كمخترق أريد أن ادخل إلى النظام أول ما أفكر فيه هو اسم المستخدم الذي يأتي مع النظام **preset account**، بالاضافه إلى أن اغلب أنظمه ويندوز يكون فيها اسم المستخدم الخاص بالمدير هو **administrator** وبدون باسورد، وللأسف الكثير من المستخدمين يتركون هذا الحساب بدون تغيير، وفي هذه الحالة الدخول إلى النظام أمر في منتهى البساطة وسوف اشكر الشركة المنتجة على هذه لصنيعه التي لا تنسى ☺ .

للأسف المستخدم طلع عامل حسابه ومغير الباسورد، اذا سأبحث عن طريق أخر وهو البحث عن اسم المستخدم والباسورد يعني تخمينه، في الأفلام والمسلسلات الأمر سهل للغاية، دقيقه أو اثنين ويتم الكشف عن هذا الباسورد ويتم الدخول إلى النظام، لكن الحقيقة تختلف كثيرا، ربما اذا بحثت في المكتب تجد بعض الأوراق مكتوب عليها الباسورد (أيضا هذه في الأفلام فقط) .

حسنا، على العموم هناك طريقه تستخدمها الكثير من الجامعات والمؤسسات وهي اسم المستخدم هو نفسه اسم الباسورد، وقد حصل هذا الأمر معي في الجامعة ودخلت إلى النظام، كان اسم المستخدم والباسورد عبارة عن اسم الشركة المصنعة للشاشة، مكونه من ثلاث حروف، طبعا بعد العديد من المحاولات البائت بالفشل، ولم انتبه إلى انه الباسورد مكتوب في أسفل الشاشة.

حسنا ، في حال اسم المستخدم لم يكن هو الباسورد ، ماذا افعل ؟ مع الأخذ بالاعتبار إني اعرف اسم المستخدم ، لا توجد طريقه إلا بالتخمين حول الباسورد ، اسم الزوجة ، رقم الهاتف ، تاريخ الميلاد ، اسم الحبيبة ، مممم مشكله أليس كذلك ! بالطبع لا ، فهناك الكثير من البرامج تقوم بعمليات التخمين نيابة عنك **password cracker** ، وفي حاله الباسورد ضعيف ، سوف تدخل إلى النظام في خلال دقائق .

هناك برنامج اسمه **l0phtCrack** يستخدم من قبل مدراء الانظمه ، وظيفته تغيير الباسودرات المستخدمة في الشبكة ، (بالطبع في حال المدير يستطيع ذلك ، الكراكر يفعلها أيضا)

نوع أخر من أنواع الهجوم هو تجاوز نظام التشغيل ، وهو يتطلب بعض الخبرة في هذا المجال ، مثلا Data Recovery Attack ، وهنا سوف يقوم بقراءة الهارديسك بت بت وتجميعها لبناء الملف الأصلي ، وهذه البرامج الغرض منها ليس للهجوم ولكن الكراكرز هم الذين استفادوا منها فاغلب برامج استعاده البيانات يتم استخدامها من قبل المختصين في استرجاع البيانات ، مثلا خرب عليك النظام System Crash أو حدث Bad Sector في الهادريسك الخاص بك ، كل ما عليك (في حال انك مستخدم) الذهاب إلى خبراء استرجاع البيانات ، وهو سوف يستخدموا هذه البرامج لاستعاده بياناتك . نفس الأمر سوف يقوم المخترق باستخدام هذه البرامج لتجاوز نظام التشغيل..

نوع أخر من الهجوم وهو الهجوم على الذاكرة Memory Reconstruction Attack ، في البداية عندما نتعامل مع برنامج ما بالطبع سوف تكون جميع التعلميات موجودة في الذاكرة ، وسوف تكون هناك اشاره في الموقع المحفوظ فيها تعليمات البرنامج ، وعندما ننتهي من البرنامج ونقوم بإغلاقه ، فسوف يقوم مدير الذاكرة في النظام بحذف هذه الاشاره دون حذف المحتوى الحقيقي لها ، بالطبع من الممكن أن يأتي أي برنامج أخر ويحل في نفس الموقع ويحذف تلك البيانات ، ومن الممكن أن تكون موجودة .. هجوم الذاكرة يقوم بعمل مسح للذاكرة وكتابه تلك البيانات التي لا توجد عليها اشاره ، (لا اعلم كم يتم تطبيق هذا الهجوم على ارض الواقع) .

مشكله أخرى ، وهي الذاكرة الظاهرية ، اغلب انظمه التشغيل تحتوي على Virtual Memory