TUCTF 2022 - Kraken Solution

Author: Declan Oberzan (TNAR5)
Category: Forensics

Solution

- Mount vmdk/raw file and copy the SAM and system registry hives. (Contains user credentials and system crypt key)
- Extract the raw password hashes from the hives using samdump2 or something similar.
- Because LM splits the password into two 7 character parts it is possible to crack each half separately in under 8 minutes.

```
                         LM                                  NT
Davy Jones:e87fb6a088f49b34e3a25c34d8c6db5d:4e93a45528d4cb5aea1a4c903ddf2b2e:::
```

Full LM Hash: `e87fb6a088f49b34e3a25c34d8c6db5d`
Cracked Segments:

```
e87fb6a088f49b34:#UNCRA(
e3a25c34d8c6db5d:K4BL3%!
```

Full Password: `#UNCRA(K4BL3%!`

- With both halves you get the full password, but LM only stores all uppercase characters.
- The real password to decrypt the zip is toggle case and not fully represented by the LM hash.
- To find the real password you will have to crack the NT hash with the previously found LM hash which preserves the toggle case giving the actual password.

Cracked Password:

```
4e93a45528d4cb5aea1a4c903ddf2b2e:#UnCrA(k4bl3%!
```

- The flag.zip file in Davy Jones Confidential folder can be decrypted using this password.

flag.txt contains: `TUCTF{I_l0vE_T0gGlE_(aS3_N!#8790}`