NeverLAN CTF

Pcap : FTP

Value : 100 pts

Difficulty : Easy

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

Attachment : It looks like someone forgot to use a secure version of ftp…

ftp.pcap

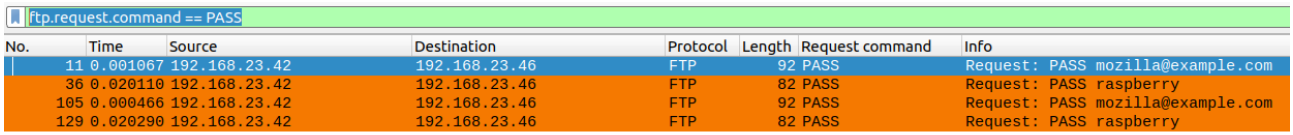
Solution :

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

This time, the user is accessing files with FTP. Credentials and files are sent in clear text through the network.

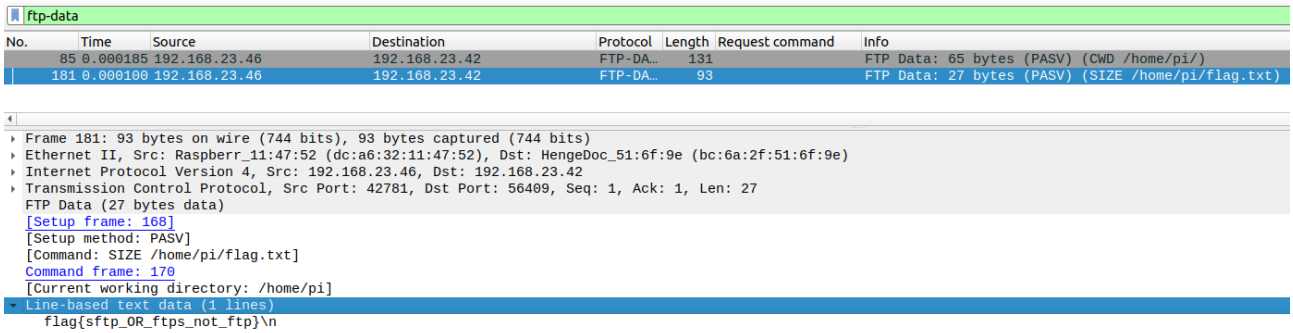
First, we'll try to search the credentials of the user to see if the flag is the password.

Passwords are sent with PASS commands, with this protocol. We can search these requests in Wireshark by applying he following filter: ftp.request.command == PASS.



It seems that this time, the flag isn't a password.

The next thing we can search are files. To search for file transfers, we can search for ftp-data in the filter. A file flag.txt was accessed:



flag{sftp_OR_ftps_not_ftp}