

## Forensics : My First Pcap 50

Description : Find the flag in the network traffic

Attachment : easy.pcap

Challenge


266 Solves

×

# My First Pcap 50

Find the flag in the network traffic

Author: freethepockets

 easy.pcap

Flag

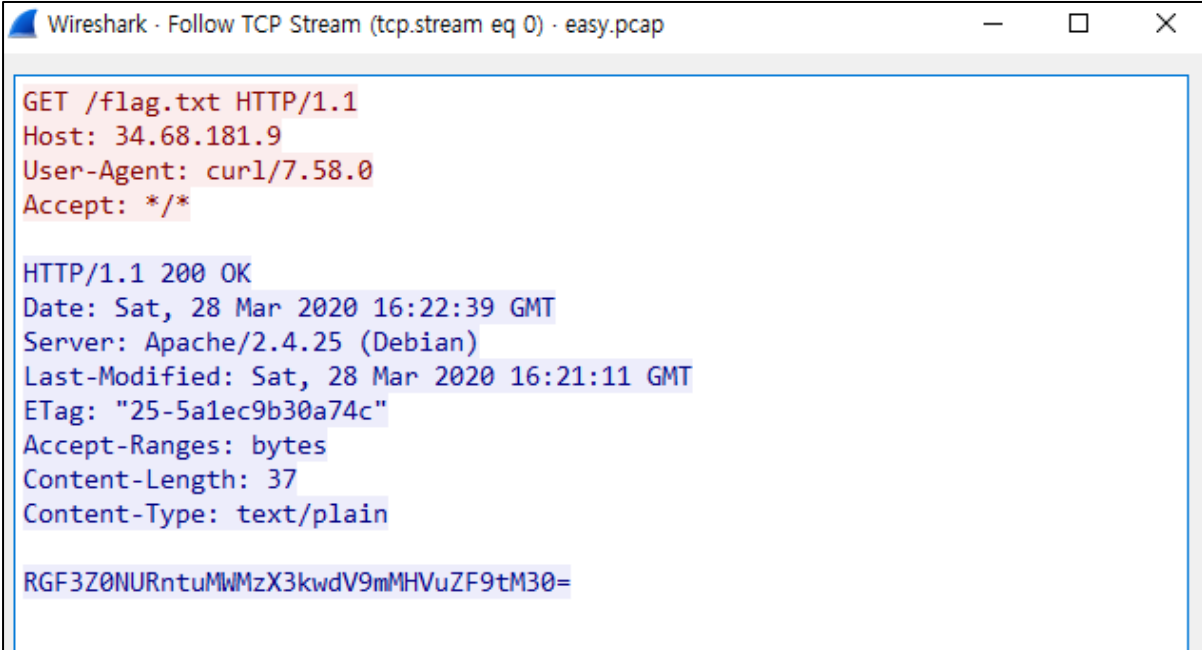
Submit

Solutions :

1. Opening Attachment file in WireShark.
2. Check the packet in conversation.

Ethernet · 1 IEEE 802.11 IPv4 · 6 IPv6 TCP · 1 UDP · 5 USB													
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.11	59356	34.68.181.9	80	10	1024	6	487	4	537	16.308567	0.1153	33 k	37 k

3. See the packet movement in TCP and follow stream.



```
GET /flag.txt HTTP/1.1
Host: 34.68.181.9
User-Agent: curl/7.58.0
Accept: */*

HTTP/1.1 200 OK
Date: Sat, 28 Mar 2020 16:22:39 GMT
Server: Apache/2.4.25 (Debian)
Last-Modified: Sat, 28 Mar 2020 16:21:11 GMT
ETag: "25-5a1ec9b30a74c"
Accept-Ranges: bytes
Content-Length: 37
Content-Type: text/plain

RGF3Z0NURntuMWMzX3kwdV9mMHVuZF9tM30=
```

4. Extract flag.txt file.

Packet	Hostname	Content Type	Size	Filename
45	34.68.181.9	text/plain	37 bytes	flag.txt

5. The contents of the file are the same as those found in the packet.

RGF3Z0NURntuMWMzX3kwdV9mMHVuZF9tM30=

6. However, since the flag is encrypted, the encryption type is detected and decrypted.

### Enter Ciphertext here

RGF3Z0NURntuMWMzX3kwdV9mMHVuZF9tM30=

Analyze TextCopyPasteText Options...

Note: To get accurate results, your ciphertext should be at least 25 characters long.

7. Encryption type is Base64.

### Analysis Results

RGF3Z0NURntuMWMzX3kwdV9mMHVuZF9tM30=

Your ciphertext is likely of this type:

[Base64 \(click to read more\)](#)

8. Thus, when decrypting this ciphertext, the flag is appeared.

#### Decode from Base64 format

Simply enter your data then push the decode button.

RGF3Z0NURntuMWMzX3kwdV9mMHVuZF9tM30=

UTF-8

Source character set.

Decode each line separately (useful for multiple entries).

Live mode OFF

Decodes in real-time when you type or paste (supports only UTF-8 character set).

< DECODE >

Decodes your data into the textarea below.

DawgCTF{n1c3\_y0u\_f0und\_m3}

9. Flag is DawgCTF{n1c3\_y0u\_f0und\_m3}

**Flag :** DawgCTF{n1c3\_y0u\_f0und\_m3}