- **الاختراق او القرصنة الالكترونية (Hacking)**

الاختراق بشكل عام هو القدرة على الوصول لهدف معين(جهاز شخص ما) بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف بغض النظر عن الأضرار التي قد يحدثها، فحينما يستطيع الدخول الى جهاز آخر فهو مخترق (Hacker) أما عندما يقوم بالاختراق وحذف ملف أو تغييره أو تعطيله فهو مخرب(Cracker) .

تقسم هجمات المخترقين إلى نوعين، و ذلك بناءً على الضرر الذي ستسببه الهجمة، فإذا كان الهجوم سيُسبب ضرراً أو تعديلاً او تغييراً بالنظام فإنه يُسمى بالهجوم النشط *Active Attack*، و لكن إذا كان هدف الهجوم الحصول على البيانات فقط دون إحداث أي تعديل أو ضرر فيُسمى بالهجوم الخامل *Passive Attack*.

الهجمات النشطة Active Attacks

1. **التعديل Modification**
2. **الخداع Spoofing**
3. **إعادة الإرسال Replaying**
4. **الإنكارRepudiation**
5. **حجب الخدمة Denial of Service (Dos)**

الهجمات الخاملة Passive Attacks

1. **التجسس Snooping**
2. **تحليل البيانات المرسلة Traffic Analysis**

انواع المخترقون

١. أصحاب القبعات البيضاء White Hat Hackers

أصحاب القبعات البيضاء ويعرفوا أيضا بالـ Ethical Hackers أو الهاكر الأخلاقي .هذا الشخص يملك خبرات ومهارات الهاكرز وهو قادر على اختراق الأنظمة والشبكات بنفس الأسلوب والأدوات التي يستخدمها المخترقين لكنّه يستغل خبرته في الأمور الجيدة كأن يبلّغ الشركات عن وجود ثغرة في احدى منتجاتها أو يعمل Penetration Tester أو ان يكون مسؤول الحماية في احدى الشركات.

٢. أصحاب القبعات الرماديّة Gray Hat Hackers

أصحاب القبعات الرماديّة, يمكننا القول أنهم هاكرز أخلاقيين أيضاً وهم يشبهون الصنف الأول (أصحاب القبعات البيضاء) كثيراً لكن بنفس الوقت قد يقوموا ببعض الاختراقات بغرض التحدي مثلاً أو لاثبات وجود ثغرة أو لايصال رسالة معيّنة.

٣. أصحاب القبعات السوداء Black Hat Hackers

أصحاب القبعات السوداء ، هؤلاء الأشخاص يستغلون معرفتهم وخبراتهم في الأمور التخريبية ويخترقون المواقع والسيرفرات بغرض المتعة واثبات الوجود أو لغايات أخرى غالبا تكون غير شرعية كالابتزاز وسرقة المعلومات أو اختراق مواقع الشركات وحسب وجهة نظر مختصي امنية المعلومات فيجب اطلاق لقب Crackers عليهم وليس Hackers

٤. اطفال الاكواد Script Kiddies

ان هذه الفئه هي المنتشره على الانترنت وهي مجموعه من عديمي الخبرة يستخدمون البرامج الجاهزه لتقوم ببعض العمليات البرمجيه بشكل عشوائي للتخريب والاختراق.

كيف يتم الاختراق

لا يمكن ان يتم الاختراق الا فى حاله وجود ملف تجسس داخل الجهاز المُخترق ويعتمد الإختراق على السيطرة عن بعد وهي لاتتم إلا بوجود عاملين مهمين : الأول البرنامج المسيطر ويعرف ب العميل Client والثاني الخادم Server الذي يقوم بتسهيل عملية الأختراق ذاتها .

وبعبارة أخرى لابد من توفر برنامج على كل من جهازي المخترق والضحية ففي جهاز الضحية يوجد برنامج الخادم وفي جهاز المخترق يوجد برنامج العميل . تختلف طرق إختراق الأجهزة والنظم بإختلاف وسائل الإختراق ، ولكنها جميعا تعتمد على فكرة توفر إتصال عن بعد بين جهازي الضحية والذي يزرع به الخادم (server)الخاص بالمخترق ، وجهاز المخترق على الطرف الأخر حيث يوجد برنامج المستفيد او العميل Client

- **الجرائم الالكترونية Cyber Crimes**

عبارة عن نشاط اجرامي تُستخدم فيه تقنيات الحاسوب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي كعمليات الاختراق والقرصنة، كما تضم أيضا أشكال الجرائم التقليدية التي يتم تنفيذها عبر الإنترنت والجرائم التي قد تهدد أمن الدولة وسلامتها المالية، او والتجارة غير القانونية (كتجارة المخدرات)، كما تضم انتهاك خصوصية الآخرين عندما يتم استخدام معلومات سرية بشكل غير قانوني.

أنواع الجريمة الإلكترونية

١. **جريمة إلكترونية تستهدف الأفراد ويُطلق عليها أيضاً مسمى جرائم الإنترنت الشخصية والتي تقتضي على الحصول بطريقة غير شرعية على هوية الأفراد الإلكترونية كالبريد الإلكتروني وكلمة السر الخاصة بهم وكما تمتد لتصل إلى انتحال الشخصية الإلكترونية وسحب الصور والملفات المهمة من جهاز الضحية لتهديده بها وإخضاعه للأوامر، كما تُعتبر سرقة الاشتراك أيضاً من الجرائم ضد الأفراد.**

٢. جريمة إلكترونية تستهدف الملكيّة يستهدف هذا النوع من الجريمة الجهات الحكوميّة والخاصة والشخصية ويركّز على تدمير الملفات الهامة أو البرامج ذات الملكية الخاصة ويكون ذلك عبر برامج ضارة يتم نقلها إلى جهاز المستخدم بعدة طرق من أبرزها الرسائل الإلكترونية

٣. جريمة إلكترونية تستهدف الحكومات وهي هجمات يشنّها القراصنة على المواقع الرسميّة الحكومية وأنظمة شبكاتها والتي تركز جل اهتمامها على القضاء على البنية التحتيّة للموقع أو النظام الشبكي وتدميره بالكامل ومثل هذه الهجمات في الغالب يكون الهدف منها سياسيّاً.

٤. النصب والاحتيال الإلكتروني.

٥. الجرائم السياسية الإلكترونية والتي تركز على استهداف المواقع العسكرية لبعض الدول لسرقة المعلومات التي تتعلّق بأمن الدولة.

٦. سرقة المعلومات الموثّقة إلكترونياً ونشرها بطرق غير شرعيّة

٧. جرائم الشتم والسبّ والقدح.

٨. جرائم التشهير ويكون هدفها الإساءة لسمعة الأفراد.

٩. جرائم الاعتداء على الأموال أو الابتزاز الإلكتروني.

١٠. الوصول إلى مواقع محجوبة.

١١. الإرهاب الإلكتروني.

١٢. الجرائم الجنسية الإلكترونية.

١٣. الجرائم المالية (مؤسسات مصرفية ومالية وبنوك)