

## Laboratório OSINT - Open Source Intelligence Tecnologais Hackers - Prof. Rodolfo Avelino

### Laboratório 1 - SpiderFoot

SpiderFoot é uma ferramenta de automação de inteligência de código aberto (OSINT). Ele se integra a praticamente todas as fontes de dados disponíveis e utiliza uma variedade de métodos para análise de dados, facilitando a navegação desses dados.

SpiderFoot tem um servidor web embutido para fornecer uma interface baseada na web limpa e intuitiva, mas também pode ser usado completamente através da linha de comando. Está escrito em Python 3 e licenciado pelo MIT.

#### I - Instalando

##### Baixe o execute o SpiderFoot

```
# wget https://github.com/smicallef/spiderfoot/archive/v4.0.tar.gz
```

```
# tar zxvf v4.0.tar.gz
```

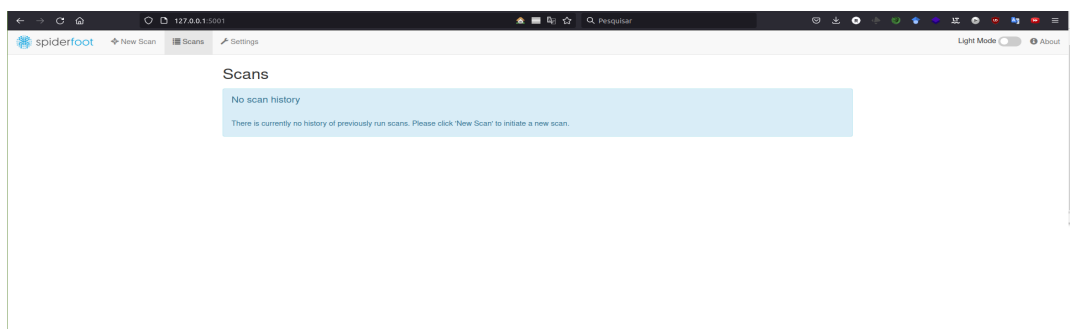
```
# cd spiderfoot-4.0
```

```
# pip3 install -r requirements.txt
```

```
# python3 ./sf.py -l 127.0.0.1:5001
```

# Insper

Acesse o dashboard através do seu navegador digitando o endereço  
127.0.0.1:5001



Vamos fazer a primeira análise a partir das informações que serão coletadas por sua conta de e-mail. No menu superior clique em New Scan e em seguida preencha os campos:

**Scan Name:** Aula

**Scan Target:** <COM SEU EMAIL>

**New Scan**

Scan Name:

Scan Target:

**Help:** Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:

- Domain Name: e.g. example.com
- IPv4 Address: e.g. 1.2.3.4
- IPv6 Address: e.g. 2001:4700:4700::1111
- Hostname-Sub-domain: e.g. abc.example.com
- Subnet: e.g. 1.2.3.0/24
- Bitcoin Address: e.g. 1HesYJSP1QoqyPEjO9vZBL1wjuuNGe7R
- E-mail address: e.g. bob@example.com
- Phone Number: e.g. +12345678901 (E.164 format)
- Human Name: e.g. "John Smith" (must be in quotes)
- Username: e.g. "jsmith2000" (must be in quotes)
- Network ASN: e.g. 1234

**By Use Case** | By Required Data | By Module

☒ **All** **Get anything and everything about the target.**  
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

☐ **Footprint** **Understand what information this target exposes to the Internet.**  
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

☐ **Investigate** **Best for when you suspect the target to be malicious but need more information.**  
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

☐ **Passive** **When you don't want the target to even suspect they are being investigated.**  
As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

[Run Scan Now](#)

Agora espere e explore o resultado



### **Exercício 1**

Seu e-mail foi exposto em algum vazamento?

### **Exercício 2**

Desvende e apresente as evidências:

- A) Qual o CNPJ que é responsável pelo domínio usp.br?
- B) Quantas reportagens possui o Rodolfo Avelino no grupo uol.com.br?
- C) Encontre uma url que tenha possíveis arquivos de backup (cópia de segurança), expostos de forma insegura.