University of Piraeus
Department of Digital Systems

Master's Thesis

Εφαρμογή υποκλοπής κωδικού ασύρματου δικτύου από router, σχεδιασμένο για μικροϋπολογιστή τύπου Rpi Zero W

Γεωργίου Κωνσταντίνος
ΜΤΕ 1706, kostisgeorgiou@ssl-unipi.gr

Επιβλέπων Καθηγητής: **Κ. Νταντογιάν Χριστόφορος, dadoyan@unipi.gr**

Πειραιάς 2018-19

Περιεχόμενα

Πίνακας Εικόνων

Περίληψη

Η εργασία αυτή πραγματεύεται τη δυνατότητα εκμετάλλευσης ενός μικροϋπολογιστή για να μπορέσουμε να πιστοποιηθούμε σε ένα δίκτυο υπολογιστών και να εκμεταλλευτούμε τυχόν αδυναμίες που θα συναντήσουμε. Χρησιμοποιώντας λοιπόν ένα Raspberry pi Zero W, το οποίο, λόγω του μεγέθους του, μπορεί εύκολα να περάσει απαρατήρητο ή να καμουφλαριστεί σε μια συσκευή που χρειάζεται το δίκτυο, προσπαθούμε να συλλέξουμε όσον το δυνατόν περισσότερες πληροφορίες για το δίκτυο που εξετάζουμε και να ανοίξουμε όσον το δυνατό περισσότερες πόρτες προς αυτό. Φυσικά, όλα αυτά με όσο το δυνατόν λιγότερες κινήσεις, για να προσομοιώσουμε ένα ρεαλιστικό σενάριο.

Κεντρικός μας στόχος λοιπόν, είναι να μπορέσουμε να συνδέσουμε μία τέτοια μικροσυσκευή ενσύρματα στο router, η οποία θα λειτουργήσει ως Access Point για εμάς, έτσι ώστε όταν συνδεθούμε σε αυτή να λειτουργήσει ως πύλη για εμάς στο δίκτυο. Εκμεταλλευόμενοι την έλλειψη αυθεντικοποίησης των router σε ενσύρματα συνδεδεμένες συσκευές, θα μπορέσουμε να εισέλθουμε στο δίκτυο μέσω του Rpi Zero. Αυτό είναι πολύ κρίσιμο για την επιτυχή εισχώρησή μας και εκμετάλλευσης στο εξεταζόμενο δίκτυο, διότι, σε περίπτωση που υπάρχει άλλη πολιτική ασφαλείας για ασύρματα συνδεδεμένες συσκευές, αυστηρότερης σε προσβάσεις, θα μπορέσουμε να την αποφύγουμε, εφόσον η συσκευή μας λειτουργεί σαν πύλη για εμάς κι αυτή είναι συνδεδεμένη ενσύρματα. Επιπλέον, εφόσον συνδεθεί στο router, έχουμε τη δυνατότητα να τρέξουμε μέσω του Rpi προγράμματος το οποίο θα προσπαθήσει να κάνει login στο router, και να πάρει τον κωδικό του Wi-Fi του δικτύου.

Abstract

This thesis examines the possibility of using a microcomputer to be able to be certified in a computer network and take advantage of weaknesses that we will encounter. Using a Raspberry pi Zero W, which due to its size can easily go unnoticed or camouflaged on a device that needs the network, we try to collect as much information as possible about the network we are looking at and open as possible ports as we can to it. Of course, all this with as few moves as possible to simulate a realistic scenario.

Our main goal, therefore, is to be able to connect such a small device wired to the router, which will act as an Access Point for us, so that when we connect to it, it will act as a gateway for us on the network. Taking advantage of the lack of authentication of routers on wired devices, we will be able to enter the network through Rpi Zero. This is critical for our successful penetration and exploitation on the referred network, because if there is another security policy for wirelessly connected devices , tougher in access, we will be able to avoid it as long as our device acts as a gateway to us and it is connected wiresely. In addition, once connected to the router, we are able to run through the Rpi program, which will attempt to login to the router, and get the network Wi-Fi password.

1. Hardware

1.1 Raspberry Pi Zero W

EIKONA 1 - Rasberry Pi Zero W

Το Raspberry Pi Zero W είναι ένα μικρού κόστους αλλά και μικρού μεγέθους ηλεκτρονικός υπολογιστής πολύ μικρότερος από το εξαιρετικά μικρό αρχικό Raspberry Pi. Η έκδοση η W διαθέτει On-Board Wi-Fi και Bluetooth.

Το μέγεθος του είναι στα 65mm x 30mm και είναι εξαιρετικό για σχεδιασμό εφαρμογών, wearables, prototyping και οποιαδήποτε άλλη Raspberry Pi εφαρμογή θα θέλατε να κάνετε σε μικρό μέγεθος.
Το Raspberry Pi Zero W διαθέτει τον chipset BCM2835 το οποίο είναι υπερχρονισμένο στο 1Ghz με 512 MB RAM και τον ίδια έξοδο Video στα 1080p. Το Raspberry Pi Zero W χρησιμοποιεί μόνο 140mA στα 5V.

Τεχνικά χαρακτηριστικά:

- BCM2835 chipset, Overclocked to 1Ghz
- 1GHz ARM11 core (40% faster than Raspberry Pi 1, ARMv6 architecture)
- 512MB of LPDDR2 SDRAM
- Micro-SD card slot
- A mini-HDMI socket for 1080p60 video output
- Micro-USB sockets for data and power
- CSI camera connector
- Micro-USB for Power
- Micro-USB OTG Host for Data
- 40-pin GPIO header (same pinout as Model A+/B+/2B/3B)
- 2.4GHz 802.11 b/g/n Wi-Fi
- Bluetooth 4.1 LE

Το Raspberry Pi Zero W έχει υποβληθεί σε εκτεταμένες δοκιμές συμμόρφωσης και πληροί τα ακόλουθα Ευρωπαϊκά πρότυπα:

- Electromagnetic Compatibility Directive (EMC) 2014/30/EU
- Restriction of Hazardous Substances (RoHS) Directive 2011/65/EU

1.2 ZTE H108N Router

ΕΙΚΟΝΑ 2 - ZTE H108N Router

Το H108N είναι ασύρματο μόντεμ ADSL2 + με τέσσερις διασυνδέσεις Ethernet και διεπαφή Wi-Fi IEEE 802.11 b / g / n και μία διασύνδεση USB. Χρησιμοποιείται για ευρυζωνική πρόσβαση και την υπηρεσία IPTV στο σπίτι. Η ενσωμάτωση των τεχνολογιών TR-069, διευκολύνει την αυτόματη εγκατάσταση και την αυτόματη παροχή υπηρεσιών. Χρησιμοποιείται ευρέως από τους παρόχους Internet, Wind και Vodafone, σε οικιακές εγκαταστάσεις.

Τεχνικά χαρακτηριστικά ZTE H108N Router:

Architecture:	MIPS
Vendor:	Broadcom
System-On-Chip:	Broadcom BCM63281 KFBG
CPU/Speed	320Mhz
Flash-Chip:	Macronix MX25L6406E 8MiB)
RAM:	Nanya Technology Corporation NT5TU32M16DG-AC (64MiB)
Wireless:	Broadcom BCM43225 2.4ghz 802.11bgn
Ethernet:	in-SoC
Internet:	ADSL/ADSL2+
USB:	1

1.3 Sagem Fast 2404 Router

ΕΙΚΟΝΑ 3 - Sagem Fast 2404 Router

Το Sagem Fast 2404 είναι ένα ασύρματο router ADSL2 / 2 + με μία θύρα WAN RJ-11 και τέσσερις θύρες LAN 10 / 100Base-T.

Το ενσωματωμένο σημείο πρόσβασης συμμορφώνεται με τα πρότυπα IEEE 802.11b / g, παρέχοντας ταχύτητες ασύρματης μετάδοσης μέχρι και 54Mbps. Υποστηρίζει ασύρματη κρυπτογράφηση WEP και WPA / WPA2 και χρησιμοποιεί το WMM (QoS) για να δώσει προτεραιότητα στην κίνηση μέσω του δικτύου.

Αυτός ο δρομολογητής υποστηρίζει τη διέλευση VPN για IPSec, L2TP και PPTP. Ένα ενσωματωμένο τείχος προστασίας SPI προστατεύει το δίκτυο από κακόβουλες επιθέσεις.

Τεχνικά χαρακτηριστικά Sagem Fast 2404 Router:

Architecture:	MIPS
Vendor:	Broadcom
Board Id:	F@ST2404
System-On-Chip:	BCM6348SKFBG
CPU/Speed	BMIPS3300 V0.7 / 256 MHz
Flash-Chip:	A29L320ATV-70F SST39VF3201
Flash size:	4 MiB
RAM:	16 MiB
Wireless:	Broadcom 4318 802.11b/g (onboard)
Ethernet:	Broadcom BCM5325 w/ vlan support swconfig
Internet:	ADSL2+
USB:	No
Serial:	Yes
JTAG:	Yes

2. Software

2.1 Python Libraries

2.1.1 Selenium Web driver

Η βιβλιοθήκη της Python Selenium παρέχει ένα απλό API με το οποίο μπορούμε να γράψουμε λειτουργικό κώδικα χρησιμοποιώντας το Selenium WebDriver. Μέσω του API του Selenium μπορούμε να έχουμε πρόσβαση σε όλες τις λειτουργίες του Selenium WebDriver με δυναμικό τρόπο.

Παρέχεται, λοιπόν, ένα αποτελεσματικό API, για να έχουμε πρόσβαση σε Selenium Web Drivers, όπως το Firefox, το Internet Explorer, το Chrome. Οι τρέχουσες εκδόσεις Python που υποστηρίζονται είναι 2.7, 3.5 και άνω.

2.1.2. Beautiful Soup

Το Beautiful Soup είναι μια βιβλιοθήκη Python που αναλύει έγγραφα HTML ή XML σε μια δομή δέντρου που διευκολύνει την εύρεση και εξαγωγή δεδομένων. Συχνά χρησιμοποιείται για web scraping από ιστότοπους. Το Beautiful Soup διαθέτει μια απλή, διεπαφή μέσω Python και αυτόματη μετατροπή κωδικοποίησης για να είναι εύκολο να εργαστείτε με δεδομένα κάποιου ιστότοπου.

Οι ιστοσελίδες είναι δομημένα έγγραφα και το Beautiful Soup μας δίνει τα εργαλεία για να περιηγηθούμε μέσα από αυτήν την σύνθετη δομή και να εξαγάγουμε κομμάτια των πληροφοριών που χρειαζόμαστε.

2.1.3 Xvfb – PyVirtualDisplay

Εάν θέλουμε να εκτελέσουμε τις δοκιμές μας σε έναν υπολογιστή δίχως έξοδο οθόνης, θα συνειδητοποιήσουμε γρήγορα ότι θα αντιμετωπίσουμε πρόβλημα εφόσον το πρόγραμμα περιήγησης ζητάει την οθόνη που θα ανοίξει.

Το Xvfb λοιπόν, είναι ένας διακομιστής προβολής εντός μνήμης για λειτουργικό σύστημα που μοιάζει με UNIX (π.χ. Linux). Με αυτό, έχουμε τη δυνατότητα να εκτελέσουμε γραφικές εφαρμογές χωρίς εμφάνιση (π.χ. δοκιμές προγράμματος περιήγησης), έχοντας επίσης τη δυνατότητα λήψης στιγμιότυπων οθόνης.

Από κώδικα Python, υπάρχει μια βιβλιοθήκη που ονομάζεται pyvirtualdisplay,την οποία μπορούμε να χρησιμοποιήσουμε για να εκκινήσουμε την εικονική εμφάνιση Xvfb. Με αυτόν τον τρόπο, ο περιηγητής ιστότοπων θα ανοίξει στην εικονική οθόνη μας.

2.2 Gecko (Marionette) Driver Selenium

Τι είναι το Gecko Driver;

Είναι μια μηχανή προγράμματος περιήγησης στο Web η οποία είναι ενσωματωμένη στο πρόγραμμα περιήγησης Mozilla Firefox. Το πρόγραμμα οδήγησης λειτουργεί ως μεσολαβητής μεταξύ των Web Driver enabled προγραμμάτων οδήγησης (Eclipse, Netbeans κ.λπ.) και του προγράμματος περιήγησης Mozilla Firefox.

Με λίγα λόγια, το πρόγραμμα οδήγησης Gecko λειτουργεί ως σύνδεσμος μεταξύ των δοκιμών του προγράμματος Selenium Web Driver και του προγράμματος περιήγησης Mozilla Firefox. Πριν από το Selenium 3, το πρόγραμμα περιήγησης Mozilla Firefox ήταν το προεπιλεγμένο πρόγραμμα περιήγησης για το Selenium.

Μετά το Selenium 3, οι δοκιμαστές χρειάστηκε να προετοιμάσουν το σενάριο χρήσης του Firefox χρησιμοποιώντας ειδικά το Gecko Driver. Το Selenium χρησιμοποιεί το πρωτόκολλο W3C Webdriver για την αποστολή αιτημάτων στο GeckoDriver, το οποίο μεταφράζει σε ένα πρωτόκολλο που ονομάζεται Marionette. Ο Firefox θα κατανοήσει τις εντολές που μεταδίδονται με τη μορφή πρωτοκόλλου Marionette και τις εκτελεί.

ΕΙΚΟΝΑ 4 - Επίπεδα Διασύνδεσης Selenium με Firefox browser

Πλεονέκτημα της χρήσης του Gecko Driver

Το Selenium Webdriver v.2.53, δεν είναι συμβατό με το Mozilla Firefox v. 47.0+. Το πρόγραμμα οδήγησης Firefox που χρησιμοποιείται σε προηγούμενες εκδόσεις του Mozilla Firefox θα διακοπεί και θα χρησιμοποιηθεί μόνο η εφαρμογή Gecko Driver. Ως εκ τούτου, οι δοκιμαστές αναγκάζονται να χρησιμοποιούν το Gecko Driver εάν θέλουν να εκτελούν αυτοματοποιημένες δοκιμές στο Mozilla Firefox έκδοση 47.0+.

Αλλά το μεγάλο ερώτημα είναι: ποιο είναι το πλεονέκτημα;

Το κύριο πλεονέκτημα της χρήσης του Gecko Driver σε αντίθεση με το προεπιλεγμένο πρόγραμμα οδήγησης Firefox είναι η συμβατότητα. Το Gecko Driver χρησιμοποιεί πρωτόκολλο W3C WebDriver για επικοινωνία με το Selenium. Το W3C είναι ένα καθολικά καθορισμένο πρότυπο για το πρόγραμμα οδήγησης Web. Αυτό σημαίνει ότι οι προγραμματιστές του Selenium (άτομα που κωδικοποιούν βάση του) δεν χρειάζεται να δημιουργήσουν μια νέα έκδοση του προγράμματος οδήγησης Web για κάθε έκδοση προγράμματος περιήγησης. Το ίδιο πρόγραμμα οδήγησης Web μπορεί να χρησιμοποιηθεί για πολλές εκδόσεις προγράμματος περιήγησης. Ως εκ

τούτου, το Gecko Driver προτιμάται σε σύγκριση με την προηγούμενη εφαρμογή του προγράμματος οδήγησης του Firefox.

Συχνές εξαιρέσεις εμφανίστηκαν κατά τη χρήση του Gecko Driver:

- ✓ Α. Η διαδρομή προς το εκτελέσιμο πρόγραμμα οδήγησης πρέπει να οριστεί από την ιδιότητα συστήματος webdriver.gecko.driver:

Αυτή η εξαίρεση εμφανίζεται όταν ο χρήστης προσπαθεί να δημιουργήσει ένα instance στον οδηγό του Firefox χωρίς να ρυθμίσει την ιδιότητα συστήματος για τον οδηγό gecko. Αυτό γίνεται συνήθως από αρχάριους στο Selenium που δεν γνωρίζουν τις αλλαγές που έγιναν στο Selenium 3 από προηγούμενες εκδόσεις.

Η λύση για την παραπάνω εξαίρεση είναι να ορίσετε την ιδιότητα συστήματος για το πρόγραμμα οδήγησης gecko με τη θέση του αρχείου geckodriver.exe.

Σημειώστε ότι πρέπει να ορίσετε την ιδιότητα του προγράμματος οδήγησης gecko πριν δημιουργήσετε μια παρουσία του προγράμματος οδήγησης Mozilla Firefox.

- ✓ Β. Firefox Not Connected Exception: org.openqa.selenium.firefox. NotConnectedException: Δεν είναι δυνατή η σύνδεση με τον κεντρικό υπολογιστή 127.0.0.1 στη θύρα 7055 μετά από 45000 ms.

Αυτή η εξαίρεση συνήθως εμφανίζεται όταν η έκδοση του Firefox έχει αναβαθμιστεί στην πιο πρόσφατη έκδοση. Η λύση αυτής της εξαίρεσης είναι να ενημερώσετε το εκτελέσιμο αρχείο του Selenium και το πρόγραμμα οδήγησης gecko στην πιο πρόσφατη έκδοση και να χρησιμοποιήσετε το ίδιο.

- ✓ Γ. Session Not Created Exception: org.openqa.selenium.SessionNotCreatedException: Δεν είναι δυνατή η δημιουργία νέας απομακρυσμένης περιόδου σύνδεσης.

Αυτή η εξαίρεση προκύπτει λόγω ζητημάτων συμβατότητας μεταξύ προγράμματος οδήγησης Selenium και Gecko. Το πρόγραμμα οδήγησης Gecko λειτουργεί με Firefox έκδοση 47 ή παραπάνω. Μπορεί να επιλυθεί με την ενημέρωση της έκδοσης Firefox σε 47 ή παραπάνω.

- ✓ Δ. Connection Refused Exception: WebDriver Exception: Connection Refused

Αυτή η εξαίρεση είναι το μήνυμα που δημιουργείται όταν το πρόγραμμα οδήγησης web δεν είναι σε θέση να δημιουργήσει μια σύνδεση με τον Firefox. Μπορεί να επιλυθεί χρησιμοποιώντας οποιαδήποτε από τις ακόλουθες τεχνικές.

- Χρησιμοποιήστε τη μέθοδο driver.quit () για να κλείσετε τις προηγούμενες συνεδρίες του προγράμματος οδήγησης web.
- Καθαρίστε την προσωρινή μνήμη του προγράμματος περιήγησης πριν εκτελέσετε τις αυτόματες δοκιμές.
- Χρησιμοποιείτε πάντα την τελευταία έκδοση του προγράμματος οδήγησης Selenium Gecko και την πιο πρόσφατη έκδοση του προγράμματος περιήγησης Firefox.

2.3 SSH (Secure Socket Shell)

Το SSH, επίσης γνωστό ως Secure Shell ή Secure Socket Shell, είναι ένα πρωτόκολλο δικτύου που δίνει στους χρήστες και ιδιαίτερα τους διαχειριστές συστημάτων, έναν ασφαλή τρόπο πρόσβασης σε έναν υπολογιστή μέσω ενός μη ασφαλούς δικτύου. Το SSH αναφέρεται επίσης στη σουίτα βοηθητικών προγραμμάτων που υλοποιούν το πρωτόκολλο SSH.

Το Secure Shell παρέχει ισχυρή επικοινωνία ταυτότητας και κρυπτογραφημένων δεδομένων μεταξύ δύο υπολογιστών που συνδέουν ένα ανοιχτό δίκτυο όπως το Διαδίκτυο. Το SSH χρησιμοποιείται ευρέως από διαχειριστές δικτύου για την εξ αποστάσεως διαχείριση συστημάτων και εφαρμογών, επιτρέποντάς τους να συνδεθούν σε άλλον υπολογιστή μέσω δικτύου, να εκτελέσουν εντολές και να μετακινήσουν αρχεία από έναν υπολογιστή σε άλλο.

Το SSH αναφέρεται τόσο στο πρωτόκολλο κρυπτογραφικού δικτύου όσο και στη σειρά βοηθητικών προγραμμάτων που εφαρμόζουν το πρωτόκολλο αυτό. Το SSH χρησιμοποιεί το μοντέλο πελάτη-διακομιστή, συνδέοντας μια ασφαλή εφαρμογή πελάτη κελύφους, το τέλος στο οποίο εμφανίζεται η περίοδος σύνδεσης, με ένα διακομιστή SSH, το τέλος στο οποίο εκτελείται η περίοδος σύνδεσης. Οι υλοποιήσεις SSH περιλαμβάνουν συχνά υποστήριξη για πρωτόκολλα εφαρμογών που χρησιμοποιούνται για εξομοίωση τερματικών ή μεταφορές αρχείων.

Το SSH μπορεί επίσης να χρησιμοποιηθεί για τη δημιουργία ασφαλών καναλιών επικοινωνίας για άλλα πρωτόκολλα εφαρμογών, όπως π.χ., για την ασφαλή εκτέλεση των γραφικών περιόδων του X Window System εξ αποστάσεως. Ένας διακομιστής SSH, by default, "ακούει" στην τυπική θύρα πρωτοκόλλου ελέγχου μετάδοσης (TCP) 22.

Παρόλο που είναι δυνατή η χρήση SSH με ένα συνηθισμένο αναγνωριστικό χρήστη και κωδικό πρόσβασης ως πιστοποιήσεις, το SSH βασίζεται συχνότερα σε ζεύγη δημόσιων κλειδιών για τον έλεγχο της ταυτότητας μεταξύ των κεντρικών υπολογιστών. Οι μεμονωμένοι χρήστες πρέπει να εξακολουθούν να χρησιμοποιούν το αναγνωριστικό χρήστη και τον κωδικό πρόσβασής τους (ή άλλες μεθόδους ελέγχου ταυτότητας) για να συνδεθούν με τον ίδιο τον απομακρυσμένο κεντρικό υπολογιστή, αλλά το τοπικό μηχάνημα και το απομακρυσμένο μηχάνημα πιστοποιούνται ξεχωριστά μεταξύ τους. Αυτό επιτυγχάνεται δημιουργώντας ένα μοναδικό ζεύγος δημόσιου κλειδιού για κάθε κεντρικό υπολογιστή στην επικοινωνία.

Μία μεμονωμένη περίοδος απαιτεί δύο ζεύγη δημόσιων κλειδιών: ένα ζεύγος δημόσιων κλειδιών για τον έλεγχο της ταυτότητας του απομακρυσμένου μηχανήματος στο τοπικό μηχάνημα και ένα δεύτερο ζευγάρι δημόσιου κλειδιού για τον έλεγχο της ταυτότητας του τοπικού μηχανήματος στο απομακρυσμένο μηχάνημα.

Οι συνδέσεις SSH έχουν χρησιμοποιηθεί για τη διασφάλιση πολλών διαφορετικών τύπων επικοινωνιών μεταξύ τοπικού υπολογιστή και απομακρυσμένου υπολογιστή, συμπεριλαμβανομένης της ασφάλειας απομακρυσμένης πρόσβασης σε πόρους, απομακρυσμένης εκτέλεσης εντολών, παράδοσης ενημερωμένων εκδόσεων λογισμικού και ενημερωμένων εκδόσεων και άλλων διοικητικών ή διαχειριστικών εργασιών.

Οι λειτουργίες που ενεργοποιεί το SSH περιλαμβάνουν:

- Ασφαλής απομακρυσμένη πρόσβαση σε συστήματα ή συσκευές δικτύου με δυνατότητα SSH, για χρήστες καθώς και αυτοματοποιημένες διαδικασίες.
- Ασφαλείς και διαδραστικές συνεδρίες μεταφοράς αρχείων.
- Αυτοματοποιημένες και ασφαλείς μεταφορές αρχείων.
- Ασφαλής έκδοση εντολών σε απομακρυσμένες συσκευές ή συστήματα.
- Ασφαλή διαχείριση των στοιχείων της υποδομής δικτύου.

Το SSH μπορεί να χρησιμοποιηθεί διαδραστικά για να ενεργοποιήσει τις συνεδρίες τερματικού και πρέπει να χρησιμοποιηθεί αντί για το λιγότερο ασφαλές πρόγραμμα Telnet. Το SSH χρησιμοποιείται επίσης συχνά σε σενάρια και άλλο λογισμικό για να επιτρέψει στα προγράμματα και τα συστήματα να έχουν πρόσβαση εξ αποστάσεως και με ασφάλεια σε δεδομένα και άλλους πόρους.

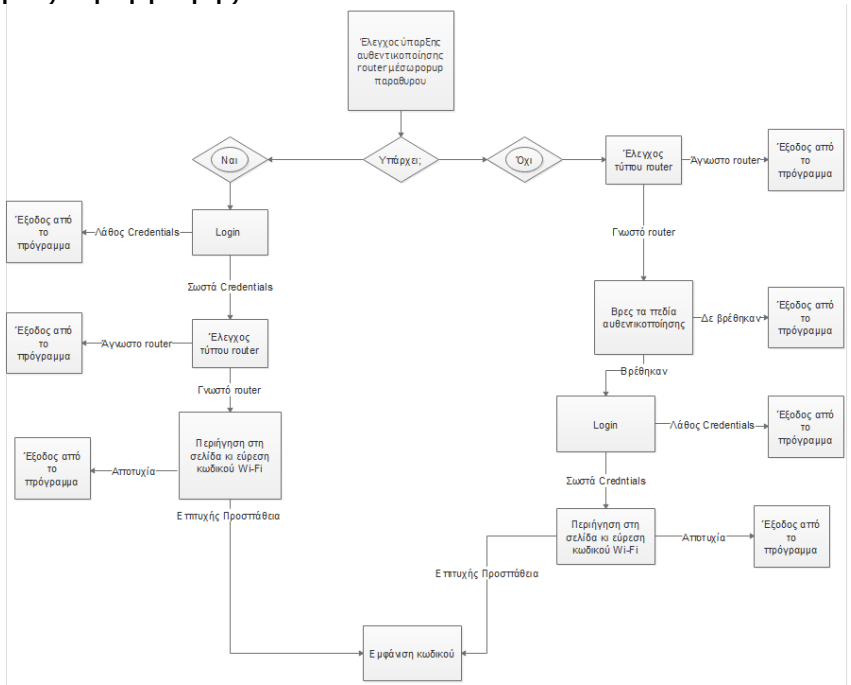
3. Ανάπτυξη εφαρμογής

Σκοπός μας σε αυτήν την ενότητα , είναι να περιγράψουμε τα κυριότερα σημεία ανάπτυξης εφαρμογής σε Python , η οποία θα μπορεί να μας εξάγει τον κωδικό Wi-Fi από το router που θα είναι ενσύρματα συνδεδεμένο.

Έχουμε καλύψει συγκεκριμένα router (2), το κύριο όμως σημείο αναφοράς είναι ο διαφορετικός τρόπος αυθεντικοποίησης τους.

Στη μία περίπτωση αυτή γίνεται μέσα από τη σελίδα HTML του router (login page), ενώ στην άλλη περίπτωση, πριν μπεις στη login σελίδα, υπάρχει ένα javascript popup παράθυρο αυθεντικοποίησης.

3.1. Σχεδιασμός Εφαρμογής



ΕΙΚΟΝΑ 5 - Σχεδιασμός UML εφαρμογής

3.2 Παρατηρήσεις κώδικα εφαρμογής

Παρακάτω, θα περιγράψουμε τα κύρια κομμάτια του κώδικα της εφαρμογής, όπου θα σταθούμε στα πιο σημαντικά και κρίσιμα σημεία του, που έχουν και ενδιαφέρον ανάπτυξης. Στις πρώτες γραμμές του κώδικα, συναντάμε λοιπόν τις μεταβλητές, οι οποίες έχουν αποθηκευμένες κάποιες παραμέτρους, σταθερές και καθολικές για το πρόγραμμά. Στον κώδικα, θα βρείτε σχόλια τα οποία βοηθούν στην κατανόηση των λειτουργιών της εφαρμογής.

3.2.1 Αρχική συνάρτηση αρχικοποίησης διαδικασίας

Η συνάρτηση εκκίνησης η οποία σε πρώτη φάση βρίσκει την Default Gateway όπου είναι η IP του router και ανοίγει ένα εικονικό παράθυρο περιήγησης σε αυτήν (σελίδα του router). Σε δεύτερη φάση, ελέγχεται εάν σε αυτή την κλήση έχει εμφανιστεί popup παράθυρο για αυθεντικοποίηση. Αν ναι, καλεί την αντίστοιχη συνάρτηση για login σε router με popup παράθυρο και ύστερα ελέγχει τον τίτλο της σελίδας του router (αν το login επιτευχθεί επιτυχημένα), ειδάλλως, μπαίνει στη σελίδα του router, ελέγχει αν το router είναι γνωστό κι έπειτα εκκινεί τη διαδικασία αυθεντικοποίησης σε αυτό.

3.2.2 Συναρτήσεις αυθεντικοποίησης για τα διαφορετικά τύπου routers

3.2.2.1 Αυθεντικοποίηση σε router με popup παράθυρο

Σε πρώτο στάδιο, ζητάμε είσοδο από τον χρήστη για τη μέθοδο εισαγωγής των credentials προς δοκιμή. Υποστηρίζονται 2 τρόποι, εισαγωγή από τον χρήστη κι από το αρχείο. Χρησιμοποιούμε τη μέθοδο driver.switch_to.alert.send_keys(), η οποία κάνει focus το παράθυρο αυθεντικοποίησης και εισάγει τις παραμέτρους που του εισάγουμε μέσα στις παρενθέσεις σαν εισόδους. Συνήθως τα alert popup παράθυρα αυθεντικοποίησης, αποτελούνται από 2 πεδία, ένα για το όνομα χρήστη κι ένα για τον κωδικό, με την προαναφερθείσα σειρά. Χρησιμοποιούμε το πλήκτρο Tab, για τη μετάβαση από το ένα πεδίο στο άλλο, οπότε και η είσοδός μας θα είναι της μορφής [userinput + Keys.TAB + passwdinput]. Για τη δοκιμή των εισόδων που επιλέξαμε, χρησιμοποιούμε τη μέθοδο driver.switch_to.alert.accept(), η οποία προσομοιώνει το πάτημα του κουμπιού «Αποδοχή» στο παράθυρο.

Σε επόμενο χρόνο, με την εισαγωγή των credentials αυθεντικοποίησης, αναμένουμε το event της επανεμφάνισης του παράθυρου αυθεντικοποίησης. Αν εμφανιστεί, σημαίνει πως ήταν λάθος η εισαγωγή μας και ξαναδοκιμάζουμε, αλλιώς υποθέτουμε πως βρήκαμε το όνομα χρήστη και τον κωδικό. Συνήθως, σε τέτοιες μεθόδους αυθεντικοποίησης, δεν παρατηρείται κάποιο χρονικό όριο στις προσπάθειες, οπότε δε χρειάζεται να προβλέψουμε αυτό το σενάριο.

3.2.2.2 Αυθεντικοποίηση σε router χωρίς popup παράθυρο

Σε πρώτο στάδιο, ζητάμε είσοδο από τον χρήστη για τη μέθοδο εισαγωγής των credentials προς δοκιμή. Υποστηρίζονται 2 τρόποι , εισαγωγή από τον χρήστη κι από το αρχείο. Πριν την κλήση αυτής της συνάρτησης, καλείται η find_login_fields(), η οποία θα επιστρέψει σαν αποτέλεσμα τα ids των πεδίων που χρησιμοποιούνται σαν πεδία εισαγωγής credentials, τα οποία χρησιμοποιούνται σαν ορίσματα αυτής.

Γεμίζουμε λοιπόν τα πεδία αυτά με τις επιλογές εισόδου μας και πατάμε κάθε φορά το κουμπί που έχει σαν χαρακτηριστικό id, το λεκτικό «LoginId». Έχει παρατηρηθεί πως στην πλειοψηφία των routers, τα πεδία για την εισαγωγή credentials καθώς και το κουμπί αποδοχής, έχουν κοινότυπα ονόματα, τα οποία μπορούν να μπουν σε έναν γενικότερο κανόνα.

Σε κάθε προσπάθειά μας λοιπόν, προσπαθούμε να καλέσουμε το jframe που παράγεται κατά τη σωστή αυθεντικοποίησης, για το συγκεκριμένο router, με id "mainframe". Αν το βρούμε , σημαίνει πως τα στοιχεία εισαγωγής μας είναι σωστά, αλλιώς ξαναπροσπαθούμε. Σε αυτά τα router, ειδικότερα στα πιο καινούρια, παρατηρούμε πως υπάρχει χρονικός περιορισμός προσπαθειών. Για αυτό το λόγο, έχουμε προβλέψει πως κάθε 3 προσπάθειες θα υπάρχει μία καθυστέρηση για να επαναλάβουμε την προσπάθεια μας.

3.3 Συνάρτηση εύρεσης πεδίων εισαγωγής

Συνάρτηση υπεύθυνη για την εύρεση των χαρακτηριστικών πεδίων εισαγωγής του όνομα χρήστη και του κωδικού, τα οποία θα χρησιμοποιηθούν από το Selenium Web driver για την αυθεντικοποίηση. Σε αυτή τη συνάρτηση, θα χρησιμοποιηθεί η βιβλιοθήκη BeautifulSoup για web scraping της σελίδας , η οποία μας δίνει πιο πολλά εργαλεία για την βαθύτερη αναζήτηση των χαρακτηριστικών των πεδίων. Στη συνάρτηση αυτή λοιπόν, μπορείτε να δείτε πως αναζητούμε τα πεδία τα οποία έχουν μέσα στο όνομα τους το λεκτικό «user» και «pass» αντίστοιχα, καθώς και ανήκουν σε κάποιο html tag input, το οποίο και δηλωνει την είσοδο από τον χρήστη στη html.

3.4 Συναρτήσεις απόκτησης Wi-Fi κωδικού

Αυτές τις συναρτήσεις, τις καλούμε όταν έχουμε αυθεντικοποιηθεί με το router και προσομοιώνουν μία στοχευμένη περιήγηση στο interface του router, ώστε να αποκτήσουμε αυτό που χρειαζόμαστε. Η διαδικασία αυτή καλεί συνεχόμενα links που εμφανίζονται (σημαντικό είναι κατά την κλήση ενός link, να δίνουμε τον απαραίτητο χρόνο για την φόρτωση της σελίδας, πριν την κλήση του νέου link), εώς ότου φτάσουμε στο επιθυμητό σημείο. Δε βρέθηκε κάποιο μοτίβο, στα υπό δοκιμή router, το οποίο να μας βοηθήσει να φτιάξουμε κάποια αυτοματοποιημένη διαδικασία για την έυρεση του σημείου που βρίσκεται ο κωδικός.

Άξιο αναφοράς είναι, στην περίπτωση του router Sagem Fast 2404, πως ο κωδικός εμφανίζεται σε άλλο αναδυόμενο παράθυρο. Για να το χειριστούμε αυτό το γεγονός, αποθηκεύσαμε σε μία μεταβλητή το windows

handler του παραθύρου που ανοίγει (window_after = driver.window_handles[1]) και με αυτή την πληροφορία, μπορέσαμε να δηλώσουμε από ποιο παράθυρο θέλουμε ο Selenium web driver να πάρει την πληροφορία (driver.switch_to.window(window_after)).

3.5 Συνάρτηση εξόδου από το πρόγραμμα

Σε περίπτωση αποτυχίας κάποιας διαδικασίας στη διάρκεια του προγράμματος, έχει προβλεφθεί να γίνει ομαλά η έξοδος από το πρόγραμμα καθώς και να δοθούν στον χειριστή οι απαραίτητες πληροφορίες, ώστε να εκμεταλλευτούμε όσον το δυνατό περισσότερο την παρουσία της συσκευής μας στο router.

Καλώντας λοιπόν αυτή τη συνάρτηση εξόδου, μας δίνονται τα στοιχεία του Access Point Που έχει δημιουργηθεί από το Rpi W Zero, για να μπορέσουμε να συνδεθούμε με αυτό ακόμη και με SSH client. Η συσκευή μας έχει παραμετροποιηθεί έτσι ώστε να μπορούμε μέσω αυτής να έχουμε πρόσβαση στο δίκτυο (masquerading) και να αλληλεπιδράσουμε με το router (χειροκίνητη δοκιμή αυθεντικοποίησης).

4. Access Point λειτουργία

Προκειμένου να λειτουργήσει ως σημείο πρόσβασης, το Raspberry Pi θα πρέπει να έχει εγκατεστημένο λογισμικό σημείου πρόσβασης μαζί με το λογισμικό διακομιστή DHCP για να παρέχει συσκευές σύνδεσης με μια διεύθυνση δικτύου. Βεβαιωθείτε ότι το Raspberry Pi χρησιμοποιεί μια ενημερωμένη έκδοση του Raspbian.

- Εγκαταστήστε το απαιτούμενο λογισμικό (dnsmasq και hostapd) με αυτήν την εντολή:

  sudo apt install dnsmasq hostapd

- Διαμόρφωση στατικής IP

  Διαμορφώνουμε ένα αυτόνομο δίκτυο για να ενεργεί ως διακομιστής, οπότε το Raspberry Pi πρέπει να έχει μια στατική διεύθυνση IP που έχει αντιστοιχιστεί στην ασύρματη θύρα. Αυτή η τεκμηρίωση προϋποθέτει ότι χρησιμοποιούμε τις τυπικές διευθύνσεις IP 192.168.x.x για το ασύρματο δίκτυό μας, οπότε θα αναθέσουμε στον διακομιστή τη διεύθυνση IP 192.168.4.1. Θεωρείται επίσης ότι η ασύρματη συσκευή που χρησιμοποιείται είναι wlan0.

- Για να διαμορφώσετε τη στατική διεύθυνση IP, ανοίξτε το αρχείο διαμόρφωσης dhcpcd με την ακόλουθη εντολή:

  sudo nano /etc/dhcpcd.conf

- Μεταβείτε στο τέλος του αρχείου και επεξεργαστείτε το ώστε να μοιάζει με το εξής:

  interface wlan0

  static ip_address=192.168.4.1/24

  nohook wpa_supplicant

- Τώρα επανεκκινήστε τον dhcpcd daemon:

  sudo systemctl restart dhcpcd

- Ρύθμιση του διακομιστή DHCP (dnsmasq)

  Η υπηρεσία DHCP παρέχεται από το dnsmasq. By default, το αρχείο διαμόρφωσης περιέχει πολλές πληροφορίες που δεν χρειάζονται και είναι ευκολότερο να ξεκινήσει από το μηδέν. Μετονομάστε αυτό το αρχείο ρυθμίσεων και επεξεργαστείτε ένα νέο:

  sudo mv /etc/dnsmasq.conf /etc/dnsmasq.conf.orig

  sudo nano /etc/dnsmasq.conf

- Πληκτρολογήστε ή αντιγράψτε τις ακόλουθες πληροφορίες στο αρχείο διαμόρφωσης dnsmasq και αποθηκεύστε το:

interface=wlan0 # Use the require wireless interface - usually wlan0

dhcp-range=192.168.4.2,192.168.4.20,255.255.255.0,24h

Έτσι για wlan0, πρόκειται να παρέχουμε διευθύνσεις IP μεταξύ 192.168.4.2 και 192.168.4.20, με χρόνο μίσθωσης 24 ωρών. Αν παρέχετε υπηρεσίες DHCP για άλλες συσκευές δικτύου (π.χ. eth0), μπορείτε να προσθέσετε περισσότερες ενότητες με την κατάλληλη κεφαλίδα διεπαφής, με το εύρος διευθύνσεων που σκοπεύετε να δώσετε σε αυτήν τη διεπαφή.

Υπάρχουν πολλές περισσότερες επιλογές για το dnsmasq. Ανατρέξτε στην τεκμηρίωση dnsmasq για περισσότερες λεπτομέρειες.

- Επαναφόρτωση του dnsmasq για χρήση της ενημερωμένης ρύθμισης παραμέτρων:

  sudo systemctl reload dnsmasq

- Ρύθμιση του access point host software (hostapd)

Πρέπει να επεξεργαστείτε το αρχείο ρύθμισης hostapd, που βρίσκεται στο /etc/hostapd/hostapd.conf, για να προσθέσετε τις διάφορες παραμέτρους για το ασύρματο δίκτυό σας. Μετά την αρχική εγκατάσταση, αυτό θα είναι ένα νέο αρχείο.

sudo nano /etc/hostapd/hostapd.conf

Προσθέστε τις παρακάτω πληροφορίες στο αρχείο ρυθμίσεων. Αυτή η διαμόρφωση προϋποθέτει ότι χρησιμοποιούμε το κανάλι 7, με το όνομα δικτύου του NameOfNetwork και τον κωδικό πρόσβασης AardvarkBadgerHedgehog. Λάβετε υπόψη ότι το όνομα και ο κωδικός πρόσβασης δεν πρέπει να περιέχουν εισαγωγικά γύρω από αυτά. Ο κωδικός πρόσβασης πρέπει να έχει μήκος μεταξύ 8 και 64 χαρακτήρων.

Για να χρησιμοποιήσετε τη ζώνη των 5 GHz, μπορείτε να αλλάξετε τη λειτουργία λειτουργίας από hw_mode = g σε hw_mode = a. Οι πιθανές τιμές για το hw_mode είναι:

- a = IEEE 802.11a (5 GHz)
- b = IEEE 802.11b (2.4 GHz)
- g = IEEE 802.11g (2.4 GHz)
- ad = IEEE 802.11ad (60 GHz)

```
interface=wlan0

driver=nl80211

ssid=NameOfNetwork

hw_mode=g
```

channel=7

wmm_enabled=0

macaddr_acl=0

auth_algs=1

ignore_broadcast_ssid=0

wpa=2

wpa_passphrase=AardvarkBadgerHedgehog

wpa_key_mgmt=WPA-PSK

wpa_pairwise=TKIP

rsn_pairwise=CCMP

- Τώρα πρέπει να πούμε στο σύστημα πού θα βρει αυτό το αρχείο ρυθμίσεων.

  sudo nano /etc/default/hostapd

- Βρείτε τη γραμμή με # DAEMON_CONF και αντικαταστήστε την με αυτήν:

DAEMON_CONF="/etc/hostapd/hostapd.conf"

- Τώρα ενεργοποιήστε και ξεκινήστε το hostapd:

  sudo systemctl unmask hostapd

  sudo systemctl enable hostapd

  sudo systemctl start hostapd

  Προσθήκη της δρομολόγησης και του masquerading

- Επεξεργαστείτε /etc/sysctl.conf και αφαιρέστε από τα σχόλια αυτή τη γραμμή:

  net.ipv4.ip_forward=1

- Προσθέστε ένα iptables masquerading για την εξερχόμενη κίνηση στο eth0 και αποθηκεύουμε:

  sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

  sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"

- Επεξεργαστείτε το /etc/rc.local και προσθέστε αυτό ακριβώς πάνω από το "exit 0" για να εγκαταστήσετε αυτούς τους κανόνες κατά την εκκίνηση.

  iptables-restore < /etc/iptables.ipv4.nat

Χρησιμοποιώντας μια ασύρματη συσκευή, αναζητήστε δίκτυα. Το SSID δικτύου που καθορίσατε στη διαμόρφωση του hostapd θα πρέπει τώρα να υπάρχει και θα πρέπει να είναι προσβάσιμο με τον καθορισμένο κωδικό πρόσβασης.

Εάν το SSH είναι ενεργοποιημένο στο σημείο πρόσβασης Raspberry Pi, θα πρέπει να είναι δυνατό να συνδεθεί σε αυτό από ένα άλλο κιβώτιο Linux (ή ένα σύστημα με συνδεσιμότητα SSH που υπάρχει) ως εξής, υποθέτοντας ότι υπάρχει ο λογαριασμός pi:

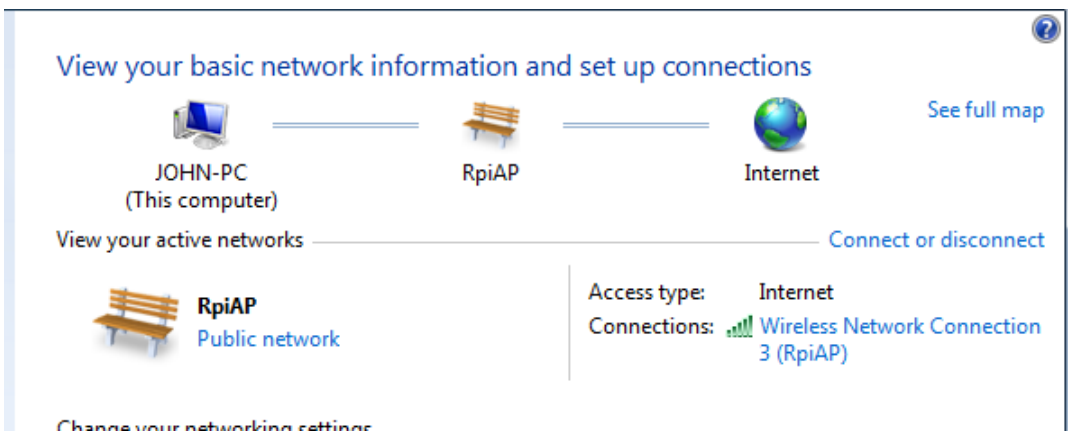
ssh pi@192.168.4.1

Μέχρι αυτό το σημείο, το Raspberry Pi λειτουργεί ως σημείο πρόσβασης και άλλες συσκευές μπορούν να συνδεθούν με αυτό. Οι συνδεδεμένες συσκευές μπορούν να έχουν πρόσβαση στο σημείο πρόσβασης Raspberry Pi μέσω της διεύθυνσης IP του για λειτουργίες όπως rsync, scp ή ssh.

5. Προσομοίωση Διαδικασίας Εκτέλεσης

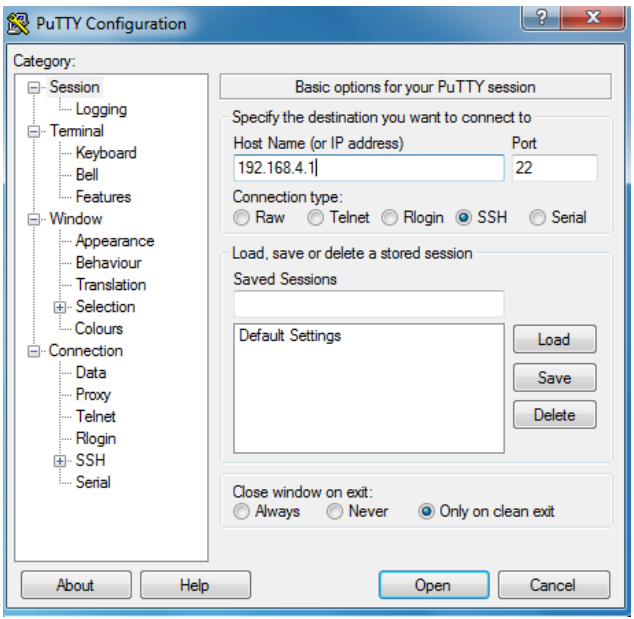
Ακολουθεί παράδειγμα ομαλής εκτέλεσης :

Βήμα 1ο : Αφού συνδέσουμε το Raspberry Pi Zero W στο router, συνδεόμαστε από laptop ή κινητό στο Access Point του, με όνομα δικτύου RpiAP και κωδικό DD$$pa$$wd!2#.

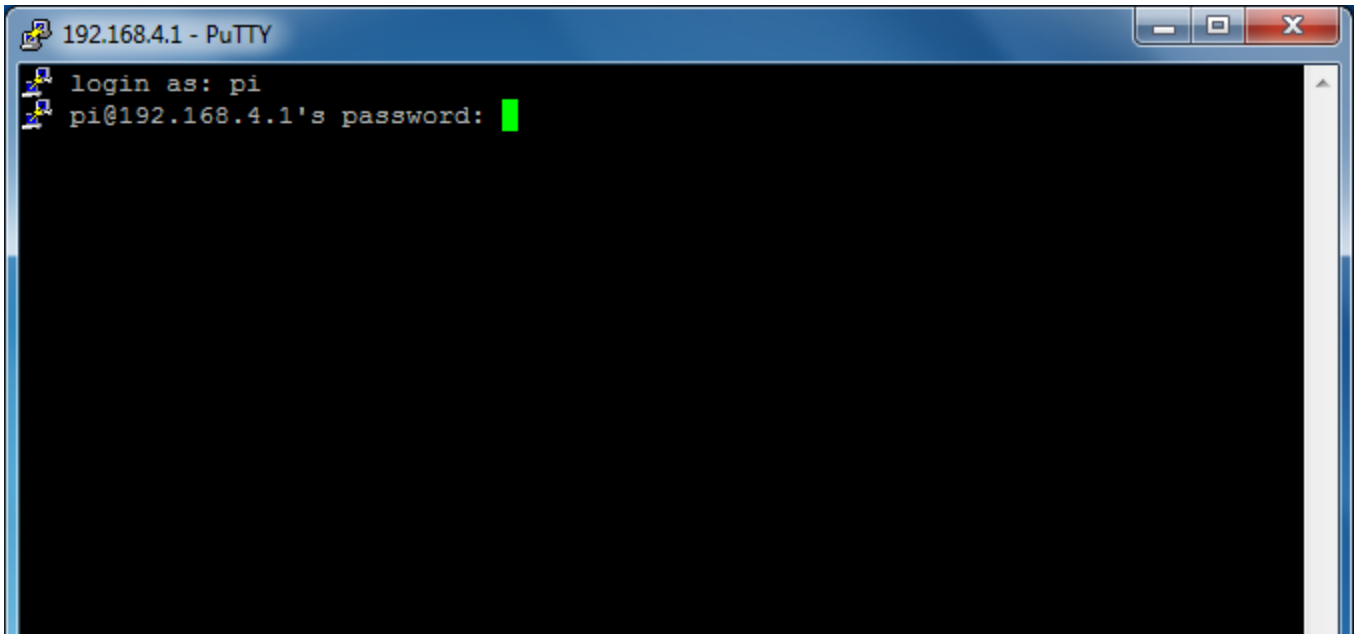


ΕΙΚΟΝΑ 6 - Σύνδεση στο Raspberry Access Point

Βήμα 2ο : Αφού συνδεθούμε, ανοίγουμε έναν SSH client, στη default port για την υπηρεσία SSH 22, με στόχο την IP 192.168.4.1 και βάζουμε το username και password για το login του Rpi [Username:pi , Password:pi].

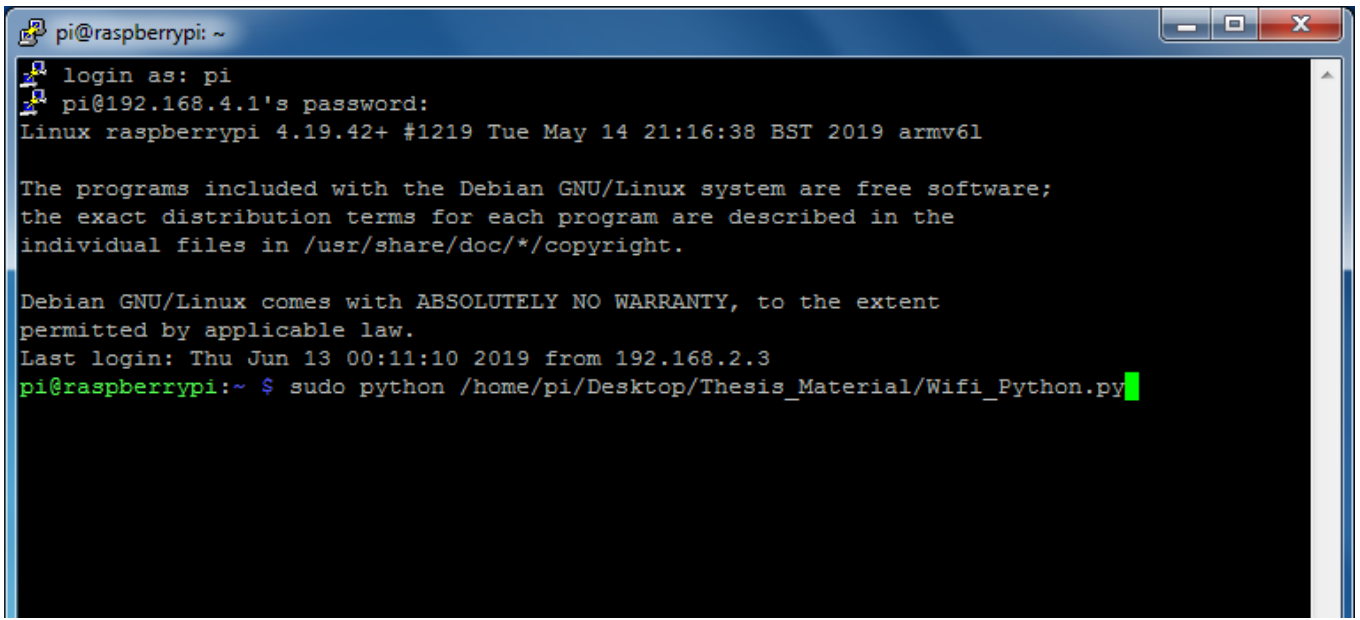


ΕΙΚΟΝΑ 7 - SSH client



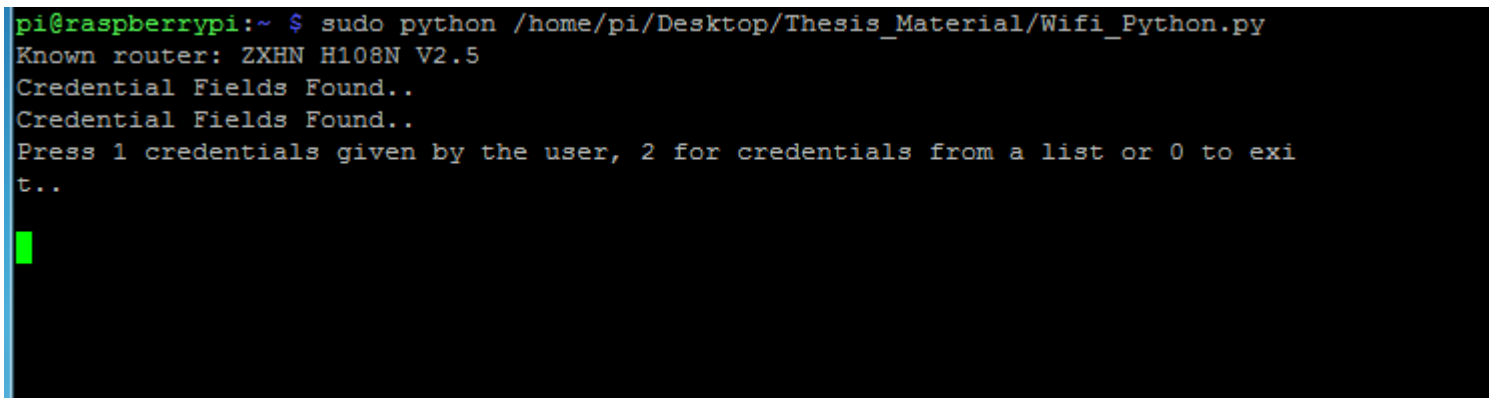
ΕΙΚΟΝΑ 8 - Login Console μέσω SSH σύνδεσης

Βήμα 3ο: Εφόσον έγινε επιτυχώς το login, πληκτρολογούμε στην κονσόλα την εντολή sudo python /home/pi/Desktop/Thesis_Material/Wifi_Python.py, για την εκκίνηση του προγράμματος.



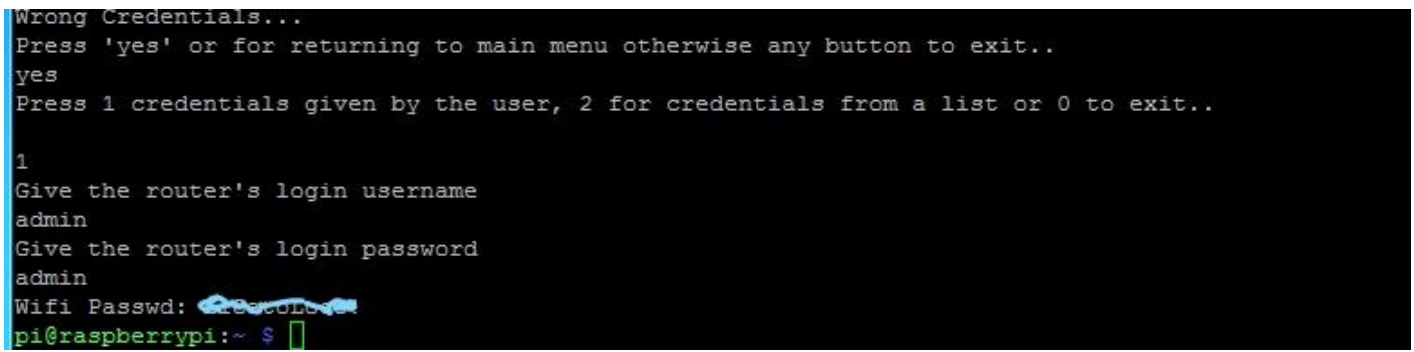
ΕΙΚΟΝΑ 9 - Εκτέλεση εφαρμογής

Βήμα 4ο : Κατά την αρχικοποίηση του προγράμματος και όταν έχει ανοίξει ο οδηγός του Selenium τη σελίδα του router, ζητείται από τον χρήστη να εισάγει είσοδο.



ΕΙΚΟΝΑ 10 - Στάδιο εισαγωγής εντολής από χρήστη

Βήμα 5ο : Επιλέγοντας την είσοδο 1, ο χρήστης έχει τη δυνατότητα να δοκιμάσει χειροκίνητα όνομα χρήστη και κωδικό για να αυθεντικοποιηθεί στο router. Αν αποτύχει του δίνεται η δυνατότητα επιλογής πάλι εισόδου για επόμενη ενέργεια, ενώ αν πετύχει τα σωστά credentials, το πρόγραμμα βρίσκει και του εκτυπώνει τον κωδικό Wi-Fi.



ΕΙΚΟΝΑ 11 - Σωστή είσοδος Credentials - Επιτυχής εξαγωγή κωδικού από το ZXHN H108N Router

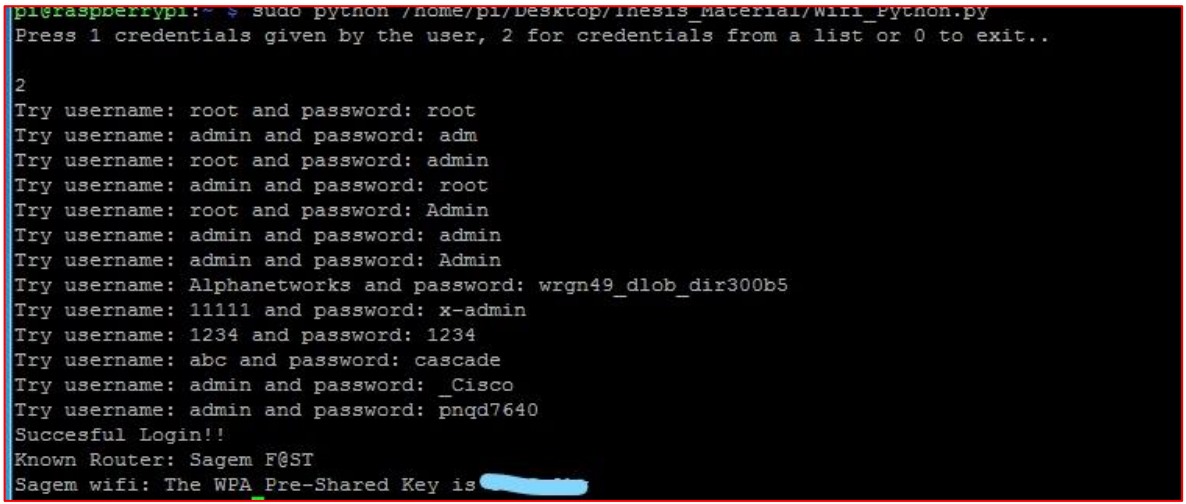
```
pi@raspberrypi:~ $ sudo python /home/pi/Desktop/Thesis_Material/Wifi_Python.py
Known router: ZXHN H108N V2.5
Credential Fields Found..
Credential Fields Found..
Press 1 credentials given by the user, 2 for credentials from a list or 0 to exi
t..

1
Give the router's login username
admin
Give the router's login password
user
Wrong Credentials...
Press 'yes' or for returning to main menu otherwise any button to exit..
```

ΕΙΚΟΝΑ 12 - Λανθασμένα Credentials – Νέα είσοδος από χρήστη

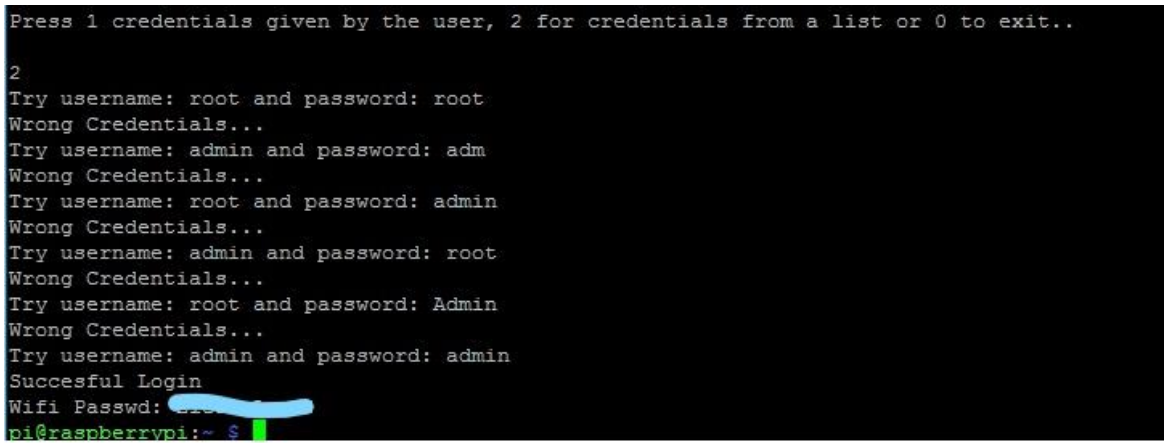
```
pi@raspberrypi:~ $ sudo python /home/pi/Desktop/Thesis_Material/Wifi_Python.py
Press 1 credentials given by the user, 2 for credentials from a list or 0 to exit..

1
Give the router's login username
admin
Give the router's login password
pnqd7640
Succesful Login!!
Known Router: Sagem F@ST
Sagem wifi: The WPA Pre-Shared Key is [redacted]
pi@raspberrypi:~ $
```

ΕΙΚΟΝΑ 13 - Σωστή είσοδος Credentials - Επιτυχής εξαγωγή κωδικού από το Sagem Fast 2404 Router

Βήμα 6ο : Επιλέγοντας την είσοδο 2, η είσοδος του προγράμματος για τα πεδία αυθεντικοποίησης έρχεται από τη λίστα, της οποίας το path έχει δηλωθεί στις αρχικές παραμέτρους του κώδικα.



ΕΙΚΟΝΑ 14 - Επιλογή εισόδου των credentials από λίστα για το Sagem Fast 2404 Router



ΕΙΚΟΝΑ 15 - Επιλογή εισόδου των credentials από λίστα για το ZXHN H108N Router

Βήμα 7ο : Σε περίπτωση αποτυχίας του κώδικα (π.χ. σε περίπτωση router που δεν έχει μελετηθεί) ή εξόδου, εκτυπώνονται τα απαραίτητα στοιχεία για σύνδεση στο AP, από όπου ο χρήστης έχει πρόσβαση στο δίκτυο που ανήκει το router, αλλά και στην ίδια τη συσκευή.

```
0
Bye bye...
Connect to AP:
Network Name :RpiAP
Password: DD$$pa$$wd!2#
Internal IP: 192.168.4.1
Username: pi
Passwd: pi
```

ΕΙΚΟΝΑ 16 - Συνάρτηση εξόδου από το πρόγραμμα , εμφάνιση απαραίτητων πληροφοριών

6. Επίλογος – Προτάσεις Βελτίωσης

Ολοκληρώνοντας τις παραπάνω ενέργειες προκύπτει μια εφαρμογή ικανή εκθέσει δίκτυα είτε υποκλέπτοντας πληροφορίες είτε ανοίγοντας πόρτες στο δίκτυο χωρίς να είναι αντιληπτές. Σαν αδυναμίες προς εκμετάλλευση, στις οποίες στηρίχθηκε η επιτυχία αυτής της εφαρμογής είναι:

- Προβλέψιμη ονομασία πεδίων για πολλούς τύπους router.
- Μεγάλο μερίδιο της αγοράς χρησιμοποιεί τα ίδια router, μεγάλων εταιρειών, χωρίς να γνωρίζουν οι χρήστες τους κινδύνους.
- Χρήση default credentials και εύκολων κωδικών login.
- Έλλειψη εκπαίδευσης προσωπικού, όσον αφορά τις συσκευές που χρειάζεται να υπάρχουν πάνω σε ένα router, με αποτέλεσμα ένα Rpi να περνάει απαρατήρητο.
- Έλλειψη πολιτικών ασφαλείας και συστημάτων ενημέρωσης σε περίπτωση που συσκευές συνδέονται πάνω στο router.
- Οι κατασκευαστές των router θα έπρεπε να χρησιμοποιούν μεθόδους διπλής αυθεντικοποίησης και να μην εμφανίζονται σε plaintext σημαντικές πληροφορίες, ακόμα κι όταν είναι συνδεδεμένος ένας χρήστης.
- Έλλειψη προστασίας του router σε περιήγηση, ενώ το πρόγραμμα περιήγησης βρίσκεται σε remote control.

Όσον αφορά την εφαρμογή μας, προτείνονται οι εξής βελτιώσεις:

- Προσθήκη στην λίστα μας περισσότερων routers

- Επιπλέον επέκταση των μηχανισμών πρόβλεψης πεδίων για ανάκτηση πληροφορίας.
- Προσθήκη δυνατότητας αλλαγής ρυθμίσεων, οι οποίες θα μας επωφελήσουν σε παραπάνω διείσδυση στο δίκτυο, χωρίς να τραβήξουμε τα βλέμματα (Low level firewall, Port Forward κτλ.)
- Δυνατότητας σύνδεσης με Bluetooth
- Δυνατότητα ορισμού path αρχείου credentials από τον χρήστη ή και εισαγωγή αυτού μέσα από απομακρυσμένη συσκευή
- Επέκταση γνωσιακής βάσης, για την αυτόματη και δυναμική περιήγηση της εφαρμογής στο router και εξαγωγή όλων των κρίσιμων πληροφοριών

7. Σχετικές εργασίες - projects

1. WiFi Pineapple [https://shop.hak5.org/products/wifi-pineapple]
2. LAN Turtle [https://shop.hak5.org/products/lan-turtle]
3. Plunder Bug [https://shop.hak5.org/products/bug]
4. Packet Squirrel [https://shop.hak5.org/products/packet-squirrel]
5. How to Setup a Raspberry Pi Network Scanner [https://pimylifeup.com/raspberry-pi-network-scanner/]
6. Raspberry Pi MAC Address Spoofing [https://pimylifeup.com/raspberry-pi-mac-address-spoofing/]
7. Raspberry Pi VPN Access Point: Setup a Basic VPN Router [https://pimylifeup.com/raspberry-pi-vpn-access-point/]

8. Βιβλιογραφία - Αναφορές

[1] Selenium Web Driver, https://www.seleniumhq.org/docs/03_webdriver.jsp

[2] Beautiful Soup web scrapper, https://www.crummy.com/software/BeautifulSoup/bs4/doc/

[3] Raspberry pi projects. set as an Access Point, https://www.raspberrypi.org/documentation/configuration/wireless/access-point.md

[4] Selenium Web Driver, https://selenium-python.readthedocs.io/

[5] Python and Selenium Web Driver library, https://realpython.com/modern-web-automation-with-python-and-selenium/

[6] Selenium Web Driver and Geckodriver, https://www.guru99.com/gecko-marionette-driver-selenium.html

[7] Python Programming Language, https://www.w3schools.com/python/

[8] Python and Selenium Web Driver library, Selenium WebDriver Recipes in Python, by *Zhimin Zhan*