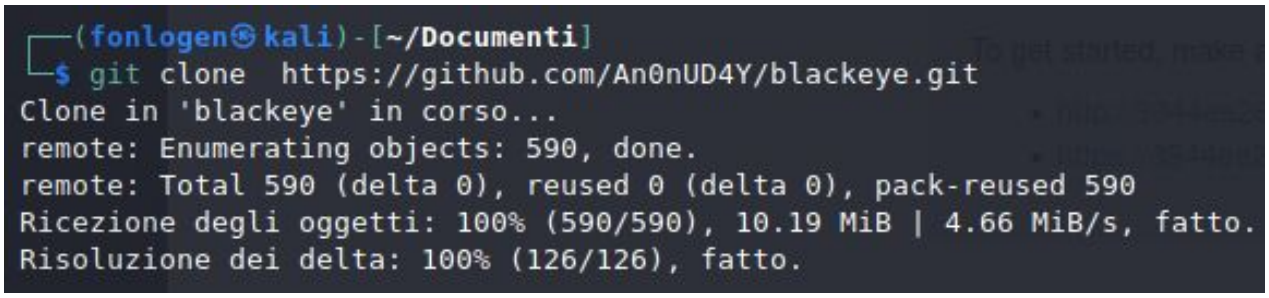
BlackEye- Tool di phishing

BlackEye è un tool che permette di creare, tramite **NGROK**, un server PHP sul proprio computer e tramite delle pagine web (pre-create all'interno della directory root del tool) di rubare i dati di accesso della vittima e l'indirizzo IP (con altre informazioni più o meno utili) ricavate dall'IP. Siccome BlackEye non è disponibile ufficialmente in nessuna distro Linux, neanche Kali e Parrot, è necessario clonare il repository tramite il progetto GitHub. Su questo abbiamo 2 modi per farlo: Il classico "Download as Zip" dalla pagina del repository, o tramite terminale. Per farlo tramite terminale bisogna avviare un terminale (in una qualsiasi directory) ed eseguire il seguente comando:

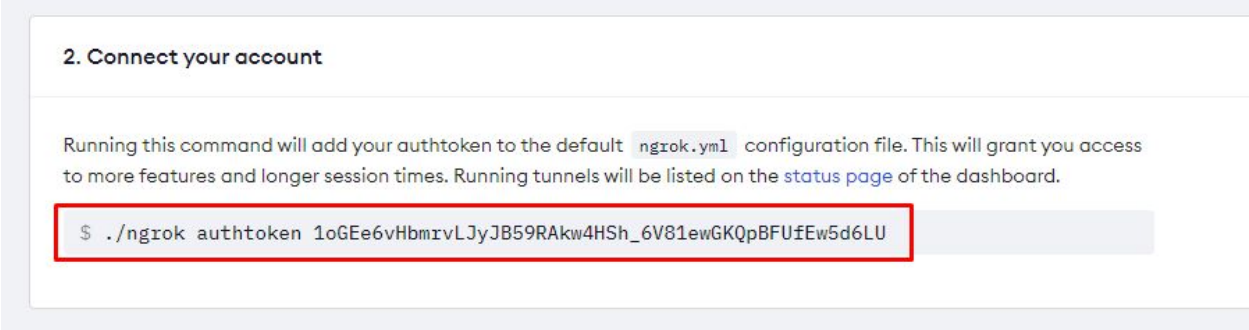
```
$ git clone https://github.com/An0nUD4Y/blackeye.git
```



Tramite questo comando cloniamo l'intero repository di BlackEye nella directory *~/BlackEye*. Adesso tramite il terminale dovremo accedere alla directory di BlackEye, quindi nella stessa posizione in cui abbiamo eseguito il comando prima digitiamo:

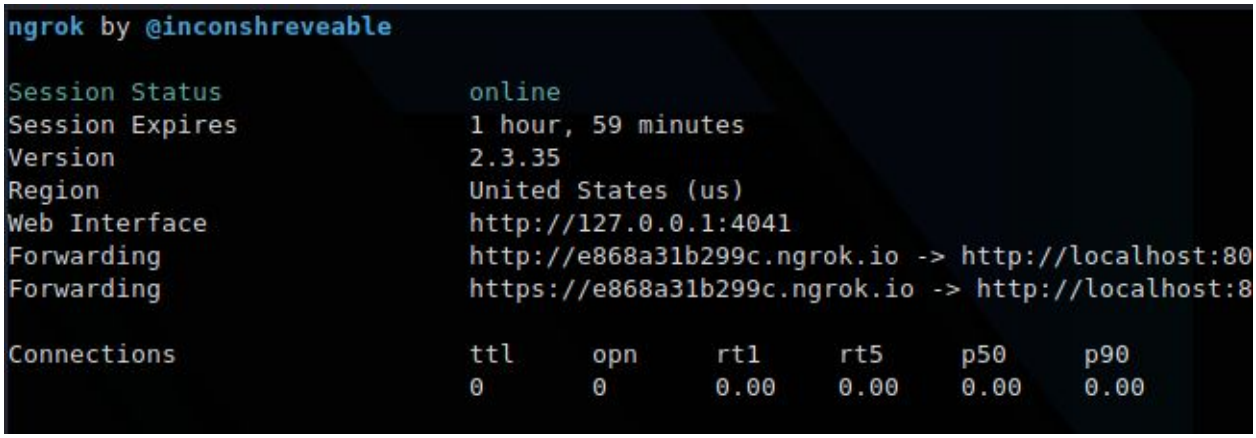
```
$ cd BlackEye
```

In questa directory bisognerà configurare NGROK. Per farlo bisognerà innanzitutto registrarsi su www.NGROK.com, va bene anche una tempmail ma consiglio di utilizzare un email statica (o di eseguire l'accesso tramite Google / GitHub). Una volta loggati all'interno del sito NGROK, sulla nostra sinistra ci sarà un menù con tutte le varie opzioni. Ciò che interessa a noi sarà Setup & Installation. Cliccandoci ci reindirizzerà ad una pagina di configurazione per NGROK. Saltiamo il primo passaggio ed andiamo direttamente al secondo, con scritto "Connect your account". Dovremmo copiare il comando che ci viene fornito ed incollarlo in un terminale nella directory di BlackEye



Eseguito questo comando, bisognerà avviare NGROK. Per farlo eseguiamo un altro comando:

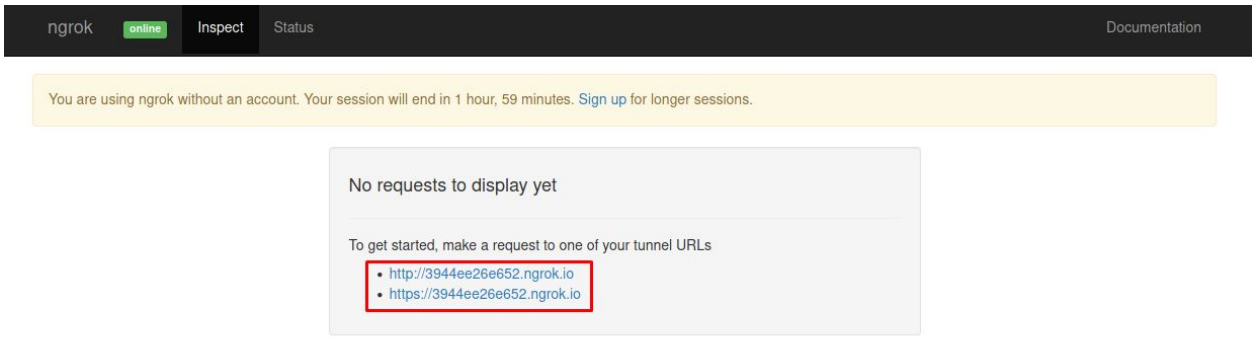
```
$ ./ngrok http 80
```



Fatto ciò possiamo finalmente avviare BlackEye. Chiudiamo il terminale attuale e apriamone un altro, sempre nella stessa directory. Una volta nella directory di BlackEye, bisognerà lanciare lo script. Per farlo digitiamo nel terminale:

```
$ sudo ./BlackEye.sh
```

Lo script verrà avviato e comparirà una schermata (a terminale) con le varie pagine web già pre-create. Selezioniamo la pagina che vogliamo e entro 15 secondi circa ci verrà fornito il link da inviare. Nel caso il link non dovesse apparire bisognerà fare un passaggio aggiuntivo. Dovremmo aprire il nostro browser web e recarci all'URL 127.0.0.1:4040/inspect/http. Una volta caricato ci apparirà una pagina contenente 2 URL i quali possiamo scegliere quale dei 2 inviare alla vittima.



Per non dare nell'occhio ci basterà camuffare il link con un Url Shortener online ed inviare quel link alla vittima.

IMPORTANTE! Se si lavora su un ambiente virtualizzato (VMWare / VirtualBox) è necessario DISATTIVARE la protezione FireWall di Windows, altrimenti le connessioni non saranno consentite.