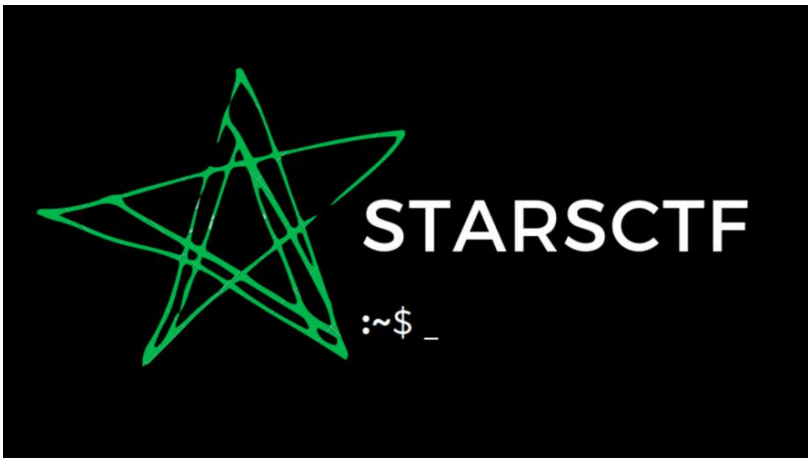

Name: Hijacked Server
Category: Network
File: *2d7c78a75e1b2cc731712a8d5fe7edd4*
Message:

Nosso servidor SMTP foi invadido.
Precisamos descobrir detalhes sobre o ataque.

Qual o IP, usuário, senha e o e-mail do destinatário utilizado pelo atacante?

Resolução:

Mais um arquivo sem extensão.
Usando o comando *file* descobrimos que é um arquivo TCPDump:

```
shellt3r@lhost:~/Downloads$ file 2d7c78a75e1b2cc731712a8d5fe7edd4
2d7c78a75e1b2cc731712a8d5fe7edd4: tcpdump capture file (little-endian) - version 2.4
(Ethernet, capture length 65535)
```

Image 1 - Comando FILE

Abrindo o arquivo no *WireShark* com o comando:

```
wireshark -r 2d7c78a75e1b2cc731712a8d5fe7edd4
```

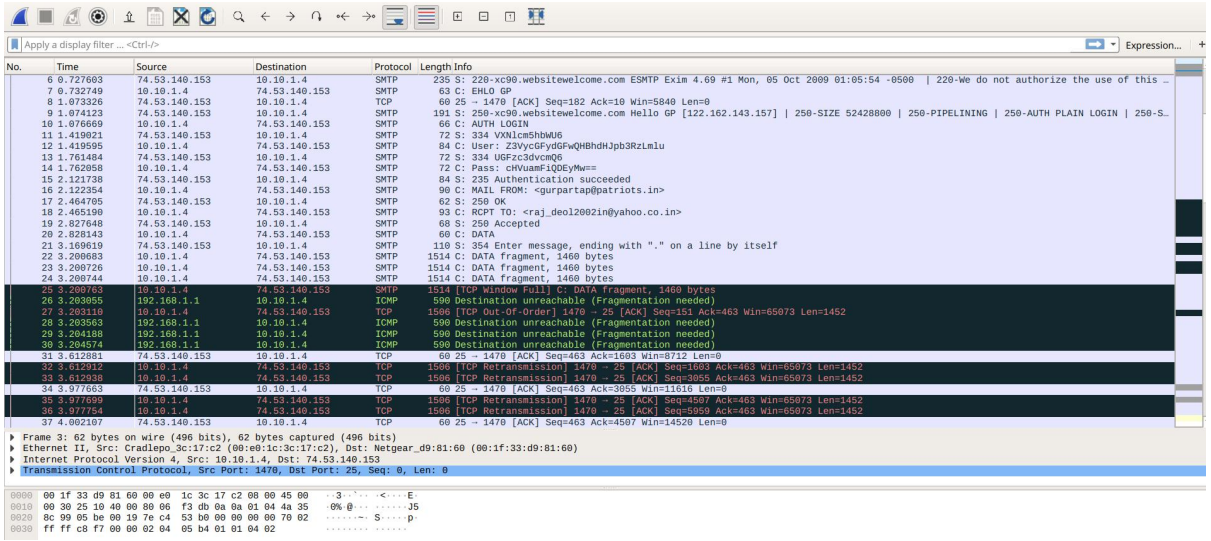

Image 2 - Leitura de pacote TCPDump com Wireshark

Seguindo o *TCP Steam* podemos ler o conteúdo completo enviado:

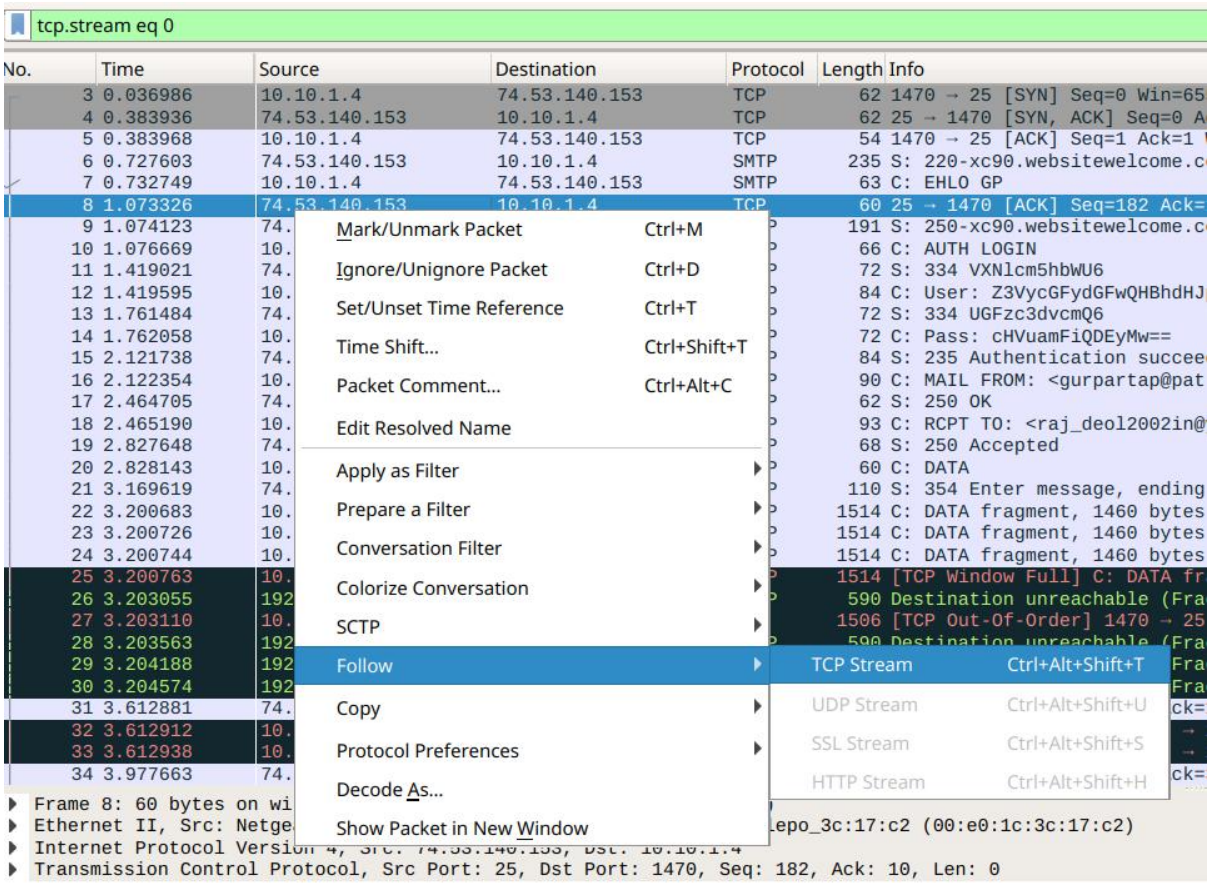

Image 3 - TCP Steam com Wireshark

```
220-xc90.websitewelcome.com ESMTP Exim 4.69 #1 Mon, 05 Oct 2009 01:05:54 -0500
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO GP
250-xc90.websitewelcome.com Hello GP [122.162.143.157]
250-SIZE 52428800
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
AUTH LOGIN
334 VXNlcm5hbWU6
Z3VycGFydGFwQHBhdHJpb3RzLmlu
334 UGFzc3dvcmQ6
cHVuamFiQDEyMw==
235 Authentication succeeded
MAIL FROM: <gurpartap@patriots.in>
250 OK
RCPT TO: <raj_deol2002in@yahoo.co.in>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
From: "Gurpartap Singh" <gurpartap@patriots.in>
To: <raj_deol2002in@yahoo.co.in>
Subject: SMTP
Date: Mon, 5 Oct 2009 11:36:07 +0530
Message-ID: <000301ca4581$ef9e57f0$cedb07d0$@in>
MIME-Version: 1.0
Content-Type: multipart/mixed;
          boundary="----=_NextPart_000_0004_01CA45B0.095693F0"
X-Mailer: Microsoft Office Outlook 12.0
Thread-Index: AcpFgem9BvjjZEDeR1Kh8i+hUyVo0A==
Content-Language: en-us
x-cr-hashedpuzzle: SeA= AAR2 ADaH BpiO C4G1 D1gW FNB1 FPkR Fn+W HFCP HnYJ JO7s Kum6 KytW LFcI LjUt;
1;cgBhAGoAXwBkAGUAbwBsADIAMAAwADIAaQBuAEAAeQBhAGgAbwBvAC4AYwBvAC4AaQBuAA==;Sosha1_v1;7;{CAA37F59-1850-45C7-8540-
AA27696B5398};ZwB1AHIAcABhAHIAdABhAHAAQABwAGEAdAByAGkAbwB0AHMALgBpAG4A;Mon, 05 Oct 2009 06:06:01 GMT;UwBNAFQAUAA=
x-cr-puzzleid: {CAA37F59-1850-45C7-8540-AA27696B5398}

This is a multipart message in MIME format.

------=_NextPart_000_0004_01CA45B0.095693F0
Content-Type: multipart/alternative;
          boundary="----=_NextPart_001_0005_01CA45B0.095693F0"


------=_NextPart_001_0005_01CA45B0.095693F0
Content-Type: text/plain;
          charset="us-ascii"
Content-Transfer-Encoding: 7bit
```

Packet 22. 19 client pkts, 10 server pkts, 18 turns. Click to select.

Image 4 - TCP Steam com Wireshark 2

Em **AUTH LOGIN** temos informações que aparentemente estão em base64.

Se decodificarmos as strings no site *Base64Decode* para ASCII teremos:

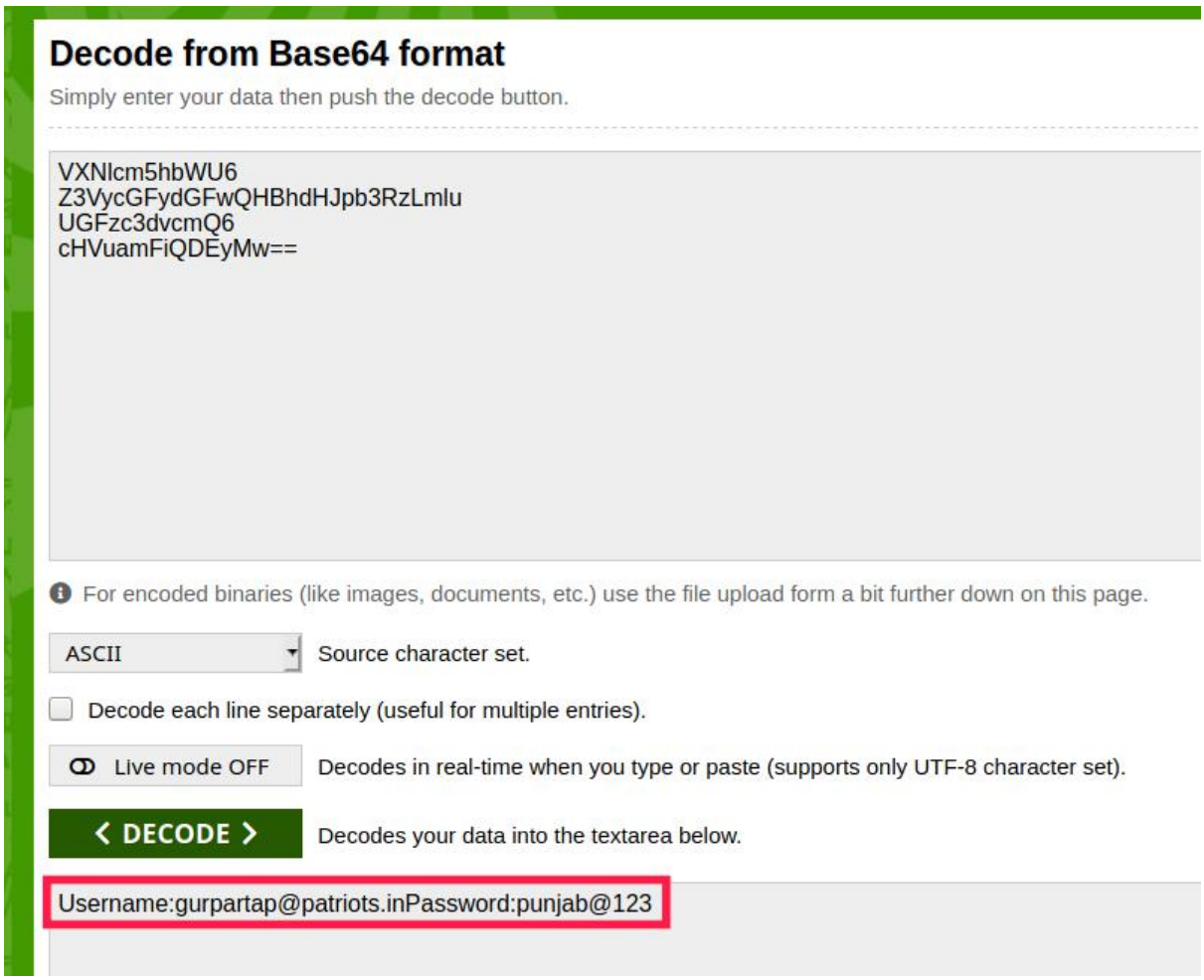

Image 5 - Site base64decode

Assim, conseguimos quase todas as informações que precisamos:

- Usuário;
- Senha;
- E-mail do destinatário.

Uma “pegadinha” do desafio é sacar que o IP que se é pedido não é o IP do alvo, mas do atacante.

Podemos achá-lo na tela inicial do Wireshark:

Source	Destination	Protocol
10.10.1.4	74.53.140.153	TCP
74.53.140.153	10.10.1.4	TCP
10.10.1.4	74.53.140.153	TCP
74.53.140.153	10.10.1.4	SMTP
10.10.1.4	74.53.140.153	SMTP
74.53.140.153	10.10.1.4	TCP
74.53.140.153	10.10.1.4	SMTP
10.10.1.4	74.53.140.153	SMTP
74.53.140.153	10.10.1.4	SMTP
10.10.1.4	74.53.140.153	SMTP
74.53.140.153	10.10.1.4	SMTP
10.10.1.4	74.53.140.153	SMTP
74.53.140.153	10.10.1.4	SMTP
10.10.1.4	74.53.140.153	SMTP
74.53.140.153	10.10.1.4	SMTP
10.10.1.4	74.53.140.153	SMTP
74.53.140.153	10.10.1.4	SMTP
10.10.1.4	74.53.140.153	SMTP
74.53.140.153	10.10.1.4	SMTP
10.10.1.4	74.53.140.153	SMTP
10.10.1.4	74.53.140.153	SMTP
10.10.1.4	74.53.140.153	SMTP

Image 6 - IP do atacante no Wireshark

Source IP = *74.53.140.153*

Assim, achamos tudo que precisamos para submeter nossa flag!

OBS.: Lembrando que a descrição do desafio pede para submetermos as respostas as separando por vírgula (**,**).

Flag(*74.53.140.153,gurpartap@patriots.in,punjab@123,raj_deol2002in@yahoo.co.in)*

Pesquisas:
encurtador.com.br/ayUW4
encurtador.com.br/nqEOP