

Forensics : Another Pcap 100

Description : The flag must be somewhere around here...

Attachment : alittleharder.pcap

Challenge


132 Solves

×

Another Pcap 100

The flag must be somewhere around here...

Author: freethepockets

 alittleharder....

Flag

Submit

Solutions :

1. Opening Attachment file in WireShark.
2. Check the packet in conversation.
3. See the packet movement in TCP and follow stream.

```
Wireshark · Follow TCP Stream (tcp.stream eq 8) · alittleharder.pcap


GET /nothinghere.tar.gz 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 16:55:36 GMT
Server: Apache/2.4.25 (Debian)
Last-Modified: Sat, 28 Mar 2020 16:53:11 GMT
ETag: "a8-5a1ed0da263c9"
Accept-Ranges: bytes
Content-Length: 168
Content-Type: application/x-gzip
```

4. Extract **nothinghere.tar.gz** file.

Packet	Hostname	Content Type	Size	Filename
214	34.68.181.9	text/html	273 bytes	nothinghere.tar.zip
314	34.68.181.9	application/x-gzip	168 bytes	nothinghere.tar.gz

5. Unzip **nothinghere.tar.gz** file.

 flag.txt	45	45
--	----	----

6. Open flag.txt file and check contents.

Contents : RGF3Z0NURnszeHRyNGN0MW5nX2YxbDM1XzFzX2Z1bn0=

```
RGF3Z0NURnszeHRyNGN0MW5nX2YxbDM1XzFzX2Z1bn0=
```

7. The content of this file is encrypted base64.

8. When decrypting this ciphertext, the flag is appeared.

Decode from Base64 format
Simply enter your data then push the decode button.

RGF3Z0NURnszeHRyNGN0MW5nX2YxbDM1XzFzX2Z1bn0=

For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

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{3xtr4ct1ng_f1l35_1s_fun}

9. Flag is **DawgCTF{3xtr4ct1ng_f1l35_1s_fun}**

Flag : **DawgCTF{3xtr4ct1ng_f1l35_1s_fun}**