SGSSI-20.InformeHA1.18.JDOR

A.7.1.1.1.I

No he encontrado ninguna limitación de las que aperecen mencionadas, tengo una copia en el ordenador, otra en Cryptpad.fr y una última en mi USB. Además cada directorio cuenta con un documento .txt donde se almacenan los hash MD5 de cada entrega. El acceso a los documentos se limita al dueño, a menos que se tenga en enlace de acceso. Permite colaborar aun sin tener una cuenta en cryptpad para los trabajos de grupo. En último lugar, en el caso de un desastre se tendrian que perder las tres copias, dificilmente alcanzable sobre todo cryptpad ya que la contraseña de mi cuenta esta guardada en un documentu de KeePassXC almacenada en una unidad USB distinta y cifrada.

Autoevaluación:
Me autoevaluo con un 98 devido ha:
-5 por cada CC en el que se haya obtenido un resultado caracterizado como “a no repetir” (color rojo) (Diría que es el resultado que obtuve en el CC1)

-1 por cada entrega de actividades realizada fuera de plazo o con limitaciones formales en la entrega (formatos, enlaces, resúmenes…) (Dos veces por lo que -2)

-5 por cada actividad no realizada

+5 por cada CC en el que se haya obtenido un resultado caracterizado como “destacado” (color verde) (CC2)

+5 si se ha asistido a todas las clases en directo (presencial o virtualmente)

A.7.1.1.4.I

3.1.1	359da9eeb8837bb9f6305b633c58c3c7
3.1.2	eeeb9a0cbdbad0ca593010bb1f86f499
lb0.2	55fe5c3e2dc86330812c883e9d0306eb
4.1.2	02dcf76b177b7d109519d755d1ce0388
5.1.4	d70d0a15d9330e6c48a3d9e054ce9387
Lb0.3	58d7d09019c28d9880819327813459a7

A.7.1.1.5.G

Ejercicios

Partimos del dato de que en SGSSI-20 hay 35 estudiantes intentando encontrar una *cadena de relleno* para completar un bloque cuyo resumen MD5 comience, en hexadecimal, por "0". Responde a las siguientes cuestiones:

- ¿Cuál es la probabilidad de que AL MENOS uno de los 35 estudiantes encuentre el número de relleno en su primer intento?
  1 - (31/32)^35

- ¿Cuál es la probabilidad de que más de un estudiante encuentre la cadena de relleno en su primer intento?
  (1 - (31/32)^35) * (1-(31/32)^34)

- ¿Cuántos intentos debe hacer un estudiante aislado para tener un 90% de posibilidades de encontrar una cadena de relleno con las características señaladas?
  73 intentos, (1- (31/32)^73) = 0.901 => %90.1

Repite los tres ejercicios anteriores considerando que el resumen MD5 debe comenzar por "00" en vez de por "0".

- (1-(31/32)^35) * (1-(31/32)^35)

- (1-(31/32)^35) * (1-(31/32)^35) * (1-(31/32)^34) * (1-(31/32)^34)

- Para mantener el porcentaje de 90%, tendría que realizar 94 intentos para el primer caracter y otros 94 el segundo. Es decir 188 intentos.
  (1-(31/32)^94) * (1-(31/32)^94) = 0.901 => %90.1

A.7.1.1.6.G

Nuestro grupo ha decidido de manera consensuada que la conferencia más interesante es la de *"Ciberseguridad para todos los públicos"* . El criterio, o razón principal, por la que hemos seleccionado este curso es, que nos permite interiorizar un discurso que podemos transmitir a nuestro entorno sin entrar en tecnicismos o en prácticas más avanzadas, que pueden resultar invasivas (además de alienígenas) a un público menos técnico.

Además de la conferencia mencionada previamente, también nos ha resultado interesante (y casi la seleccionamos) la conferencia de *"Etica hacker"* . Principalmente porque rompe con el estigma y las connotaciones negativas asociadas a la palabra "hacker", y establece un punto inicial útil (desde el punto de vista de la ciberseguridad) desde el que retomar el uso no negativo del término.

A.7.1.1.7.G

https://drive.google.com/file/d/1qMq4PAO3ESbswJBZRT5HuW5oGIxR7voW/view?usp=sharing