LAB - SEM 06 - OSINT

LAB01: 21,80,110,143

executamos a varredura do nmap q passa por todas as portas

```
nmap -v -sT -p- mail.businesscorp.com.br
```

```
PORT      STATE    SERVICE
19/tcp    filtered chargen
21/tcp    open     ftp
25/tcp    filtered smtp
80/tcp    open     http
110/tcp   open     pop3
137/tcp   filtered netbios-ns
143/tcp   open     imap
1900/tcp  filtered upnp
2378/tcp  filtered dali
10571/tcp filtered unknown
10601/tcp filtered unknown
11211/tcp filtered memcache
14324/tcp filtered unknown
14523/tcp filtered unknown
42726/tcp filtered unknown
47541/tcp filtered unknown
51819/tcp filtered unknown
63859/tcp filtered unknown
```

LAB02: 53

Executamos uma busca mais rápida do nmap

```
nmap -sU -Pn mail.businesscorp.com.br --open
```

```
└─# nmap -sU -Pn mail.businesscorp.com.br --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 16:09 -03
Nmap scan report for mail.businesscorp.com.br (37.59.174.227)
Host is up (0.17s latency).
rDNS record for 37.59.174.227: ip227.ip-37-59-174.eu
Not shown: 954 closed udp ports (port-unreach), 45 open|filtered udp ports (no
-response)
PORT   STATE SERVICE
53/udp open  domain

Nmap done: 1 IP address (1 host up) scanned in 1307.69 seconds
```

Que só retornou a porta 53 como udp aberta

LAB03: 901238127-1281321-d192919

Uma vez que a porta estava aberta, fizemos a conexão via nc

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# nc -vu mail.businesscorp.com.br 53
DNS fwd/rev mismatch: mail.businesscorp.com.br ≠ ip227.ip-37-59-174.eu
mail.businesscorp.com.br [37.59.174.227] 53 (domain) open
ola
DESEC DNS SERVER 901238127-1281321-d192919
key
DESEC DNS SERVER 901238127-1281321-d192919
pwd
DESEC DNS SERVER 901238127-1281321-d192919
cd
DESEC DNS SERVER 901238127-1281321-d192919
^C
```

LAB04: camila,ca123456
Fazendo o filtro pelo pastebin no google:
businesscorp "pastebin"

LAB05: postfix
Primeiro fizemos um brute force de diretórios com o dirb, que usou sua common word list:

```
dirb mail.businesscorp.com.br
```

Com isso, obtivemos um diretório chamado squirrelmail
Ao logar com o usuário e senha encontrados, pudemos analisar o header da mensagem recebida pelo dev
[vale lembrar que antes de resetar a máquina, a pesquisa não tinha dado certo pois a caixa de entrada estava vazia]

```
Return-Path: <dev@businesscorp.com.br>
X-Original-To: camila@businesscorp.com.br
Delivered-To: camila@businesscorp.com.br
Received: by businesscorp.com.br (Postfix, from userid 33)
     id 978964300F; Tue, 9 Oct 2018 21:32:16 -0400 (EDT)
Received: from 189.29.146.62
     (SquirrelMail authenticated user dev)
     by 37.59.174.227 with HTTP;
     Tue, 9 Oct 2018 21:32:16 -0400
Message-ID: <47c63b7b2c06622bec4d8706a2a9b4f4.squirrel@37.59.174.227>
Date: Tue, 9 Oct 2018 21:32:16 -0400
Subject: Atualizacao
From: dev@businesscorp.com.br
To: jotafsantos@businesscorp.com.br
Cc: camila@businesscorp.com.br
User-Agent: SquirrelMail/1.4.23 [SVN]
MIME-Version: 1.0
Content-Type: text/plain;charset=iso-8859-1
Content-Transfer-Encoding: 8bit
X-Priority: 3 (Normal)
Importance: Normal
```

LAB06: squirrelmail

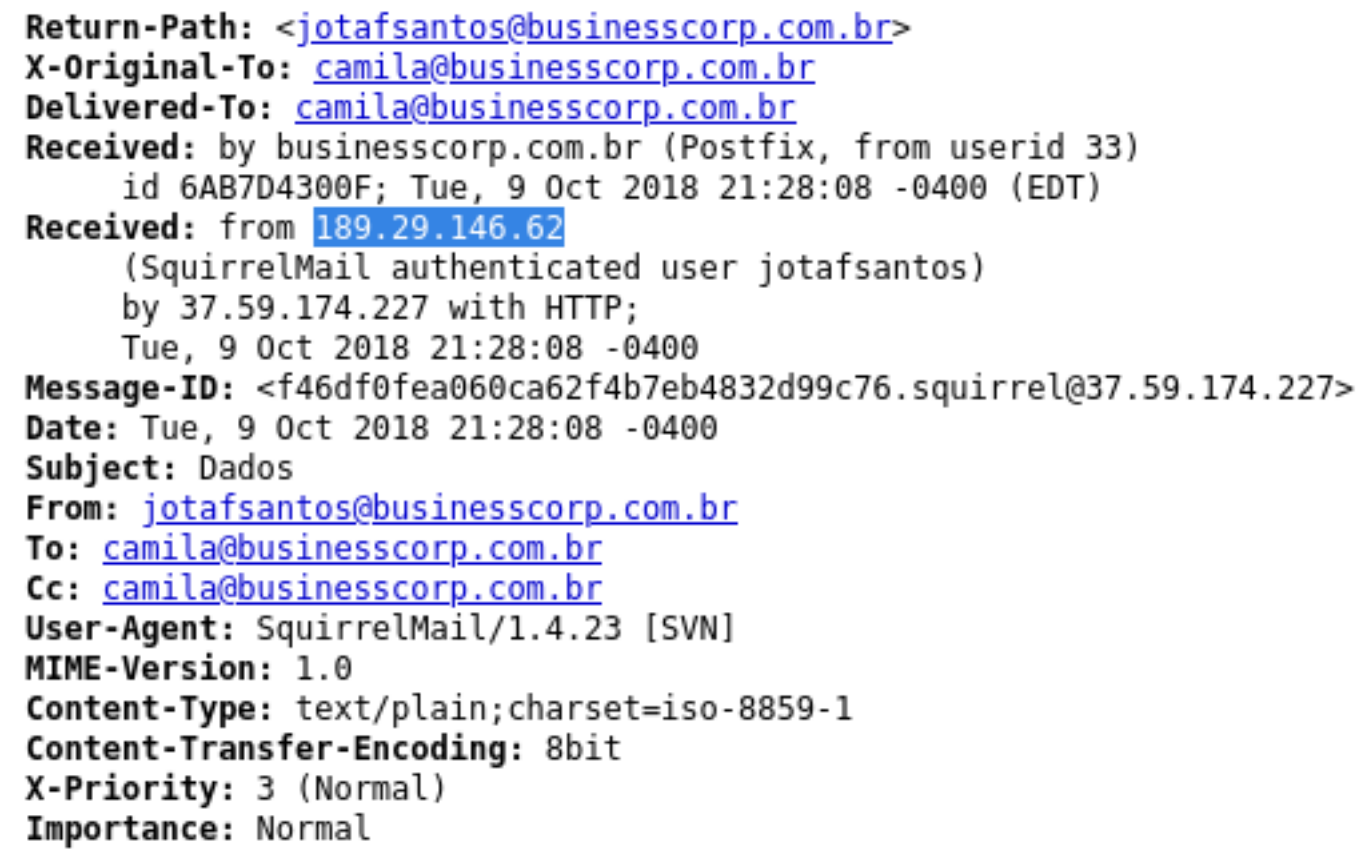
Segue do lab passado

LAB07: squirrelmail1.4.23
Basta ler o campo do User-Agent

LAB08: jotafsantos@businesscorp.com.br
Basta olhar a caixa de entrada

LAB09: 09/10/2018
Segue do lab passado

LAB10: 189.29.146.62
Veja a imagem printada



LAB11: bj9384221-
Basta ler o campo de mensagens enviadas: sents

LAB12: dev@businesscorp.com.br
Veja na caixa dos emails recebidos, só tem 2 emails

LAB13: camila,bj9384221-
O conteúdo da mensagem trocada mostra que a senha enviada pela camila é dela msm

Message List | Unread | Delete Previous | Next

Subject: Dados
From: jotafsantos@businesscorp.com.br
Date: Tue, October 9, 2018 9:28 pm
To: camila@businesscorp.com.br
Cc: camila@businesscorp.com.br
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file

```
Ca,

Estou precisando da sua senha para cadastro, a minha esta bloqueada.

Pode me passar?

Bjs
```

LAB14: 327-9931231-48848d3
Basta entrar no site da businesscorp e ir para o servidor de email que será apresentada uma página para logar na intranet. Fazemos o login com o usuário e senha do lab passado