CT212 Computer Forensics
HW2 Hashes
Professor Tarbutton

The Challenge:

This week we focus on the importance of hashes in Forensics.

Use the links provided in the Week 8 folder in BbLearn as well as online research to answer the questions. Be sure to answer the questions in your own words and not just "copy and paste".

1. What is a hash value?

2. Why do we use hashes in Forensics and why are they important?

3. What part of the CIA Triad do hashes belong to?

4. What is MD5? What are the pros and cons?

5. What is SHA1? What are the pros and cons?

6. What is SHA256? What are the pros and cons?

7. Name 2 other hashing algorithms that are widely used today. (That haven't been cracked yet.)

8. What hashing algorithm was used to create this hash?
   172eee54aa664e9dd0536b063796e54e

9. What is the plaintext of this hash?
   172eee54aa664e9dd0536b063796e54e

10. What is the MD5 hash for this plain text below? (Be careful not to copy an extra space after the #)
    Pa$$word123#

11. How many entries does CrackStation have in its look up table for MD5 and SHA1 hashes? Be sure to read about "How CrackStation Works."

12. What is the plain text password for this SHA256 hash?
6A934B45144E3758911EFA29ED68FB2D420FA7BD568739CDCDA9251FA9609B1E

13. What is the plain text password for this SHA256 hash?
B5692500175FAD6BB2B306AA20FF58423C79B130EF310FB3CAA924E0F28BC61D

14. What is the plain text password for this SHA256 hash?
1D92DAE504A70FBCAE6D3721A55D7EACAF94D3133EA5F0394B7D203D64841110

15. The SHA256 hash for password123 is this:
    ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
    CrackStation breaks it easily even though SHA256 is relatively complex.
    The CRC32 hash for password123 is this: d043df23
    But CrackStation can't crack it even though CRC32 is relatively simple. Why?

16. How many of these hashes can CrackStation crack?
    Which ones can be cracked and what are the passwords?
    What hashing algorithm was used?
    e64b78fc3bc91bcbc7dc232ba8ec59e0
    751cb3f4aa17c36186f4856c8982bf27
    e66055e8e308770492a44bf16e875127
    f134cfa7858e5c4674ef55d3d3284b1c
    9ab9813a23276d72e0b3e592cf5dfcdc
    d568e43eeb1d52cb6fb39312a0fc3940

17. What is the original input of this SHA-1 hash?
    e10f235999f9caa83da76e68f32f3ff4df19e451

18. According to the UK cyber survey results table, what are the most popular passwords?

19. What types of services are primarily offered at a regional computer forensics lab (RCFL)?

Learning Question

20. What did you learn today that you didn’t know before?