# Challenge 2: ICMP Exfiltration

Contexte: Nous avons remarqué des échanges curieux avec le serveur dash.pasfastoche.lan. Il semblerait que de nombreuses requêtes ping soient envoyées par là-bas. Trouvez ce qu'il s'y trame..

Hint : Les trames intéressantes possède un ttl modifié.

=> Les trames modifiées ont un ttl à 20. Pour filtrer ceci avec wireshark, ip.ttl==20 pour passer à la Step-2.

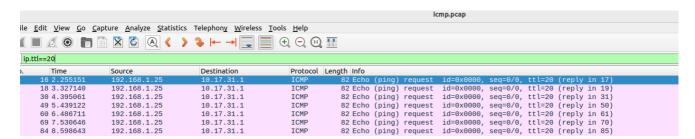
### Step 1 : Retrouver les trames intéressantes

Il faut tout d'abord retrouver l'IP de la machine distante :

dns.qry.name=="dash.pasfastoche.lan", nous retrouvons 10.17.31.1, on va pouvoir s'en servir pour filtrer un peu plus avec ip.addr==10.13.31.1.

Parmi toutes les trames envoyées, seules les trames ICMP à destination de la machine 10.17.31.254 nous intéressent.

Seulement, il faut aussi faire attention, seules celles avec un TTL à 20 sont vraiment intéressantes ^:)



### Step 2 : Se rendre compte de ce qui est vraiment intéressant

Maintenant qu'on a les bonnes trames, il faut également se rendre compte que le champ data est modifié et ce qui est envoyé est en base64.

On peut voir que la dernière trame se termine par '==', c'est caractéristique d'un base64.

## Step 3: Reconstruire le base64

Ecrire un script permettant de reconstruire le base64 en entier, par exemple :

```
from scapy.all import *

pcap_flow = rdpcap('icmp.pcap')

solv = list()
for packet in pcap_flow:

if 'ICMP' in packet and packet.ttl == 20:
    payload = packet[ICMP].payload
    solv.append(payload.load.decode("utf-8"))
```

PROF

```
print("Base64 : ", end = '')
print(''.join(solv))
```

# Step 4: Retrouver l'information utile

Premier reflexe: https://base64decode.org

#### **Decode from Base64 format** Simply enter your data then push the decode button. iVBORw0KGgoAAAANSUhEUgAAAUoAAAAjCAIAAAB9x9R0AAAACXBIWXMAAA7EAAAOxAGVKw4bAAAQNklEQVR4nO2ce1RTV77Hv5CcBD0pJIgENMgjiqkgOA 1zwceUXpWxhd7lg6WuqdyxapW5LaWtrKV4x8eqdap2Xdpetd6FrTJ2ZKbSZattsVqkU9oRpEOqRGiDEoQmWg6PnITmQHJOEu4fAQwWEkUcZ+j5/AVnv/tZ39/+7d8+44AVnVfZ39/-7d8+44AVnVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7d8+44AVNVfZ39/-7dDdt2jTw8PCMR/wfdAd4eHjuF7y8eXjGLby8eXj PLVqmDYnRHr35Uyfku4BshgJgVazNlzStPF+sYsAwHgD69KeM0ZE/sLV45Fo2MJf4Llq9Y3nEuVxOyb0NsTfGnH3QDACFT/PbRmSnhgVJSwFk6a77WHNGaGc9yAulurdenseted (Control of the Control of the Co/PrU4K9R68t2yP3UAABn/WMnjUzxysDWnPtijdxGK1MOrZJ8f/fRPNAAg/JfFT4X+7d2yjyN+ffjfQ37aofqz721rcAEA5JPTIgV0FI4qKuf6VUEELf/LwwkSj+xa/b7NHfaxmg0 8 JZefXVKoEyL2F1dlhNpWFl5cMve58 IASJUJoNRq21 nxsRgPBBEoYoZDurjv1653 u0MjZu1Pn2R1P7JrkbbQLr/jLlzUtDNeBxGmKa/v/QuQYTP2pkuq/nky7Mml9nk8tJEuple12 nvgVp18 nvgVp1e8OFlwwEASA0fuvjk+o/+fJjEwCYuwdLycQS1t6g5W6pguuu2Ky9lBKnbl1T6fUlpYyDto+xtvuxX97TeMtfsHKdd1BGlidA0y3N3E+7RJ25/tFYdm+MoC2f77XcayWjfCmjmeG775uzpbbXMUckIUCNgRyFZ86cBgAUnD5TgAHnfOT85KwVm9YuilPIg0WsyXDI9OHX37/CDCQ9vWVTRqIMt05MJbNoKVmyuuDTezS0dwrTeHFL48AvP/x9avST/ 6EKIRqN7pEQ4bPzpnce+SvyskJvlbEz1zsAsY2FkzaZr3b4asOdH4CQBZzmYYqlAPQ5WM9HfZbmHgtcVhYOxn5D1zMkv0ySkhOZkkxKRS6zwXzhgF6j64vMfyQrpscs CwxhuirL/VKygwP0xpLNN29w4nlvJSVRVJs8OEouAG2+UKiv0fUN1OWwGnqo5qH9IYOWvx0rPVV/tNQGQJAYmbNb2rRN+5m2T56TiLNsAgDgoefOTgNuOeeR+Y+s// 1 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page. ASCII Source character set. Decode each line separately (useful for when you have multiple entries). Decodes in real-time as you type or paste (supports only the UTF-8 character set). ✓ DECODE ➤ Decodes your data into the area below.

Intéressant : On observe qu'il s'agit d'une image PNG!

IHDR◆◆岡J◆◆◆#醞園◆◆◆身★◆◆ pHYs◆◆ 配◆◆園田+園園◆◆園日ATX{TSW園=)\$園4#"8

Deuxième reflexe : google : base64 to PNG

Base64 to Image

Convert Base64 to image online using a free decoding tool which allows you to decode Base64 as image and preview it directly in the browser. In addition, you will receive some basic information about this image (resolution, MIME type, extension, size). And, of course, you will have a special link to download the image to your device. If you are looking for the reverse process, check Image to Base64.

PROF

iVBORw0KGgoAAAANSUhEUgAAAUoAAAAjCAIAAAB9x9R0AAAACXBINXMAAA7EAAAOxAGVKw4bAAAQNklEQVR4n02celRTV77Hv5CcB00pJIgENMgjIqkg0AlzwceUXpWxhd7lg6WuqdyxapW5LaWtrV4x8eqdap2Xdpetd6Fr712ZKb5ZattsVqkU9oRpE0qRGi
DEOdmig6Pn1TmCH10Eu4fAQwMEkUc2-j5/A7nv/f239/-7d8+A0dt2jTw3PCNR/wfdAdeHjUF7ye8XjGLby8eXjGLby /Lwk/sj-xa //DTHF1amp035UnNf5B7NgLD90Ubbv06L4K56XYncude1NRTLgfr9EyyarvqRXaPR5zmpYsaCNSvqecNVxWZHf0FVcyxNa03RjcETZkmPPvmpLphNcz6NUWZ25hhCt0Fo3gpo53hu8JZefXVKoEyL2F1dlNpWF15cMvc581ASJUJoNRq21nxsRgPBBE0YoZDur

Decode Base64 to Image

Preview Image | Toggle Background Color

Bingo!