

طريقة للحصول على ما يظهر على شاشة الدوس دون استخدام ال: pipe صالحة لكل لغات البرمجة

مقدمة:

بكل صراحة هذه الطريقة كنت أستخدمها في الاختراق و لكنها مفيدة في بعض الأحيان و هي جد سهلة

الدرس:

قم بفتح الدوس و قم بكتابة التعليمة التالية:

```
Echo Hello
```

بالتأكيد ستظهر كلمة : Hello
و لكن لنفترض أننا داخل برنامج فكيف يمكن نتيجة الأمر الذي مررناه الى الدوس ؟
الطريقة سهلة نضيف FileName.Txt > إلى التعليمة السابقة لتصبح:

```
Echo Hello > tahmi.txt
```

لن نلاحظ أي شيء عند تنفيذ التعليمة السابقة
قم بكتابة :

```
Tahmi.txt
```

تحليل المثال:

echo هي تعليمة التي نريد الحصول على نتائجها و يمكن استبدالها بأي تعليمة من
تعليمات الدوس الداخلية أو الخارجية
> محور الموضوع
Tahmi.txt هو اسم الملف الذي سيحتوي على النتيجة

تمرير الأوامر من برنامج و الحصول على النتيجة:

الحل بسيط جدا فمثلا اذهب إلى Run في الأنظمة الانجليزية أو Exécuteur في
الأنظمة الفرنسية
ثم أكتب :

```
cmd.exe /c echo Hello > c:\tahmi.txt
```

لن نلاحظ أي أمر
اذهب إلى الملف c:\tahmi.Txt افتحه لترى أن الكلمة التي أردنا كتابتها ظهرت
حيث أن الأمر echo يقوم بإظهار نص معين

تحليل المثال:

التعليمة /c تعني أن الدوس سينتهي بمجرد انتهاء تنفيذ التعليمة الممررة له و هذا
مهم جدا في الاختراق خاصة

من داخل لغة برمجة الأمر نفسه المهم أن تكون تعرف الدالة التي تقوم بتنفيذ برنامج
فمثلا يكون الكود أعلاه في الفيجوال بزيك:

```
Shell "cmd.exe /c echo my cat > c:\tahmi.txt",0
```

و في السي++:

```
WinExec ("cmd.exe /c echo my cat > c:\tahmi.txt ",0):
```

ونفس الكود بالنسبة إلى الدلفي

ملاحظة: في حالة ما إذا كنت تريد الإضافة للملف لأن الطريقة أعلاه تقوم بحذف الملف إذا كان موجودا ضاعف العلامة > لتصبح >> و لا شيء يتغير في التعليمات الأخرى

خاتمة:

و بالطبع echo كانت للشرح فقط فمثلا لتبرمج برنامج task Manager في ثواني ما عليك سوى استبدال التعليمة echo ب: tasklist وهناك العديد من التطبيقات ومنها ما لا يجب ذكره

By Tahmi in 12/04/2008 06:32 ALGIERS

tahmi15@gmail.com