

# Réseau - PingFrenesy - 75 points

Kévin DUVERGER

## Table des matières

<b>1</b>	<b>Résolution PingFrenesy :</b>
----------	---------------------------------

**2**

# 1 Résolution PingFrenesy :

Encore une fois, tentons d'ouvrir le fichier .pcap qui nous est donné pour voir ce qu'il contient. Le challenge se nommant PingFrenesy, il faut probablement aller voir du côté des paquets ICMP :

64	3.562848	192.168.1.44	192.168.1.99	ICMP	42 Echo (ping) request	id=0x0000, seq=0/0, ttl=64 (no response found!)
65	4.075475	192.168.1.44	192.168.1.114	ICMP	42 Echo (ping) request	id=0x0000, seq=0/0, ttl=64 (no response found!)
66	4.583639	192.168.1.44	192.168.1.121	ICMP	42 Echo (ping) request	id=0x0000, seq=0/0, ttl=64 (no response found!)
67	4.920068	192.168.1.44	142.250.201.170	UDP	71 63540 → 443	Len=29
68	4.968352	142.250.201.170	192.168.1.44	UDP	67 443 → 63540	Len=25
69	5.098453	192.168.1.44	192.168.1.112	ICMP	42 Echo (ping) request	id=0x0000, seq=0/0, ttl=64 (no response found!)
70	5.134044	146.59.227.136	192.168.1.44	TCP	82 9876 → 26018 [PSH, ACK]	Seq=29 Ack=1 Win=501 Len=28
71	5.175973	192.168.1.44	146.59.227.136	TCP	54 26018 → 9876 [ACK]	Seq=1 Ack=57 Win=254 Len=0
72	5.609577	192.168.1.44	192.168.1.116	ICMP	42 Echo (ping) request	id=0x0000, seq=0/0, ttl=64 (no response found!)
73	6.126292	192.168.1.44	192.168.1.105	ICMP	42 Echo (ping) request	id=0x0000, seq=0/0, ttl=64 (no response found!)
74	6.629677	192.168.1.44	192.168.1.115	ICMP	42 Echo (ping) request	id=0x0000, seq=0/0, ttl=64 (no response found!)

  

> Frame 64: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)	0000	ff ff ff ff ff ff f0 9e	4a ce 5b 03 08 00 45 00	..... J.[...E
> Ethernet II, Src: Intel_ce:5b:03 (f0:9e:4a:ce:5b:03), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	0010	00 1c 00 01 00 00 40 01	f7 00 c0 a8 01 2c c0 a8	.....@: ..... ,..
> Internet Protocol Version 4, Src: 192.168.1.44, Dst: 192.168.1.99	0020	01 63 08 00 f7 ff 00 00	00 00	.C..... ..
> Internet Control Message Protocol				

Cette fois-ci il semble y avoir de très nombreux pings qui n'aboutissent pas vraiment. En revanche, on peut voir que le dernier octet de l'adresse IP change très souvent de valeur, peut être est-ce un message !

Nous pouvons envoyer le premier ensemble de nombres, [ 99, 114, 121, 112, 116, 105, 115 ] dans un site pour nous convertir des codes ASCII vers de texte, ce qui nous donne le texte assez familier suivant :

```
1 cryptis
```

Pour résoudre ce challenge, il faut toujours récupérer le dernier octet et voici un code qui permet de le faire de manière complètement automatique (en gros il recherche tous les endroits où les 3 premiers octets de l'IP apparaissent puis enregistre le dernier) :

```
1 fichier = open("capture.pcap", "rb")
2 data = fichier.read()
3 fichier.close()
4
5 for i in range(0, len(data) - 3) :
6     if data[i] == 192 and data[i + 1] == 168 and data[i + 2] == 1 :
7         if data[i + 3] != 44 and data[i + 3] >= 32 and data[i + 3] <= 127 :
8             print(chr(data[i + 3]), end="")
9 print()
```