SHARKY CTF

Network : RattataTACAS

Value : 167 points (234 solves)

File : Chall.pcapng

Description : Silence is gold. I listen to every move on this network. And I think I got something interesting.

Creator : MrErne / Nofix

Solution :

First we can see in the title the protocol TACAS. When we open the file with wireshark, we an see some cipher on TACAS it's TACAS+ protocol. We can also find TFTP protocol (Trivial File Transfer Protocol) where we can see a CISCO configuration (with follow udp stream).

On it, we can find 'enable secret 5 1cPBj$qwX7keZqu6vF1UqNZxgCU0' and 'username cisco password 7 05080F1C2243' and 'tacacs-server host 192.168.1.100 key 7 0325612F2835701E1D5D3F2033'. We know that secret 5 is a salted hash which is strong. But, cisco password 7 is not very strong and that we the weakness that allow us to have the password 'cisco' and for tacas ' AZDNZ1234FED' by using that type of tool : http://ibeast.com/tools/CiscoPassword/index.asp

[You can check https://www.root-me.org/fr/Challenges/Reseau/CISCO-mot-de-passe which is quiet the same challenge]

Then, by using this password on wireshark on 'Preferences >Protocol >TACAS+', we can see all TACAS+ data in clear and you can take the flag.