ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ  
ΣΥΣΤΗΜΑΤΩΝ

ΕΡΓΑΣΙΑ 4

**Συντελεστές εργασίας**

Χριστοφορίδης Χαράλαμπος – Π19188

Γεωργιάδης Νικόλαος – π19032

Καρκάνης Ευστράτιος – Π19064

8 δεκεμβριου 2022

**Περιεχόμενα**

[1. Πρώτο συνθηματικό 2](#_Toc121360877)

[2. Δεύτερο συνθηματικό 3](#_Toc121360878)

[3. Τρίτο συνθηματικό 5](#_Toc121360879)

[4. Τέταρτο συνθηματικό 10](#_Toc121360880)

1. **Πρώτο συνθηματικό**

Στο πρώτο ερώτημα της εργασίας καλούμαστε, με βάση τα χαρακτηριστικά του «hash value», να βρούμε ποια συνάρτηση έχει χρησιμοποιηθεί και να εφαρμόσουμε την καταλληλότερη επίθεση με κάποιο «password cracker». Για να βρούμε τη συνάρτηση θα χρησιμοποιήσουμε ένα hash-identifier (<https://sourceforge.net/projects/hashidentifier/>) και για την επίθεση θα χρησιμοποιήσουμε το JohnTheRipper. Αναλυτικότερα:

* Θα βάλω το συνθηματικό (**d4927dda05af693bff7dfd4c7b40eafb0ef92a78**) στο hash-identifier και θα πάρω τη συνάρτηση που χρησιμοποιήθηκε για να παραχθεί.

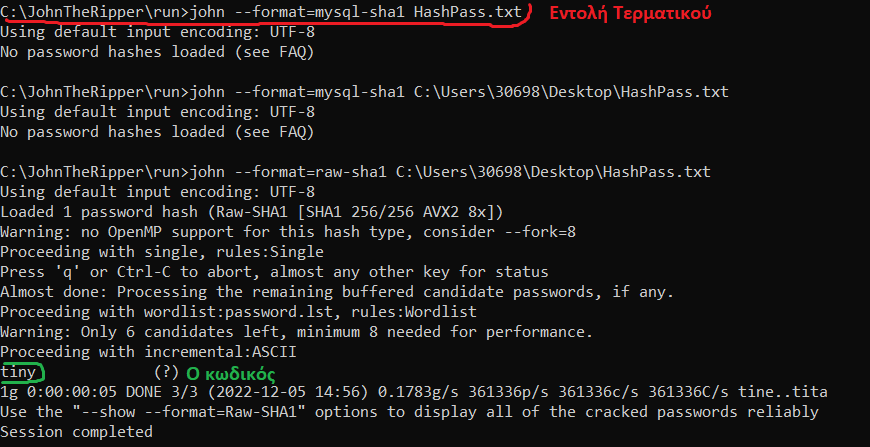


* Αποθηκεύω το συνθηματικό σε ένα αρχείο

Εικόνα που περιέχει κείμενο

Περιγραφή που δημιουργήθηκε αυτόματα

* Ύστερα θα κατευθυνθώ από το τερματικό μου στο φάκελο όπου έχω το JohnTheRipper και θα πραγματοποιήσω την επίθεση ορίζοντάς του και το είδος του Hash που χρησιμοποίησα, αφού το βρήκα στο προηγούμενο βήμα.



* Ο κωδικός είναι «tiny» και ο χρόνος που χρειάστηκε ήταν ελάχιστος όπως φαίνεται και στο τερματικό.

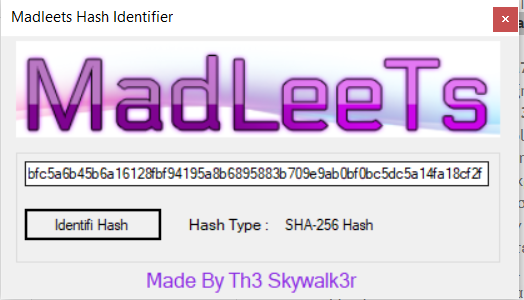
1. **Δεύτερο συνθηματικό**

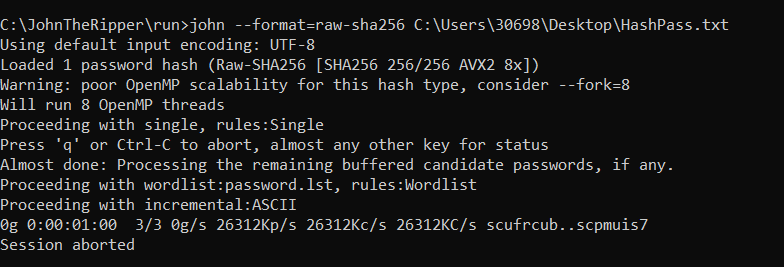
Σε αυτό το ερώτημα, θα επαναλάβουμε την παραπάνω διαδικασία για ένα διαφορετικό Hash, το **bfc5a6b45b6a16128fbf94195a8b6895883b709e9ab0bf0bc5dc5a14fa18cf2f** .

Θα βρούμε την συνάρτηση που χρησιμοποιήθηκε και πάλι και θα βάλουμε το φάκελο στο JohnTheRipper ώστε να κάνει την πιο αποδοτική επίθεση.

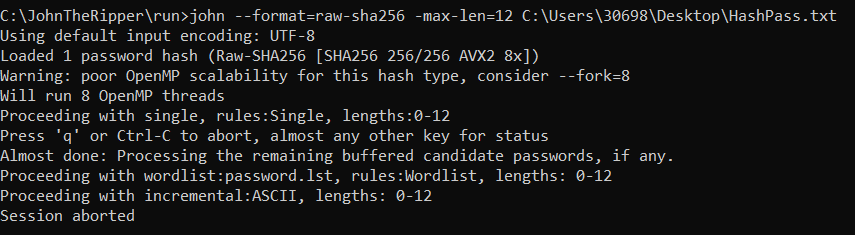
Εικόνα που περιέχει κείμενο

Περιγραφή που δημιουργήθηκε αυτόματα





* Παρατηρώ ότι με τον απλό τρόπο παίρνει πάρα πολύ χρόνο καθώς δεν είναι εύκολο να σπάσω το Hash λόγω του sha-256. Αφού ξέρω όμως το μέγεθος του Password θα το περάσω ως όρισμα στον JohnTheRipper και θα ξαναδοκιμάσω. Πάλι παίρνει μεγάλο χρόνο για να ολοκληρωθεί.



1. **Τρίτο συνθηματικό**

Το hashed password που προσπαθούμε να σπάσουμε είναι το εξής:

**23997786f8c60122a711f040a7acb4faa5ddd0681d5d658807ab0f9e987d6042**

**Από την εκφώνηση γνωρίζουμε πως το password είναι μία Ελληνική λέξη. Για αυτό τον λόγο επιλέγουμε να εφαρμόσουμε dictionary attack.**

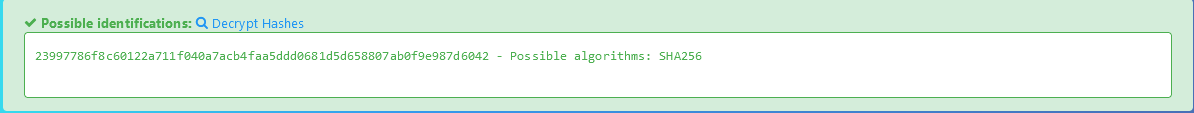
**Μεταβαίνουμε στην ιστοσελίδα:** [**https://hashes.com/en/tools/hash\_identifier**](https://hashes.com/en/tools/hash_identifier) **για να εντοπίσουμε τον τύπο του hash αλγόριθμου που έχει εφαρμοστεί στο password.**

Graphical user interface, text, application, email

Description automatically generated

Copy-paste του hashed password

Πατάμε το κουμπί «SUBMIT & IDENTIFY» για να δούμε τα αποτελέσματα:



Πιθανός hash αλγόριθμος: SHA256

Αφού εντοπίσουμε τον hash αλγόριθμο, ανοίγουμε το περιβάλλον Cain και επιλέγουμε το tab «Cracker»:

Graphical user interface, application, table, Excel

Description automatically generated

Cracker tab στο Cain

Επιλέγουμε το SHA-2 από το αριστερό μενού καθώς ο SHA256 είναι αυτής της κατηγορίας. Πατάμε το κουμπί «+» για να εισάγουμε το hashed password:

Graphical user interface, application

Description automatically generatedGraphical user interface, application, table

Description automatically generated

Στη συνέχεια κάνουμε δεξί κλικ στο hashed password🡪Dictionary Attack🡪SHA2 256 Hashes:

Graphical user interface, application, table

Description automatically generated

Στο παράθυρο που εμφανίζεται κάνουμε δεξί κλικ στη περιοχή «Dictionary» και επιλέγουμε «Add to list» για να εισάγουμε το αρχείο με το ελληνικό λεξικό:

Graphical user interface, application

Description automatically generated

Εισαγωγή του αρχείου gr\_dic.txt από τα χρήσιμα έγγραφα του μαθήματος(gunet2)

Αλλάζοντας τα Options αφήνοντας μόνο το πρώτο κουτάκι τικαρισμένο, πατάμε «Start». Σε μερικά δευτερόλεπτα έχουμε αποτέλεσμα:

Graphical user interface, application

Description automatically generated

Επιτυχής cracking του password

Graphical user interface

Description automatically generated with medium confidence

To password δεν έχει εκτυπώσιμη τιμή στο Cain καθώς χρησιμοποιούνται Unicode χαρακτήρες(Ελληνικά)

Να σημειωθεί, πως κρατήσαμε μόνο το option «As Is (Password)» καθώς γνωρίζουμε πώς το password είναι μια λέξη του λεξικού που βγάζει νόημα. Έτσι γλυτώνουμε να ελέγξουμε πολλές περιπτώσεις.

Σαν έξτρα κομμάτι αυτής της άσκησης, υλοποιήθηκε ένα script σε python που διαβάζει μία μία τις λέξεις από το αρχείο λεξικό και βρίσκει την sha256 τιμή τους. Αν αυτή συμπίπτει με αυτήν που θέλουμε τότε τυπώνει στην κονσόλα «found» και σταματάει:

Text

Description automatically generated

Το password είναι «παράδειγμα»

**To script:**

import hashlib

import io

#hash value we are looking for

wanted\_hash = "23997786f8c60122a711f040a7acb4faa5ddd0681d5d658807ab0f9e987d6042"

for word in io.open("gr\_dic.txt", mode="r", encoding="utf-8").readlines():

m = hashlib.sha256()

m.update(word[:-1].encode()) #ascii to bytes

print(word[:-1])

print(m.digest().hex()) #byte form of hash, then hex form

print()

if(m.digest().hex() == wanted\_hash):

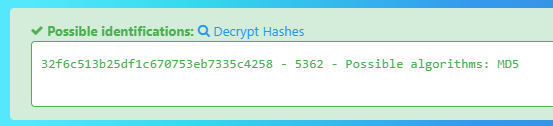
print("found")

break

1. **Τέταρτο συνθηματικό**

Στην συγκεκριμένη περίπτωση προσπαθήσαμε να σπάσουμε το συνθηματικό: **32f6c513b25df1c670753eb7335c4258**, το οποίο είναι ένα ΡΙΝ με 4 ακέραια ψηφία. Επομένως, γνωρίζουμε ότι οι αποδεκτές τιμές του κωδικού είναι τα ψηφία 0,1,2,3,4,5,6,7,8 και 9.

Το πρώτο βήμα είναι να βρούμε με ποιον αλγόριθμο έχει γίνει hash το μήνυμά μας. Μεταβαίνοντας στην ιστοσελίδα [**https://hashes.com/en/tools/hash\_identifier**](https://hashes.com/en/tools/hash_identifier) και πληκτρολογώντας το hash, η εφαρμογή μας απαντάει πως έχει γίνει χρήση του αλγορίθμου MD5.

****

Επομένως, χρησιμοποιώντας τις παραπάνω πληροφορίες, μπορούμε να φτιάξουμε ένα rainbow table χρησιμοποιώντας κωδικοποίηση MD5, αλφάβητο “numeric” και μήκος κωδικού 4. Η σχετική εντολή για δημιουργία του πίνακα αυτού φαίνεται παρακάτω:

Εικόνα που περιέχει κείμενο

Περιγραφή που δημιουργήθηκε αυτόματα

Δημιουργία rainbow table με το rtgen

Στην συνέχεια, μπορούμε με μία εντολή (φαίνεται στην εικόνα παρακάτω) να σπάσουμε το hash, να βρούμε δηλαδή σε ποιον αριθμό που έχει καταχωρηθεί στον πίνακα (rainbow table) αντιστοιχεί το εν λόγω hash που έχουμε να σπάσουμε.

Εικόνα που περιέχει κείμενο

Περιγραφή που δημιουργήθηκε αυτόματα

Συνολικός χρόνος που χρειάστηκε: 0.63 δευτερόλεπτα. Ο 4-ψήφιος κωδικός είναι ο αριθμός 5362!