1º Semestre	2º Semestre	3º Semestre	4º Semestre
Word	Como Hackear Facebook	Excel	Como Formatar um computador em 20 minutos
Edição de Imagens	Como consertar eletrodoméstico	Como Editar Pdf	Como Desinstalar o Baidu
Digitação	Power Point	Como consertar Ar condicionado	Como usar Bola de Cristal
Mágica I	Manutenção de Impressora	Hackear Whatsapp	Mágica II
Instalação de Impressora	Como fazer a Internet ficar mais rápida	Como criar um site em uma hora	Projeto Final: Como virar Hacker

Curso de programação - LIpE

Esta apresentação contém uma Demonstração prática:
entrem nesse wifi
Oi_velox_wifi_9EB2 !
e busquem por esse link:
192.168.1.2/chat.php

1º Semestre	2º Semestre	3º Semestre	4º Semestre
Word	Como Hackear ~~Facebook~~ algumas coisas ai	Excel	Como Formatar um computador em 20 minutos
Edição de Imagens	Como consertar eletrodoméstico	Como Editar Pdf	Como Desinstalar o Baidu
Digitação	Power Point	Como consertar Ar condicionado	Como usar Bola de Cristal
Mágica I	Manutenção de Impressora	Hackear Whatsapp	Mágica II
Instalação de Impressora	Como fazer a Internet ficar mais rápida	Como criar um site em uma hora	Projeto Final: Como virar Hacker

Curso de programação - LIpE

Chegou o dia!

Python orientado a ~~segurança~~ hackinagem

Em 15 minutos. Ou um pouco mais.

Uma brevíssima introdução sobre redes e utilizando python. Além de algumas aplicações de segurança ofensiva.

Feito por GRIS :
José Luiz & Franklin Martins

Básico

O que é um endereço IP?

É um número único atribuído à um computador em uma rede. Permite a comunicação entre computadores

Será que é possível se comunicar pela internet usando o python?

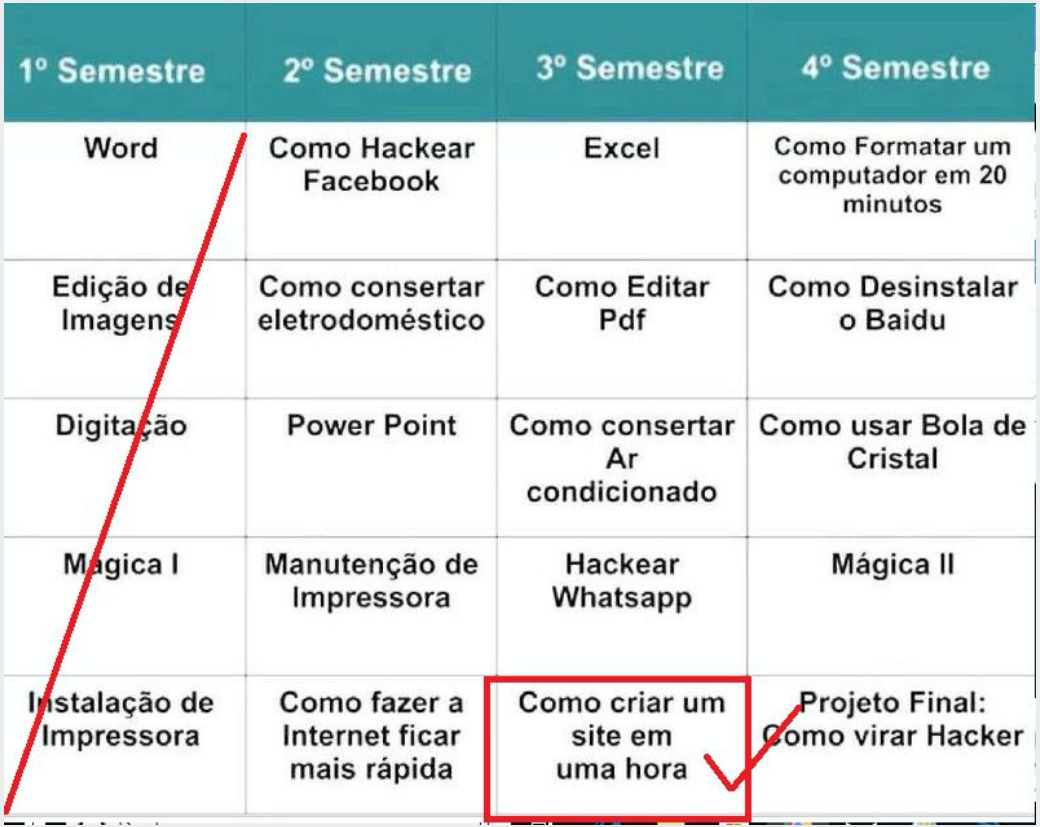
179.218.123.123 your IP FIND

Your IP address	179.218. 123 . 123
Latitude	-22.9201
Longitude	-43.3307
Country	Brazil
Region	Rio de Janeiro
City	Rio de Janeiro
Organization	NET Virtua

1.Criando um site extremamente simples

```
#usamos o comando import quando desejamos usar
#funcoes e comandos especiais que nao estao no python
from meu_soquete import *

#uma string indica qual o conteúdo do site que deve ser mostrado
minhaPaginaWeb="""
<html>\r
<head>\r
<title>Bem vindo ao meu siteeeee</title>\r
</head>\r
<body>\r
<h1>Meu site esta rodando em python</h1>\r
<p>Este nao eh o jeito usual de criar um site, mas funciona.</p>\r
<p>Seu IP eh : %s .</p>\r
</body>\r
</html>\r
"""

#manda o servidor se conectar a uma porta
servidor =meu_soquete_servidor("0.0.0.0",8081)

#define qual pagina sera enviada
servidor.enviar_mensagem(minhaPaginaWeb)
```

1.Criando um site extremamente simples



1º Semestre	2º Semestre	3º Semestre	4º Semestre
Word	Como Hackear Facebook	Excel	Como Formatar um computador em 20 minutos
Edição de Imagens	Como consertar eletrodoméstico	Como Editar Pdf	Como Desinstalar o Baidu
Digitação	Power Point	Como consertar Ar condicionado	Como usar Bola de Cristal
Mágica I	Manutenção de Impressora	Hackear Whatsapp	Mágica II
Instalação de Impressora	Como fazer a Internet ficar mais rápida	Como criar um site em uma hora	Projeto Final: Como virar Hacker

Curso de programação - LIpE

Foi sem querer....

2.Criando um navegador extremamente simples

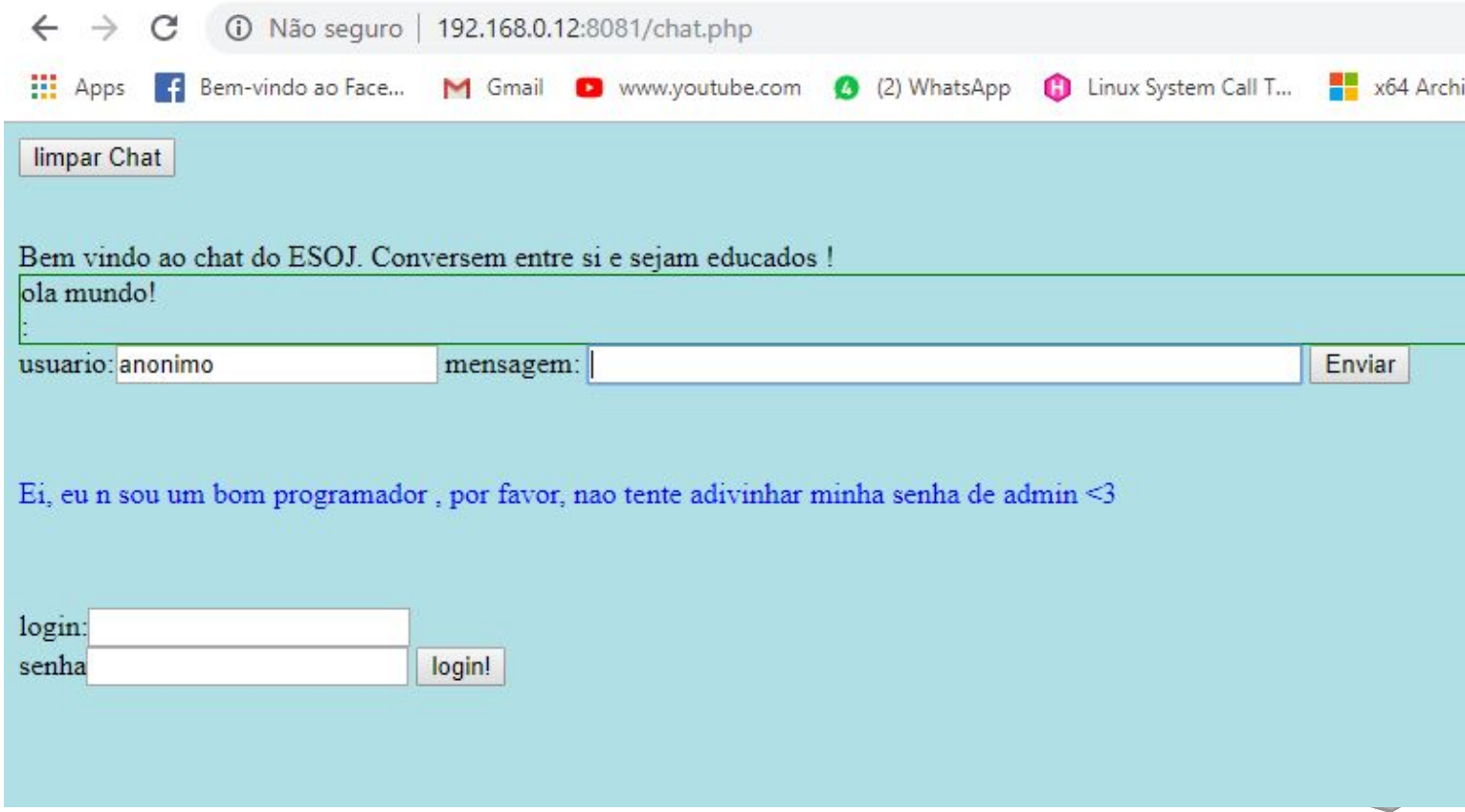
```
from meu_soquete import *

#criamos um cliente e dizemos a qual IP queremos se conectar
cliente =meu_soquete_cliente("127.0.0.1",80)

#dizemos qual paagina queremos visualizar
cliente.pedir_pagina("/chat/chat.php?")

#mostramos a resposta na tela
print("o que foi recebido :\n",cliente.receber_resposta())
```

2.Criando um navegador extremamente simples

```
 RESTART: C:/Users/zeka2/Documents/python scripts2/apresentacao/navegador.py
o que foi enviado:
 GET /chat/chat.php? HTTP/1.0
Host: 127.0.0.1


o que foi recebido :
 HTTP/1.0 200 OK
Host: 127.0.0.1
Date: Mon, 20 May 2019 19:19:32 +0000
Connection: close
X-Powered-By: PHP/7.1.29
Content-type: text/html; charset=UTF-8

<html>
 <head>
 <title>Bem vindo ao meu chat</title>
 </head>
 <body>



<!DOCTYPE html>
<html>
<body>



 <style>
    body {
      background-color: powderblue;
    }
    h1  {
      color: blue;
    }
```

2.Criando um navegador extremamente simples

1.5 O chat para testes



```
from meu_soquete import *

cliente =meu_soquete_cliente("127.0.0.1",80)

#pegamos uma resposta errada
cliente.testar_login("/chat/login.php","login=admin&password=aaaa")
resposta_errada=cliente.receber_resposta()
print("resposta errada",resposta_errada)
```

Testando uma senha no nosso chat

```
 RESTART: C:/Users/zeka2/Documents/python scripts2/apresentacao/testeSenha.py
o que foi enviado:
 POST /chat/login.php HTTP/1.1
Host: 127.0.0.1/chat/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 25

login=admin&password=aaaa


resposta errada HTTP/1.1 200 OK
Host: 127.0.0.1/chat/login.php
Date: Mon, 20 May 2019 19:24:57 +0000
Connection: close
X-Powered-By: PHP/7.1.29
Content-type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<body>


senha incorreta, tu ta me zoando?<br><img src="imagens/cat.jpg" >postagem:aaaa


</body>
</html>
>>>
```

3.Ataque de força bruta

Será que conseguimos adivinhar a senha do nosso chat?

3.Ataque de força bruta- Estrutura de repetição: Próxima matéria de vocês

for e while são comandos que servem para repetir um bloco de código, quantas vezes forem necessárias.

```
>>> for i in [0,2,4,5]:
        print (i)


0
2
4
5
>>>
```

3.Ataque de força bruta

Enviamos as possíveis senhas para o site e esperamos uma hora acertar qual é a correta.

Por que as senhas pedem 8 caracteres no mínimo?

26 ^ 8 =

208.827.064.576 = 671 anos / 10 senhas por segundo

```
 RESTART: C:\Users\zeka2\Documents\python scr
testando senha: aaaa
testando senha: aaab
testando senha: aaac
testando senha: aaad
testando senha: aaae
testando senha: aaaf
testando senha: aaag
testando senha: aaah
testando senha: aaai
testando senha: aaaj
testando senha: aaak
testando senha: aaal
testando senha: aaam
testando senha: aaan
testando senha: aaao
testando senha: aaap
testando senha: aaaq
testando senha: aaar
testando senha: aaas
testando senha: aaat
```

Contra-medidas

Punição

-Brute Force e phishing:

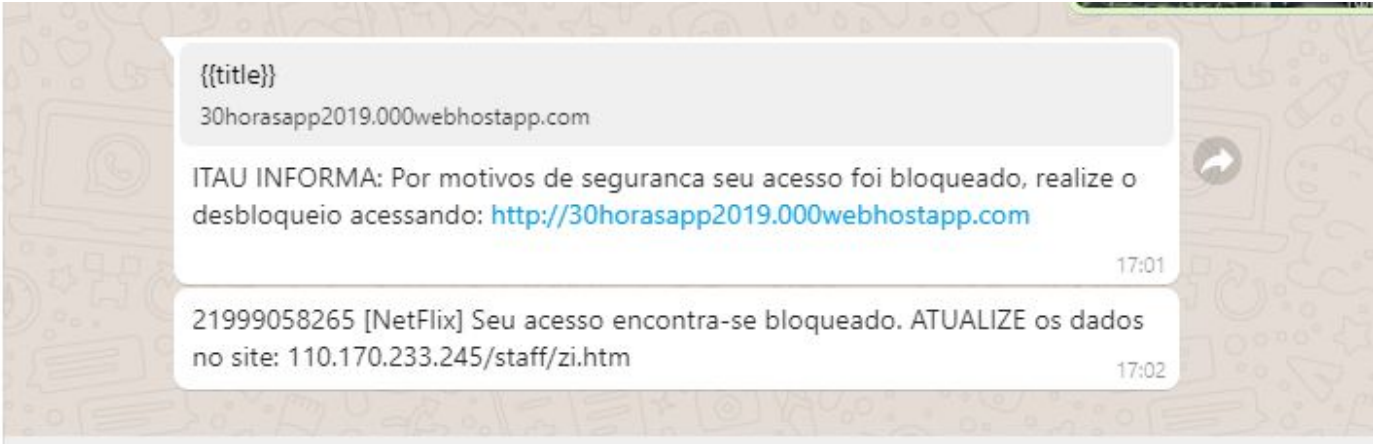
"Hey, eu sei a quem esse ip pertence!" → processo criminal → cadeia.

Prevenção

Brute Force : reCaptcha , política de senhas, mínimo 8 caracteres...

Phishing : Conscientização do usuário

4.Phishing



Phishing é uma maneira desonesta que cibercriminosos usam para enganar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando você a websites falsos.

Teste Prático, link no chat, se houver internet!

4.Phishing

Exemplo:

http://30horasapp2019.000webhostapp.com/

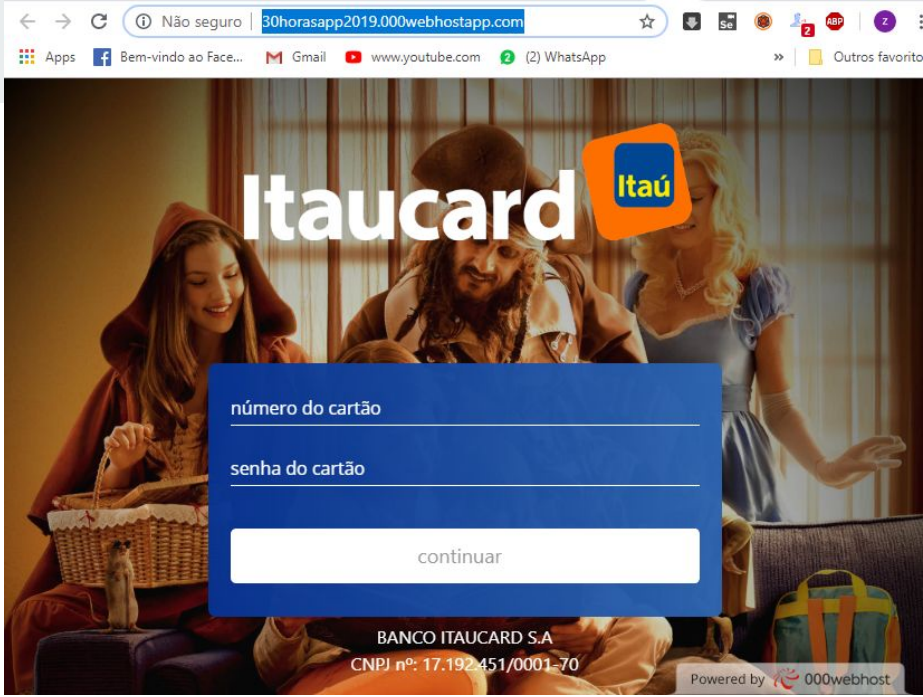
O que fazer quando encontrar um phishing?

POST SPAM (?).py

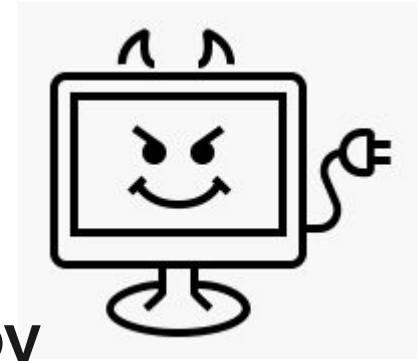
Reportar https://safebrowsing.google.com/safebrowsing/report_phish/?hl=pt-BR

https://new.safernet.org.br/denuncie

http://www.senado.gov.br/noticias/jornal/cidadania/Infraestruturarodovias/not005.htm

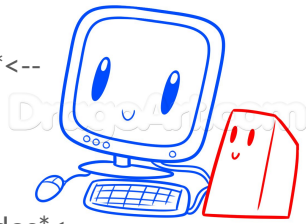


5. Backdoor.py



→ Hey ! Roda meu programa no seu pc ai!

Ok←



Programa inicia comunicacao com atacante<--

-->*atacante envia comandos para vítima*

programa roda os comandos e devolve os resultados<--

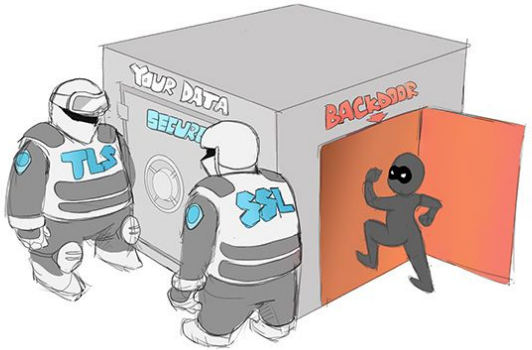
atacante lê arquivos da vítima, rouba senhas e até minera cripto moedas

Será que é possível controlar o PC de outra pessoa remotamente e sem que ela saiba?

Bom, já sabemos como fazer conexões pela internet. E se pudéssemos rodar comandos

-É um mecanismo que permite controlar remotamente uma máquina, sem que o usuário sabia.

Por isso Não se abre .exe de fontes desconhecidas



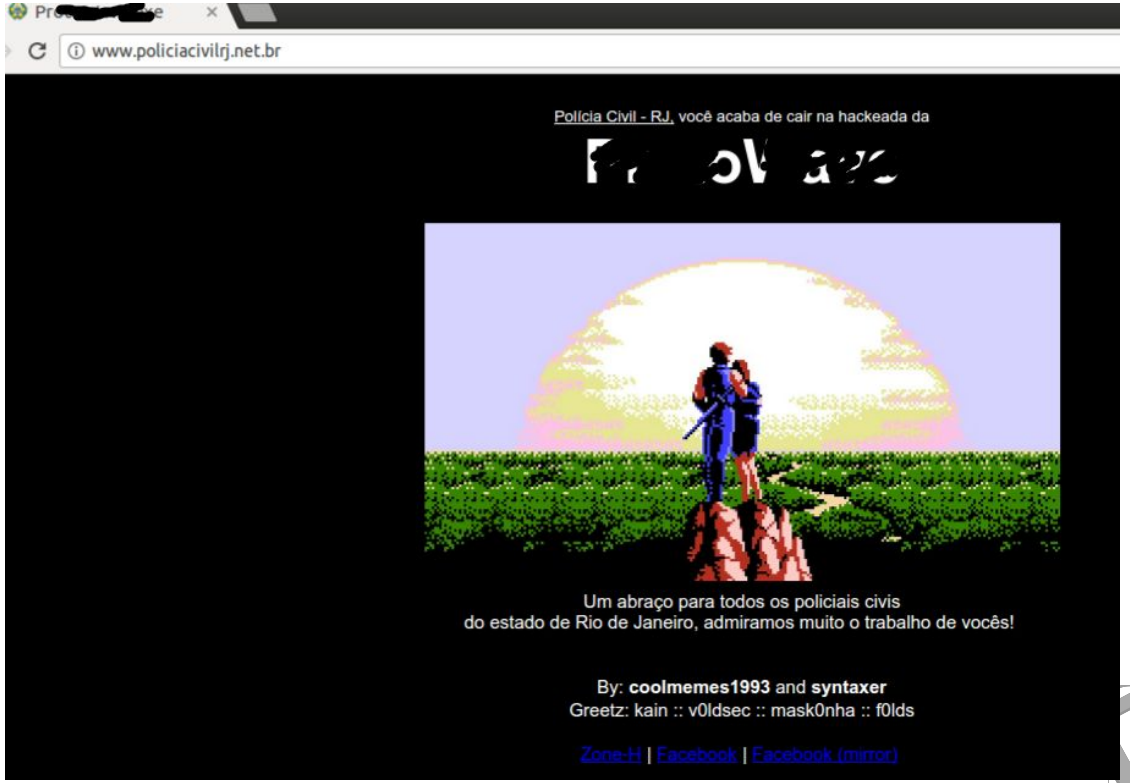
if estou_com_tempo == True:

-Deface → O site é vulnerável a injeção de código HTML (tipo esse chat que eu fiz). Será que é possível desfigurar o site por completo?

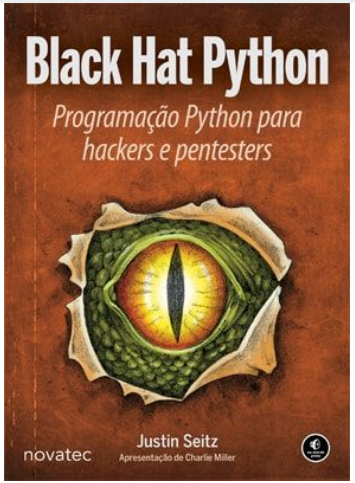
-Não envolve necessariamente python, mas é um ataque muito comum e nem sempre é malicioso.

-Não façam , é crime!!

-Aconteceu com alguns sites da UFRJ ano passado.



Referências e conteúdos adicionais



- link para os códigos:
- https://github.com/zekkametallica/pythonSec
- Leitura recomendada: Black Hat Python
- Segurança WEB:
- https://github.com/jpedrodelacerda/websec101/
- https://cartilha.cert.br/golpes/
- Obs: Fiz o chat em php, não em python.
- Página do Grupo de Resposta a Incidentes de Segurança (GRIS - UFRJ)
- https://www.facebook.com/grisdccufrj/?ref=br_rs
- O outro slide, bem mais detalhado https://docs.google.com/presentation/d/1GZt9aSiAt2q6h_Xrs-YSvpcEHFjBDSXEqgHyXPIw__8/edit?usp=sharing