمجيات الخبيثة ثم يتم تسليمة الى متصفح الضحية.

الجذور الخفية (rootkit)
مجموعة من البرامج يتم استخدامها لإخفاء الأنشطة على النظام يستخدمها المهاجمين لإخفاء نشاط وحركة البرمجيات الخبيثة حتى لا يتم اكتشافها من قِبل المستخدم او أنظمة كشف التسلل IDS.

هجمات إنترنت الأشياء (IoT)
المهاجمين يستغلون عدم وجود بروتكولات امان في أجهزة انترنت الأشياء يقومون بالدخول الى البيانات الحساسة باستخدام أجهزة IoT تتم العملية عن طريق بتثبيت البرمجيات الخبيثة في الجهاز و الحاق الضرر بالجهاز او الوصول الى البيانات الشخصية.

البرمجيات الخبيثة
وهي برامج ضارة ومتطفلة على الكومبيوتر او نظام الكومبيوتر تقوم بسرقة البيانات او تخريبها. أشهرها الفايروسات الديدان وحصان طروادة.

التصيد الالكتروني
هو نوع من هجمات الهندسة الاجتماعية يُستخدم غالبًا لسرقة بيانات المستخدم، بما في ذلك بيانات تسجيل الدخول وأرقام بطاقات الائتمان. يحدث ذلك عندما يخدع مهاجم، متنكرا ككيان موثوق به، يرسل للضحية لفتح بريد إلكتروني أو رسالة فورية أو رسالة نصية.

هجمات الرجل في الوسط (MitM)
هو مصطلح عام عندما يضع الجاني نفسه في محادثة بين مستخدم وتطبيق - إما للتنصت أو لانتحال شخصية أحد الطرفين، مما يجعل الأمر يبدو كما لو كان تبادلًا طبيعيًا للمعلومات قيد التنفيذ.

هجوم رفض الخدمة (DOS)
هو هجوم يهدف إلى إغلاق جهاز أو شبكة، مما يجعل الوصول إليها غير ممكن للمستخدمين المقصودين. يتم DOS عن طريق ارسال كمية كبيره من الطلبات لزيادة التحميل على الأنظمة ومنع الطلبات المشروعة.

حقن SQL
ضعف في امن الويب تسمح للمهاجم بالدخول الى الاستعلامات التي يقوم بها أحد التطبيقات في قاعدة البيانات. بشكل عام تسمح للمهاجم بمشاهدة البيانات واسترجاعها ومن الممكن أيضا التعديل او الحذف.