Redblood Review

بسم الله الرحمن الرحيم اليوم بنسوي شرح بسيط على Redblood

What is redblood?

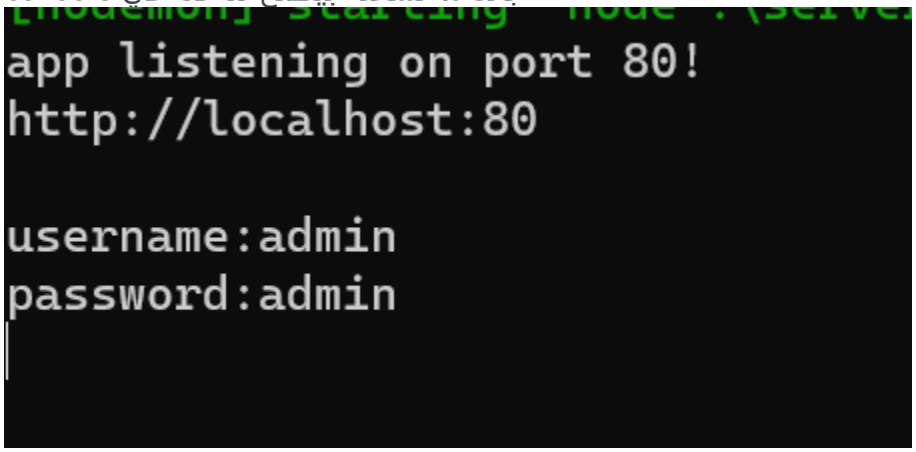
باختصار هو C2 framework سويته بنفسي و نشرته قبل فتره Redblood

installation

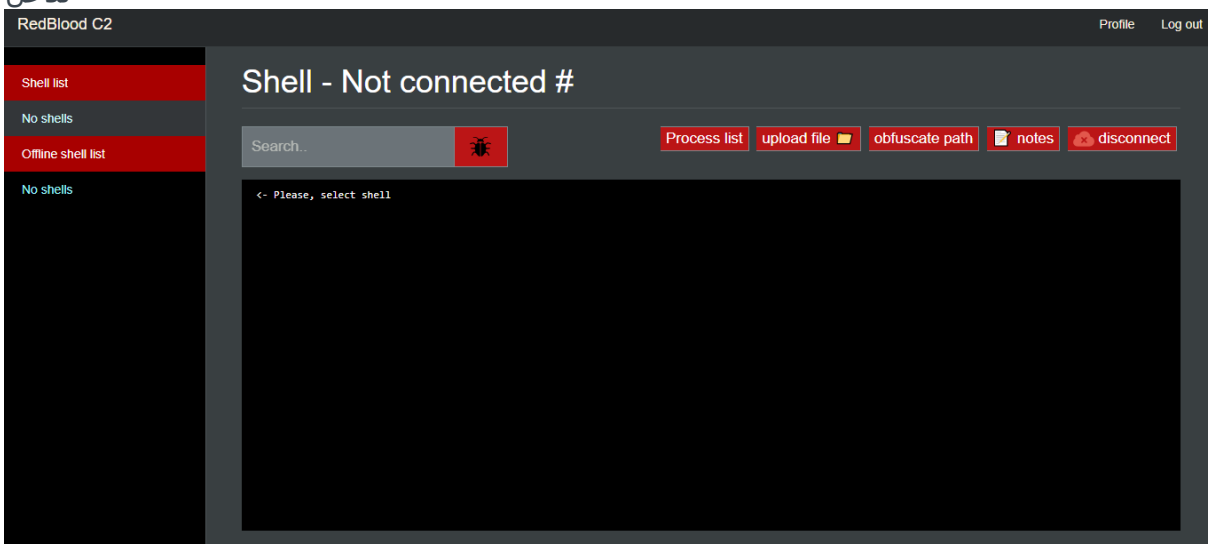
راح تحتاج node.js فقط تحملها على الجهاز و يشتغل معك سواء كنت ويندوز او لينكس كل اللي عليك تسويه تنفذ اوامر التحميل البسيطه هذي

```
$ git clone https://github.com/kira2040k/RedbloodC2.git
$ cd RedbloodC2
$ npm install
$ node server.js
```

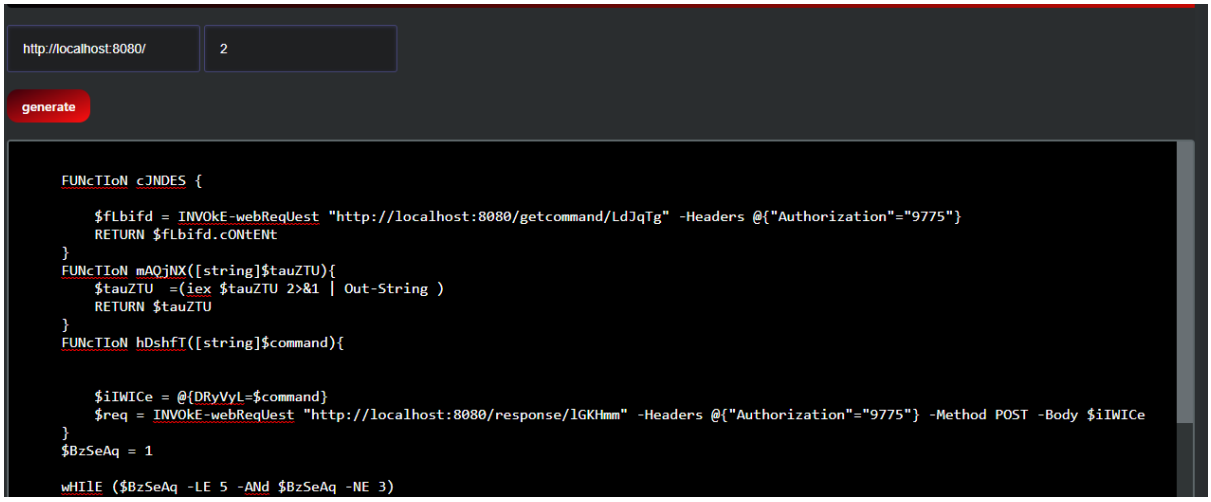
بعد ما نشغله بيطلع لنا كذا في console



الحين بس ندخل للموقع على بورت 80 اليوزر و الباس admin admin يفضل انك تغيرهم اول ما تدخل

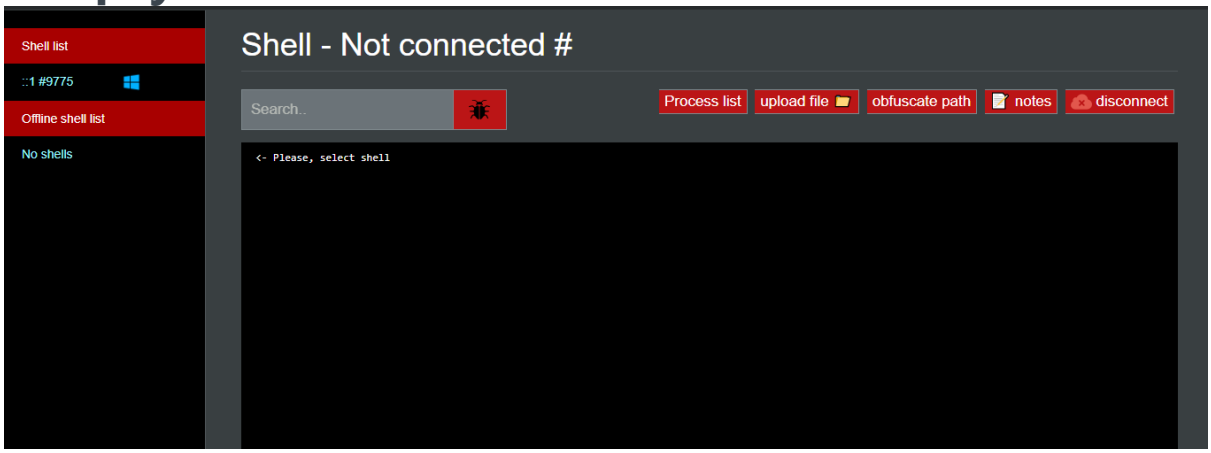


الحين نروح لصفحه البروفايل و ندخل عشان نسوي powershell payload



الحين بس نحدد الموقع اللي يتصل عليه و sleep time تقدر تعدل البورت من 8080 الى اي بورت تبغاه من config.js

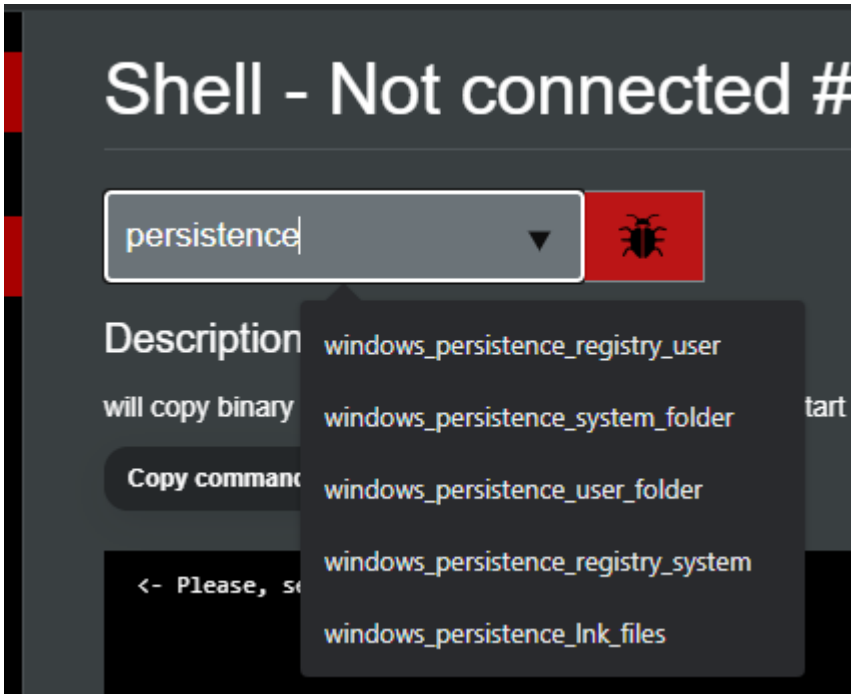
run payload



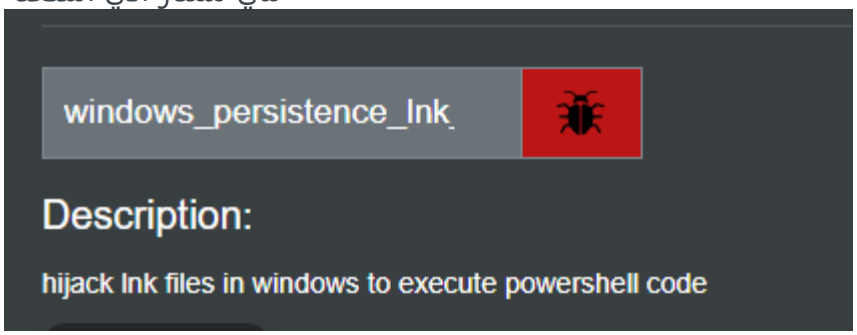
جاني الشل و تخطى AV بكل سهوله على اخر تحديث ويندوز 10

Windows persistence

فيه modules كثير ممكن تستعملها بس عشان المقاله تكون بسيطه بس بنسوي persistence



تقدر تبحث عن ال Modules بكل سهوله و عندنا 5 modules حاليا تسوي persistence بشكل مختلف ماراح اجربها كلها بس راح اختار lnk files لأن كثير من blue teamers يغفل عنها ف تعتبر شي ممتاز اني استغله



اذا حددت ال module بيطلع لك شرح بسيط لها الحين بشغلها بس اول شي بغير مساري الى desktop

راح اسوي ملف lnk لكروم بحيث انه يشغل قوقل كروم و الشل حقي بنفس الوقت

بيحتاج مني 4 اشياء

IconLocation

Arguments

hotkey

lnkfile

تقدر تحط اللي تبي انا بحط

IconLocation: C:\Program Files\Google\Chrome\Application\chrome.exe

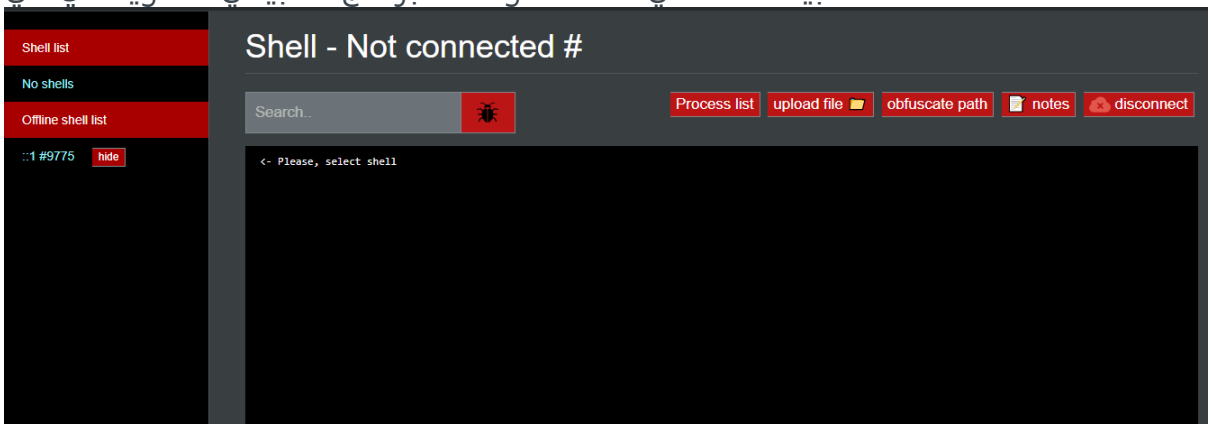
Arguments: -noprofile -WindowStyle hidden <payload>

hotkey: ""

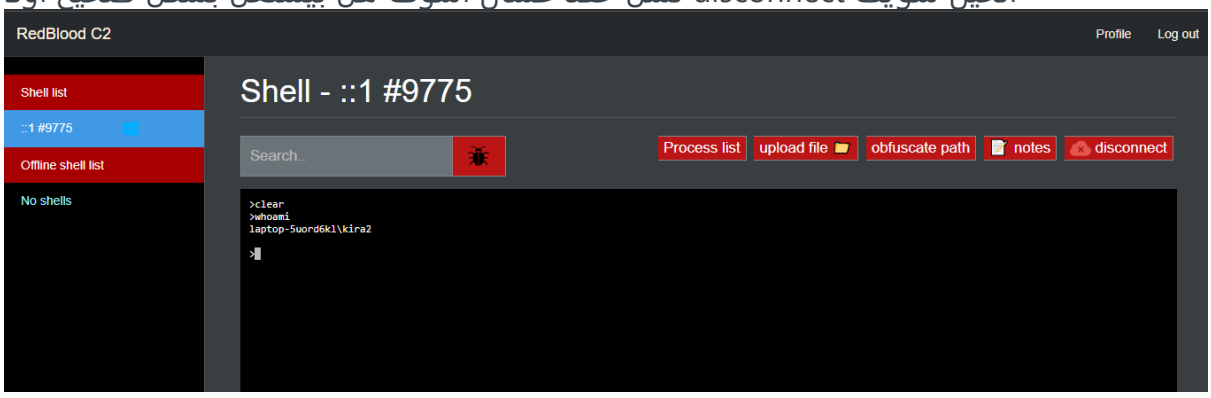
lnkfile: C:\USers\kira2\Desktop\chrome.lnk

بعد ما اشغل ال Module و اعبي هذي المتغيرات

بينضاف معي chrome و كأنه البرنامج الطبيعي ماسويت اي شي



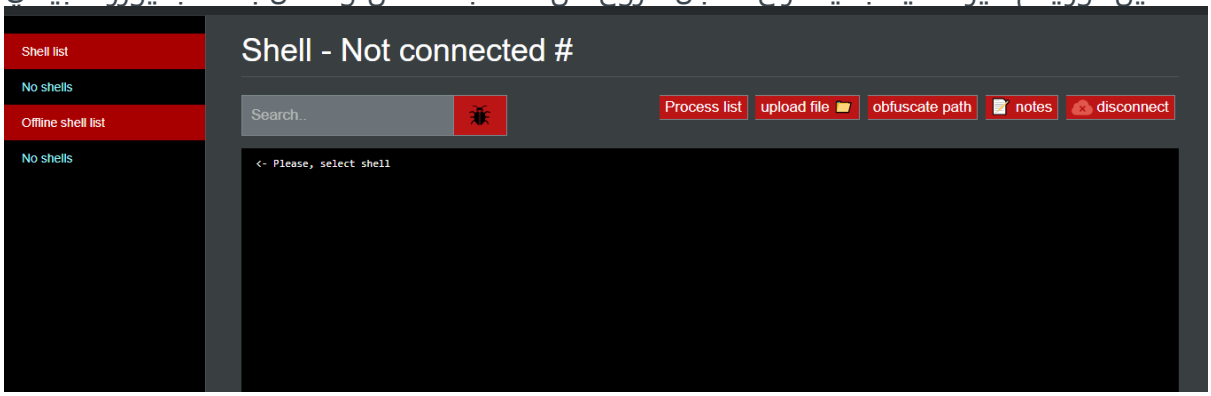
الحين سويت disconnect لشل حقنا عشان اشوف هل بيشتغل بشكل صحيح اولا



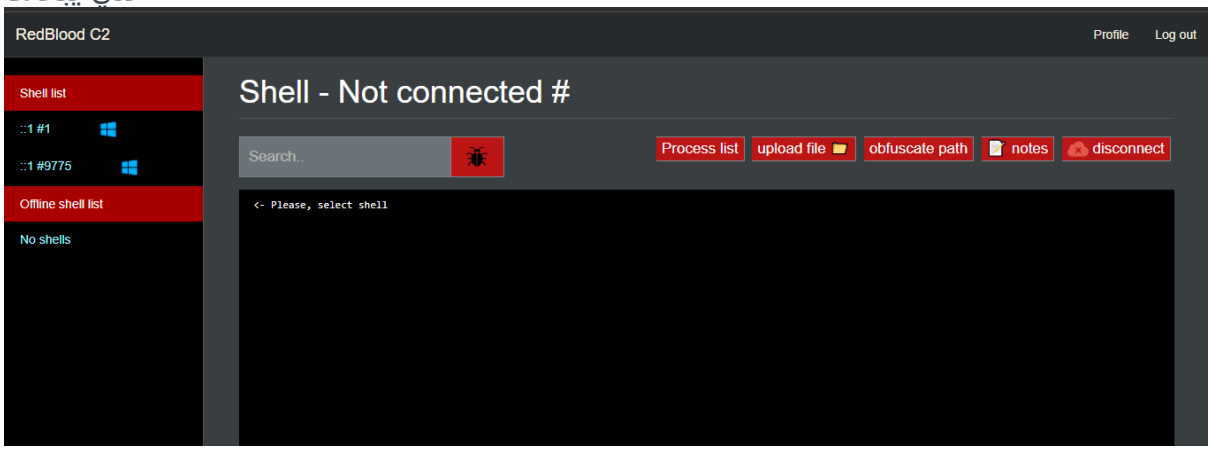
و اشتغل معي مثل ما ابي بدون مشاكل

POC:

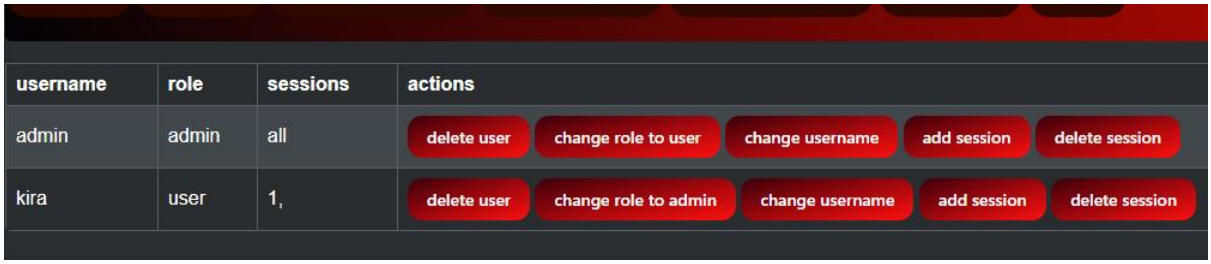
الحين نوريكم ميزة ثانيه جميله راح اسجل خروج من حساب الادمن و ادخل بحساب يوزر طبيعي



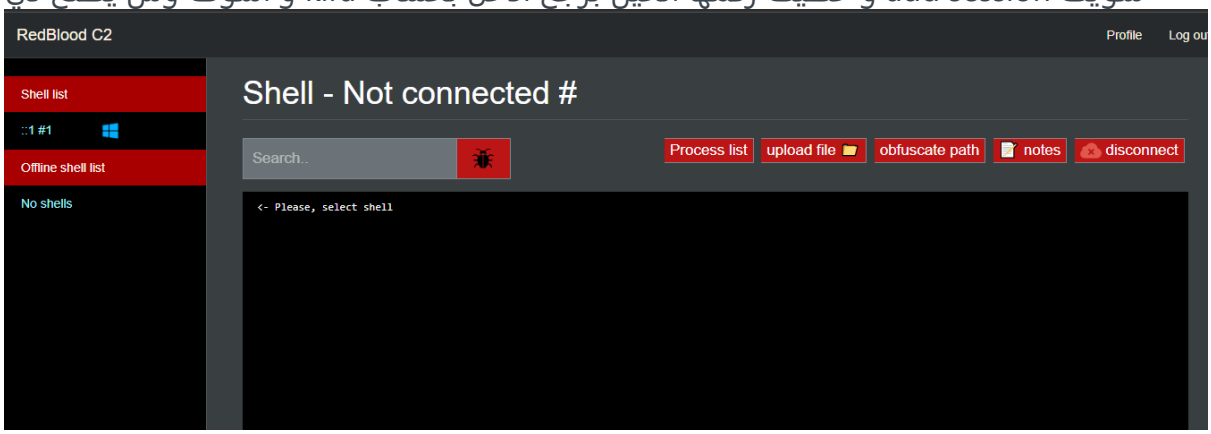
ماراح يطلع لي اي شي مع انه موجود بس ليه ما طلع لي؟ الادمن ما اعطيك اذن تخش السيشن اللي يبغاها



بعد مارجعت لحساب الادمن هنا عندي two sessions رقم 1 و رقم9775 راح اعطي يوزر kira صلاحيات بس ل سيشن 1



سويت add session و حطيت رقمها الحين برجع ادخل بحساب kira و اشوف وش يطلع لي



راح يطلع لي سيشن وحده فقط و هي اللي اعطاني اياها الادمن الميزة هذي جميله اذا عندك سيشنات كثير و تشتغل انت و اكثر من شخص بحيث يكون الشغل مقسم بينكم بكل سهوله