



ISH ✓
Segurança Ofensiva
Pentest101

Segurança Ofensiva

Pentest 101

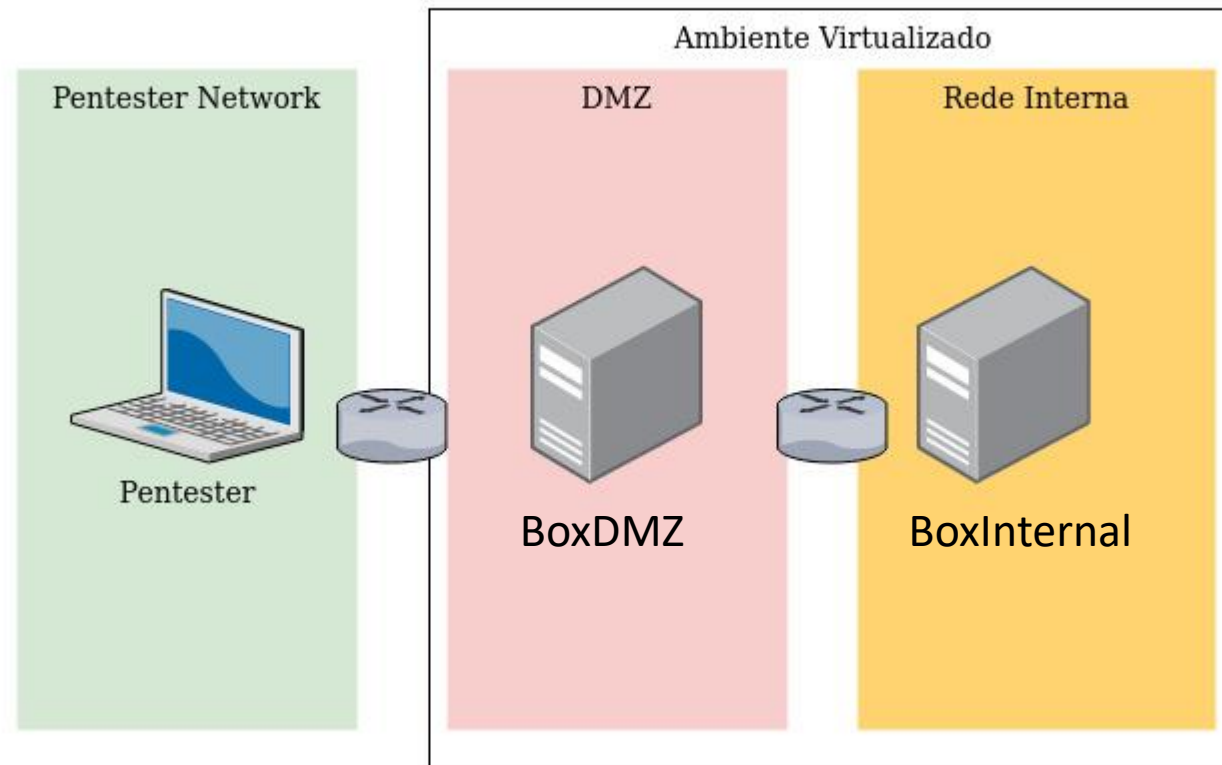
Preparação de Ambiente

Prerando o ambiente

Requisitos:

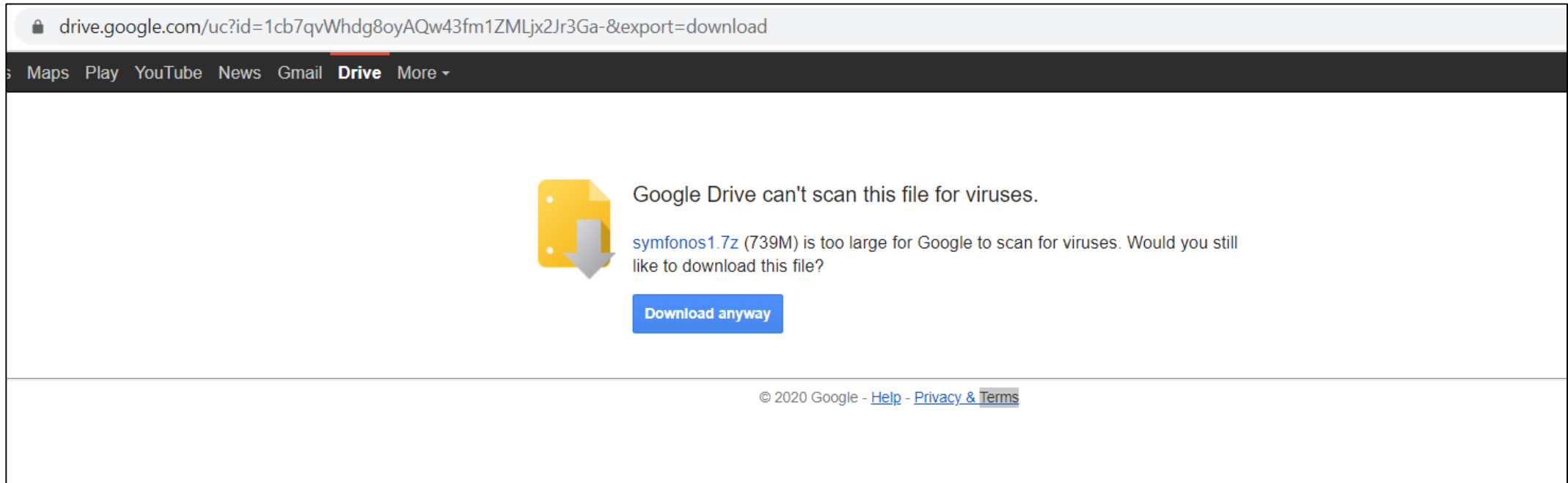
- VirtualBox Version 6.1.12 r139181 (Qt5.6.2)
- 7-zip File Manager
- Internet
- Capacidade de suportar duas VM's (2Gb)
- Kali Linux

Pentest101 - Lab

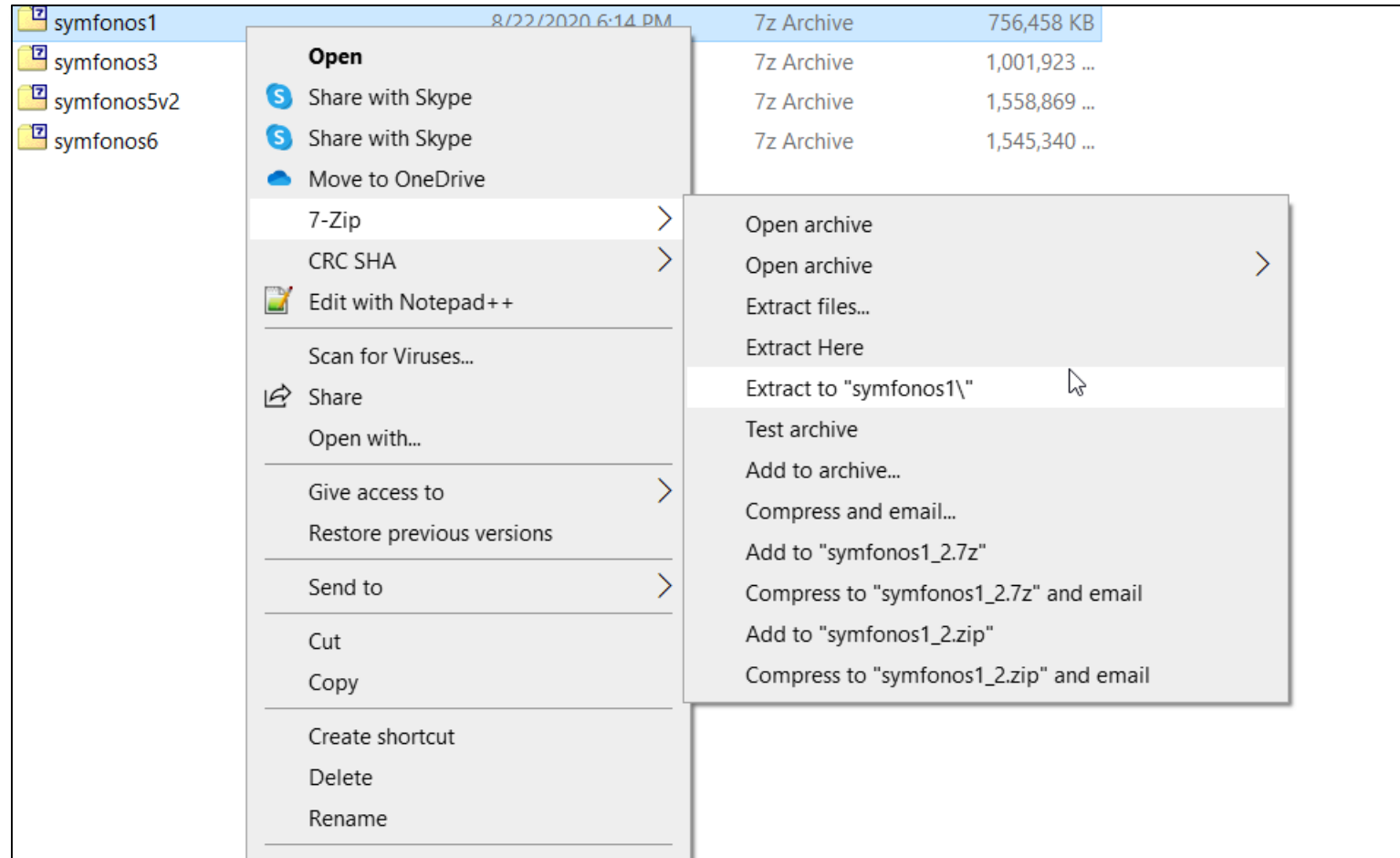


- Realize o download da VM symfonos – 1 através da url:
<https://drive.google.com/uc?id=1cb7qvWhdg8oyAQw43fm1ZMLjx2Jr3Ga-&export=download>
- Descompacte o arquivo utilizando o 7z
- Realize a importação para o Virtual Box
- Altere a configuração da primeira interface de rede para **BRIDGE**
- Adicione uma nova interface e configure para a rede **Nat Network**

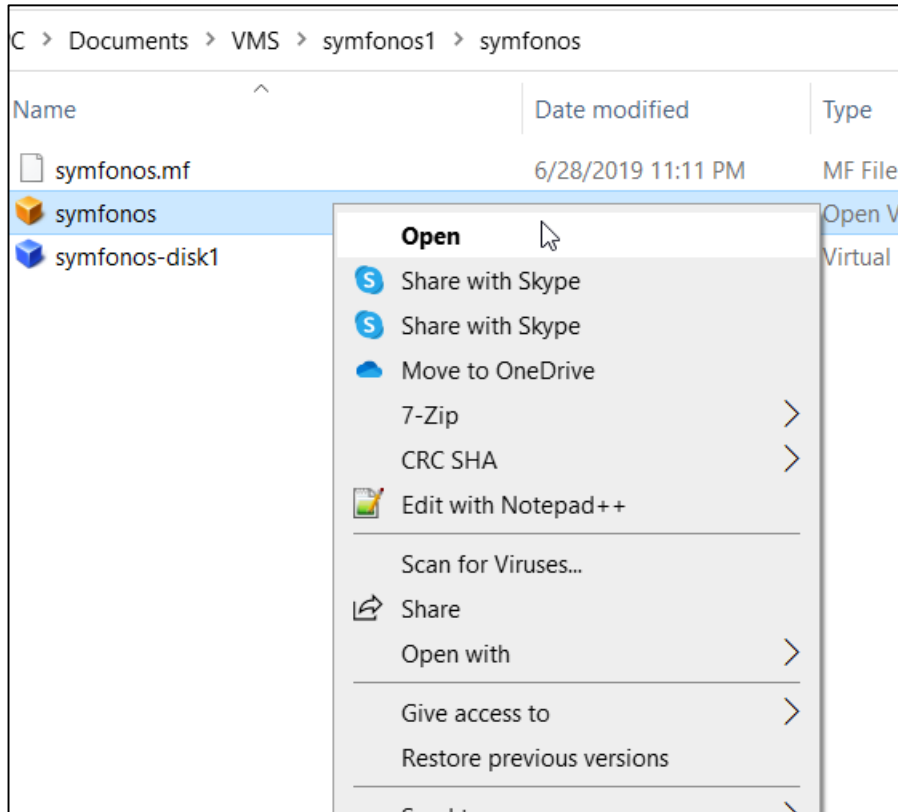
Download VM 1



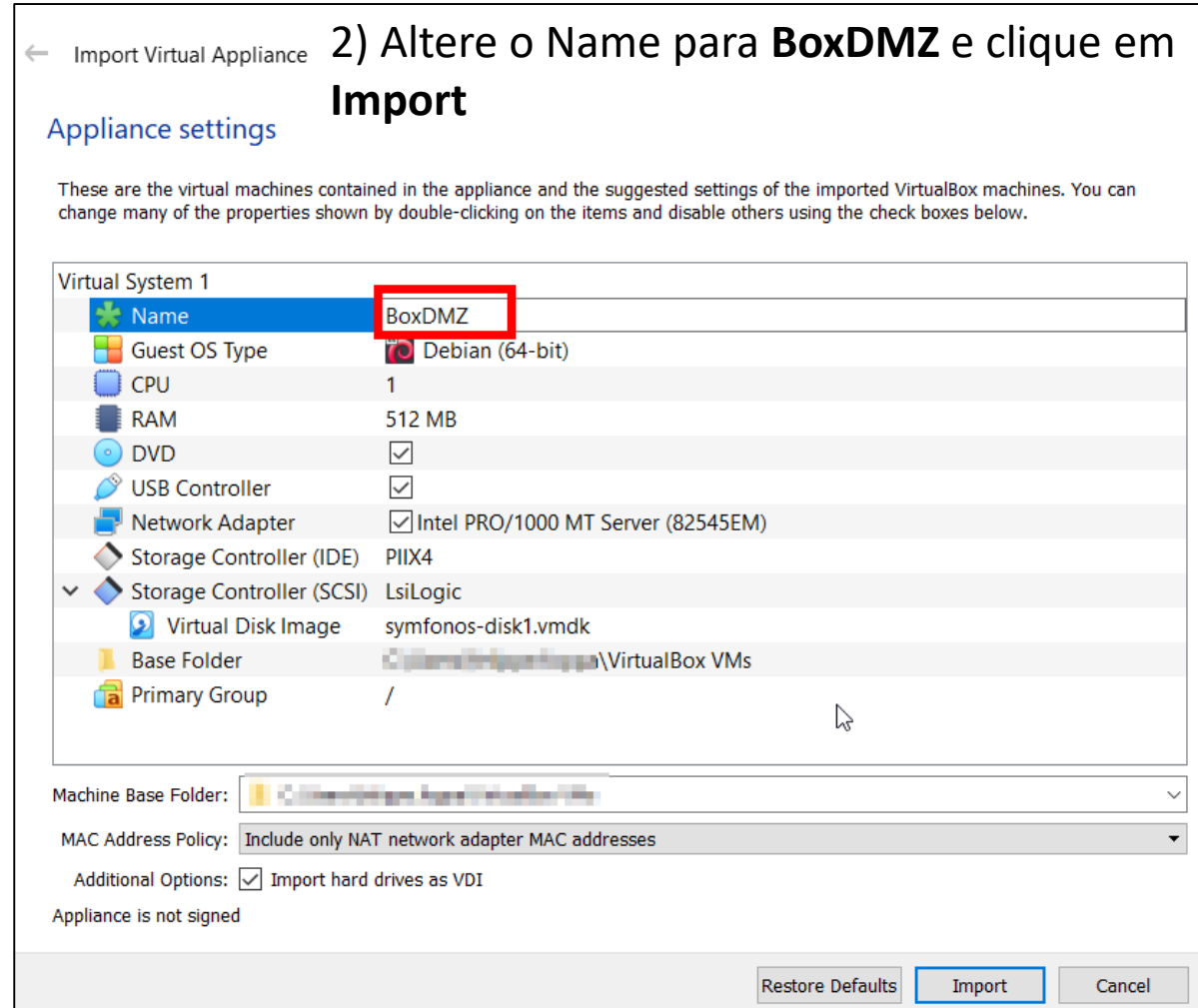
Descompressão



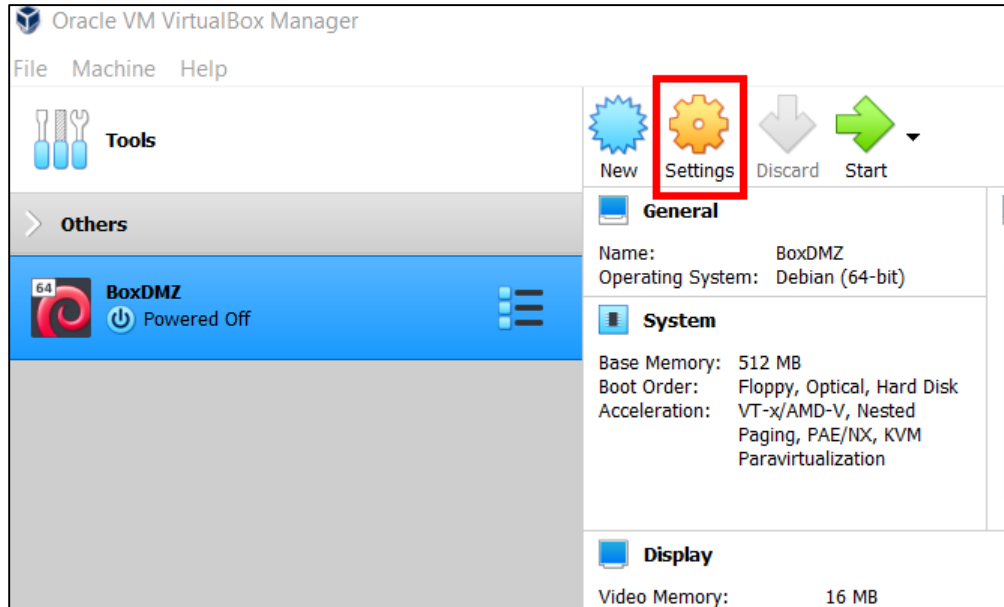
Import



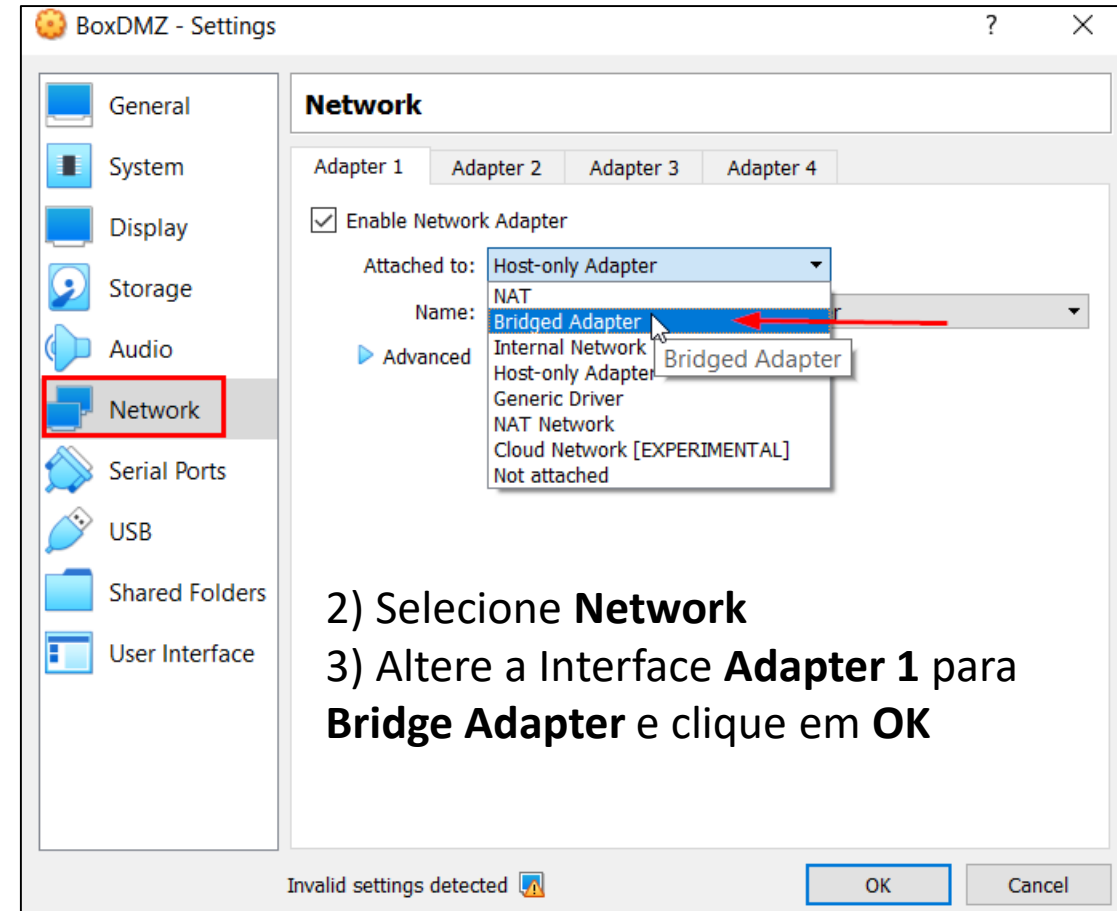
1) Clique com o **botão direito** do mouse em cima do arquivo ovf e clique em **Open**



Bridge Interface



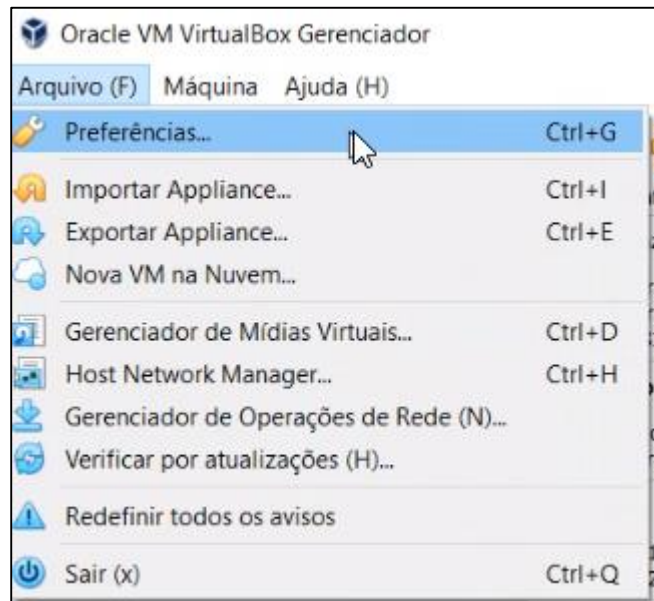
1) Selecione **Settings**



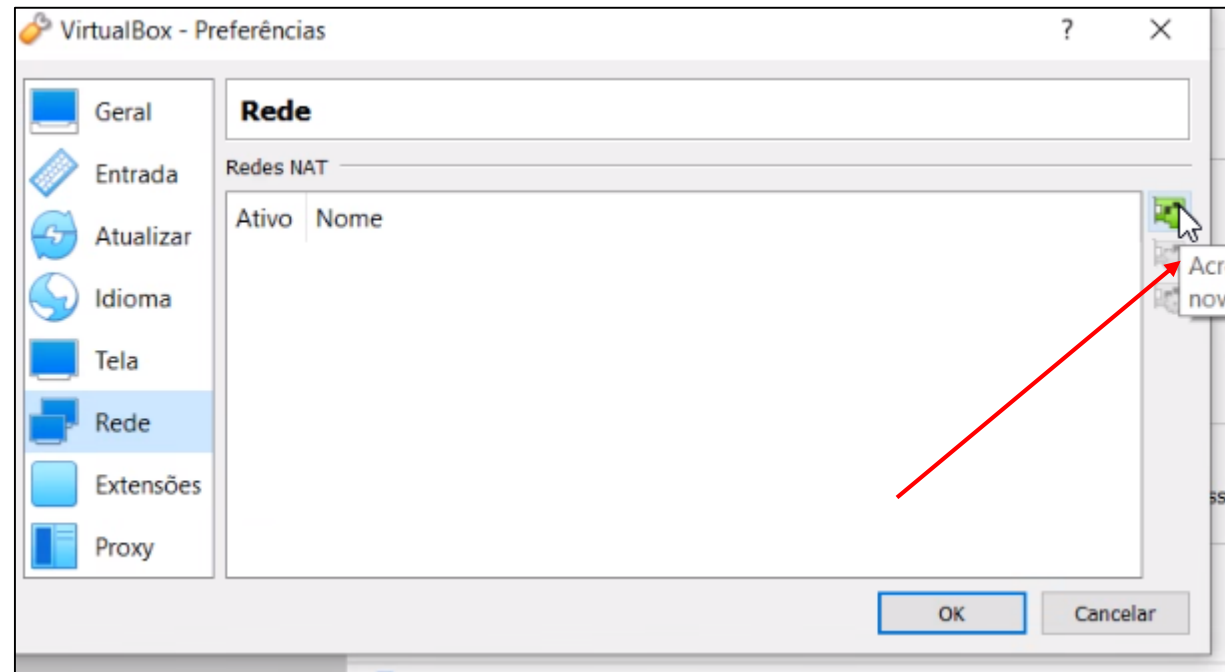
2) Selecione **Network**

3) Altere a Interface **Adapter 1** para **Bridge Adapter** e clique em **OK**

Nat Network



1) Vá em preferências.

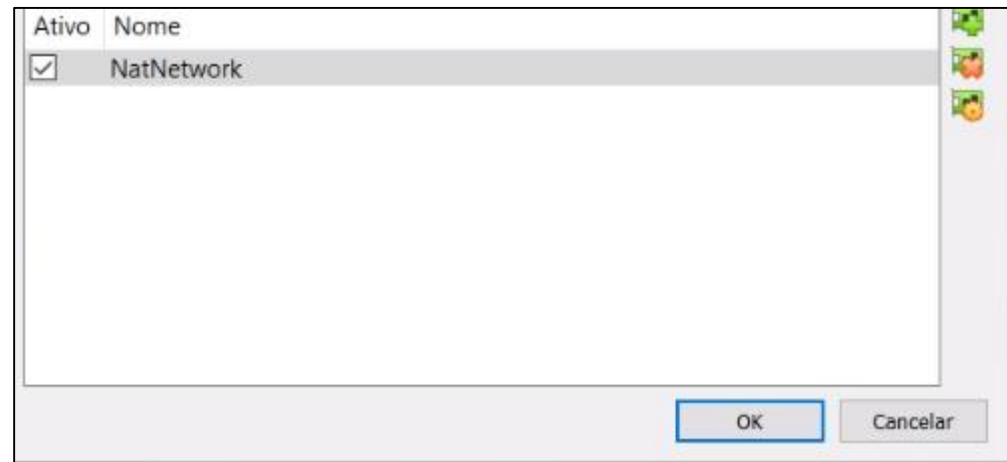


2) Abra o menu de Rede

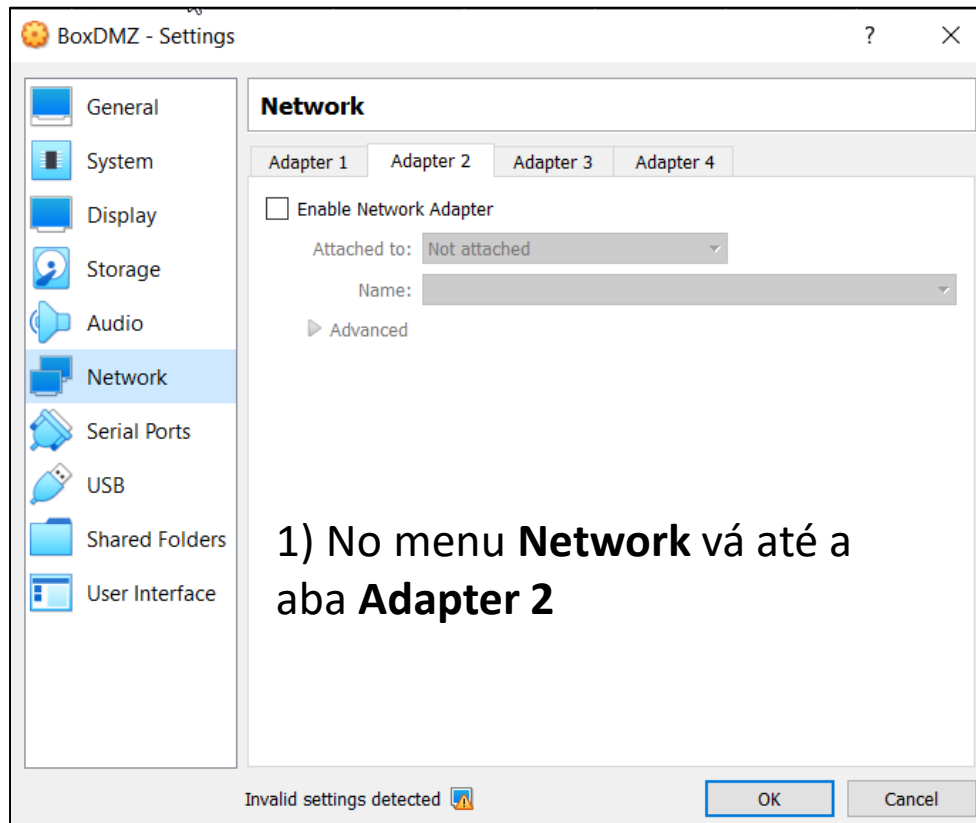
3) Do lado direito, selecione Adicionar

Nat Network

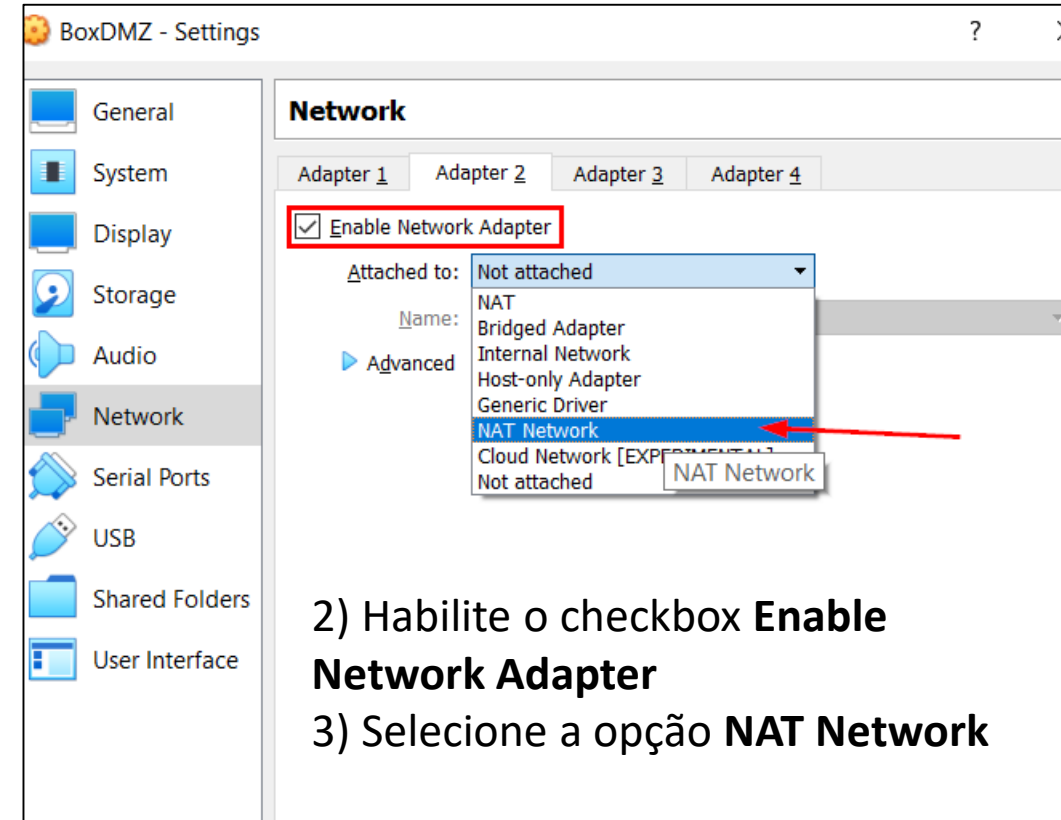
Selecione **OK** e prossiga.



Nat Network



1) No menu **Network** vá até a aba **Adapter 2**

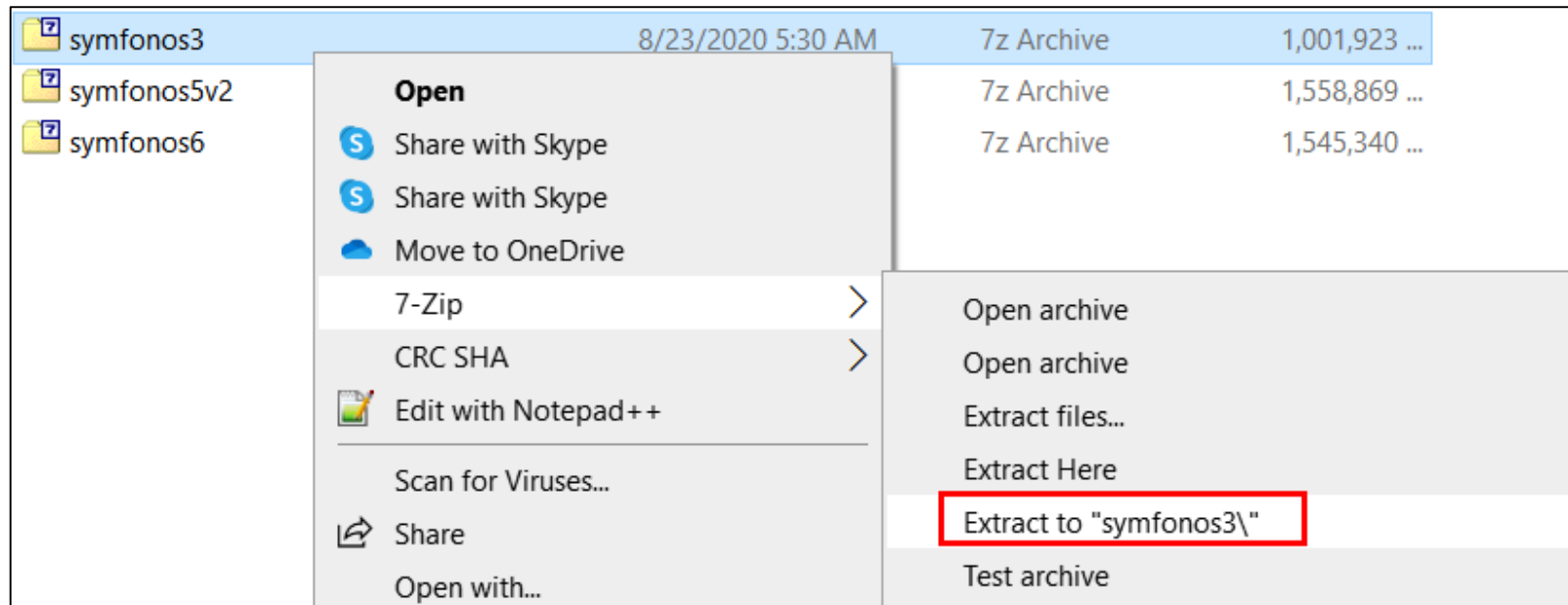


2) Habilite o checkbox **Enable Network Adapter**

3) Selecione a opção **NAT Network**

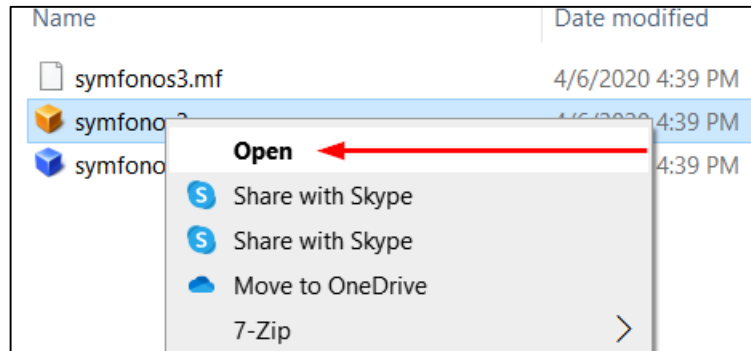
- Realize o download da VM symfonos -3 através da url:
<https://zayotic.s3.amazonaws.com/vm/symfonos3.7z>
- Descompacte o arquivo utilizando o 7z
- Realize a importação para o Virtual Box
- Altere a configuração da primeira interface de rede para **Nat Network**

Descompressão

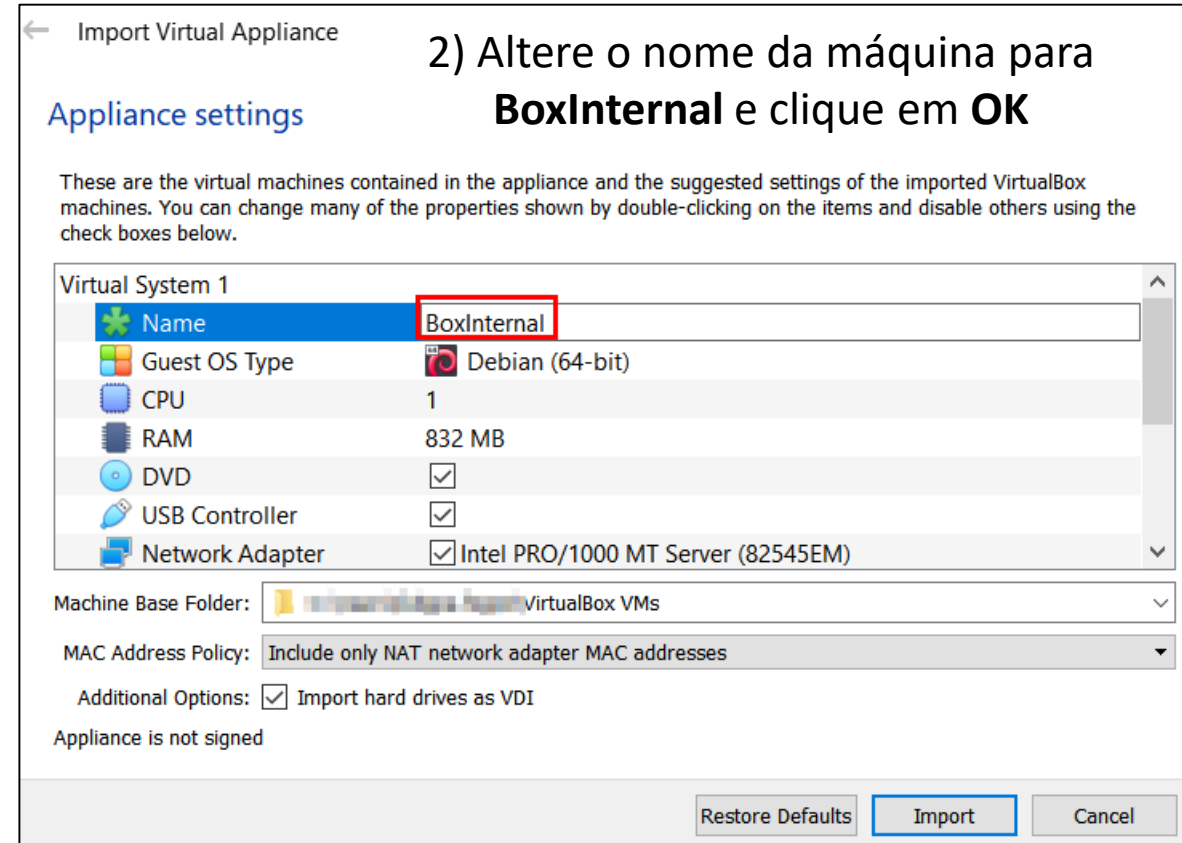


Posteriormente o download através do link fornecido no slide anterior, realize a extração do arquivo **symfonos3.7z**.

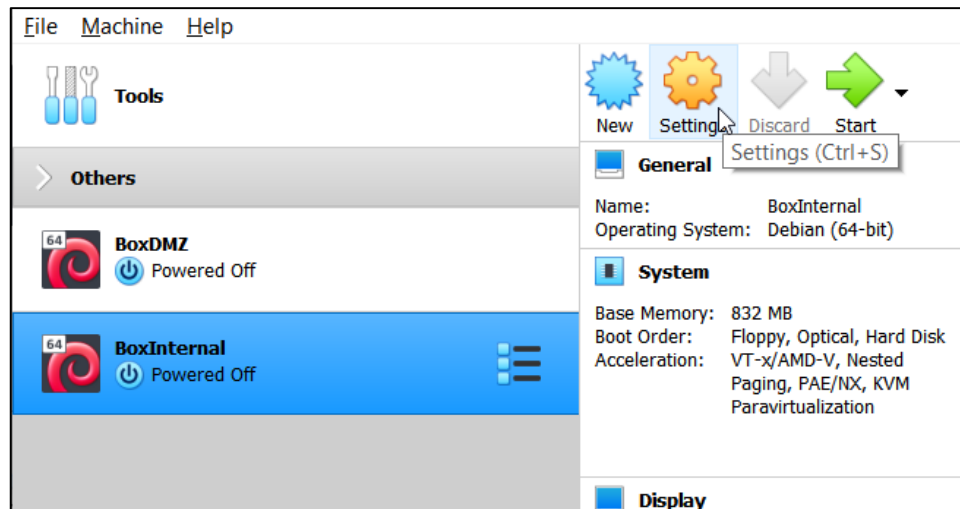
Import



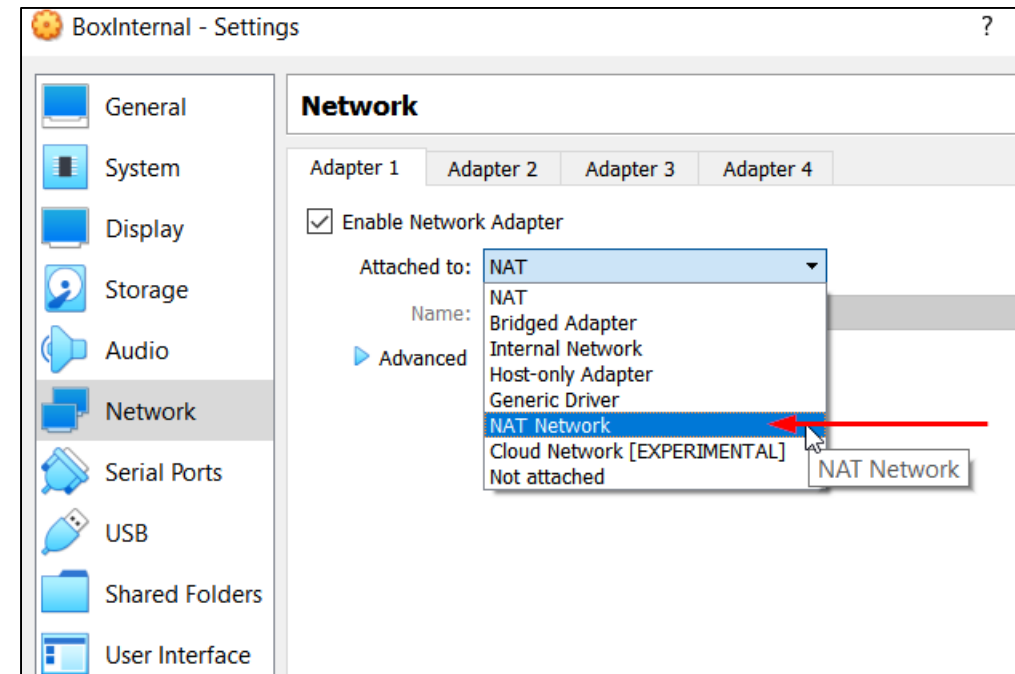
1) Clique com o **botão direito** do mouse no arquivo OVF e selecione **Open**



NAT Network



1) Selecione a VM **BoxInternal** e clique em **Settings**



2) Selecione a opção **Network** no menu
3) Altere a interface para **NAT Network**

- Criação de conta FREE em <https://wpvulndb.com/api>
- Instalação de ferramenta dirsearch

API wpvulndb

https://wpvulndb.com/api

WordPress Vulnerability Database API

The WPScan Vulnerability Database API is provided for users and developers to make use of our vulnerability database data. Our data includes WordPress vulnerabilities, plugin vulnerabilities and theme vulnerabilities. This API is also used by our [WordPress Security Scanner](#), our [Online WPScan WordPress Security Scanner](#) and our [WordPress Security Plugin](#).

Free	Starter	Professional	Enterprise
€0/month	€5/month	€25/month	€x/year
<ul style="list-style-type: none">✓ 50 API requests a day✓ Monthly email digests✗ Latest API endpoints✗ Get vulnerability details by ID✗ New vulnerability Webhooks✗ Slack Incoming Webhooks✗ Description API field✗ PoC API field✗ CVSS Risk Scores	<ul style="list-style-type: none">✓ 50 API requests a day✓ Instant/daily email alerts✗ Latest API endpoints✗ Get vulnerability details by ID✗ New vulnerability Webhooks✗ Slack Incoming Webhooks✗ Description API field✗ PoC API field✗ CVSS Risk Scores	<ul style="list-style-type: none">✓ 250 API requests a day✓ Instant/daily email alerts✓ Latest API endpoints✓ Get vulnerability details by ID✗ New vulnerability Webhooks✗ Slack Incoming Webhooks✗ Description API field✗ PoC API field✗ CVSS Risk Scores	<ul style="list-style-type: none">✓ Unlimited API requests a day✓ Instant/daily email alerts✓ Latest API endpoints✓ Get vulnerability details by ID✓ New vulnerability Webhooks✓ Slack Incoming Webhooks✓ Description API field✓ PoC API field✓ CVSS Risk Scores
REGISTER	REGISTER	REGISTER	CONTACT US

Acesse o endereço <https://wpvulndb.com/api> e inicie seu cadastro na opção FREE

Register a new user

* Name

* Email

* Password

* Password confirmation

Your Website


Twitter Username

► Billing Details

☐ Receive a monthly digest for new vulnerabilities

☐ Receive updates about WPVulnDB



☐ Receive updates about WPScan

☒ I'm not a robot 

[Privacy - Terms](#)

[REGISTER](#)

1) Preencha seus dados e registre.

 noreply@wpvulndb.com
Hoje, 04:28
Felippe 

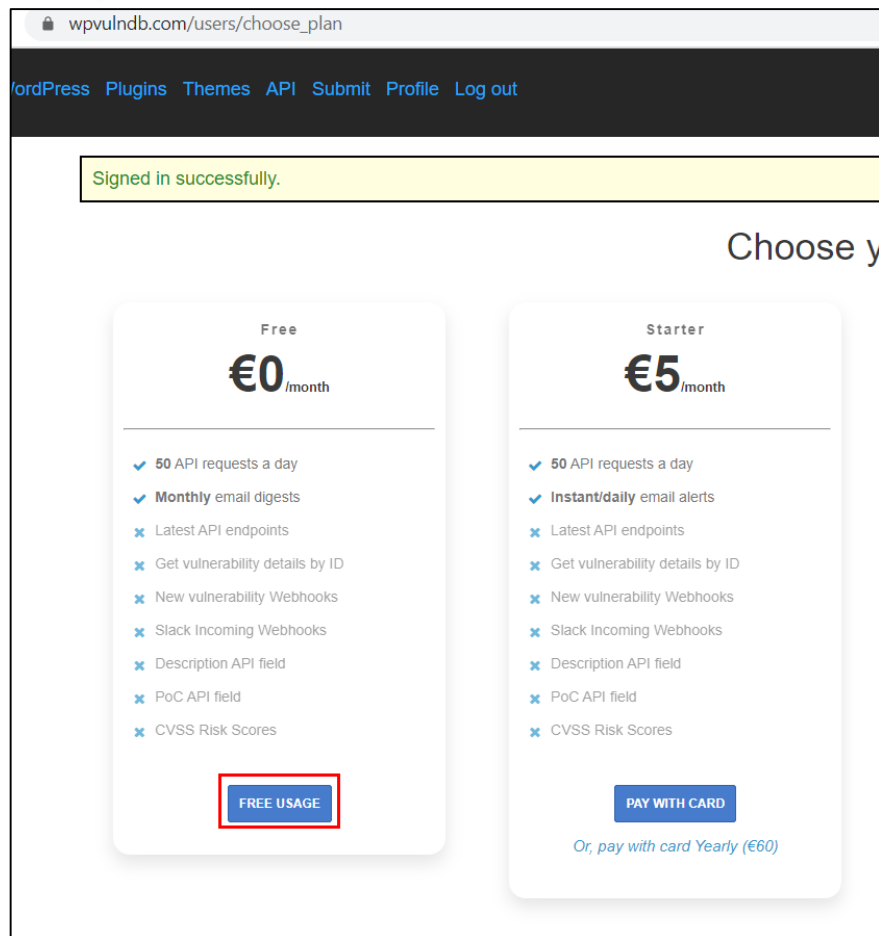
Welcome Felipe!

You can confirm your account email through the link below:

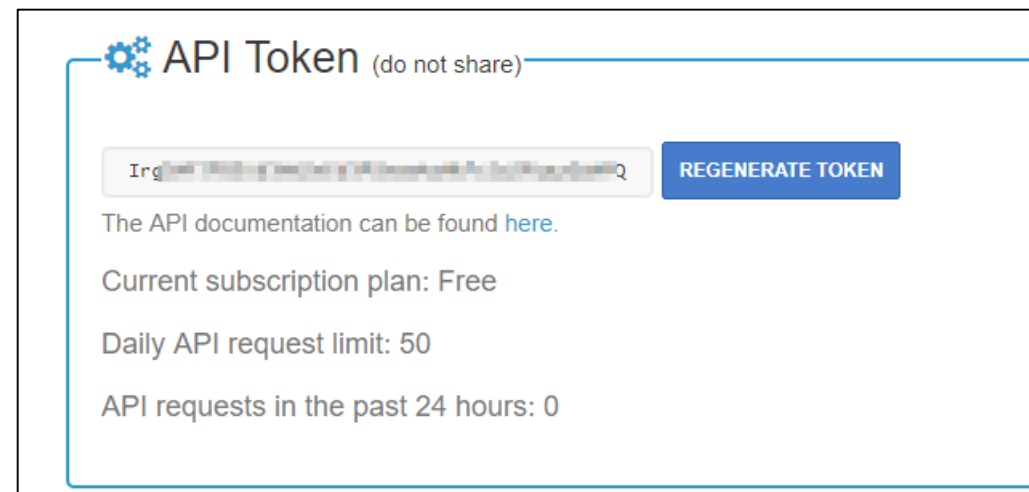
[Confirm my account](#)

2) No e-mail cadastrado, valide sua conta.

API wpvulndb



1) Selecione o plano **Free Usage**.



2) Obtenha sua chave na mesma página, logo abaixo em **API Token**

Dirsearch

```
kali@kali:~/Documents/workshop/dmz$ cd /opt/  
kali@kali:/opt$ sudo git clone https://github.com/maurosoria/dirsearch.git
```

1) No seu sistema Kali, no diretório */opt*, execute o comando: ***sudo git clone https://github.com/maurosoria/dirsearch.git***

```
kali@kali:/opt/dirsearch$ cd ..  
kali@kali:/opt$ cd dirsearch/  
kali@kali:/opt/dirsearch$ sudo ln -s /opt/dirsearch/dirsearch.py /usr/bin/dirsearch
```

2) Crie um link simbólico com o seguinte comando: ***sudo ln -s /opt/dirsearch/dirsearch.py /usr/bin/dirsearch***



Vai sobrar mais tempo e energia para sua empresa crescer.

ISH Tecnologia S/A

ish.com.br

comercial.sp@ish.com.br