طرق حماية الملفات وطرق كشفها

النسخة الثانية.

الكاتب: التنين الجامح

كتب في : 5/2009

بسم الله الرحمن الرحيم

الفهرس:

المقدمة :

بسم الله الرحمن الرحيم وأفضل الصلاة وأتم التسليم على سيدنا محمد وعلى آله وصحبه وأجمعين

أما بعد :

- بعون الله تعالى تم الانتهاء من إعداد هذا الكتاب بحلته الجديدة بعد تصليح بعض الأخطاء التقنية واللغوية وإضافة بعض الأمور.

- أهدي هذا العمل المتواضع لكل مسلم يقرأ اللغة العربية .

- إذا أعجبك الكتاب أو استفدت منه فلا تنسني من دعوة صالحة في ظهر الغيب فتنفعني يوما ما .

- في هذا الكتاب أعرض كل طريقة بدرس و بنهايته طريقة الكشف وكل مجموعة دروس بمستوى، والمستوى حسب صعوبة التطبيق والفهم ولكن كلها سهلة إن شاء الله، و بإمكانك الدمج بين الطرق حسب حاجتك ومدى فهمك للطرق.

- لقد وضعت قسما بسيطا للمهارات المطلوبة لكي تستطيع التعامل مع الكتاب في حال كانت خبرتك التقنية ليست جيدة كفاية، ولكي لا أشرح الأمر كل مرة.

- لقد وضعت درسا عن كيفية إنشاء كلمة مرور قوية .

- لقد وضعت جميع الملفات التي سوف تنشئها أثناء الكتاب في ملف مرفق اسمه Attach.zip لكي إذا واجهت صعوبة في إنشاء الملف تجده جاهزا وتتعلم من خطأك .

- الكتاب عمل بشري فلابد من وجود أخطاء به ولكنني حاولت قدر المستطاع تلافيها وخصوصا التقنية منها، فالكمال لله وحده.

قسم ومهارات مطلوبة :

- إظهار الملفات المخفية: اذهب إلى أدوات (موجودة في شريط قوائم المجلد)ثم خيارات المجلد ومنه قائمة عرض إظهار الملفات و المجلدات المخفية.

- إظهار ملفات النظام المخفية: تكون بالذهاب إلى خيارات المجلد ثم عرض ثم إظهار ملفات النظام.

- إظهار لواحق الملفات: تكون بالذهاب إلى خيارات المجلد ثم عرض ثم إزالة إشارة صح أمام إخفاء ملحقات الملفات....

- مصطلح ملف دفعي : هو ملف فيه أوامر الدوس DOS ويمكن إنشاءه بواسطة ملف نصي TXT ثم تغيير اللاحقة إلى .bat ويمكن التعديل عله بعد صناعته بالضغط باليمين على الملف الدفعي ثم تحرير .

كلمة مرور أكثر قوة:

١) أن تكون كلمة المرور طويلة جدا، لأن البعض يجعل خانات كلمة المرور عبارة عن خمس أو سبع خانات و الأفضل أن تجعلها أكثر من عشرين خانة.

٢) أن تحتوي كلمة المرور على خليط من الرموز ، الأرقام و الحروف مثال
١٩MYO~QM/+-^%BO*ZP37

٣) أن لا تضع كلمة المرور بسيطة الإدخال على لوحة المفاتيح حتى وان اشتملت على النقطتين السابقتين ١ و ٢ لأن البعض يجعل كلمة المرور بهذا الشكل !@#$%^&*QWERTYUIOP123
لا حظوا أدخلنا الرموز أولا بالترتيب لأنها في الجزء الأعلى من لوحة المفاتيح ثم أدخلنا الأحرف التي أسفل من الرموز في لوحة المفاتيح أيضا بالترتيب ثم ادخلنا الأرقام مرتبة ، والأفضل التنقل في جميع أجزاء لوحة المفاتيح بشكل عشوائي حتى يصعب تخمينا أو قد يتمكن شخص من الحصول على كلمة المرور بضربة حظ. !

٤) أن لا تكون كلمة المرور عبارة عن أرقام تسلسلية أو أرقام عشوائية قد تراها أنت صعبة لكن سهلة عندما يكون هناك برنامج لإنتاج الأرقام سواء تسلسلية أو عشوائية مهما طالة الخانات .
والبعض يستخدم أرقام تسلسلية مثل ١٢٣٤٥٦٧٨٩ أو ١٢٢٣٣٣٤٤٤٤ أو ١٠٢٠٣٠٤٠٥٠٦٠
والكثير من هذه الأمثلة والبعض يستخدم كلمات مرور بهذا الشكل بكل ثقة. !

٥) ألا تشتمل على اسم المستخدم أو اسمك الحقيقي.

٦) ألا تشتمل على كلمة أو اسم شائع أو كثير الاستخدام.

عند اتباعك لهذه المواصفات سوف تحصل على كلمة سر أكثر قوةً إن شاء الله.

المستوى المبتدأ :

الدرس الأول : إخفاء ملف أو مجلد

لإخفاء أي ملف أو مجلد اضغط بالزر اليمين عليه ثم اختر خصائص

انظر إلى الأسفل سوف تجد السمات ومن بينها مخفي

أشر على هذا المربع بإشارة صح ثم اضغط موافق سوف تلاحظ أنه اختفى

طريقة الكشف:و تكون بطريقة إظهار الملفات المخفية أو إذا نظرنا إلى شريط المعلومات فإنه يكتب عدد الملفات المخفية .

الدرس الثاني : إخفاء مجلد

أولا: اضغط باليمين ثم خصائص ثم تخصيص ثم تغيير الرمز و اختر رمز فارغ(يوجد أربع منها) واختر موافق ثم موافق.

ثانيا:اضغط باليمين ثم تغيير الاسم

اضغط ALT و٠١٦٠ ثم اترك زر ALT (الأرقام يجب أن يكونوا من القسم اليميني من لوحة المفاتيح) و يطلق عليهم اسم Numpad

طريقة الكشف: تكون ب عد الملفات ومقارنتها مع شريط المعلومات أو بالضغط على الفأرة وتحريكها في المجلد .

الدرس الثالث:جعل الملف مجهول الهوية.

اذهب إلى الملف المطلوب ثم إعادة التسمية وأزل اللاحقة (مثل rar.).

الآن الملف لن يفتح إلا إذا كتبت اللاحقة مرة أخرى.

طريقة الكشف:تعتمد على التجريب والتفكير فقط ولا يوجد أي طريقة أخرى .

إذا كانت ملفاتك غريبة اللاحقة سوف يكون من الصعب كشفها ،أما إذا كان من الملفات المضغوطة فإنها الأسهل لأن الجميع يجربون لواحق الضغط في البداية.

الدرس الرابع:حماية الملفات الهامة بعد الحذف.

أولا: اذهب إلي الملف المطلوب وغير امتداده إلى TXT.

ثانيا: انتظر قليلاً حتى تفتح المفكرة وسوف تجد بداخلها كود ، قم بإضافة أي شيء أو حذف.

ثالثا: احفظ التغييرات ، واخرج.

رابعا: بعد الانتهاء لن تستطيع مشاهدة ما بداخل الملف قم الآن بحذف الملف بالطريقة التقليدية.

نصائح وإرشادات قبل وبعد إجراء التعديلات على الملف المراد حذفه :

١ -انتبه بعد التعديل على الملف لن تتمكن من فتح مره أخرى حتى لو قمت بحذف ما كتبته .

٢ -إذا كان حجم الملف كبير قد لا يفتح بالمفكرة لذلك عليك فتحه ببرامج متطورة أكثر مثل++NotePad

٣ -البرامج التي تقوم باسترجاع الملفات المحذوفة سترجعه لكن لن يتمكن أحد من فتحه.

٤ -يفضل بعد عمل التعديلات داخل كود الملف تغيير اسم الملف وصيغته إلى أي اسم من أسماء ملفات النظام قبل حذفه.

المستوى المتوسط:

الدرس الأول:قفل مجلد

أنشأ ملف دفعي وضع فيه الكود التالي

```
cls
@ECHO OFF
title Folder Private
if EXIST "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" goto UNLOCK
if NOT EXIST Private goto MDLOCKER
:CONFIRM
echo Are you sure you want to lock the folder(Y/N(
set/p "cho"<=
if %cho%==Y goto LOCK
if %cho%==y goto LOCK
if %cho%==n goto END
if %cho%==N goto END
echo Invalid choice.
goto CONFIRM
:LOCK
ren Private "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D"{
attrib +h +s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D"{
echo Folder locked
goto End
:UNLOCK
echo Enter password to unlock folder
set/p "pass"<=
if NOT %pass%== password here goto FAIL
attrib -h -s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D"{
ren "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" Private
```

```
echo Folder Unlocked successfully

goto End

:FAIL

echo Invalid password

goto end

:MDLOCKER

md Private

echo Private created successfully

goto End

:End
```

بالسطر رقم ٢٣ فيه عبارة باللون الأحمر"password here" استبدلها بالرقم السري الذي تحب أن تضعه، ثم احفظ الملف.

اضغط عليه فيقوم بإنشاء مجلد جديد يحمل اسم Private ،انسخ ما شئت من ملفات بداخله .. ثم ارجع مره ثانيه إلى الملف الدفعي الذي انشأته واضغط عليه سيسألك هل تريد إقفال المجلد ؟

اختر Yes ، وبذلك أصبح المجلد مخفيا .ولإعادة المجلد اضغط على الملف الدفعي واكتب كلمة السر.

طريقة الكشف:تكون من خيارات المجلد عرض ثم إظهار ملفات النظام المخفية،

وبذلك يظهر مجلد بشكل لوحة التحكم غير اسمه مع لاحقته سوف يعود مجلد عادي.

أو قم بالضغط على اليمين ثم اختر تحرير واذهب إلى مكان كلمة المرور .

الدرس الثاني:تحويل المجلد إلى مجلد من مجلدات النظام المعروفة.

ضع ملفاتك في مجلد ثم :

أولا : يجب أن يكون إظهار لواحق الملفات مفعل.

ثانيا:ضع أحد هذه الأسماء في اسم المجلد على هذا الشكل

Control Panel. {21EC2020-3AEA-1069-A2DD-08002B30309D}

هذا للوحة التحكم (يعمل على الإكس بي ، لم يعمل على الفيستا)

٣١. {645FF040-5081-101B-9F08-00AA002F954E}

أما هذا لسلة المهملات.(مع العلم أن الاسم لا يهم فقط اللاحقة هيه المهمة.)

طريقة الكشف:تكون بضغط المجلد بإحدى برامج الضغط فتظهر الملفات التي بداخلها

أو بحذف اللاحقة

الدرس الثالث:جعل أي ملف أو مجلد نظام وإخفاؤه.

انشأ ملف دفعي واكتب فيه

attrib yourfile.txt +s +h

حيث تضع بعد attrib اسم الملف و لاحقته ،و للعكس ضع – بدل +

ملاحظة:لجعله نظام فقط احذف +h .

أما بالنسبة للمجلدات فيجب أن تضع علامة التنصيص فيكون الكود على الشكل التالي

attrib "newfolder" +h +s

طريقة الكشف: تكون بإظهار ملفات النظام.

المستوى المتقدم:

الدرس الأول:إخفاء ملفات في صورة.

أولا :قم بضغط الملفات المراد إخفائها بأي برنامج ضغط ولكن يفضل أن تكون لاحقتها rar.

ثانيا :أحضر صورة بلاحقة jpg.

ثالثا: انشأ ملف دفعي واكتب فيه ما يلي

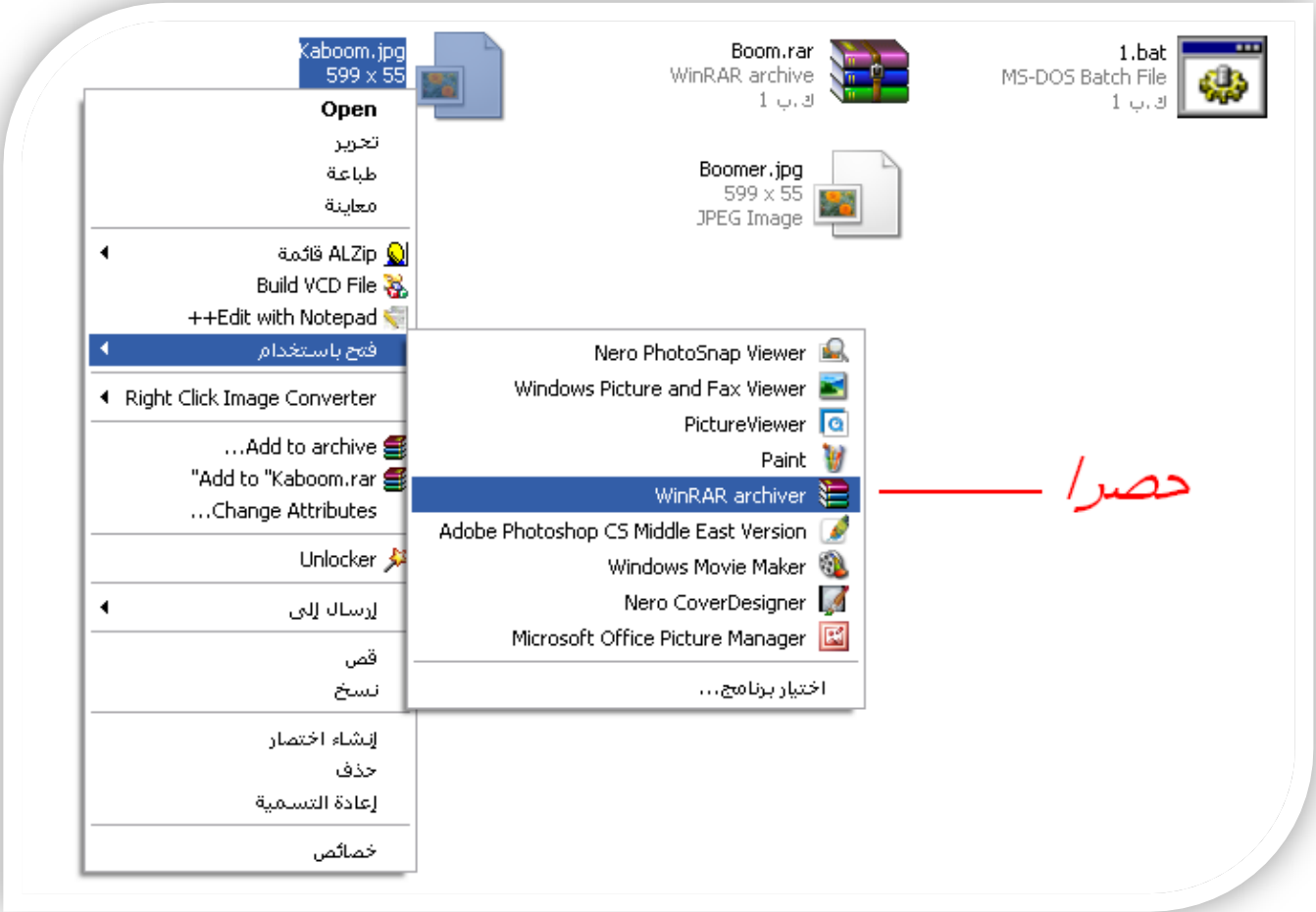
copy /b Boomer.JPG + Boom.rar Kaboom.jpg

اسم الصورة الأول يجب أن يكون موافق لاسم الصورة الموجودة وكذلك اسم الملف المضغوط

بينما اسم الصورة الثاني لا يهم فأنت حر باختياره.

رابعا:ضع كل هذه الملفات في مجلد واحد واضغط على الملف الدفعي الذي أنشأته.

وبذلك أنشأت صورة جديدة تأكد من أن الملفات موجودة فيها .



طريقة الكشف: تكون بتغيير اللاحقة إلى rar. أو فتح باستخدام واختيار برنامج الضغط.(حصرا WinRar)

كما أنه من الممكن أن يكون حجم الصورة الكبير علامة على وجود شيء مخبئ

الدرس الثاني:إخفاء ملفات في ملف وورد .

أولا: تضغط الملفات.

ثانيا: تحمل الملف المضغوط و ترميه داخل ملف الورد فيصبح هناك مثل لينك ورمز وأحيانا لا يوجد رمز.

ثالثا: اضغط عليه للتأكد من وجود الملف ثم احفظ المستند وعاود التأكد.

رابعا: اجلب صورة و ضع تعليق عليها لكي لا يشك أحد بالأمر.

خامسا: ضع الملف وسط الشاشة .

سادسا: ضع الصورة أمام الملف بطريقة عرض الصورة أمام النص.

سابعا: احمي ملف الورد بحماية التعديل فقط.

طريقة الكشف: لا يمكن كشفها إلا بمعرفة كلمة السر وهذا ليس مستحيل لأنه يوجد برامج تقوم بهذا الأمر ولكن عملها ليس بالسهل فإنها تأخذ الكثير من الوقت وقد لا تنجح في النهاية إذا كانت كلمة السر قوية.

الدرس الثالث:تحويل مجلد إلى مجلد نظام معروف وإخفاؤه .

أولا:أنشأ مجلد جديد وضع فيه ما تريد .

ثانيا:أنشأ مستند نص بداخله واكتب فيه ما يلي

.[ShellClassInfo]

CLSID={645FF040-5081-101B-9F08-00AA002F954E}

هذا الكود يحوله إلى سلة محذوفات أما إذا أردت أن تجعله لوحة تحكم فضع بدل عن آخر سطر

CLSID={21EC2020-3AEA-1069-A2DD-08002B30309D{

واحفظه باسم desktop.ini

ثالثا:اجعل المجلد مجلد نظام واجعله مخفيا إن شئت.

سوف تلاحظ أن المجلد تحول إلى مجلد نظام .

تحذير: إياك أن تضع الملف في منطقة من مناطق النظام لأنه في حال حدوث أي خلل في النظام ثم تصليحه فمن الممكن أن يتم حذف الملف .

طريقة الكشف: تكون بضغط المجلد بإحدى برامج الضغط فتظهر الملفات التي بداخلها ، أو بإزالة خاصية النظام .

الدرس الرابع:منع النسخ إلى الوسائط المحمولة.

أولا:انشأ مستند نصي واكتب فيه ما يلي

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\storagedevicepolicies]

"writeprotect"=dword:00000001
```

واحفظه باسم Write-Protect.reg .

ثانيا : أضف القيمة، كما في الصورة

أما للتعطيل فبدل ١ ب ٠ (في آخر سطر بآخره) ثم أضف القيمة

طريقة الكشف:عند النسخ إلى الوسائط المحمولة تظهر رسالة المنع التالية .

إذا كان الشخص يعرف هذه الطريقة فإنه سوف يبطلها ،وإذا كان لا يعرفها فسوف يجن قليلا.

- **ملاحظة هامة : إذا كان الويندوز أقدم من الاكس بي فيجب تغيير أول سطر في الملف إلى** REGEDIT4

أي استبدال Windows Registry Editor Version 5.00

ب REGEDIT4

الخاتمة:

أرجو أن تكون قد استفدت وتعلمت من هذا الكتاب ما يفيدك وينفعك.ولا تنس كل من شارك بإعداد هذا العمل من صالح دعائك .

واعلم أنه ليس هناك طريقة حماية كاملة تماما، فطريقة الحماية الوحيدة التي لا تقهر أن تضع ملفاتك في خزنة حديد وليس في حاسبك.

ملاحظة: جميع الدروس مأخوذة من مصادر مختلفة إلا:

تحويل مجلد إلى مجلد نظام معروف وإخفاؤه

إخفاء ملفات في ملف وورد ، فهما من اكتشافي

+ طرق الاكتشاف لجميع الدروس فإنها جهد شخصي.

تأليف: التنين الجامح Dragon The UnTamed

معلومة: من مواليد ١٩٩٤دمشق (منعا لتشابه الأسماء).

للأسئلة أو المشاكل أو الإضافات يمكنك التعليق على تدوينة الكتاب

وهي بعنوان طرق حماية الملفات وطرق كشفها النسخة الثانية

مدونتي : عرين التنين :

www.dtut.wordpress.com

ملاحظة: اسمي القديم كان التنين الجارح ومن قبله التنين الخائن.