NeverLAN CTF

Pcap : Teletype Network

Value : 125 pts

Difficulty : Easy

Description : Your flag will be in the normal flag{flagGoesHere} syntax.

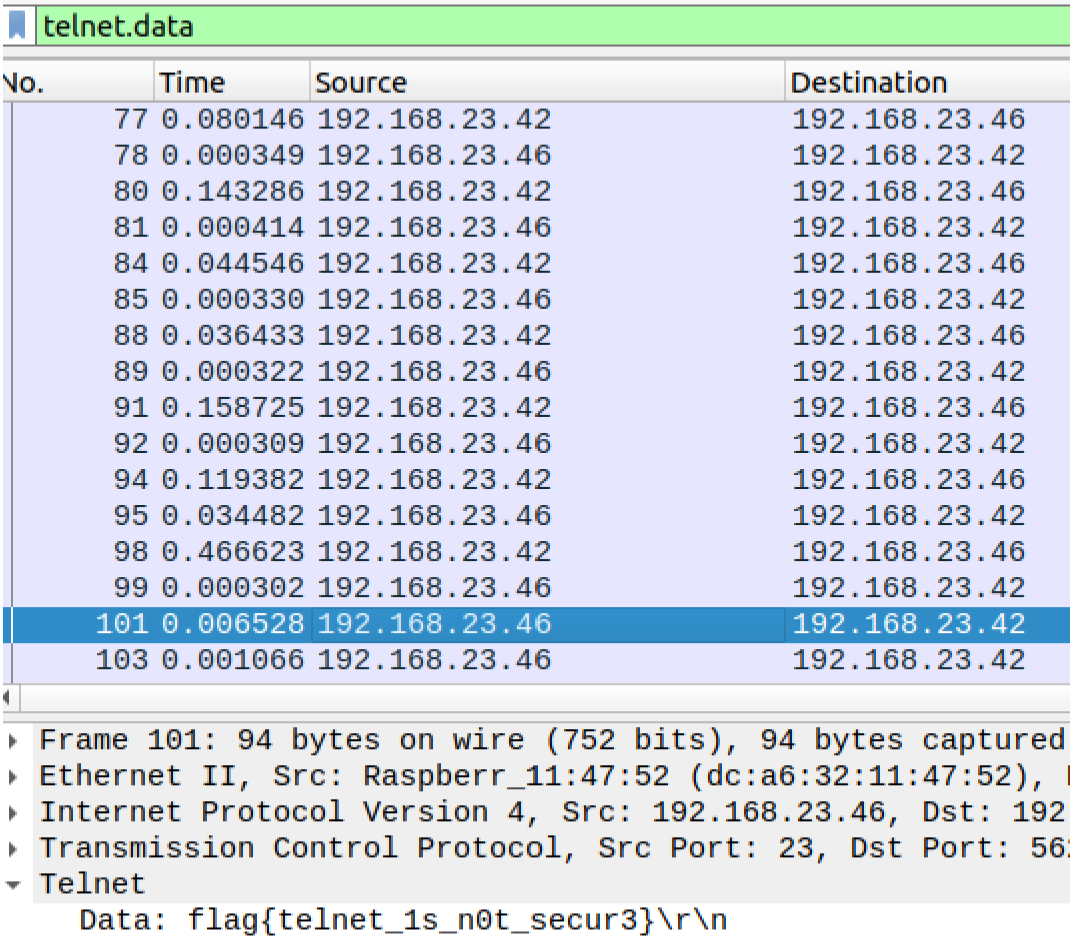
Attachment : It looks like someone hasn't upgraded to ssh yet...

telnet.pcap

Solution :

A pcap file is given. It can be opened with Wireshark.

A user used telnet to get a remote access. Contrary to SSH, all the data is in clear text. One of the Telnet Data packets may contain the flag. We can search with Wireshark filters.
The password of the user is ‘raspberry’. Each character has been sent in its own packet, after the one containing ‘password:’.
It’s not the flag, so we can continue to search in the commands written by the user. He used ‘cat’ on a file named flag.txt. We can get the flag in the packet with the output of the command.



telnet.data

No.	Time	Source	Destination
77	0.080146	192.168.23.42	192.168.23.46
78	0.000349	192.168.23.46	192.168.23.42
80	0.143286	192.168.23.42	192.168.23.46
81	0.000414	192.168.23.46	192.168.23.42
84	0.044546	192.168.23.42	192.168.23.46
85	0.000330	192.168.23.46	192.168.23.42
88	0.036433	192.168.23.42	192.168.23.46
89	0.000322	192.168.23.46	192.168.23.42
91	0.158725	192.168.23.42	192.168.23.46
92	0.000309	192.168.23.46	192.168.23.42
94	0.119382	192.168.23.42	192.168.23.46
95	0.034482	192.168.23.46	192.168.23.42
98	0.466623	192.168.23.42	192.168.23.46
99	0.000302	192.168.23.46	192.168.23.42
101	0.006528	192.168.23.46	192.168.23.42
103	0.001066	192.168.23.46	192.168.23.42

```
▸ Frame 101: 94 bytes on wire (752 bits), 94 bytes captured
▸ Ethernet II, Src: Raspberr_11:47:52 (dc:a6:32:11:47:52),
▸ Internet Protocol Version 4, Src: 192.168.23.46, Dst: 192
▸ Transmission Control Protocol, Src Port: 23, Dst Port: 56
▾ Telnet
    Data: flag{telnet_1s_n0t_secur3}\r\n
```

flag{telnet_1s_n0t_secur3}