



**Name:** Ajude o admin!

**Category:** Network

**File:** 1d7fdcab411184f372d9ee54ecf955de

**Message:**

A senha do admin foi vazada. Ajude-nos a encontrar!

---

### Resolução:

Neste desafio estamos procurando por uma senha;  
Temos um arquivo sem extensão.

Baixamos e usamos nosso conhecido comando *file* para descobrir a extensão:

```
shell1t3r@lhost:~/Downloads$ file 1d7fdcab411184f372d9ee54ecf955de
1d7fdcab411184f372d9ee54ecf955de: tcpdump capture file (little-endian) - version 2.4
(Ethernet, capture length 262144)
```

Image 1 - Comando file em arquivo

Se trata de um arquivo TCPDump, podemos ler com a ferramenta  
[WireShark](#) usando o comando:

```
wireshark -r 1d7fdcab411184f372d9ee54ecf955de
```

No.	Time	Source	Destination	Protocol	Length	Info
4	0.017465	127.0.0.1	127.0.0.1	DNS	152	Standard query response 0x2d97 AAAA web.whatsapp.com CNAME mmx-ds.cdn.whatsapp.net AAAA 2a03:2880:f205:c5:face:b00c:0:167 OPT
5	1.443749	127.0.0.1	127.0.0.1	TCP	74	50002 → 1010 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=3291457162 TSecr=0 WS=128
6	1.443754	127.0.0.1	127.0.0.1	TCP	74	1010 → 50002 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=3291457162 TSecr=3291457162 WS=128
7	1.443767	127.0.0.1	127.0.0.1	TCP	66	50002 → 1010 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3291457162 TSecr=3291457162
8	6.983732	127.0.0.1	127.0.0.1	TCP	76	1010 → 50002 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=10 TSval=3291462702 TSecr=3291457162
9	6.983762	127.0.0.1	127.0.0.1	TCP	66	50002 → 1010 [ACK] Seq=1 Ack=11 Win=65536 Len=0 TSval=3291462702 TSecr=3291462702
10	11.343150	127.0.0.1	127.0.0.1	TCP	78	50002 → 1010 [PSH, ACK] Seq=1 Ack=11 Win=65536 Len=12 TSval=3291467061 TSecr=3291462702
11	11.343181	127.0.0.1	127.0.0.1	TCP	66	1010 → 50002 [ACK] Seq=11 Ack=13 Win=65536 Len=0 TSval=3291467061 TSecr=3291467061
12	15.367337	127.0.0.1	127.0.0.1	TCP	76	1010 → 50002 [PSH, ACK] Seq=11 Ack=13 Win=65536 Len=10 TSval=3291471085 TSecr=3291467061
13	15.367367	127.0.0.1	127.0.0.1	TCP	66	50002 → 1010 [ACK] Seq=13 Ack=21 Win=65536 Len=0 TSval=3291471085 TSecr=3291471085
14	22.479514	127.0.0.1	127.0.0.1	TCP	82	50002 → 1010 [PSH, ACK] Seq=13 Ack=21 Win=65536 Len=16 TSval=3291478197 TSecr=3291471085
15	22.479538	127.0.0.1	127.0.0.1	TCP	66	1010 → 50002 [ACK] Seq=21 Ack=29 Win=65536 Len=0 TSval=3291478197 TSecr=3291478197
16	30.166521	127.0.0.1	127.0.0.1	TCP	92	1010 → 50002 [PSH, ACK] Seq=21 Ack=29 Win=65536 Len=26 TSval=3291485884 TSecr=3291478197
17	30.166548	127.0.0.1	127.0.0.1	TCP	66	50002 → 1010 [ACK] Seq=29 Ack=47 Win=65536 Len=0 TSval=3291485884 TSecr=3291485884
18	39.178494	127.0.0.1	127.0.0.1	TCP	168	1010 → 50002 [PSH, ACK] Seq=47 Ack=29 Win=65536 Len=102 TSval=3291494896 TSecr=3291485884
19	39.178413	127.0.0.1	127.0.0.1	TCP	66	50002 → 1010 [ACK] Seq=29 Ack=149 Win=65536 Len=0 TSval=3291494896 TSecr=3291494896
20	39.178434	127.0.0.1	127.0.0.1	TCP	165	1010 → 50002 [PSH, ACK] Seq=149 Ack=29 Win=65536 Len=99 TSval=3291494896 TSecr=3291494896
21	39.178442	127.0.0.1	127.0.0.1	TCP	66	50002 → 1010 [ACK] Seq=29 Ack=248 Win=65536 Len=0 TSval=3291494896 TSecr=3291494896
22	39.178458	127.0.0.1	127.0.0.1	TCP	168	1010 → 50002 [PSH, ACK] Seq=248 Ack=29 Win=65536 Len=102 TSval=3291494896 TSecr=3291494896
23	39.178455	127.0.0.1	127.0.0.1	TCP	66	50002 → 1010 [ACK] Seq=29 Ack=350 Win=65536 Len=0 TSval=3291494896 TSecr=3291494896
24	39.178458	127.0.0.1	127.0.0.1	TCP	174	1010 → 50002 [PSH, ACK] Seq=350 Ack=29 Win=65536 Len=108 TSval=3291494896 TSecr=3291494896
25	39.178461	127.0.0.1	127.0.0.1	TCP	66	50002 → 1010 [ACK] Seq=29 Ack=458 Win=65536 Len=0 TSval=3291494896 TSecr=3291494896
26	39.178463	127.0.0.1	127.0.0.1	TCP	115	1010 → 50002 [PSH, ACK] Seq=458 Ack=29 Win=65536 Len=49 TSval=3291494896 TSecr=3291494896
27	39.178466	127.0.0.1	127.0.0.1	TCP	66	50002 → 1010 [ACK] Seq=29 Ack=507 Win=65536 Len=0 TSval=3291494896 TSecr=3291494896
28	40.157652	127.0.0.1	127.0.0.1	TCP	120	1010 → 50002 [PSH, ACK] Seq=507 Ack=29 Win=65536 Len=54 TSval=3291495876 TSecr=3291494896
29	40.157665	127.0.0.1	127.0.0.1	TCP	66	50002 → 1010 [ACK] Seq=29 Ack=561 Win=65536 Len=0 TSval=3291495876 TSecr=3291495876
30	44.222832	127.0.0.1	127.0.0.1	TCP	71	1010 → 50002 [PSH, ACK] Seq=561 Ack=29 Win=65536 Len=5 TSval=3291499941 TSecr=3291495876
31	44.222847	127.0.0.1	127.0.0.1	TCP	66	50002 → 1010 [ACK] Seq=29 Ack=566 Win=65536 Len=0 TSval=3291499941 TSecr=3291499941
32	45.940619	127.0.0.1	127.0.0.1	TCP	66	1010 → 50002 [FIN, ACK] Seq=566 Ack=29 Win=65536 Len=0 TSval=3291501659 TSecr=3291499941
33	45.940706	127.0.0.1	127.0.0.1	TCP	66	50002 → 1010 [FIN, ACK] Seq=29 Ack=567 Win=65536 Len=0 TSval=3291501659 TSecr=3291501659
34	45.940712	127.0.0.1	127.0.0.1	TCP	66	1010 → 50002 [ACK] Seq=567 Ack=30 Win=65536 Len=0 TSval=3291501659 TSecr=3291501659

Image 2 - Arquivo TCPDump pelo Wireshark

Nessa captura de pacotes de rede, temos apenas uma requisição TCP. Para visualisarmos melhor usamos a opção *TCP Stream*:

Protocol	Length	Info
DNS	87	Standard query 0x5594 A web.whatsapp.com OPT
DNS	87	Standard query 0x2d97 AAAA web.whatsapp.com OPT
DNS	140	Standard query response 0x5594 A web.whatsapp.com CNAME mmx-ds.cdn.whatsapp.net
DNS	152	Standard query response 0x2d97 AAAA web.whatsapp.com CNAME mmx-ds.cdn.whatsapp.net
TCP	74	50002 → 1010 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=3291457162 TSecr=0 WS=128
TCP	74	1010 → 50002 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=3291457162 TSecr=3291457162 WS=128
TCP	66	50002 → 1010 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3291457162 TSecr=3291457162
TCP	76	1010 → 50002 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=10 TSval=3291462702 TSecr=3291457162
TCP	66	50002 → 1010 [ACK] Seq=1 Ack=11 Win=65536 Len=0 TSval=3291462702 TSecr=3291462702
TCP	78	50002 → 1010 [PSH, ACK] Seq=1 Ack=11 Win=65536 Len=12 TSval=3291467061 TSecr=3291462702
TCP	66	1010 → 50002 [ACK] Seq=11 Ack=13 Win=65536 Len=0 TSval=3291467061 TSecr=3291467061
TCP	76	1010 → 50002 [PSH, ACK] Seq=11 Ack=13 Win=65536 Len=10 TSval=3291471085 TSecr=3291467061
TCP	66	50002 → 1010 [ACK] Seq=13 Ack=21 Win=65536 Len=0 TSval=3291471085 TSecr=3291471085
TCP	82	50002 → 1010 [PSH, ACK] Seq=13 Ack=21 Win=65536 Len=16 TSval=3291478197 TSecr=3291471085
TCP	66	1010 → 50002 [ACK] Seq=21 Ack=29 Win=65536 Len=0 TSval=3291478197 TSecr=3291478197
TCP	92	1010 → 50002 [PSH, ACK] Seq=21 Ack=29 Win=65536 Len=26 TSval=3291485884 TSecr=3291478197
TCP	66	50002 → 1010 [ACK] Seq=29 Ack=47 Win=65536 Len=0 TSval=3291485884 TSecr=3291485884
TCP	168	1010 → 50002 [PSH, ACK] Seq=47 Ack=29 Win=65536 Len=102 TSval=3291494896 TSecr=3291485884
TCP	66	50002 → 1010 [ACK] Seq=29 Ack=149 Win=65536 Len=0 TSval=3291494896 TSecr=3291494896
TCP	165	1010 → 50002 [PSH, ACK] Seq=149 Ack=29 Win=65536 Len=99 TSval=3291494896 TSecr=3291494896
TCP	66	50002 → 1010 [ACK] Seq=29 Ack=248 Win=65536 Len=0 TSval=3291494896 TSecr=3291494896
TCP	168	1010 → 50002 [PSH, ACK] Seq=248 Ack=29 Win=65536 Len=102 TSval=3291494896 TSecr=3291494896
TCP	66	50002 → 1010 [ACK] Seq=29 Ack=350 Win=65536 Len=0 TSval=3291494896 TSecr=3291494896
TCP	174	1010 → 50002 [PSH, ACK] Seq=350 Ack=29 Win=65536 Len=108 TSval=3291494896 TSecr=3291494896
TCP	66	50002 → 1010 [ACK] Seq=29 Ack=458 Win=65536 Len=0 TSval=3291494896 TSecr=3291494896
TCP	115	1010 → 50002 [PSH, ACK] Seq=458 Ack=29 Win=65536 Len=49 TSval=3291494896 TSecr=3291494896
TCP	66	50002 → 1010 [ACK] Seq=29 Ack=507 Win=65536 Len=0 TSval=3291494896 TSecr=3291494896
TCP	120	1010 → 50002 [PSH, ACK] Seq=507 Ack=29 Win=65536 Len=54 TSval=3291495876 TSecr=3291494896
TCP	66	50002 → 1010 [ACK] Seq=29 Ack=561 Win=65536 Len=0 TSval=3291495876 TSecr=3291495876
TCP	71	1010 → 50002 [PSH, ACK] Seq=561 Ack=29 Win=65536 Len=5 TSval=3291499941 TSecr=3291495876
TCP	66	50002 → 1010 [ACK] Seq=29 Ack=566 Win=65536 Len=0 TSval=3291499941 TSecr=3291499941
TCP	66	1010 → 50002 [FIN, ACK] Seq=566 Ack=29 Win=65536 Len=0 TSval=3291501659 TSecr=3291499941
TCP	66	50002 → 1010 [FIN, ACK] Seq=29 Ack=567 Win=65536 Len=0 TSval=3291501659 TSecr=3291501659
TCP	66	1010 → 50002 [ACK] Seq=567 Ack=30 Win=65536 Len=0 TSval=3291501659 TSecr=3291501659

Image 3 - TCP Stream no Wireshark

```
Username:
myusername
Password:
MyP@ss!aoba!01
Logged in! Listing files:
-rwsr-xr-x 1 root root 67816 mar 5 14:23 su
-rwxr-xr-x 1 root root 18664 mar 5 14:23 mountpoint
-rwsr-xr-x 1 root root 55528 mar 5 14:23 mount
-rwxr-xr-x 1 root root 43160 mar 5 14:23 more
-rwxr-xr-x 1 root root 133352 mar 5 14:23 lsblk
-rwxr-xr-x 1 root root 73128 mar 5 14:23 findmnt
-rwxr-xr-x 1 root root 84440 mar 5 14:23 dmesg
lrwxrwxrwx 1 root root 4 mar 11 16:32 lsmod -> kmod
-rwxr-xr-x 1 root root 166232 mar 11 16:32 kmod
-rwxr-xr-x 1 root root 196792 mar 23 09:25 hciconfig
Bye!
```

Image 4 - TCP Stream no Wireshark 2

Achamos então, o *username* e *password* do usuário.

E aqui está nossa flag;

**Flag**(MyP@ss!aoba!01)

---

**Pesquisas:**

[encurtador.com.br/ipEOY](https://encurtador.com.br/ipEOY)