

بسم الله الرحمن الرحيم

الحمد لله رب العالمين ونصلي ونسلم على من لا نبي بعده
المبعوث رحمة للعالمين سيدنا محمد وعلى آله وصحبه أجمعين وبعد
تم تصميم هذا الكتاب لمساعدة أخواني الذين يعانون من نسيان كلمات المرور وما
يترتب على ذلك من المشاكل خاصة مع المستخدمين الجدد للكمبيوتر والذين تنقصهم
الخبرة وأسأل من الله أن يأجرني على هذا الجهد المتواضع
ونبدأ شرحنا بسم الله

يوجد عدة طرق لكسر كلمة السر التي نطالب بكتابتها عندما نريد الدخول
للويندوز للوصول إلى سطح المكتب

* يمكن كسر كلمات المرور في وندوز xp بعدة طرق وهي كالتالي:

- 1- نقوم بعمل ريسيت للكمبيوتر وأول ما يبداً الوندوز في الإقلاع نضغط على المفتاح
f8 ونختار الأمر safe mode ونضغط المفتاح أن تريظهر لنا مستخدم جديد
هو administrator نقوم بفتحه ونظهر لنا رسالة تخبرنا بأنه تم فتح الكمبيوتر في الوضع
الآمن نختار نعم فنلاحظ إن الألوان متغيرة وليست طبيعية بعدها نقوم بالدخول على
حسابات المستخدم ونختار الحساب المراد تغيير كلمة المرور له فنلاحظ انه لم يطلب
كلمة السر القديمة وإنما نقوم بتغييرها مباشرة وبعدها نعيد التشغيل ونفتح بكلمة
المرور الجديدة التي قمنا بإصلاحها بدلاً من الكلمة القديمة أو نقوم بحذف كلمة السر
فنجد أنه لم يطلب كلمة السر القديمة
- 2- الطريقة الثانية: نفتح جهاز الكمبيوتر وأول ما يطلب كلمة المرور نقوم بالضغط على
المفتاح ctrl+alt+del

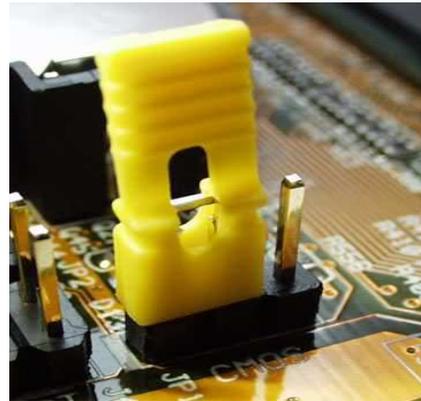


يظهر لنا مربع مكتوب اسم المستخدم ونحت كلمة المرور نقوم بحذف اسم المستخدم
ونكتب بدلاً منه الكلمة التالية administrator ونترك كلمة السر فارغة لأن دخل كلمة سر
ثم أنتر فيتم فتح ال administrator بعدها ندخل على حسابات المستخدم ونغير كلمة
المرور نكتب كلمة مرور جديدة من دون ما يطلب كلمة السر القديمة وال

- administrator دائما لا يطلب كلمة مرور لان الويندوز لا يضع كلمات مرور من تلقاء نفسها اذ كان هناك احد قد عبث بالويندوز
- ٣- عند ما يطلب الويندوز كلمة المرور ندخل الكلمة التالية award_sw وهذه الكلمة نسبة تجاهها ٩٥ بالمائة
- ٤- نقوم بفتح الكيس وننزع بطارية السيموس الموجودة داخل الكيس

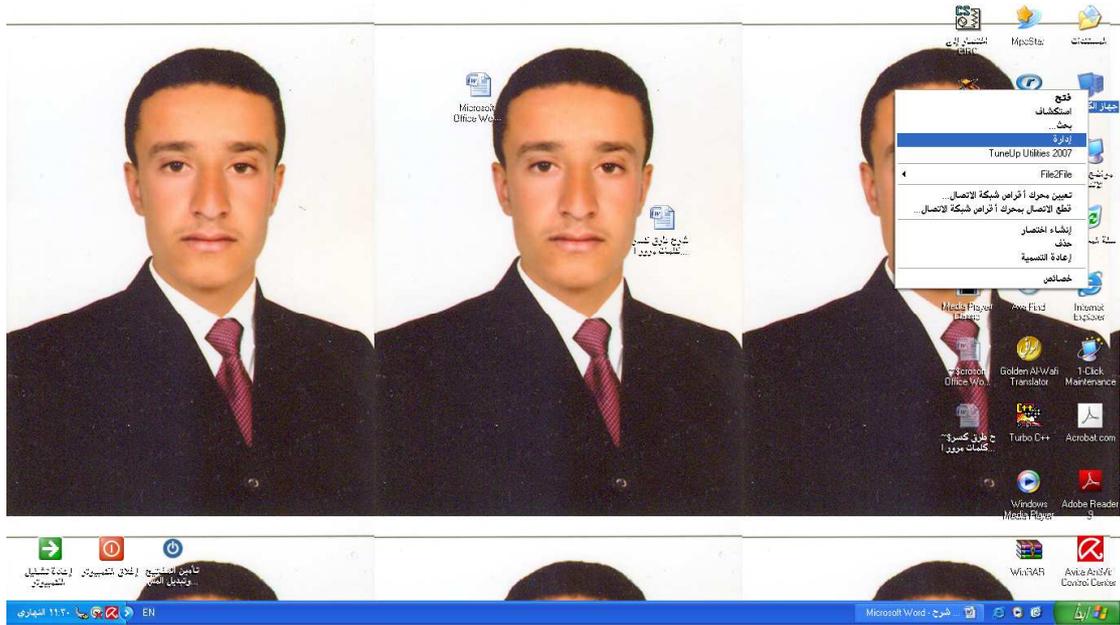


ويوجد بجانبها اثنين جناير نقوم بالتوصيل بينهما بسلك معدني لمدة ١٥ ثانية ليتم تفريغ الشحنة

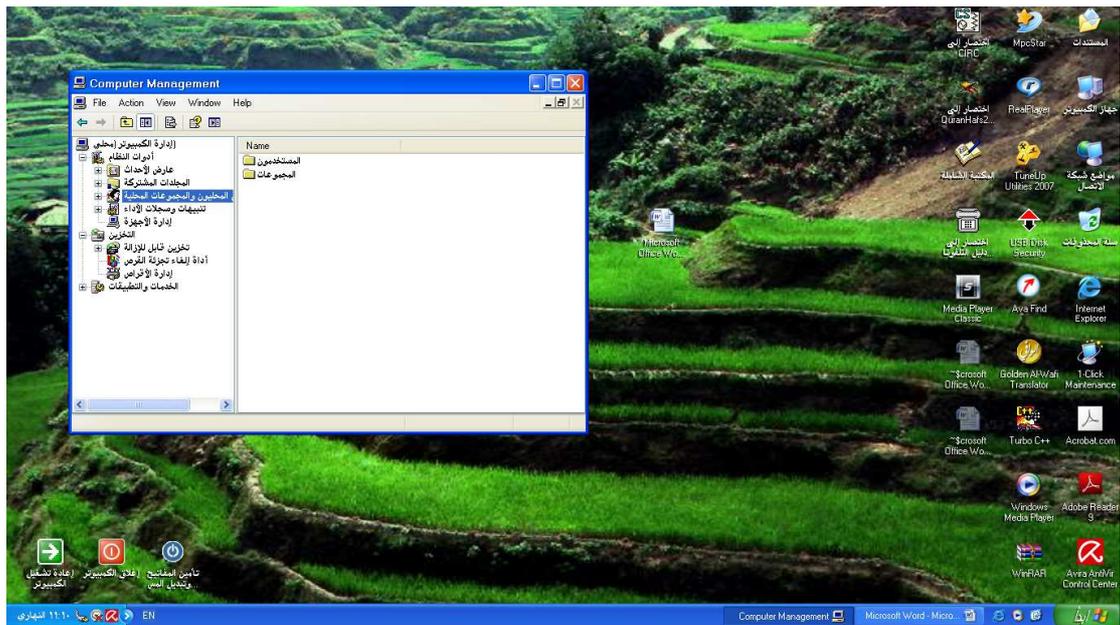


وننتظر لمدة نصف ساعة قبل تركيب البطارية ثم نعيدها فنجد ان كلمة السر قد ازيلت

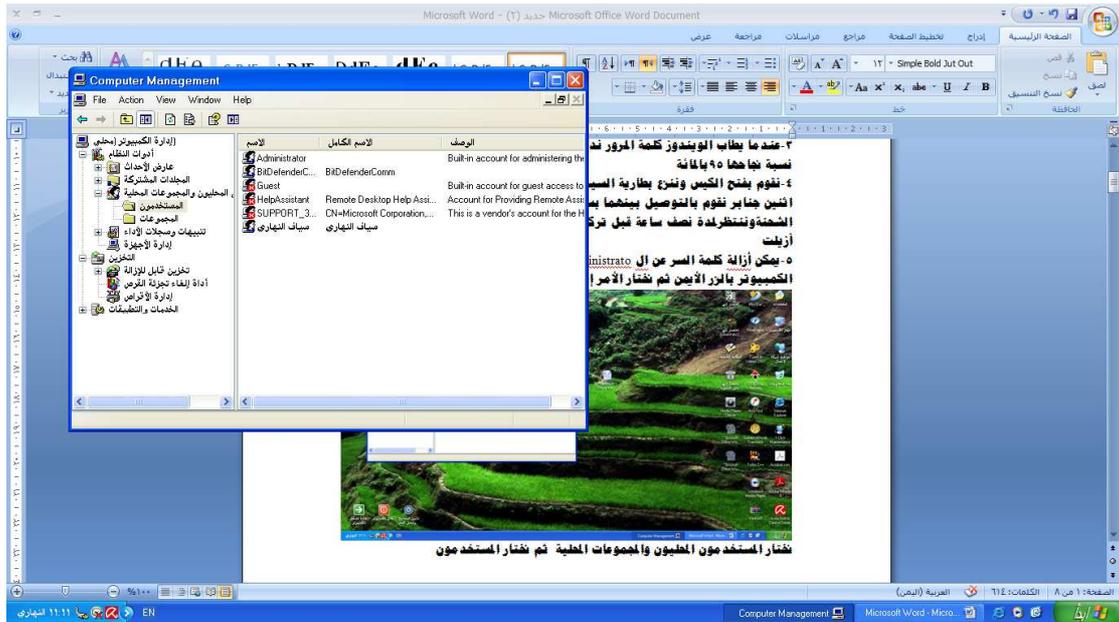
٥- يمكن ازاله كلمة السر من ال administrato بالطريقة التالية نقوم بالنقر على جهاز الكمبيوتر بالزر الايمن ثم نختار الامر ادارة ونتبع الصورة التالية



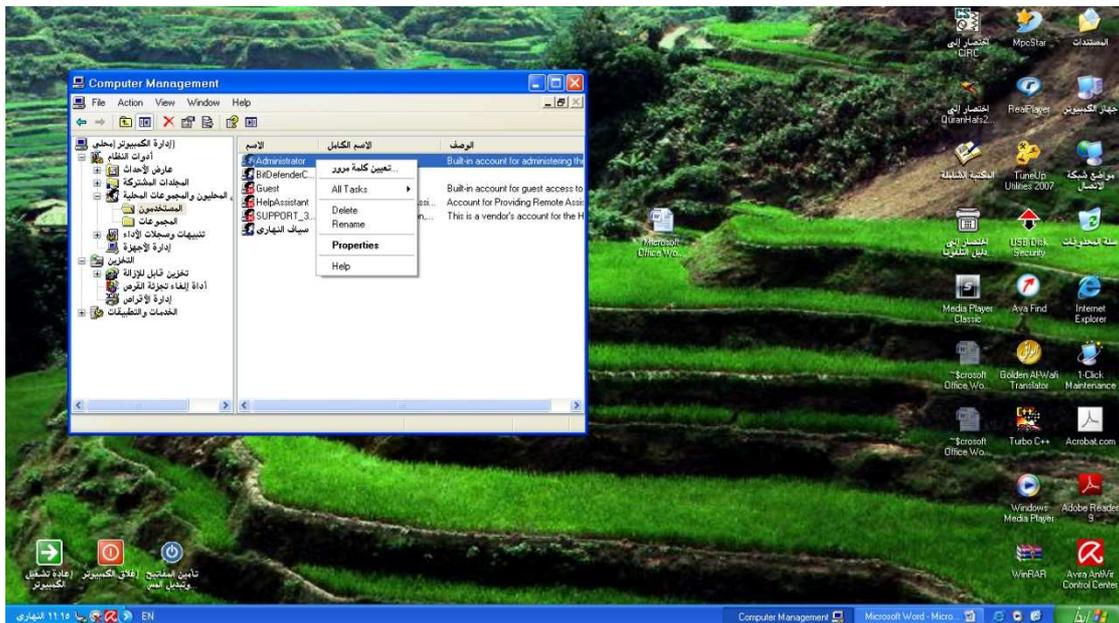
ثم نختار الأمر المستخدم من المليون والمجموعات المحلية



نختار المستخدم من



فيظهر لنا جميع حسابات المستخدم مين نقوم بالنقر على الحساب المراد تعطيل كلمة السر عنه أو تغييرها ننقر عليه بالزر الأيمن تظهر لنا القائمة التالية



نختار الأمر الأول تعيين كلمة مرور ثم متابعة ثم ندخل كلمة مرور جديدة إذا اردنا تغيير كلمة المرور أو المتابعة لتعطيلها مع العلم إن هذه الطريقة لا يمكن استخدامها الا اذا كان الكمبيوتر مفتوح

الطريق الخامسة وهي طريقة حرفية بالشرح والصورة عن طريق **hiren's boot**

٦- شرح طريقة كسر كلمة المرور للمستخدم administrator وغيره باستخدام hiren's boot cd

شرح طريقة كسر كلمة المرور للمستخدم administrator وغيره باستخدام hiren's boot cd

مقدمة:

كثيراً ما نتعرض لنسيان كلمة مرور المستخدم التي يطلب كتابتها عند الدخول لسطح المكتب و يمكن كسرها بالدخول إلى المستخدم administrator الذي يكون في العادة مخفياً و قليل من الناس يضع له كلمة سر

وأريد أن أذكر المستخدمين الجدد على الكمبيوتر أو من ليس لديه خبرة كبيرة بأن لا يعتاد قراء المواضيع التي يعرف عنها شيئاً أو يعرفها فقط بل يجب أن تقرأ ما لا تعرفه من مواضيع حتى ترتقي و يزداد رصيدك العلمي

لكن ماذا لو:

-ماذا لو كان المستخدم administrator محمي بكلمة مرور ؟
-ماذا لو كان نظام التشغيل هو windows vista و لا تنفع معه الطرق العادية ؟

الإجابة على الأسئلة في الشرح التالي:

أسلحة العمل:

في هذه الحالة يمكن الاستعانة بأسطوانة الصيانة الرهيبة hiren's boot و يوجد بها البرنامج في الإصدار ١٠ من اسطوانة الهيرنز بوت الشهيرة

الإصدارات التي تعمل عليها الطريقة:

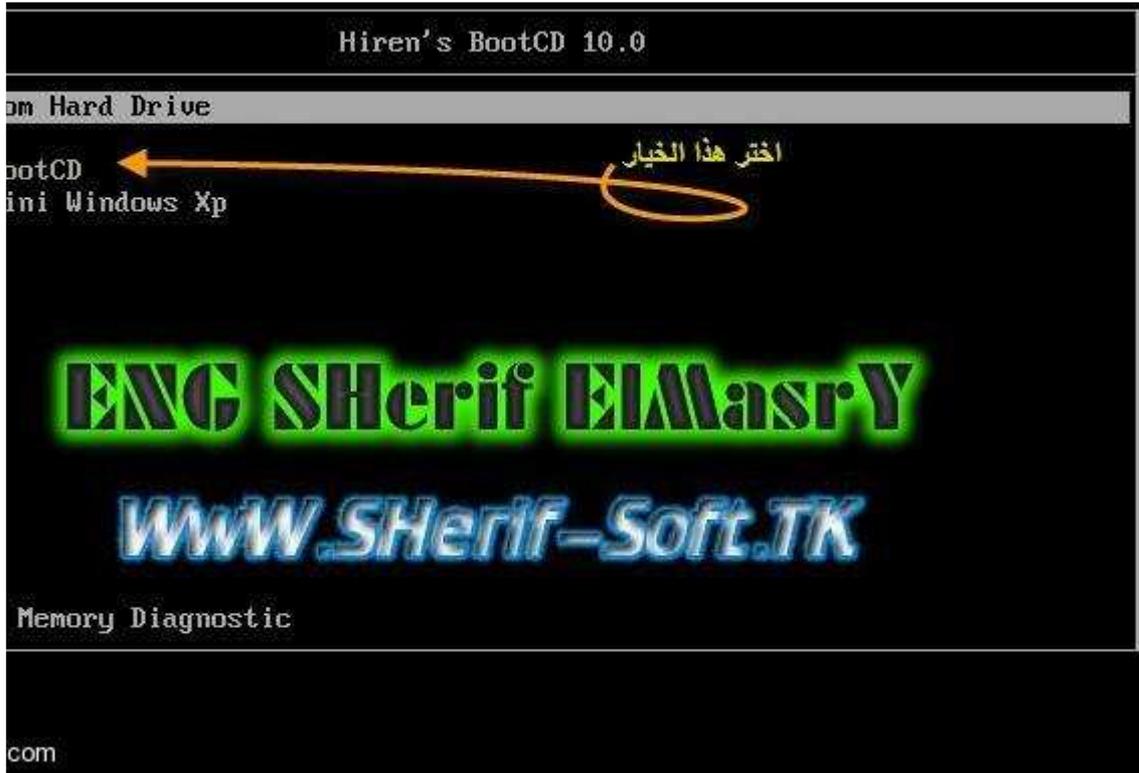
كافة إصدارات ويندوز
windows xp
windows vista
windows seven7

الشرح:

الطريقة الأولى نجعل الإقلاع من السيدي و يم الإقلاع من السيدي بالطريقة التالية يتم إعادة تشغيل جهاز الكمبيوتر بعمل reset للجهاز أول ما يبدأ الجهاز بالإقلاع نقوم بالضغط على المفتاح delete+f2 باستمرار فتظهر لنا النافذة التالية
إذا دخلت على شاشة البايوس تنقل عن طريق الأسهم كما في الصورة التالية



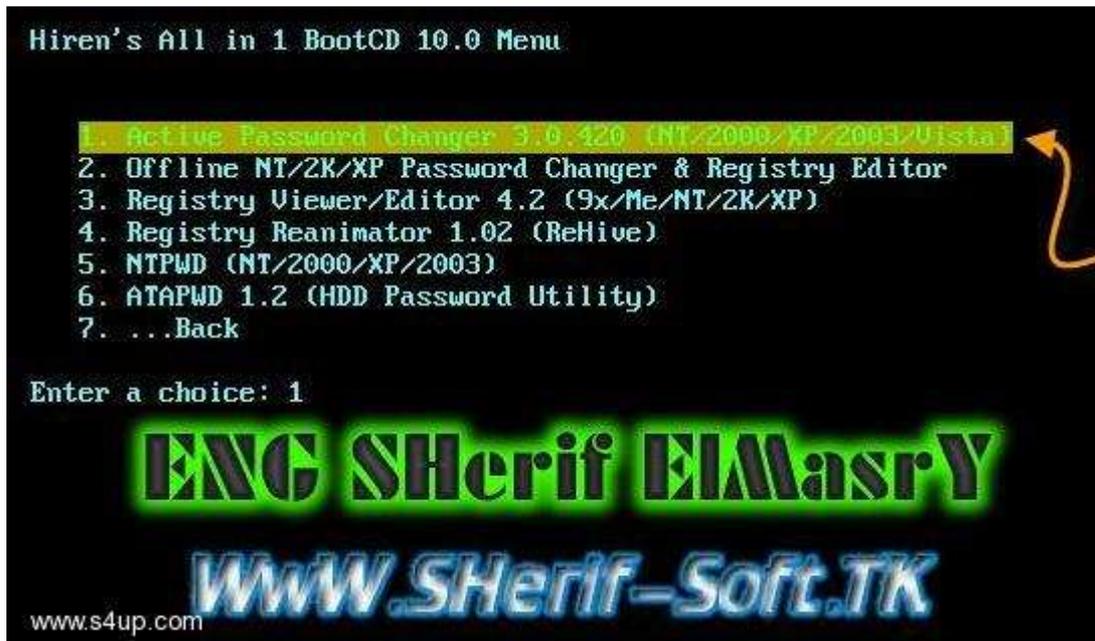
نضع القرص و نقله عن طريقه حتى تظهر النافذة التالية



ثم تظهر أقسام برامج الاسطوانة 10 Hiren's boot cd



نختار الخيار رقم 3 كما هو موضح في الصورة أعلاه
ثم تظهر لنا قائمة بالبرامج في هذا المجال نختار 3 active password changer



في النافذة التالية نكتب رقم ١ ثم نضغط enter



Your choice: [1]

نضغط بعد ذلك enter كما هو مطلوب في الصورة التالية

```
Active@ Password Changer v.3.0 (build 0420)

Logical drives list:
-----
No|HDD|Partition| Type   | Disk Label| Size (Mb)
-----
0 (0)      (0)      NTFS           16370

ENG SHerif ElMasr-Y
WWW.SHerif-Soft.TK

Press Enter to continue...
-----
Press Esc to exit

(C) Active Data Recovery Software      www.password-changer.com
Licensed by: anthony torkelson, Turnkey Systems, tonyt@tk.net
```

يبدأ بعد ذلك البحث عن أنظمة التشغيل الموجودة على كمبيوترك و التي فيها مستخدمين

```
Active@ Password Changer v.3.0 (build 0420)

MS SAM Databases at disk(0)partition(0)Label<>, FS:NTFS
-----
No| MS SAM Database Path
-----
Please wait:\

ENG SHerif ElMasr-Y
```

ستكون النتيجة مشابهة لما يلي في حال وجود نظام تشغيل واحد

SAM Databases at disk(0)partition(0)Label<>, FS:NTFS

No | MS SAM Database Path

0 \WINDOWS\SYSTEM32\CONFIG\sam

ENG SHerif ElMasr·Y

WWW.SHerif-Soft.TK

There is one MS SAM database detected.
Press Enter to continue...

Press Esc to exit

4up.com

بعدها نصل إلى الخطوة المهمة و هي قائمة بأسماء المستخدمين الموجودين على الجهاز بما فيهم administrator وإذا أردنا مثلا الحصول على أسم المستخدم الخاص بنا فإنه يأتي دائما بحروف غير مفهومة لأننا غالبا ما نضع أسم المستخدم الخاص بنا بأسمائنا وبحروف عربية لذلك حسابات المستخدمين المكتوبة بالعربية تأتي بحروف غريبة وغير مفهومة لكن نحن يهمنا الذي أمامه علامة [x] نقوم باختياره والضغط على حرف y

Active@ Password Changer v.3.0 (build 0420)

USER LIST

path: \WINDOWS\SYSTEM32\CONFIG\sam
disk(0)partition(0)Label<>, FS:NTFS

Total users: 0004

ID	User Name	Description
01f4	Administrator	Built-in account for administering the comp
01f5	Guest	Built-in account for guest access to the co
03e8	HelpAssistant	Account for Providing Remote Assistance
03ea	SUPPORT_388945a0	This is a vendor's account for the Help and

WWW.SHerif-Soft.TK

choice: [_]

ENG SHerif ElMasr·Y

(C) Active Data Recovery Software

www.password-changer.com

Consented by: anthony torkelson, Turnkey Systems, tonyt@tk.net

في قسم your choice نكتب الرقم الموافق للمستخدم الذي نريد إزالة كلمة السر التي عليه و ذلك كما في الأرقام التي في القائمة فوق في نفس الصورة

```
Active@ Password Changer v.3.0 (build 0420)

User's Account parameters:

Database: (0)(0)<>\WINDOWS\SYSTEM32\CONFIG\sam
Administrator's name is "Administrator" (RID=0x000001F4)

: ""
ion: "Built-in account for administering the computer/domain"
ing: Change to:
  [ ] User must change password at next logon
  [X] Password never expires
  [ ] Account is disabled
  [ ] Account is locked out
  [X] Clear this User's Password

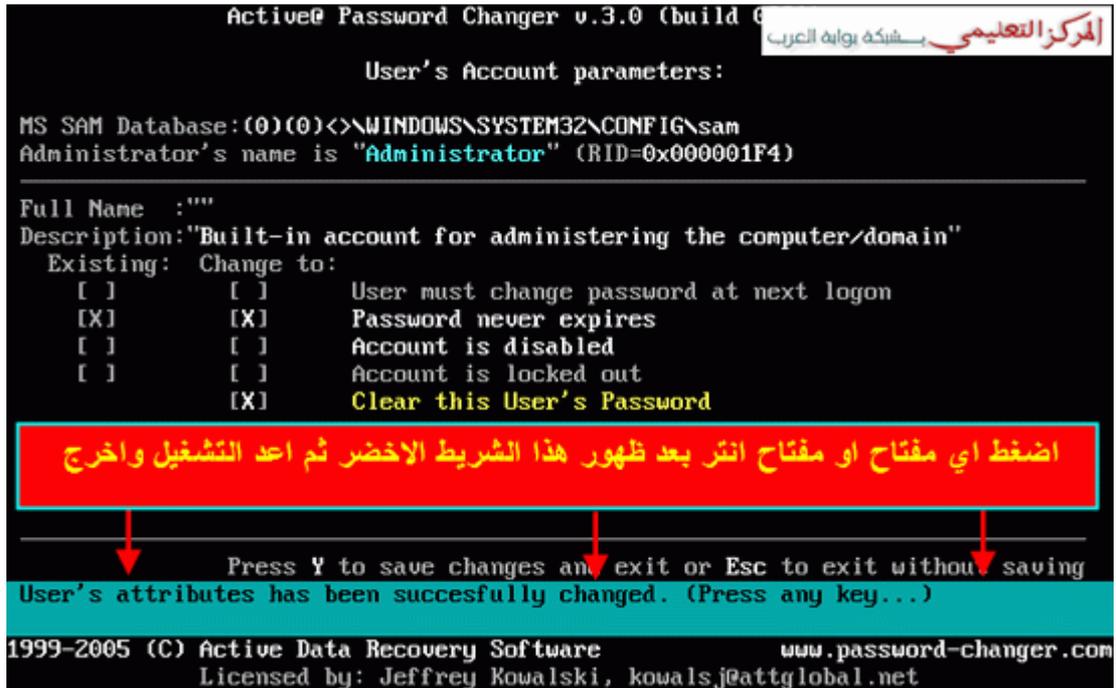
ENG SHERIF ELMASRY

Press Y to save changes and exit or Esc to exit without saving

(C) Active Data Recovery Software www.password-changer.com
Licensed by: anthony torkelson, Turnkey Systems, tonyt@tks.net
```

لاحظ الخيارات المفعلة تلقائياً في الأعلى و هي ما يهمنا صراحة و التي عليها علامة x و الآن نضغط على زر y كما هو مبين

بعد ذلك تظهر الرسالة الجميلة و التي تخبرنا بأنه تم إزالة كلمة السر للمستخدم المحدد العملية كما لاحظتم ليست صعبة جربوها و ستنتج معكم بالتأكيد..

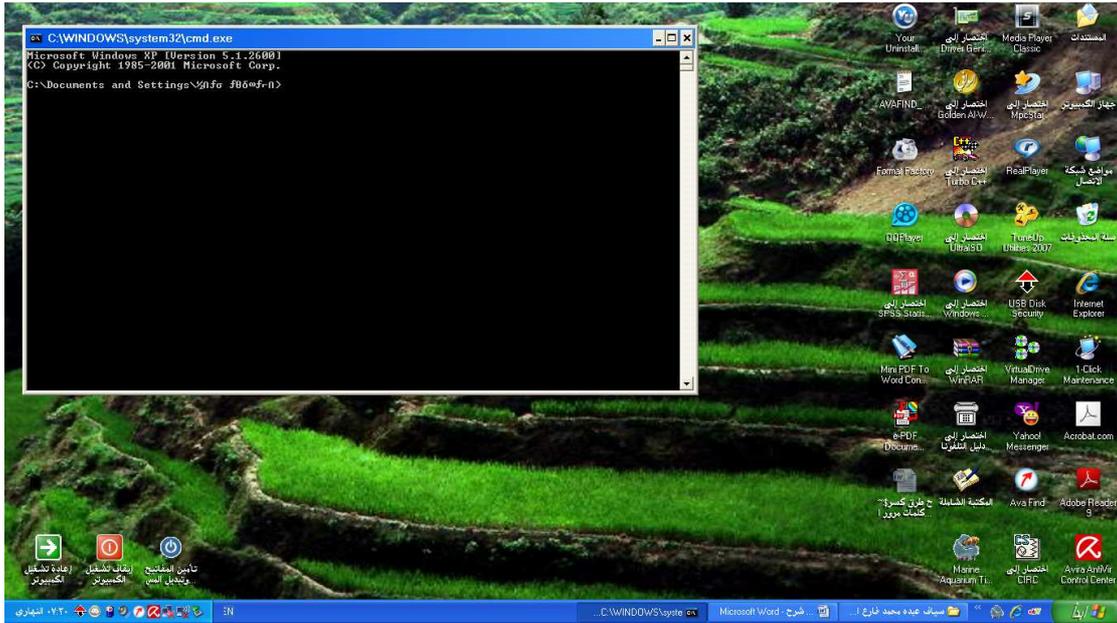


الآن ظهرت الرسالة السابقة تخبرك بأنه قد تم كسر كلمة المرور بالتأكيد أضغط أي مفتاح للخروج نرجو أن تكونوا قد استفدتم من هذا الشرح كما نرجو ممن استفاد من هذا الكتاب أن ينشره ليستفيد منه غيره نرجوا منكم المعذرة ان كان هناك خطأ أو تقصير في الشرح أو عدم وضوح الفكرة

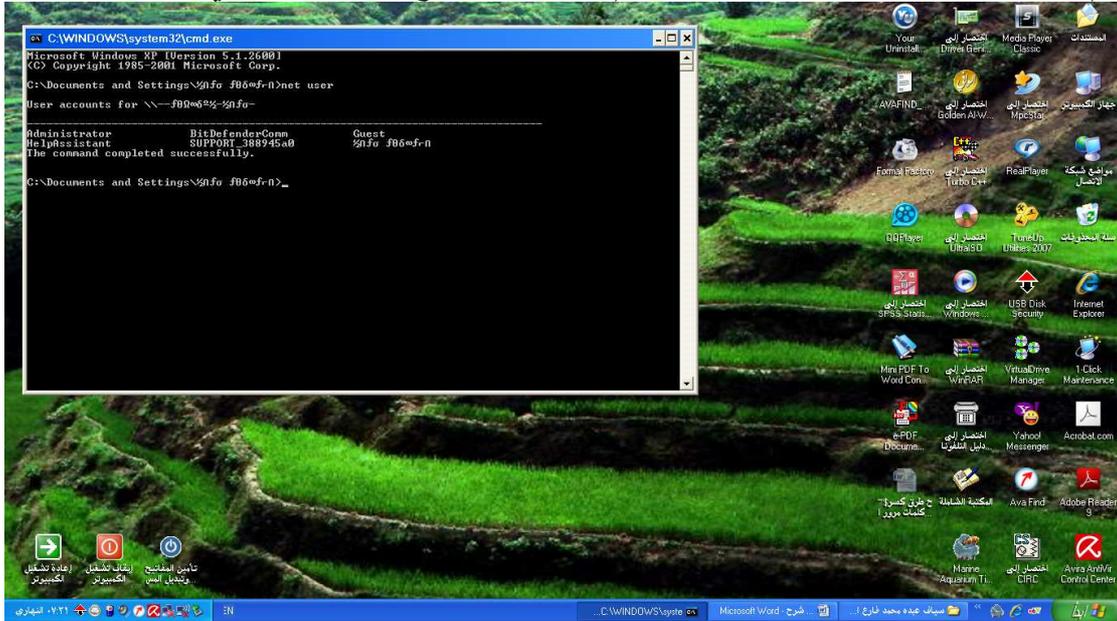
٧- الطريقة السابعة وهي متاحة عندما نكون داخل الويندوز حيث نقوم بكسر كلمة السر عن طريقها حيث نقوم بفتح محث الدوس من قائمة ابداء تشغيل نكتب الأمر cmd ثم موافق كما في الصورة التالية



يفتح لنا محث الدوس كما في الصورة التالية



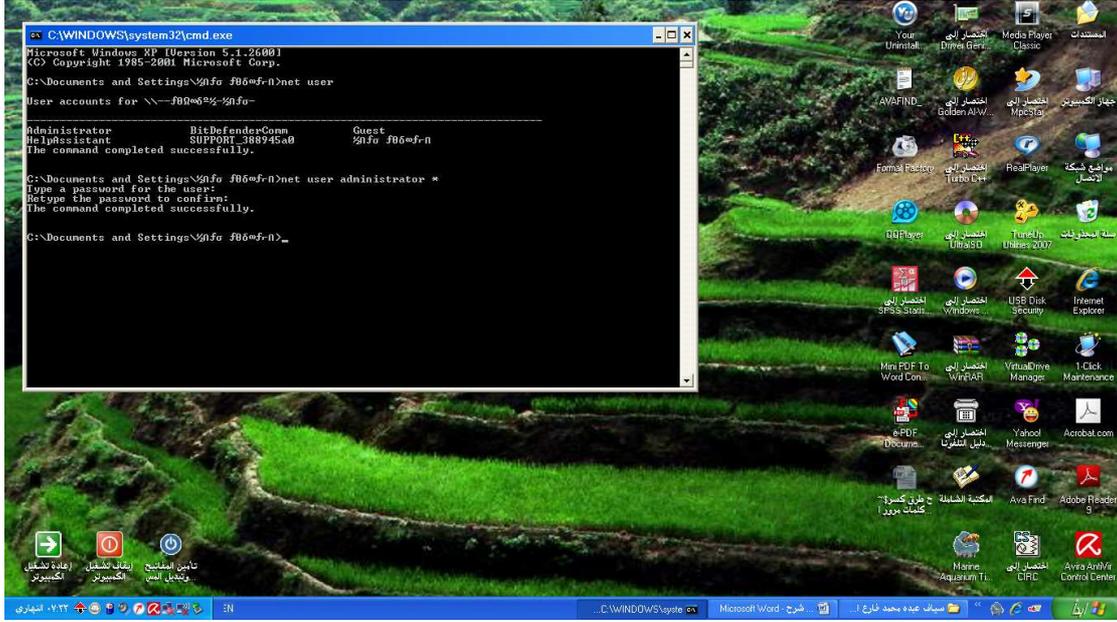
ثم بعد ذلك نكتب الأمر **net user** ثم نضغط المفتاح **enter** كما في الصورة التالية



ثم بعد ذلك تظهر لنا حسابات المستخدمين كما شاهدنا في الصورة السابقة نقوم بكتابة الأمر **net user** ثم أسم الحساب ثم رمز النجمة مع مراعاة الفراغات كما هو في الصورة التالية فمثلا لو أردنا أن نكسر كلمة السر للحساب الافتراضي الأدمينستراتور نكتب السار التالي * **net user administrator**

ثم نقر **Enter**

ثم نقر المفتاح **Enter** ثلاث مرات متتاليات كما في الصورة التالية فنكون بذلك قد تخلصنا من كلمة السر للحساب



وفي الأخير تقبلوا خالص تحياتي أخوكم في الله / سيف النهاري
ونرجو منكم الدعاء

اليمن_ذمار ت ٧٧٠٢٧٢٧٤٥-٧١٤٧٢٧٢٧١
البريد الإلكتروني

Sayafabdu@yahoo.com