ANCIENT SIGNAL

Author: CONSORTIUM

[Publish Date]
European Cyber Security Challenge

1.Initial Write-Up

Description

The starship Voyager received an unusual communication. The flag is with „curlybraket” word in place of ’{’ and ’}’ but you have to submit it in the CTF{sha256} format. Find the flag.

2.Challenge specifications

- Category: Network/Forensics/Cryptography
- Difficulty: Easy/Medium
- Estimated time: 3h

3.Questions and answers

What is the flag ?

CTF{8E512CF90917C19246D2E46A693C8B8949B96DE941FB951D7F63538584AFE22E}

What is the string for SHA256SUM?

SHA256SUM of word DEEPSPACE

4.Artefact hashes

FILES	MD5	SHA256
ancientsignal.pcapng	FF2AB93B8E5C70B6F71858A3F032F988	595B5495733EEF185DB0CDF8C8AAE51FD2DB8B844F78F4A977854715FA88C112
resolve.txt	22613558E3EDD94ECE48707D02AA19B1	37713C1E7E358308BABFFF75EF33208C7B4B35C04F572A8D3FE9B16F86E42E7E

5.Tools needed

- Python 3
- CTF CryptoTool (writen in Python) - https://github.com/karma9874/CTF-CryptoTool
- Wireshark

6.Walkthrough (writeup)

The challenge is based on a network capture file.

The capture file contains two communication streams. An FTP stream and a TLS stream. The FTP stream contains the TLS sessions keys used to decrypt the TLS stream.

After the decryption of TLS stream an HTTP stream will result with the following conversation:

Ensign: Captain we receive a communication on a multifrquency band.
Captain: Let's hear it.
Ensign: This is the message : <encrypted message>. I will try to clear it with a dual tone filter.
.....
Ensign: It is clear now. But I don't understand the communication language.
Captain: I think I know what it is. I read about this ancient comunication when in old times people used some sort of device to send this kind of signal.
Captain: The device is called telegraph. Ensign, try to use one of the old ciphers from our

database.
Ensign: Now is clear. Is some sort of coordonates.
Captain: Good. Punch the coordonates in the keyboard and lay an intercept course.
Ensign: Ready.
Captain: Engage.

From the above conversation and from the form of encrypted message we can identify that the encrypted message is writen using DTMF (dual tone multi frequency) frequencies in pairs of 7 numbers (example: 6971209 is the representation of digit '1' where 697 is the low frequency in Hz and 1209 is the hight frequency in Hz)

After the substituion of frequencies with the digits we obtain a string with only numbers. Also from the conversation we can identify that the string is a representation of a communication used on telegraph. We know that the thelegraph used 'morse code' for communication so the string is some sort of morse code cypher (morbit cypher). We run the CTF CryptoTool on the string and we search for word CTF to narrow the displayed posibilites. We extract the perfect match and we find the flag.

7. References

https://en.wikipedia.org/wiki/Dual-tone_multi-frequency_signaling

https://www.cryptogram.org/downloads/aca.info/ciphers/Morbit.pdf

https://github.com/karma9874/CTF-CryptoTool