

>TEL'S WIFI TUTORIALS

>PART 2

>Ξεκλείδωμα τυπικών ελληνικών δικτύων με το Greek WPA Finder/GreekWiFi

>Τι θα κάνουμε σήμερα

- Γνωριμία με τις δυνατότητες του Greek WPA Finder
- Εύρεση κωδικών ασφαλείας των τυπικών δικτύων της περιοχής

>Τι θα χρειαστείτε

- Ένα PC ή οποιαδήποτε συσκευή με λογισμικό Android και πρόσβαση στο Google Play Store

- Δυνατότητα σύνδεσης με WiFi δίκτυα

(Smartphones και tablets Android έχουν by default, το ίδιο και τα περισσότερα laptop. Σε περίπτωση που έχετε σταθερό υπολογιστή όπως εγώ, χρειάζεστε έναν αντάπτορα WiFi. Εγώ χρησιμοποιώ [αυτό](#) που πήρα το 2008, είναι εξαιρετικά απαρχαιωμένο αλλά κάνει τη δουλειά του. Πλέον αν πάτε σε ένα κατάστημα που πουλάει τεχνολογικά μαραφέτια μπορείτε να πάρετε έναν σε μέγεθος ψείρας. Φροντίστε όμως να μην πληρώσετε πάνω από €20, διότι αν είναι να κάνετε προχειροδουλειά με €200 αντάπτορα, ας πάρετε καλύτερα ένα πακέτο σύνδεσης διαδικτύου που να είναι δικό σας.)

- Στην περίπτωση PC, το πρόγραμμα [7zip](#)

>Πρόλογος

Όπως σίγουρα θυμάστε από το προηγούμενο μάθημα, στην ερώτηση «Τι κωδικό να βάλω στο WiFi μου;», η απάντηση ήταν «οτιδήποτε που να μην είναι ο εργοστασιακός κωδικός». Τώρα θα μάθετε το γιατί.

Το Greek WPA Finder (ή GreekWiFi) είναι μια εφαρμογή που δημιουργήθηκε γύρω στο 2013 από την ομάδα της ιστοσελίδας hakkers.tk. Ουσιαστικά πρόκειται για ένα “key generator”, γεννήτρια κλειδιών δηλαδή, που βρίσκει ασύρματα δίκτυα στην περιοχή και, αν είναι στη λίστα γνωστών κατασκευαστών, βγάζει αυτόματα τους πιθανούς εργοστασιακούς κωδικούς τους.

Σημειωτέο είναι ότι η διαδικασία εύρεσης κλειδιών γίνεται χωρίς καμία επαφή με το ρούτερ που ψάχνουμε τον κωδικό του. Ουσιαστικά το πρόγραμμα λειτουργεί όπως ένας τηλεφωνικός κατάλογος: Στον μεν κατάλογο, γνωρίζοντας το όνομα του ανθρώπου, βρίσκω το τηλέφωνό του, ενώ στο δε Greek WPA Finder, γνωρίζοντας το όνομα του δικτύου, βρίσκω τον κωδικό του.

Γενικά, όπως θα δείτε, είναι τρομακτικά εύκολο να αλιεύσετε τους κωδικούς των γύρω ασύρματων δικτύων. Πριν βγει αυτό το πρόγραμμα, η αλίευση κωδικών απαιτούσε εγκατάσταση λογισμικού linux και ατελείωτες ώρες ψαξίματος με διάφορα προγράμματα wifi cracking (το οποίο θέμα μπορεί να καλυφθεί σε ένα επόμενο μάθημα).

Ας ξεκινήσουμε!

>Χρήση του Greek WPA Finder

Σε πρώτη φάση, κατεβάστε το πρόγραμμα στη συσκευή της επιλογής σας.

[-Android](#)

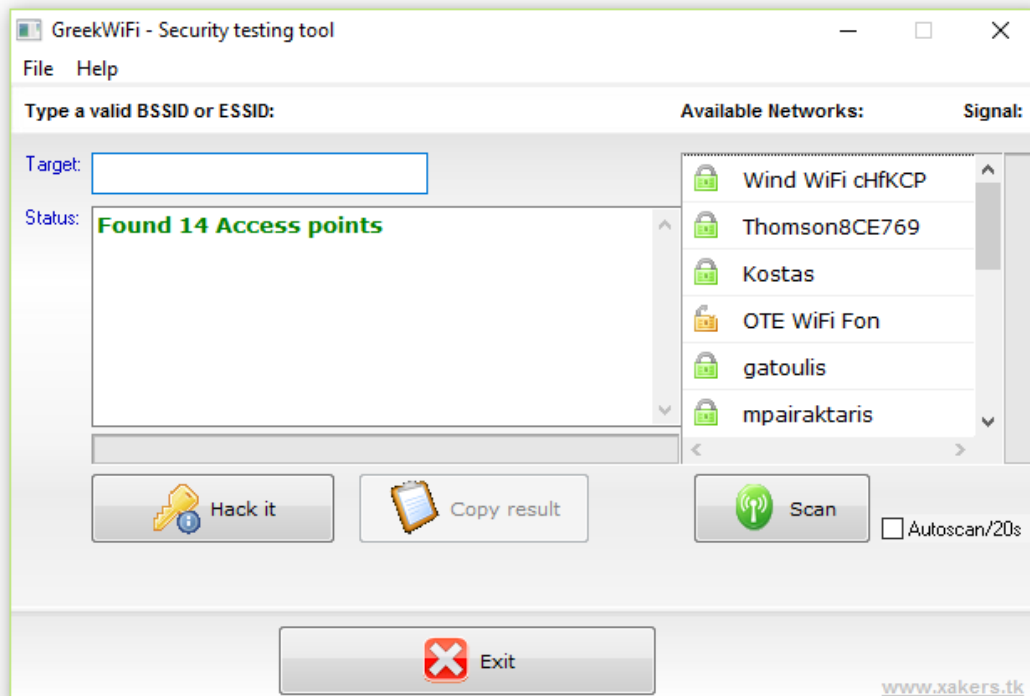
[-Windows](#)

(Το Windows link είναι δικό μου, δεν κατάφερα να βρω ασφαλές link στο διαδίκτυο που να έχει μείνει ενεργό. Δεν ξέρω για πόσο καιρό θα μείνει ενεργό το link, οπότε ΕΛΛΗΝΕΣ ΔΙΑΔΩΣΤΑΙ)

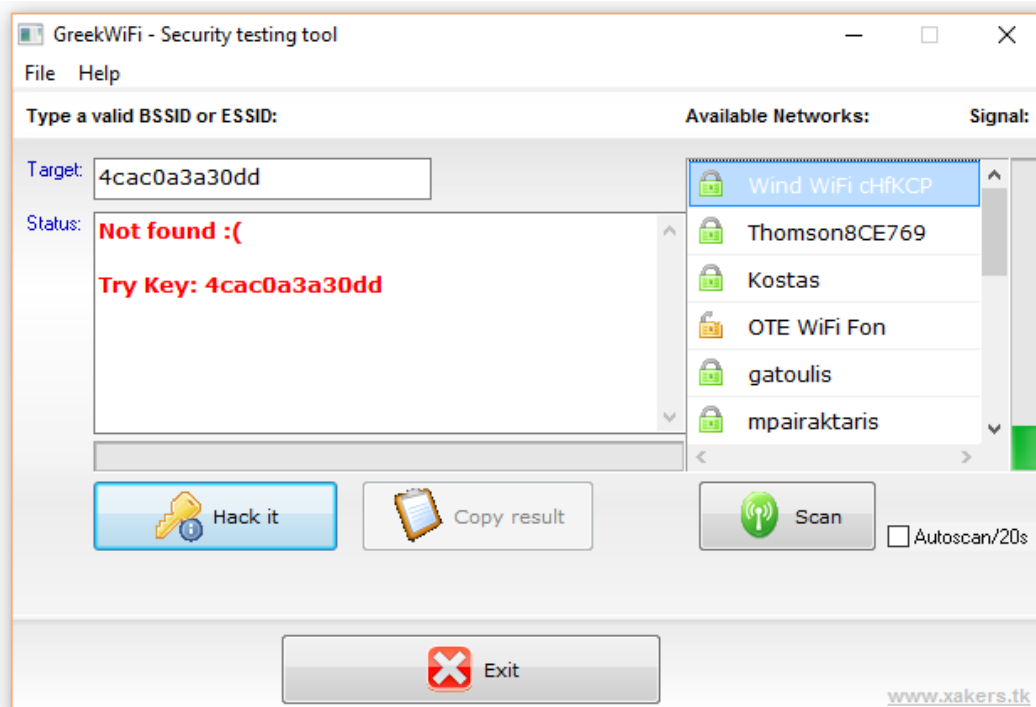
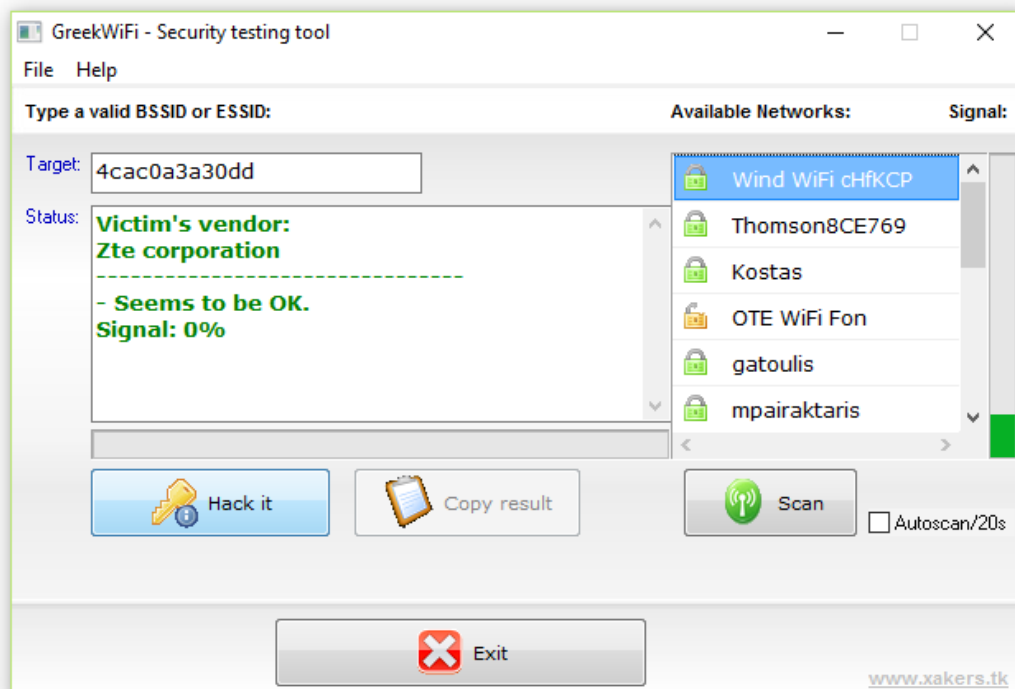
(Θα αποσυμπίεσετε το 7z αρχείο με το πρόγραμμα 7zip που μπορείτε να κατεβάσετε από [εδώ](#). Δεξί κλικ στο αρχείο -> 7-zip -> Αποσυμπίεση Εδώ/Extract Here.)

(Υπάρχει πιθανότητα να σκούζει το antivirus σας. Αγνοήστε το. Τον εμπιστεύεστε τον παλιόφιλό σας τον TEL, έτσι δεν είναι;)

Ανοίγουμε το πρόγραμμα και βλέπουμε το εξής:

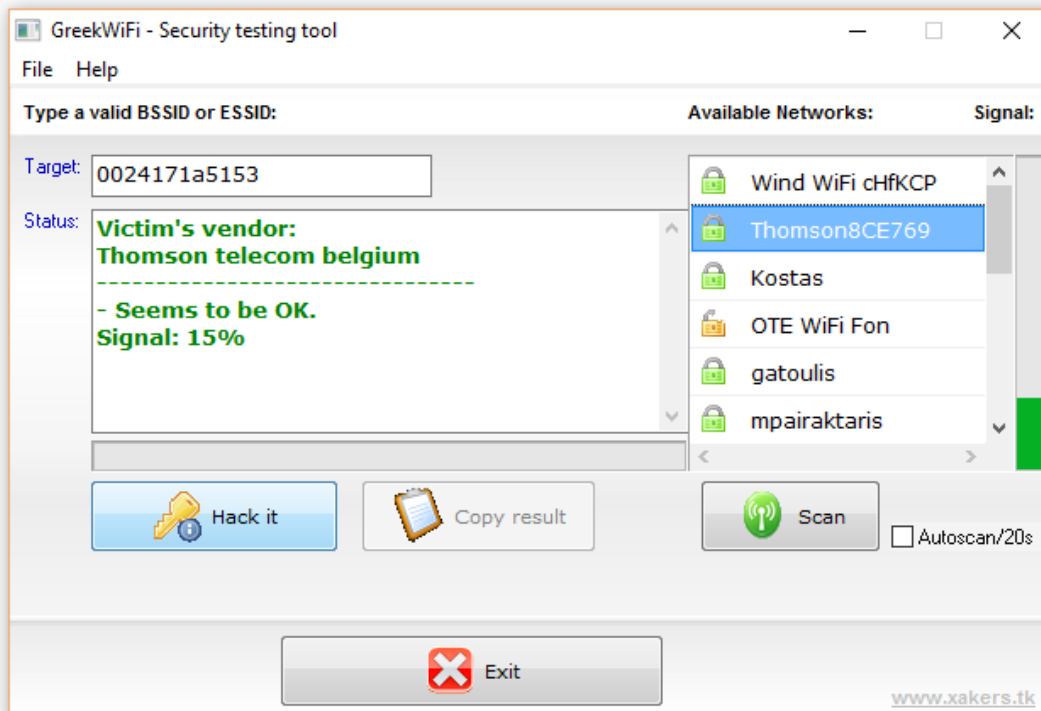


Επιλέγουμε το πρώτο δίκτυο και πατάμε Hack it.

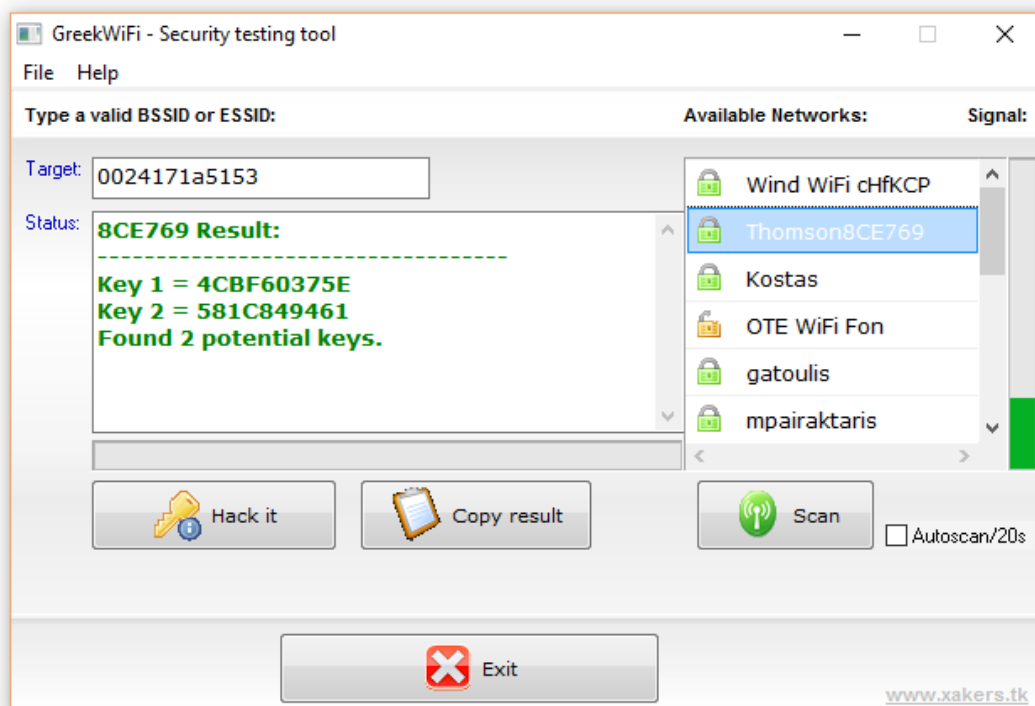


Εδώ δεν βρήκε κωδικό, και μας δίνει έναν να δοκιμάσουμε (ο οποίος είναι η MAC address του ρούτερ, ένα ακόμα στοιχείο ταυτοποίησης του). Συνήθως δεν είναι αυτός ο κωδικός.

Πάμε στο επόμενο δίκτυο. Το επιλέγουμε και πατάμε Hack It.



Και μετά από ~20 δευτερόλεπτα...



Μας βγάζει δύο πιθανά κλειδιά. Δοκίμασα το πρώτο, και δουλεύει. Συγχαρητήρια, μόλις μπήκατε στο δίκτυο. Καλό;

>Σχόλια

1) Τώρα κάποιος μπορεί να ψαρώσατε και να λέτε: «Ουάου TEL, είσαι hacker! Βάλε να παίξει το soundtrack του Mr Robot!»

ΟΧΙ, ΔΕΝ ΕΙΜΑΙ. Αυτό που μόλις έκανα μπορεί να το κάνει ο οποιοσδήποτε ηλίθιος με ένα smartphone και 5 λεπτά στη διάθεσή του. Δεν αποτελεί διαδικασία hacking, αφού δεν έχει υπάρξει ουδεμία επαφή με το δίκτυο που βρήκα τον κωδικό του. Εάν ο χρήστης του ρούτερ είχε μπει στον κόπο να αλλάξει κωδικό WiFi, η μέθοδος αυτή δε θα δούλευε, καθώς το Greek WPA Finder θα μου έδινε ακόμα τους ίδιους 2 κωδικούς, χωρίς όμως αυτοί να είναι σωστοί.

2) Το πρόγραμμα αυτό έχει τη μεγαλύτερη επιτυχία σε ρούτερ του ΟΤΕ και κυρίως όσα είναι μάρκας Thomson, αυτά που έδινε ο ΟΤΕ περίπου το 2008-2014. Να προσθέσω εδώ ότι τα ρούτερ αυτά θεωρούνται καλής ποιότητας, και δίνονταν σε όσους έπαιρναν το ακριβότερο πακέτο της εποχής (τότε ήταν 12Mbit/s).

3) Γενικά δουλεύει καλύτερα σε ρούτερ με κωδικό WPA, μετά σε κωδικούς WPA2. Δε δουλεύει για κωδικούς WEP, τουλάχιστον σε όσα δίκτυα δοκίμασα κοντά μου.

4) Εφόσον μπείτε σε ένα δίκτυο, μπορείτε να επισκφθείτε τη σελίδα του ρούτερ απομακρυσμένα. Τα συνήθη στοιχεία είναι:

username: admin

password: admin

Και από εκεί μπορείτε να αλλάξετε τις ρυθμίσεις του δικτύου, όπως μάθαμε στο πρώτο μάθημα. Μην το κάνετε σε ξένα δίκτυα, είναι εξαιρετικά παράνομο.

5) Η ύπαρξη αυτού του προγράμματος δείχνει πόσο μεγάλη σημασία έχει να αλλάξετε τον κωδικό στο δίκτυό σας, αν φοβάστε ότι το χρησιμοποιούν άλλοι. Οπότε:

>Πώς προστατεύω το δίκτυό μου από
«επιθέσεις» μέσω Greek WPA Finder;

Με δύο απλά βήματα:

Πρώτον, βάζετε κωδικό στο δίκτυο, και όχι τον εργοστασιακό.

Δεύτερον, αλλάζετε την SSID (όνομα δικτύου). Και πάλι όμως είναι εφικτό σε κάποια δίκτυα να βρεθεί ο κωδικός τους και με αλλαγμένο όνομα.

>Επίλογος

Αυτό είναι το πρώτο μάθημα στο οποίο διδάσκω την τέχνη ξεκλειδώματος δικτύων. Στις περισσότερες περιπτώσεις, ιδίως δε για κάτοικους Αθήνας, από τα 20 σήματα ασύρματων δικτύων που σας διαπερνούν, τουλάχιστον τα δύο ξεκλειδώνονται μέσω της εφαρμογής αυτής.

Σε αυτό το σημείο σας παροτρύνω να μην κάνετε κατάχρηση της δύναμης που έχετε. Μην ξεχνάτε ότι το να μάθεις πώς να διαρρήξεις μια κλειδαριά δε σε κάνει κλέφτη, μέχρι να μπεις σε σπίτι άλλου.

“With great power, comes great responsibility.”

-Benjamin “Uncle Ben” Parker, Spider-Man

Τα λέμε στο επόμενο μάθημα.

-TEL9021