



Τμήμα Ηλεκτρονικών Μηχανικών Τ.Ε.

Ανάπτυξη συστήματος ανίχνευσης ευπαθειών σε ασύρματα δίκτυα δεδομένων

Πτυχιακή Εργασία

Φοιτητής: Αλέξανδρος Ζαρκαδούλας
ΑΜ: 40288

Επιβλέπων Καθηγητής

Χαράλαμπος Πατρικάκης
Αναπληρωτής Καθηγητής

Ημερομηνία: 5/5/2017

Περίληψη

Στην παρούσα πτυχιακή εργασία σας παρέθεσα ένα θεωρητικό υπόβαθρο για την δοκιμή διείσδυσης όπως επίσης και τα κυριότερα είδη επιθέσεων που χρησιμοποιούνται για παραβίαση με ορισμένες λύσεις για να αποφύγουμε την υποκλοπή των προσωπικών μας, κι όχι μόνο, δεδομένων. Στη συνέχεια, αφού παρουσίασα τον μικροϋπολογιστή Raspberry Pi και την εγκατάσταση ειδικής έκδοσης του Kali Linux σε αυτό, μέσω της υπηρεσίας SSH κατάφερα να έχω απομακρυσμένη πρόσβαση ώστε οι δοκιμές να μπορούν να γίνουν από οπουδήποτε για να μην γίνω αντιληπτός. Βέβαια, για νομικούς λόγους, οι επιθέσεις πραγματοποιήθηκαν στο δικό μου ασύρματο οικιακό δίκτυο Wi-Fi και στο προσωπικό μου smartphone όσον αφορά το Bluetooth. Ανέπτυξα, λοιπόν, ένα σύστημα όπου με απομακρυσμένη πρόσβαση και χωρίς γραφικό περιβάλλον χρήστη κατάφερα να αποκτήσω τον κωδικό του δικτύου αρκετά γρήγορα ώστε να μπορέσω να συνδεθώ και να εισχωρήσω στο δίκτυο για περαιτέρω επιθέσεις. Αντίθετα, η ανίχνευση ευπάθειας σε Bluetooth δεν ήταν επιτυχής αφού δεν κατάφερα να αποκτήσω πρόσβαση στο smartphone που στοχοποίησα και ο λόγος είναι ότι η ευπάθεια που πήγα να εκμεταλλευτώ έχει πλέον διορθωθεί και το εργαλείο που χρησιμοποίησα έχει χρόνια να ανανεωθεί. Όλα δείχνουν, όμως, ότι το Bluetooth επανέρχεται σε μεγάλα επίπεδα δημοτικότητας και χρήσης λόγω της όλο και αυξανόμενης αγοράς του Internet of Things (Διαδίκτυο των Αντικειμένων), άρα και στο επίκεντρο ερευνών και επιθέσεων.

Λέξεις – κλειδιά

Έλεγχος διείσδυσης, εκμετάλευση, επιθέσεις κωδικών, εκμετάλευση από την πλευρά του πελάτη, κοινωνική μηχανική, παράκαμψη εφαρμογών προστασίας από ιούς, μετά την εκμετάλλευση, δοκιμή εφαρμογής διαδικτύου, ασύρματες επιθέσεις, Kali Linux, Raspberry Pi, ζευγάρισμα, εξυπηρετητής, διακομιστής, χαρακτηριστικό ίχνος, SSH, BSSID, CH, ESSID, χειραγία WPA, Mac address