

Description

How about some hide and seek heh?Download this [file](#) and find the flag.

Hints

- (None)

Solución

Abrimos el archivo y vamos recorriendo los paquetes para ver su contenido. Poco a poco vemos que nos van dando pistas.

trace.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.253.0.55	10.253.0.6	IPv4	48	IPv6 hop-by-hop optio
2	0.000855	10.253.0.55	10.253.0.6	TCP	40	1337 → 22 [SYN] Seq=0
3	0.001376	10.253.0.55	10.253.0.6	ICMP	28	Echo (ping) request
4	0.001845	172.16.0.2	10.253.0.6	FTP	74	Request: username
5	0.002492	127.0.0.1	127.0.0.1	DNS	55	Unknown operation (14
6	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
7	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
8	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
9	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
10	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
11	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
12	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
13	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
14	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
15	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
16	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
17	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
18	0.002992	10.253.0.55	192.168.5.5	EXEC	62	Client -> Server data
19	0.002992	10.253.0.55	192.168.5.5	Rlogin	62	Data: gc2VjcmV0OiBwaw
20	0.002992	10.253.0.55	192.168.5.5	RSH	62	Client -> Server data
21	0.002992	10.253.0.55	192.168.5.5	LPD	62	LPD continuation
22	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
23	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
24	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes
25	0.002992	10.253.0.55	192.168.5.5	FTP-DA...	62	FTP Data: 22 bytes

Frame 5: 55 bytes on wire (44 bytes captured) on interface 0:0:0:0:0:0

Internet Protocol Version 4, Src: 127.0.0.1, Destination: 127.0.0.1

User Datagram Protocol, Src Port: 54321, Destination Port: 53

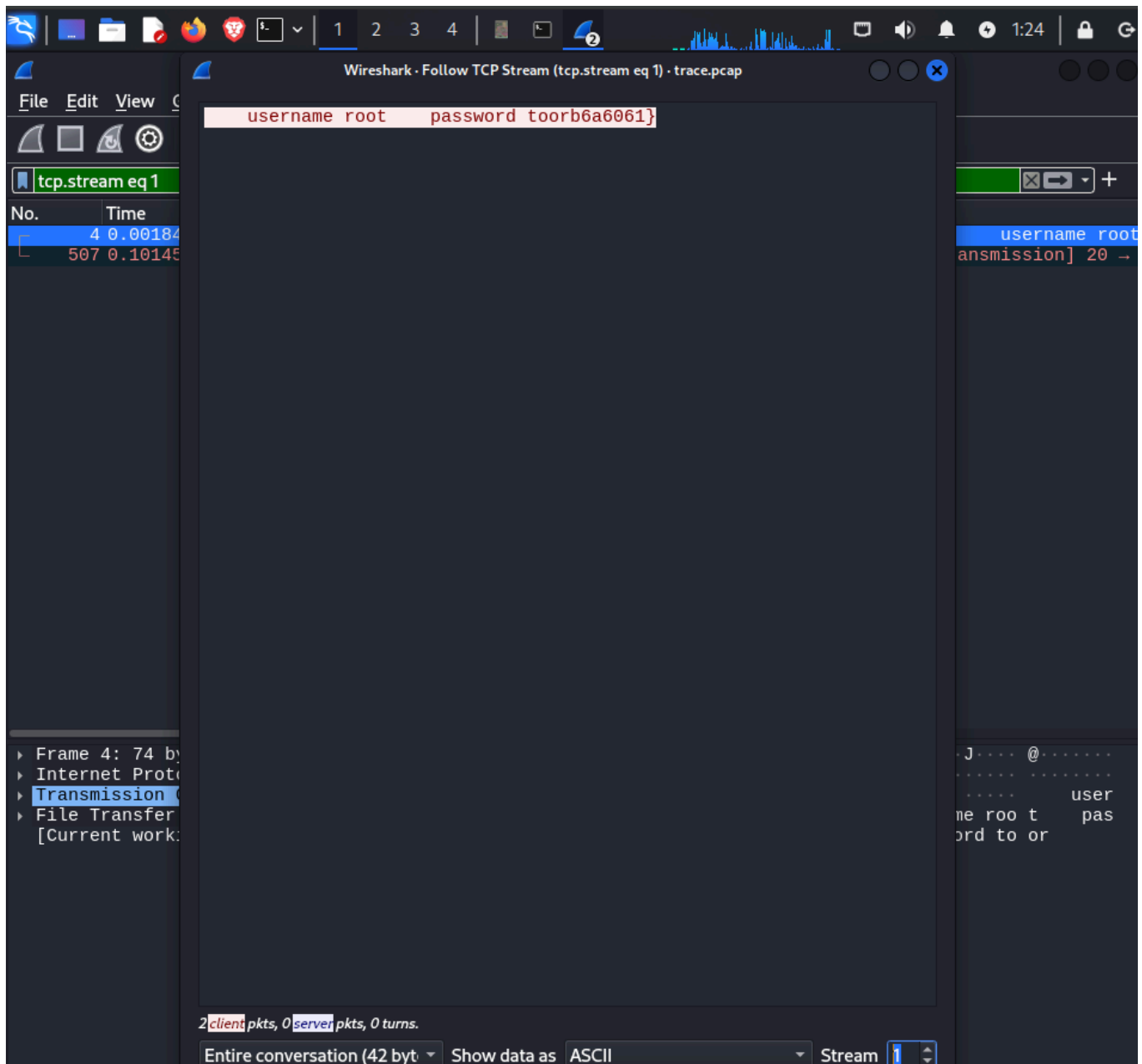
Domain Name System (query) Standard query query

[Malformed Packet: DNS]

E 7 @ . |
 5 5 . # . . iBwa
 WNVQ1RGe 1Flag is
 close=

trace.pcap Packets: 1510 · Displayed: 1510 (100.0%) Profile: Default

Siguiendo el primer paquete:



Finalmente preferimos optar por una opción más viable y rápida para este problema:

```
(kali㉿kali)-  
[~/.../parciales/parcial_02/parte_03_forensic_01/pcap_poisoning]  
└─$ strings trace.pcap | grep "picoCTF{"  
picoCTF{P64P_4N4L7S1S_SU55355FUL_5b6a6061}@~
```

Bandera

```
flag: picoCTF{P64P_4N4L7S1S_SU55355FUL_5b6a6061}
```

Notas Adicionales

Referencias

-