

Dreamhack-Snowing!(level1)

[mics, forensics]

Description

드림이 : 우와! 밖에 눈이 많이와요!

드림맘 : 그렇네~

드림이 : 거의 모두 하얀공간뿐이네요. (2021.07.11)

Write up

- 사용 도구: HxD, SNOW.EXE
- HxD를 통해 `flag.txt` 파일 내부 확인

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	44	48	7B	66	61	6B	65	5F	73	6E	6F	77	7D	09	20	20	DH(fake_snow).
00000010	20	20	20	09	20	20	20	20	09	09	20	20	20	20	09	20
00000020	20	20	20	20	20	09	09	20	20	20	20	20	09	20	20	20
00000030	0A	20	09	20	09	09	20	20	20	20	20	09	20	09	20	20
00000040	09	20	20	20	20	20	20	20	09	20	20	09	20	20	0A	09
00000050	20	20	09	20	20	20	09	20	20	20	20	09	20	20	20	20
00000060	20	20	09	20	20	20	20	20	09	20	20	20	20	09	09	20
00000070	20	20	20	09	20	20	20	20	20	20	0A	09	20	20	20	20
00000080	20	09	20	20	20	09	20	09	20	09	09	20	20	20	20	20
00000090	09	20	09	20	20	09	20	20	20	20	20	20	0A	20	20	20
000000A0	09	20	20	09	09	20	20	09	20	20	20	09	20	20	20	20
000000B0	09	20	20	20	20	20	20	09	20	20	20	20	20	09	20	20

- “거의 모두 하얀공간뿐이네요.”라는 문구를 통해 **Whitespace Steganography**(공백 문자 기반 스테가노그래피) 기법이 사용되었음을 유출할 수 있음
 - Whitespace Steganography: 탭, 공백, 줄바꿈과 같은 보이지 않는 문자를 사용하여 텍스트 파일에 데이터를 은닉하는 기법

- **SNOW.EXE -c filename** 명령어를 통해 숨겨진 메시지 추출 가능

[illegible]

- FLAG $\stackrel{L}{=}$, DH{w0w_1t_Sn0w5}

FLAG

DH{w0w_1t_Sn0w5}