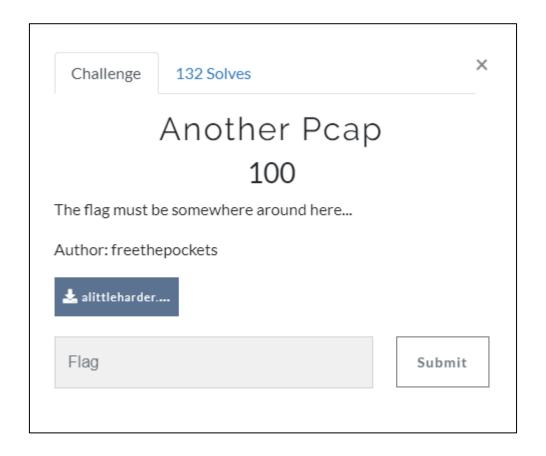
Forensics: Another Pcap 100

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

Attachment : alittleharder.pcap



Solutions:

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



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

| _ | | | | | Ξ |
|--------|-------------|--------------------|-----------|---------------------|---|
| Packet | Hostname | Content Type | Size | Filename | 1 |
| 214 | 34.68.181.9 | text/html | 273 bytes | nothinghere.tar.zip | 1 |
| 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.

| ecode from Base64 format | |
|---|---|
| mply 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. | pload form a bit further down on this page. |
| JTF-8 ▼ Source character set. | |
| Decode each line separately (useful for multiple entries). | |
| Decodes in real-time when you type or paste (supports only UTF-8 character set). | ste (supports only UTF-8 character set). |
| C DECODE > Decodes your data into the textarea below. | |
| awgCTF{3xtr4ct1ng_f1l35_1s_fun} | |

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

Flag: DawgCTF{3xtr4ct1ng_f1l35_1s_fun}