**الاختراق**

الاختراق (بالإنجليزية: Hacking) بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف. وحينما نتكلم عن الاختراق بشكل عام فنقصد بذلك قدرة المخترق على الدخول إلى جهاز شخص ما بغض النظر عن الأضرار التي قد يحدثها، فحينما يستطيع الدخول إلى جهاز آخر فهو مخترق (بالإنجليزية: Hacker) أما عندما يقوم بحذف ملف أو تشغيل آخر أو جلب ثالث فهو مخرب ويوجد نوعان من الأشخاص المخترقين ..النوع الأول هم مايسمى بأصحاب القبعات البيضاء وهذا النوع من المخترقين يقوم بمساعدة الناس ويعرف بالمخترقين الأخلاقين. ..والنوع الثاني مايسمى بأصحاب القبعات السوداء وهم مخترقين غير أخلاقين يقومون بأعمال تخريب ... (بالإنجليزية: Cracker).

**وسائل الاختراق**

**اختراق الأجهزة**

هو كأي اختراق آخر لشيءٍ ما. له طرق وأسس يستطيع من خلالها المخترق التطفل على أجهزة الآخرين عن طريق معرفة الثغرات الموجودة في ذلك النظام. وغالباً ما تكون تلك الثغرات في المنافذ (بالإنجليزية: Ports) الخاصة بالجهاز. وهذه المنافذ يمكن وصفها بأبسط شكل على أنها بوابات للجهاز. على سبيل المثال: المنفذ 80 غالباً ما يكون مخصصاً لموفر الخدمة كي يتم دخول المستخدم الإنترنت وفي بعض الأوقات يكون المنفذ رقمه 8080... هناك طرق عديدة للاختراق أبسطها والتي يمكن للمبتدئين استخدامها هي البرامج التي تعتمد نظام (الزبون/الخادم) (بالإنجليزية: client/server) حيث تحتوي على ملفين أحدهما Server يرسل إلى الجهاز المصاب بطريقة ما، والآخر Client يتم تشغيله من قبل المخترق للتحكم في الجهاز المصاب وعند تشغيل ملف الـ Server من قبل الضحية يصبح الكمبيوتر عرضة للاختراق حيث يتم فتح أحد المنافذ (بالإنجليزية: Ports) وغالباً ما يكون البورت 12345 أو 12346 وبذلك يستطيع الاختراق ببرنامج مخصص لذلك ويفعل ما يحلو له. كما يستطيع أشخاص آخرون (إضافة إلى من وضع الملف في جهازك) فعل نفس الشيء بك حينما يقومون بعمل مسح للمنافذ (بالإنجليزية: Port Scanning) فيجدون المنفذ لديك مفتوح. هذه الطريقة التي ذكرتها هي أبسط أشكال الاختراق، فهناك طرق عديدة تمكن المتطفلين من اختراقك مباشرة بدون إرسال ملفات!

**الفيروسات**

هي سكربتات برمجية يكتبها المخترقون ويقومون بتضمينها في جهاز الضحية بطريقة من الطرق وهي تنفذ ما تم تكليفها به. يكون هدفها في أغلب الأحيان ملفات الضحية عبر تخريبها ومحوها.

**التروجان**

يطلق عليه بالعربية أحصنة طروادة لكونه برنامجا يقوم الضحية بتحميله بكامل إرادته واستعماله كذلك ويبدو في ضاهره مفيدا بينما يعمل على التلاعب بالملفات الأم للحاسوب

**كيف تواجه الاختراق**

يجب أن تعرف في المقام الأول أنك مادمت متصلاً على الشبكة (بالإنجليزية: Network) فأنت معرض للاختراق في أي وقت وبأي طريقة كانت وقد يستهدفك أحد المخترقين (بالإنجليزية: Hacker) لسبب ما أو عشوائياً حتى، وربما يكون هذا الهاكر خبيراًَ فيمكنه اختراقك بحيث لا تحس بما يفعله تجاهك!! وعلى هذا فأفضل طريقة هي عدم وضع أشيائك الهامة والخاصة داخل جهازك كرقم بطاقة الائتمان أو أرقامك السرية، وهناك طريقة أفضل وهي استخدام جهاز خاص للاتصال بالإنترنت فقط لا يحتوي على معلومات هامة، وان كانت هذه الطريقة مكلفة بعض الشيء ولكن للضرورة أحكام. هناك برامج مضادة للاختراق ولكن عموماً فهي ليست مضمونة تماماً ولكن لا مانع من استخدامها حيث ستفيدك في التخلص من بعض الهاكرز ولكن ليس الخبراء منهم. بالنسبة للبرامج التي تخترق عن طريق إرسال ملف تجسس كملفات التصحيح (بالإنجليزية: Patch) فلا داعي للخوف منها طالما كنت تمتلك برنامج مضاد.

**نقاط متفرقة**

* الإنترنت وضعت للإفادة وتبادل المعلومات والثقافات، لذلك فمن غير اللائق استخدامها للتطفل على الآخرين وسرقة معلوماتهم.
* احذر من التباهي بقدرتك على حماية جهازك حماية تامة وبأن جهازك غير قابل للاختراق لأن هناك دائماً من هم أعلم منك وسيعتبرون ذلك تحدياً لهم.
* حاول دائماً تغيير كلمة السر بصورة دورية فهي قابلة للاختراق.
* أي ربط شبكي يترتب عليه مخاطر من الاختراق. حتى الشبكات المحلية.