

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ



– Πτυχιακή Εργασία –

Social Engineering Wi-Fi Attacks

Ιωάννης Αλεξανδρίδης Α.Μ. Π2016041

Επιβλέπων: Χριστόφορος Νταντογιάν

Φεβρουάριος 2023

Επιβλέπων

Χριστόφορος Νταντογιάν, Επίκουρος Καθηγητής,

Ιόνιο Πανεπιστήμιο

Τριμελής Επιτροπή

Αγγελική Τσώχου, Αναπληρώτρια Καθηγήτρια,

Ιόνιο Πανεπιστήμιο

Εμμανουήλ Μάγκος, Καθηγητής,

Ιόνιο Πανεπιστήμιο

Ευχαριστώ θερμά την οικογένεια μου, τους φίλους και τους καθηγητές που με
στήριξαν σε αυτό το ταξίδι...

Περίληψη

Στην παρούσα πτυχιακή εργασία θα υπάρξει μια εκτενή εξερεύνηση όλων των σημαντικών εννοιών και τεχνικών στοιχείων που σχετίζονται με το WiFi και τα χαρακτηριστικά ασφαλείας του. Διεξοδικά θα αναλυθούν οι διαφορετικοί τύποι ασύρματων δικτύων και οι τρόποι λειτουργίας τους, καθώς και τα διάφορα πρωτόκολλα κρυπτογράφησης που χρησιμοποιούνται για την προστασία τους από κακόβουλες δραστηριότητες. Επιπλέον, θα υπάρξει εμβάθυνση στις λεπτομέρειες των επιθέσεων man-in-the-middle, εξηγώντας πώς λειτουργούν και τις διαφορετικές μεθόδους που χρησιμοποιούνται για την εκτέλεσή τους.

Για να παραχωρηθούν συγκεκριμένα παραδείγματα των κινδύνων και των τρωτών σημείων των δικτύων WiFi, θα χρησιμοποιηθεί το wifiphisher, ένα εξελιγμένο εργαλείο που μπορεί να δημιουργήσει μια προσαρμοσμένη επίθεση phishing, στις παραμέτρους ενός συγκεκριμένου δικτύου. Αναλύεται ολόκληρη η διαδικασία εγκατάστασης και εκτέλεσης αυτών των επιθέσεων, περιγράφοντας όλα τα πιθανά σενάρια και τα αποτελέσματα που προκύπτουν.

Στη συνέχεια περιγράφουμε τις επιθέσεις που έγιναν σε περιβάλλον εξομοίωσης, όπου συγκεκριμένοι χρήστες του εργαστηρίου συμμετείχαν στο πείραμα με τη συγκατάθεσή τους. Οι δοκιμές έγιναν στο εργαστήριο του Πανεπιστημίου, και οι χρήστες γνώριζαν ότι κάποια στιγμή (χωρίς να ξέρουν πότε ακριβώς) θα προσπαθήσουμε να πραγματοποιήσουμε επίθεση στο συνδεδεμένο Wi-Fi δίκτυο τους. Τα αποτελέσματα των πειραμάτων δείχνει ότι μπορούμε να χρησιμοποιηθεί αυτή η κατηγορία επιθέσεων για επιθέσεις και αποτελούν σαφής απόδειξη των πιθανών κινδύνων που σχετίζονται με τα μη ασφαλή δίκτυα WiFi, καθώς και τη σημασία της εφαρμογής ισχυρών μέτρων ασφαλείας για προστασία από τέτοιες επιθέσεις.

Συνολικά, το αποτέλεσμα της έρευνας χρησιμεύει ως μια περιεκτική πηγή για την κατανόηση της πολυπλοκότητας της ασφάλειας WiFi και της ανάγκης για επαγρύπνηση έναντι πιθανών απειλών ασφαλείας. Οι πληροφορίες που παρέχονται είναι χρήσιμες τόσο για επαγγελματίες ασφαλείας όσο και για απλούς

ανθρώπους και χρησιμεύουν ως έγκαιρη υπενθύμιση της σημασίας της διασφάλισης της ολοένα και πιο ψηφιακής ζωής μας.

Λέξεις Κλειδιά

Επίθεση κοινωνικής μηχανικής, Phishing, Ασύρματο δίκτυο, Rogue access point, Man-In-The-Middle επίθεση, διαπιστευτήρια σύνδεσης

Πρόλογος

Η πρόοδος της τεχνολογίας και η ευρεία χρήση των ασύρματων δικτύων έχουν δημιουργήσει αυξημένη ευπάθεια σε απειλές στον κυβερνοχώρο. Μία από τις πιο κοινές επιθέσεις σε ασύρματα δίκτυα είναι οι επιθέσεις wifi κοινωνικής μηχανικής, οι οποίες περιλαμβάνουν την εκμετάλλευση της ανθρώπινης ψυχολογίας για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε ένα δίκτυο wifi.

Οι επιθέσεις Wi-Fi κοινωνικής μηχανικής έχουν γίνει μια σημαντική ανησυχία τόσο για άτομα όσο και για οργανισμούς. Οι εισβολείς χρησιμοποιούν διάφορες τακτικές για να εξαπατήσουν άτομα ώστε να αποκαλύψουν ευαίσθητες πληροφορίες, όπως διαπιστευτήρια σύνδεσης, τα οποία μπορούν να χρησιμοποιήσουν για να αποκτήσουν πρόσβαση σε ένα δίκτυο. Αυτές οι επιθέσεις μπορεί να είναι καταστροφικές, καθώς μπορούν να θέσουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα ευαίσθητων πληροφοριών.

Ο σκοπός αυτής της πτυχιακής εργασίας είναι να παρέχει μια ολοκληρωμένη κατανόηση των επιθέσεων wifi κοινωνικής μηχανικής και των τεχνικών τους. Θα διερευνήσει τους διάφορους τύπους επιθέσεων wifi κοινωνικής μηχανικής, συμπεριλαμβανομένων του phishing, του baiting, του pretexting. Θα αναλύσει επίσης κάποιες από τις μεθόδους που χρησιμοποιούνται από τους επιτιθέμενους για να εξαπολύσουν αυτές τις επιθέσεις, όπως τα rogue access points και man-in-the-middle επιθέσεις.

Συνολικά, αυτή η πτυχιακή εργασία στοχεύει να αυξήσει την ευαισθητοποίηση σχετικά με τις επιθέσεις wifi κοινωνικής μηχανικής και να παρουσιάσει πρακτικά την διαδικασία με την οποία λειτουργούν τέτοιου είδους επιθέσεις. Με αυτόν τον τρόπο, μπορεί να βοηθήσει άτομα και οργανισμούς μάθουν χρήσιμες πληροφορίες καθώς και να προστατεύσουν τα ασύρματα δίκτυα και τις ευαίσθητες πληροφορίες τους.

Περιεχόμενα

Εισαγωγή	1
A'.1 Wi-Fi	1
A'.1.1 Πρωτόκολλα Wi-Fi και ασφάλεια	2
A'.2 Handshakes	4
A'.3 Captive Portal attack	6
A'.3.1 Rogue – Fake access point	6
A'.4 Wi-Fi antenna specifications & Operating System	7
A'.5 Man-In-The-Middle επίθεση	10
A'.5.1 Fluxion Tool	11
A'.5.2 Wifiphisher Tool	13
A'.6 Προσαρμοσμένα Σενάρια Επίθεσης	14
A'.6.1 Εγκατάσταση νέων σεναρίων επίθεσης	17
Παρουσίαση επίθεσης	21
B'.1 Πρώτα βήματα	21
B'.2 Επιλογή δικτύου θύματος	22
B'.3 Επιλογή σεναρίου επίθεσης	24
B'.4 Από την οπτική του κακόβουλου χρήστη	25
B'.5 Από την οπτική του θύματος	28
B'.6 Επιτυχημένη περίπτωση επίθεσης	30
B'.7 Περίπτωση επίσκεψης phishing σελίδας	30
B'.8 Αποτυχημένη περίπτωση επίθεσης	31
Παρουσίαση αποτελεσμάτων επίθεσης	33
Γ'.1 Ανάλυση αποτελεσμάτων επιτυχημένης επίθεσης	33
Γ'.2 Ανάλυση αποτελεσμάτων επίσκεψης phishing σελίδας	34
Γ'.3 Ανάλυση αποτελεσμάτων αποτυχίας επίθεσης	35
Γ'.4 Συμπεράσματα	36

Βιβλιογραφία	39
Συντμήσεις	41
Γλωσσάρι Ξενικών Όρων	42

Κατάλογος Σχημάτων

Σχήμα Α'.1: Βήματα 4-way Handshake.	5
Σχήμα Α'.2: Προσαρμογέας WiFi με chipset AR9271.	9
Σχήμα Α'.3: Λογότυπο εργαλείου Fluxion.	11
Σχήμα Α'.4: Λογότυπο εργαλείου Wifiphisher.	13
Σχήμα Α'.5: Σελίδες κλώνος σύνδεσης Cosmote και Vodafone.	15
Σχήμα Α'.6: Σελίδες κλώνος σύνδεσης Nova και Cyta.	16
Σχήμα Α'.7: Σελίδα κλώνος σύνδεσης Wind.	16
Σχήμα Α'.8: Περιεχόμενα αρχείου config.ini.	17
Σχήμα Α'.9: Κώδικας HTML σελίδας κλώνου.	18
Σχήμα Α'.10: Κώδικας CSS σελίδας κλώνου.	19
Σχήμα Β'.1: Εργαλείο airodump-ng, έλεγχος κίνησης πακέτων, ενεργή κίνηση.	23
Σχήμα Β'.2: Εργαλείο airodump-ng, έλεγχος κίνησης πακέτων, ανενεργή κίνηση.	23
Σχήμα Β'.3: Wifiphisher, επιλογή δικτύου για επίθεση.	24
Σχήμα Β'.4: Wifiphisher, επιλογή σεναρίου επίθεσης.	25
Σχήμα Β'.5: Τερματικός wifiphisher, απο την οπτική του κακόβουλου χρήστη.	27
Σχήμα Β'.6: Phishing σελίδα, από την οπτική του θύματος.	29

Σχήμα Β'.7: Wifiphisher, deauthentication θύματος και απόκτηση κωδικού θύματος.	30
Σχήμα Β'.8: Wifiphisher, deauthentication θύματος με επίσκεψη στην phishing σελίδα χωρίς απόκτηση κωδικού θύματος.	31
Σχήμα Β'.9: Wifiphisher, deauthentication θύματος χωρίς επίσκεψη στην phishing σελίδα.	32
Σχήμα Γ'.1: Γράφημα συνολικών αποτελεσμάτων επίθεσης.	33
Σχήμα Γ'.2: Επισημασμένο γράφημα αποτελεσμάτων επιτυχημένων επιθέσεων.	35
Σχήμα Γ'.3: Επισημασμένο γράφημα αποτελεσμάτων επισκέψεων phishing σελίδας.	36
Σχήμα Γ'.4: Επισημασμένο γράφημα αποτελεσμάτων ανεπιτυχών επιθέσεων.	38

Κεφάλαιο Α'

Εισαγωγή

Α'.1 Wi-Fi

Το WiFi είναι η δημοφιλής ονομασία για το πρότυπο ασύρματου 802.11b για WLAN και αναφέρεται στην τεχνολογία που περιβάλλει τη ραδιομετάδοση των δεδομένων πρωτοκόλλου Διαδικτύου από μια σύνδεση Διαδικτύου ασύρματα σε έναν κεντρικό υπολογιστή. Τις περισσότερες φορές η σύνδεση στο Διαδίκτυο είναι υψηλότερης ταχύτητας, όπως δορυφορική, DSL ή καλωδιακή αντί για πιο αργές συνδέσεις μέσω τηλεφώνου. Είναι ουσιαστικά μια ασύρματη σύνδεση μεταξύ του υπολογιστή σας και της σύνδεσης στο Διαδίκτυο (όπως DSL ρούτερ ή μόντεμ με καλώδιο ή ADSL ρούτερ) στο σπίτι σας. Τα πλεονεκτήματα που έχει προσφέρει αυτή η τεχνολογία είναι πράγματι απεριόριστα, ευελιξία χωρίς την ύπαρξη καλωδίων και πρόσβαση σε πληροφορίες και δεδομένα από ολόκληρο τον κόσμο, ανάπτυξη των επιχειρήσεων, επικοινωνία σε κάθε μέρος του πλανήτη κ.α.. Αξιοσημείωτο να αναφερθεί ότι εκπεμπει στις συχνοτητες 2.4 και 5GHz. Σίγουρα όμως πίσω από όλες αυτές τις ανέσεις θα πρέπει να υπάρχει και η ερώτηση “πόση ασφάλεια μας παρέχει αυτή η τεχνολογία;”.

Η ασύρματη σύνδεση στο διαδίκτυο κάνει τη ζωή εύκολη για όσους τη χρησιμοποιούν, αλλά αν δεν υπάρχει προσοχή, είναι εξαιρετικά εύκολο να δεχθεί επιθέσεις καθώς είναι γνωστό ότι η ευκολία μιας τεχνολογίας είναι συχνά αντιστρόφως ανάλογη με την ασφάλειά της. Οπουδήποτε και να βρίσκεται κάποιος αν ενεργοποιήσει έναν ασύρματο πομποδέκτη δικτύου σε μια κατοικημένη περιοχή, θα εντοπιστούν πολλές δεκάδες δίκτυα μέσα σε λίγα δευτερόλεπτα, πολλά από τα οποία “διαρρέουν” εκτός του προβλεπόμενου εύρους λήψης. Τα ραδιοκύματα που χρησιμοποιούνται για την μεταφορά δικτύων

Wi-Fi συνήθως έχουν εμβέλεια πάνω από 50 μέτρα, πράγμα που σημαίνει ότι μπορούν να εντοπιστούν πολύ έξω από τον χώρο που προορίζεται να εξυπηρετούν. Όλα αυτά καταλήγουν στο συμπέρασμα πως κακόβουλοι έχουν την ικανότητα να τα προσεγγίσουν.

Α'.1.1 Πρωτόκολλα Wi-Fi και ασφάλεια

Τα ασύρματα δίκτυα αποτελούν μια συνεχή απειλή για την ασφάλεια των δεδομένων μεταξύ δύο σημείων, με αποτέλεσμα πολλοί οργανισμοί να συνεισφέρουν εκατομμύρια για την ασφαλή λειτουργία των συστημάτων τους. Η τεχνολογία WLAN αναφέρεται ως μια αναπτυσσόμενη ειδικότητα στην αγορά, η καινοτομία στην οποία βασίζεται άρχισε να χρησιμοποιείται επιπλέον για μια άλλη εφαρμογή, αυτή της μεταφοράς Broadband Wireless Access (BWA) σε ανοικτά συστήματα. Η αρχική ανάγκη για τη δημιουργία προτύπων IEEE έγιναν με διαφορετικό τρόπο για την αντιμετώπιση του φυσικού επιπέδου όπως διάφορες συχνότητες και ξεχωριστές στρατηγικές κωδικοποίησης. Τα WLAN υποδεικνύουν τη χρήση του 802.2 για το τμήμα λογικού ελέγχου σύνδεσης (Logical Link Control, LLC) του στρώματος σύνδεσης δεδομένων. Η ασφάλεια στα WLAN επιτυγχάνεται με την κρυπτογράφηση της πληροφορίας. Με την απουσία της κρυπτογράφησης, ορισμένες άγνωστες απομακρυσμένες συσκευές μπορούν να εντοπίσουν την κίνηση στο σύστημα (sniffing). Παρακάτω αναφέρονται τρεις από τις πιο αξιόλογες μεθοδολογίες ασφαλείας:

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- WPA2 (Wi-Fi Protected Access, version 2)
- WPA3 (Wi-Fi Protected Access, version 3)

Το WEP προορίζεται να παρέχει ασφάλεια ενσύρματου τοπικού δικτύου μέσω κρυπτογράφησης, χρησιμοποιώντας τον αλγόριθμο RC4 με διαφορετικές πλευρές αντιστοιχίας πληροφοριών. Από την πλευρά του αποστολέα, χρησιμοποιούνται

τέσσερις λειτουργίες για την κωδικοποίηση και αποστολή των πληροφοριών. Στο πρώτο βήμα το μυστικό κλειδί που χρησιμοποιείται στον υπολογισμό του WEP είναι 40-bit μαζί με 24-bit Initialization Vector (IV) το οποίο συνδέεται για να λειτουργεί τόσο ως κλειδί κρυπτογράφησης όσο και ως κλειδί αποκρυπτογράφησης. Στο δεύτερο βήμα, τα επόμενα κλειδιά λειτουργούν ως “σπόροι” για την ψευδοτυχαία γεννήτρια (Pseudo-Random Generator, PRNG). Στο Τρίτο βήμα, το plaintext ελέγχει για ορθότητα με έναν υπολογισμό και το αποτέλεσμα συνδέεται με το plaintext για άλλη μια φορά. Στο τελευταίο βήμα, το αποτέλεσμα της ακολουθίας κλειδιών και του ICV θα μεταβούν στον αλγόριθμο RC4, το κωδικοποιημένο μήνυμα πλαισιώνεται συνδέοντας το IV πριν από το κείμενο κρυπτογράφησης. Αντιθέτως, από την πλευρά του παραλήπτη, χρησιμοποιεί πέντε εργασίες για την αποκρυπτογράφηση (IV+κρυπτογραφημένο κείμενο). Πρώτον, το Pre-Shared κλειδί και το IV συνδέονται για τη δημιουργία ενός μυστικού κλειδιού. Στο δεύτερο βήμα, το κείμενο κρυπτογράφησης και το μυστικό κλειδί μεταβαίνουν στον αλγόριθμο CR4 και ως αποτέλεσμα προκύπτει plaintext. Στο τρίτο βήμα, θα απομονωθεί το ICV και το plaintext. Τέταρτον, το plaintext πηγαίνει για έλεγχο ακεραιότητας για να δημιουργήσει ένα άλλο ICV το οποίο τελικώς συγκρίνεται με το αρχικό ICV.

Το WPA, παρουσιάστηκε από την εταιρεία Wi-Fi Alliance στα τέλη του 2002. Η Wi-Fi Alliance μαζί με τους ηλεκτρονικούς μηχανικούς (IEEE) κάλυψε τα αδύναμα τμήματα του πρωτοκόλλου WEP και το παρουσίασε με την ερμηνεία WPA. Ο πρωταρχικός σκοπός ήταν να αντικατασταθεί το WEP χωρίς την αλλαγή του εξοπλισμού. Αυτό επιτεύχθηκε με τη συμπερίληψη (TKIP) Temporal Key Integrity Protocol για κρυπτογράφηση και 802.1X EAP για σκοπούς ελέγχου ταυτότητας ώστε να προσφέρει υψηλή ασφάλεια. Το WPA παρουσίασε τον υπολογισμό Έλεγχος Ακεραιότητας Μηνύματος (MIC) γνωστό ως "Michael".

Το WPA2, χρησιμοποιεί το CCMP, το οποίο είναι μια νέα τεχνική κρυπτογράφησης που βασίζεται στο AES για μεγαλύτερη ασφάλεια. Το WPA2 βασίζεται στα πρότυπα του IEEE 802.11i. Το WPA2 χρησιμοποιεί κυρίως τον αλγόριθμο Advanced Encryption Standard (AES) για την κρυπτογράφηση της

κίνησης του δικτύου. Το WPA2 χρησιμοποιεί μέγεθος κλειδιού 128 bit για την κρυπτογράφηση των δεδομένων. Η διαδικασία κρυπτογράφησης AES στο WPA2 πραγματοποιείται είτε από το AES είτε με τη χρήση TKIP (Temporal Key Integrity Protocol).

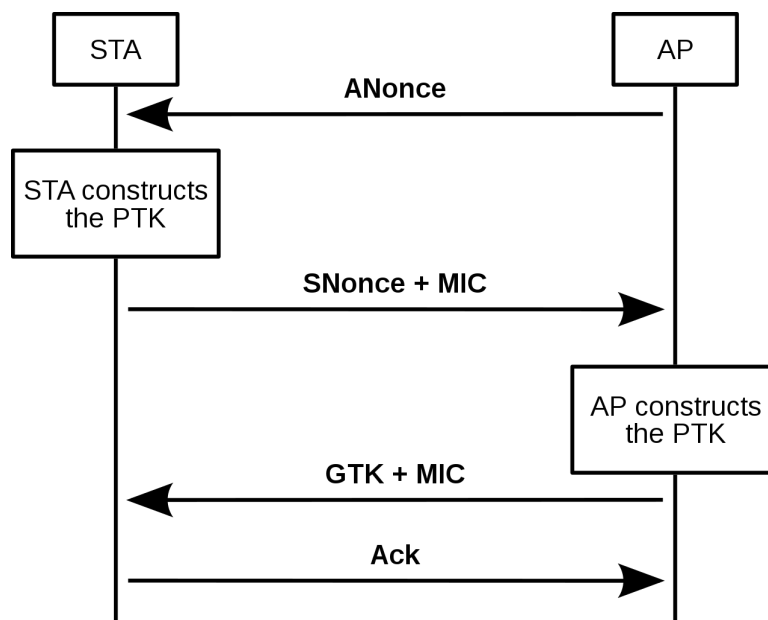
Το WPA2 δημιουργεί ασφαλή επικοινωνία σε τέσσερις φάσεις. Η πρώτη φάση είναι ο έλεγχος ταυτότητας και η μέθοδος προεπικύρωσης. Σε αυτή τη φάση η ασύρματη συσκευή (access point, AP) και ο πελάτης (client) θα συμφωνήσουν για την πολιτική ασφαλείας. Στη δεύτερη φάση θα δημιουργηθεί ένα κύριο κλειδί. Στην τρίτη φάση θα δημιουργηθούν τα προσωρινά κλειδιά. Στην τέταρτη φάση, όλα τα κλειδιά που δημιουργούνται στην τρίτη φάση θα χρησιμοποιηθούν από το πρωτόκολλο CCMP για την παροχή ακεραιότητας δεδομένων και εμπιστευτικότητας δεδομένων.

Το WPA3 είναι η επόμενη γενιά της ασφάλειας Wi-Fi. Όλες οι συσκευές που τροφοδοτούνται από το WPA3 χρησιμοποιούν τα πιο πρόσφατα μέτρα ασφαλείας και απαιτούν τη χρήση προστατευμένων πλαισίων (Protected Management Frames, PMF). Ωστόσο, οι συσκευές με WPA3 δεν είναι ακόμα άμεσα διαθέσιμες. Υπάρχουν και άλλες βελτιώσεις στο WPA3. Αυτό είναι το Opportunistic Wireless Encryption (Προαιρετική ασύρματη κρυπτογράφηση). Το OWE είναι μια τεχνολογία σχεδιασμένη για κοινωνικά δίκτυα. Με αυτήν την τεχνολογία, η αυτόματη κρυπτογράφηση θα εκτελείται χωρίς παρέμβαση του χρήστη. Με το WPA2, οποιοσδήποτε εισβολέας με πρόσβαση στο δίκτυο που βρίσκεται κάποιος, μπορεί να κάνει τις επιθέσεις Man-in-the-Middle, με το WPA3 αυτό είναι αδύνατο.

A'.2 Handshakes

Η πλήρης διαδικασία ενός ελέγχου ταυτοποίησης αποτελείται από χειραψίες μεταξύ του αιτούντος και του υπεύθυνου ελέγχου ταυτότητας, μεταξύ του επαληθευτή και του διακομιστή ελέγχου ταυτότητας και μεταξύ του αιτούντος και

του διακομιστή ελέγχου ταυτότητας. Η χειραψία 4 κατευθύνσεων χρησιμοποιεί ένα κλειδί πρόσβασης που ονομάζεται Pairwise Master Key (PMK) και συνένωση διαφόρων στοιχείων δεδομένων για τη ρύθμιση της κρυπτογράφησης των δεδομένων. Αυτά περιλαμβάνουν στοιχεία μιας χρήσης που ονομάζονται ANonce και SNonce, καθώς και τις διευθύνσεις Mac των δύο εμπλεκόμενων τελικών σημείων. Οι κύριες διεργασίες της χειραψίας 4 κατευθύνσεων γίνονται για να επιτραπεί σε ένα σημείο πρόσβασης να επαληθεύσει την ταυτότητα του στον πελάτη και να παρέχει ασφαλή κρυπτογράφηση. Το PMK δεν αποστέλλεται μέσω του δικτύου, αφήνοντας αυτό το στοιχείο μη κοινόχρηστο, κάνοντας την ασφάλεια της διαδικασίας ακόμα πιο ακαίρεα.



Σχήμα Α'.1: Βήματα 4-way Handshake.

Με πιο απλά λόγια, μια χειραψία 4 κατευθύνσεων κάνει αυτό:

1. Το AP στέλνει στον πελάτη το ANonce του. Τώρα ο πελάτης έχει όλα όσα χρειάζεται για να δημιουργήσει το PTK γιατί πήρε το ANonce.
2. Ο πελάτης στέλνει στο AP το SNonce του με ένα MIC, το MIC είναι κυρίως για να αναγνωρίσει το AP ότι αυτό το μήνυμα είναι πραγματικά από αυτόν τον πελάτη, είναι σαν μια υπογραφή. Τώρα, εφόσον το AP πήρε το μήνυμα, έχει όλα όσα χρειάζεται για να δημιουργήσει το PTK.

3. Το AP στέλνει στον πελάτη το GTK και εκείνος το εγκαθιστά.
4. Ο πελάτης στέλνει στο AP ότι όλα είναι εντάξει.

Αυτή η πολύπλοκη ρύθμιση επιτρέπει μια πιο ασφαλή διαδικασία ελέγχου ταυτότητας που ταιριάζει με την πολυπλοκότητα και τα τρωτά σημεία των σύγχρονων δικτύων.

A'.3 Captive Portal attack

Η επίθεση Captive Portal επιχειρεί να ανακτήσει το κλειδί WPA/WPA2 του στοχευμένου σημείου πρόσβασης μέσω ενός πλαστού σημείου πρόσβασης με πύλη ελέγχου ταυτοποίησης. Στη συνέχεια θα χρησιμοποιηθεί μια διεπαφή ασύρματου δικτύου για παρεμβολές (jamming) ώστε να διακόψει την επικοινωνία μεταξύ των θυμάτων που είναι συνδεδεμένοι από το δίκτυο που υπάρχει ως στόχος, προϋπόθεση είναι η διεπαφή ασύρματου δικτύου που θα χρησιμοποιηθεί να υποστηρίζει λειτουργία packet injection.

Σε αυτό το σημείο επίθεση είναι σε θέση να ξεκινήσει. Θα δημιουργηθεί το πλαστό δίκτυο και μέσω αυτού θα είναι προσβάσιμη η πύλη με σκοπό να υποκλέψει το κλειδί πρόσβασης.

A'.3.1 Rogue – Fake access point

Κάνοντας μια βαθύτερη διείσδυση στον τρόπο που θα εξελιχθεί η επίθεση, μια ενέργεια που είναι κρίσιμη στο να πραγματοποιηθεί είναι η δημιουργία ενός πλαστού σημείου πρόσβασης (Rogue/Fake Access Point).

Μία από τις πιο κοινές απειλές για την ασφάλεια του ασύρματου δικτύου είναι το πλαστό σημείο πρόσβασης το οποίο χρησιμοποιείται σε πολλές επιθέσεις, μια από αυτές και η κλοπή δεδομένων. Ένα πλαστό σημείο πρόσβασης είναι μια συσκευή που δεν έχει εγκριθεί από κάποια διαχείριση, αντιθέτως λειτουργεί πάνω στο

δίκτυο αυθαίρετα. Αυτό στην πλειονοψηφία των περιπτώσεων είναι ένα σημείο πρόσβασης που έχει δημιουργηθεί από άτομα που στις προθέσεις τους κυριαρχεί η παραβίαση δεδομένων. Βέβαια υπάρχουν τρόποι να και σημάδια ώστε να υποπτευθεί κάποιος την ύπαρξη ενός πλαστού σημείου πρόσβασης, μερικά από αυτά:

1. Αν το σημείο πρόσβασης βρίσκεται στη λίστα διαχειριζόμενων σημείων πρόσβασης ή όχι.
2. Το πλαστό σημείο πρόσβασης μπορεί να κρύβει πραγματικό ή και να έχει λανθασμένο όνομα.
3. Η διεύθυνση MAC του σημείου πρόσβασης δεν εμφανίζεται κάπου στις πληροφορίες.
4. Ασύρματα συστήματα ανίχνευσης εισβολής (WIDS). Τέτοια συστήματα υπερασπίζονται τα δίκτυα από εξωτερικούς εισβολείς, κατά κύριο λόγο σε οργανισμούς επιχειρήσεων, και είναι αποδοτικά με την χρήση εξουσιοδοτημένων διαπιστευτηρίων εντός του ορισμένου κύκλου χρηστών.

Μπορεί εύκολα λοιπόν να θεωρηθεί πως μία από τις πιο επιβλαβείς πράξεις παραβίασης είναι η εισαγωγή ενός πλαστού σημείου πρόσβασης σε ένα οποιοδήποτε δίκτυο.

A'.4 Wi-Fi antenna specifications & Operating System

Το Parrot OS θεωρείται ένα από τα πιο ευρέως χρησιμοποιούμενα λειτουργικά συστήματα δοκιμών επιθέσεων όλων των εποχών. Είναι γεμάτο με πληθώρα προγραμμάτων που μπορούν να χρησιμοποιηθούν για την εκτέλεση διαφόρων ειδών δοκιμών επίθεσης εφαρμογών, επίθεσης δικτύου καθώς και πειρατείας WiFi. Έχει μια ζωντανή και ενεργή κοινότητα που συνεχίζει να προσθέτει νέα εργαλεία και να κυκλοφορεί συνεχώς ενημερώσεις. Το μόνο πρόβλημα με το Parrot OS είναι η έλλειψη υποστήριξης για συσκευές που εγείρει το ερώτημα:

Ποιος είναι ο καλύτερος προσαρμογέας WiFi που είναι συμβατός με το Parrot OS και μπορεί να εκτελέσει διάφορες επιθέσεις χρησιμοποιώντας τα εργαλεία που είναι διαθέσιμα στο Parrot OS ;

Με αυτά τα δεδομένα, για την προσπάθεια πραγματοποίησης της επίθεσης, αναγκαία είναι η ύπαρξη ενός ειδικού ξεχωριστού προσαρμογέα ασύρματου δικτύου. Ένας ασύρματος προσαρμογέας είναι απλώς μια συσκευή που μπορεί να συνδεθεί στον κάθε υπολογιστή μέσω της θύρας USB και επιτρέπει το σύστημα να επικοινωνεί με άλλες συσκευές μέσω ενός δικτύου WiFi. Πολύ απλά είναι αυτό το ασύρματο chipset που επιτρέπει το φορητό υπολογιστή του κοινού έξυπνου κινητού τηλεφώνου ή άλλες συσκευές που επιτρέπουν την σύνδεση στο δίκτυο wifi και να υπάρχει πρόσβαση στο διαδίκτυο.

Επομένως, εύλογο είναι το ερώτημα γιατί χρειάζεται ένας προσαρμογέας ασύρματου δικτύου για να συνδεθεί στον υπολογιστή εφόσον υπάρχει η περίπτωση να έχει ήδη ένα ενσωματωμένο chipset WiFi. Η απάντηση είναι όμως ότι οι περισσότεροι φορητοί υπολογιστές πράγματι διαθέτουν ενσωματωμένο chipset WiFi, με την σημαντική διαφορά πως από την προοπτική της παραβίασης WiFi, αυτοί οι ενσωματωμένοι προσαρμογείς WiFi δεν είναι κατάλληλοι ως προς τις τεχνικές προδιαγραφές που διαθέτουν.

- Monitor mode: Η λειτουργία παρακολούθησης (Monitor Mode) είναι μια λειτουργία λήψης δεδομένων που επιτρέπει τη μετατροπή χρήσης ενός προσαρμογέα WiFi σε λειτουργία ακρόασης (listening mode). Θέτοντας σε λειτουργία αυτήν τη λειτουργία, οι κάρτες δικτύου WiFi είναι σε θέση να καταγράφουν όλους τους τύπους πακέτων διαχείρισης WiFi (συμπεριλαμβανομένων των πακέτων Beacon (Beacon packets)), πακέτων δεδομένων (Data packets) και πακέτων ελέγχου (Control packets). Με αυτόν τον τρόπο, είναι δυνατή η προβολή όχι μόνο σημείων πρόσβασης αλλά και πελατών που είναι συνδεδεμένοι και εκπέμπουν εντός των ζωνών συχνοτήτων των WiFi.
- Packet injection: Η έγχυση πακέτων (γνωστό και ως spoofing packets) στα δίκτυα υπολογιστών, θεωρείται η διαδικασία παρεμβολής σε μια υπάρχων

σύνδεση δικτύου μέσω της δημιουργίας πακέτων δεδομένων ώστε να εμφανίζονται σαν να είναι μέρος της κανονικής ροής επικοινωνίας. Η διαδικασία έγχυσης πακέτων επιτρέπει σε ένα άγνωστο τρίτο παράγοντα να διακόψει ή ακόμη και να υποκλέψει πακέτα από τις συσκευές που επικοινωνούν, πράγμα που μπορεί να καταλήξει σε υποβάθμιση ή αποκλεισμό της δυνατότητας των συνδεδεμένων χρηστών να χρησιμοποιούν συγκεκριμένες υπηρεσίες ή πρωτόκολλα δικτύου. Το packet injection χρησιμοποιείται συνήθως σε επιθέσεις man-in-the-middle και σε επιθέσεις denial-of-service.



Σχήμα Α'.2: Προσαρμογέας WiFi με chipset AR9271.

Το Chipset του προσαρμογέα WiFi που θα χρησιμοποιηθεί στην παρακάτω επίθεση είναι ένα από τα πιο γνωστά και διαδεδομένα, το AR9271, έχοντας την δυνατότητα υποστήριξης Monitor mode καθώς και Packet injection mode, συμβατό επίσης με την έκδοση του λογισμικού Parrot OS εγκατεστημένο στο κύριο μηχάνημα υπολογιστή.

A'.5 Man-In-The-Middle επίθεση

Μία από τις πιο διαδεδομένες επιθέσεις στην ασφάλεια υπολογιστών και των δικτύων είναι η επίθεση Man-In-The-Middle καθώς προκαλεί μια σοβαρή ανησυχία λόγω των κινδύνων που κρύβει. Στην κρυπτογραφία και την ασφάλεια των υπολογιστών, μια επίθεση man-in-the-middle (MITM) είναι μια επίθεση όπου ο εισβολέας μεταφέρει κρυφά και ίσως μπορεί να αλλάζει μερικά από τα δεδομένα μεταξύ των σημείων που πιστεύουν ότι επικοινωνούν άμεσα μεταξύ τους. Η επίθεση αυτή είναι ένας γενικός όρος για το πότε ένας κακόβουλος χρήστης διεισδύει σε μια επικοινωνία μεταξύ ενός πελάτη και μιας εφαρμογής, είτε για να ακούσει κρυφά είτε για να μιμηθεί ένα από τα μέρη των δεδομένων που υπάρχουν στην σύνδεση μεταξύ των σημείων, κάνοντάς το να φαίνεται σαν να βρίσκεται σε εξέλιξη μια συνηθισμένη ανταλλαγή δεδομένων. Ο στόχος μιας τέτοιας επίθεσης είναι να παρθούν με δόλιο τρόπο πληροφορίες, για παράδειγμα, πιστοποιήσεις σύνδεσης (Wi-Fi credentials), στοιχεία λογαριασμών καθώς και αριθμούς καρτών τραπέζης. Μια man-in-the-middle επίθεση δίνει την δυνατότητα σε έναν κακόβουλο χρήστη να υποκλέψει, να στείλει και να δεχθεί δεδομένα που προορίζονταν για κάποιον άλλου ή δεν προορίζονταν να σταλούν πουθενά, χωρίς κανένα από τα άλλα σημεία να αντιληφθεί κάτι μέχρι όμως να είναι πολύ αργά. Αξιοσημείωτο να αναφερθεί πως η συγκεκριμένη επίθεση μπορεί να ονομαστεί με πληθώρα τρόπων συντομογραφίας, όπως MITM, MitM, MiM ή MIM.

Ένας κακόβουλος, στα δίκτυα Wi-Fi μπορεί να κρυφακούει μια ασύρματη επικοινωνία μεταξύ δύο σημείων καθώς και σε ορισμένες περιπτώσεις, μπορεί ακόμη και να χειριστεί ενεργά τη ροή των δεδομένων από αυτές τις επικοινωνίες. Για την επιτυχή εφαρμογή επιθέσεων MitM σε δίκτυα Wi-Fi, ακολουθούνται συγκεκριμένες διαδικασίες. Στα πρώτα στάδια, αυτά της συλλογής πληροφοριών, ο κακόβουλος χρήστης μπορεί να χρησιμοποιήσει εργαλεία ανίχνευσης για να συγκεντρώσει χρήσιμες πληροφορίες για τα σημεία πρόσβασης δικτύων και τους πελάτες σε ένα WLAN. Χρησιμοποιώντας τις πληροφορίες αυτές από αυτό το στάδιο, ο κακόβουλος χρήστης δημιουργεί ένα πλαστό σημείο πρόσβασης

δικτύου (rogue AP, επίσης γνωστό ως Evil-Twin) για να αναπαράγει το πραγματικό σημείο πρόσβασης δικτύου στο δεύτερο στάδιο, το οποίο είναι καθοριστικό για την επίτευξη της επίθεσης MITM. Στο τρίτο στάδιο, ο κακόβουλος χρήστης προσπαθεί να εξαπατήσει τους πελάτες με το πλαστό σημείο πρόσβασης. Για να επιτευχθεί αυτό, το πλαστό σημείο πρόσβασης δικτύου μεταδίδει ισχυρότερα σήματα από το κανονικό με σκοπό να δελιάσει τους πελάτες και περιμένει να συνδεθούν. Το αποτέλεσμα είναι μόλις ολοκληρωθούν όλα τα παραπάνω, να ξεκινήσει η καταγραφή στην κυκλοφορία των δεδομένων.

Α'.5.1 Fluxion Tool

Ένα από τα πιο διαδεδομένα εργαλεία για επιθέσεις Man-In-The-Middle τα τελευταία χρόνια θεωρείται το Fluxion. Είναι μια ανακατασκευή ενός άλλου γνωστού εργαλείου ονόματι linset, με λιγότερα σφάλματα και περισσότερη λειτουργικότητα καθώς αρκετά συχνά δέχεται ενημερώσεις με νέες δυνατότητες, βελτιώσεις και διορθώσεις σφαλμάτων.



Σχήμα Α'.3: Λογότυπο εργαλείου Fluxion.

Το σενάριο λειτουργίας παρουσιάζεται ως εξής, επιχειρεί να ανακτήσει τα προστατευμένα κλειδιά Wifi (WPA/WPA2) των δικτύων-στόχων

προσομοιώνοντας μια MITM επίθεση. Το εργαλείο αυτό παρουσιάζει δύο επιλογές επίθεσης και συγκεκριμένα είναι οι, Handshake Snooper και Captive Portal. Ο Handshake Snooper χρησιμοποιείται για τη λήψη των δεδομένων της χειραψίας που χρησιμοποιούνται για την επαλήθευση των κλειδιών wifi που έχουν ληφθεί από τους χρήστες του δικτύου. Η επίθεση Captive Portal δημιουργεί την Evil-Twin τεχνική που αναφέρθηκε για να δελεάσει τους χρήστες/θύματα. Ένας πλαστός διακομιστής ιστού δημιουργείται από το Fluxion που προτρέπει τους χρήστες να εισαγάγουν το κλειδί wifi τους για να συνδεθούν στο (πλαστό) δίκτυο. Στη συνέχεια εάν ένα θύμα εισαγάγει μη έγκυρο ή λάθος κωδικό πρόσβασης, η Captive Portal θα τον ειδοποιήσει για τον μη έγκυρο κωδικό πρόσβασης και θα δώσει την επιλογή εισαγωγής νέου κωδικού πρόσβασης. Αυτό θα συμβεί μέχρις ότου δοθεί ο σωστός κωδικός πρόσβασης και το Fluxion τον ανιχνεύσει, το πλαστό σημείο πρόσβασης δικτύου θα εξαφανιστεί, θα σταματήσει να μπλοκάρει το κανονικό σημείο πρόσβασης και τα θύματα/χρήστες θα μπορούν να επανασυνδεθούν στο αρχικό σημείο πρόσβασης.

Σαφώς στην θεωρία όλα φαίνονται ουτοπικά, όμως καθόλη την διάρκεια προσπαθειών να λειτουργήσει το Fluxion, απέτυχαν. Πιο λεπτομερώς, θεωρείται σίγουρο ότι το πρόβλημα δεν οφείλεται στη συμβατότητα του λειτουργικού συστήματος του υπολογιστή με αυτή του εργαλείου καθώς δοκιμάστηκαν κάθε πιθανές επιλογές. Ένα από τα σημαντικότερα προβλήματα ήταν η μη διατήρηση συνέπειας σωστής λειτουργίας, δεδομένου ότι χωρίς να επηρεάζεται καμία παράμετρος και η διαδικασία επανάληψης κάθε δοκιμής να παραμένει πιστά ίδια κάθε φορά, η αντίδραση/λειτουργία του εργαλείου ήταν διαφορετική και πολύ κοντά στο μη αποδοτική. Η αδυναμία εκκίνησης της πλαστής πύλης (fake AP), ήταν το πρόβλημα που έδωσε το έναυσμα για την δοκιμή άλλου εργαλείου με παρόμοια φιλοσοφία λειτουργίας.

Α'.5.2 Wifiphisher Tool

Έπειτα από έρευνα, ο πιθανός καλύτερος αντικαταστάτης του Fluxion καταλήγει να είναι το Wifiphisher. Το Wifiphisher είναι ένα εργαλείο που μπορεί να χρησιμοποιηθεί για την πραγματοποίηση επίθεσης phishing σε δίκτυα Wi-Fi. Είναι ένα εργαλείο ασφαλείας που έχει σχεδιαστεί για να πραγματοποιεί αυτοματοποιημένες επιθέσεις phishing εναντίον ασύρματων δικτύων, προκειμένου να αποκτήσει τα διαπιστευτήρια του χρήστη/θύματος ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε δίκτυο.



Σχήμα Α'.4: Λογότυπο εργαλείου Wifiphisher.

Το εργαλείο λειτουργεί ακολουθώντας τα εξής βήματα:

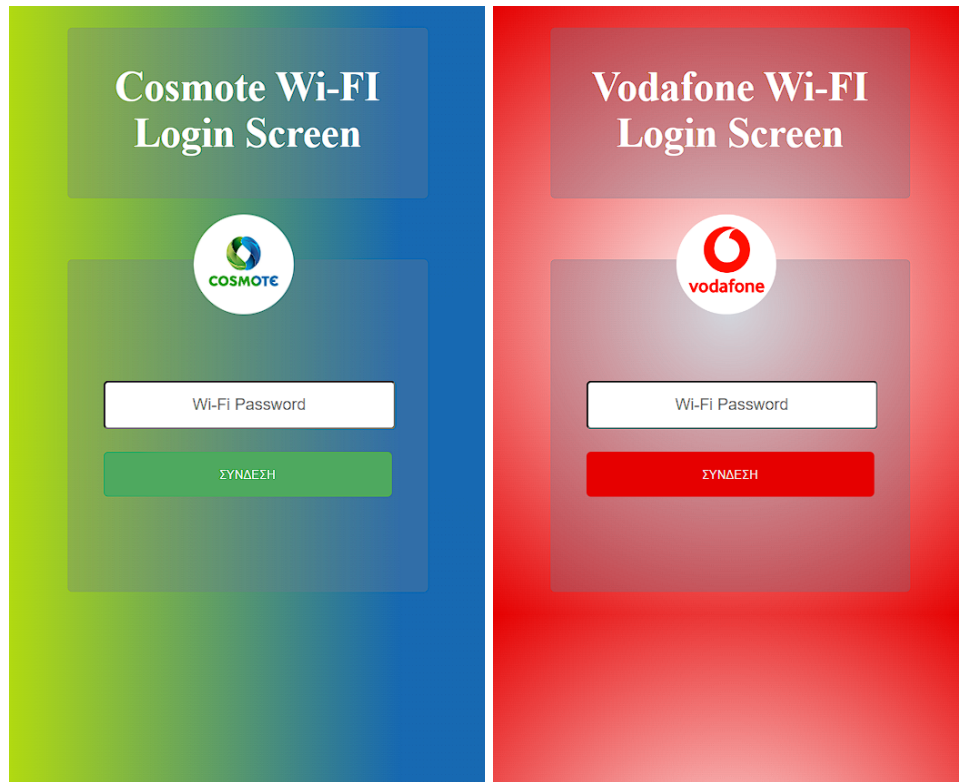
1. Ανιχνεύει όλα τα διαθέσιμα δίκτυα εντός εμβέλειας της κεραίας και όταν επιλεγθεί ένα, πραγματοποιεί deauthentication σε όλες τις συσκευές που είναι συνδεδεμένες στο δίκτυο με σκοπό να διακοπεί η σύνδεσή τους από αυτό.
2. Δημιουργεί ένα πλαστό σημείο ασύρματης πρόσβασης (fake AP) που φαίνεται να είναι αξιόπιστο. Σε αυτό το πλαστό AP συνήθως δίνεται ένα όνομα πανομοιότυπο με το όνομα του πραγματικού δικτύου που έχει τεθεί ως στόχος, προκειμένου να εξαπατηθούν οι χρήστες και να συνδεθούν σε αυτό.

3. Μόλις ο χρήστης συνδεθεί στο πλαστό AP, το Wifiphisher ανακατευθύνει τον χρήστη/θύμα σε μια πλαστή σελίδα σύνδεσης που μοιάζει με τη σελίδα σύνδεσης για το πραγματικό AP. Αυτή η σελίδα έχει σχεδιαστεί για να μιμείται την εμφάνιση και την αίσθηση της πραγματικής σελίδας σύνδεσης προκειμένου να εξαπατήσει τον χρήστη να εισάγει τα δεδομένα του.
4. Μόλις ο χρήστης εισάγει τα δεδομένα του στην πλαστή σελίδα σύνδεσης, το Wifiphisher τα καταγράφει και τα στέλνει στον εισβολέα. Στη συνέχεια, ο εισβολέας μπορεί να χρησιμοποιήσει αυτά τα διαπιστευτήρια για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο δίκτυο ή στους λογαριασμούς του χρήστη.
5. Με την ολοκλήρωση και τερματισμό της επίθεσης, διακόπτεται το deauthentication, εξαφανίζεται το πλαστό AP και αυτόματα οι συσκευές του θύματος συνδέονται στο πραγματικό δίκτυο.

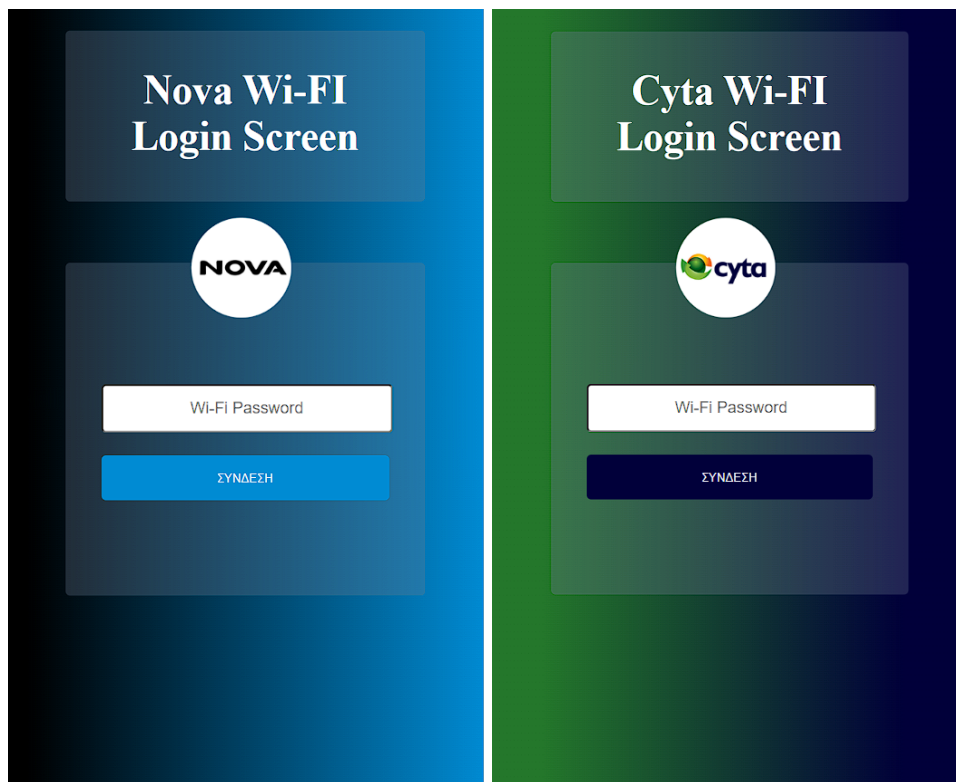
Το αξιοσημείωτο με το Wifiphisher είναι ότι δίνει την δυνατότητα να γίνει τροποποίηση και προσαρμογή της πλαστή σελίδας σύνδεσης, με την οποία θα έχει αλληλεπίδραση το θύμα και θα είναι η πύλη ώστε να γίνει η υποκλοπή των δεδομένων. Ένα τέτοιο χαρακτηριστικό προσφέρει μεγιστοποίηση των πιθανοτήτων μιας επιτυχημένης επίθεσης.

Α'.6 Προσαρμοσμένα Σενάρια Επίθεσης

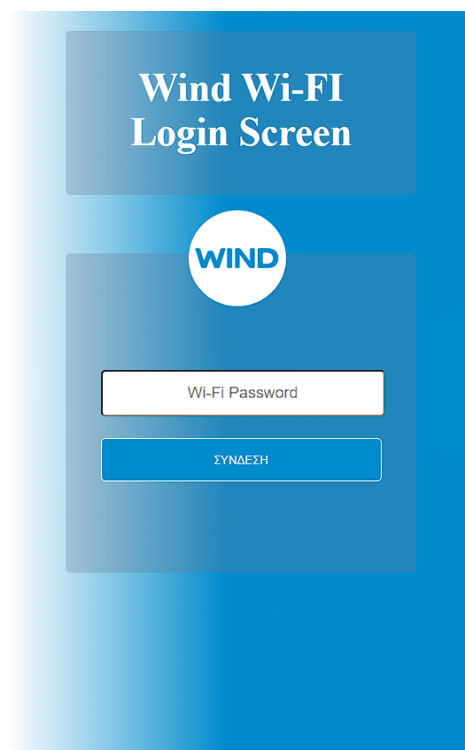
Όπως αναφέρθηκε παραπάνω, η τροποποίηση των σελίδων κλώνων σύνδεσης θα προσφέρει περισσότερες πιθανότητες να ξεγελαστεί το θύμα. Στην περίπτωση μας χρειάστηκε να υλοποιηθούν 5 διαφορετικά σενάρια επίθεσης, ένα για κάθε πιθανό πάροχο ίντερνετ.



Σχήμα Α'.5: Σελίδες κλώνος σύνδεσης Cosmote και Vodafone.



Σχήμα Α'.6: Σελίδες κλώνος σύνδεσης Nova και Cyta.



Σχήμα Α'.7: Σελίδα κλώνος σύνδεσης Wind.

Οι σελίδες κλώνων σύνδεσης (βλέπε Σχήμα Α'.4, Α'.5 και Α'.6) υλοποιήθηκαν ώστε να μιμηθούν όσο το περισσότερο δυνατόν μια πραγματική σελίδα σύνδεσης αντίστοιχα για κάθε πάροχο ίντερνετ. Κύριος παράγοντας που λήφθηκε υπ όψιν για την υλοποίηση και τη επίτευξη του στόχου αυτού ήταν η χρήση των αυθεντικών χρωματικών παλετών κάθε παρόχου σε συνδυασμό με την προβολή του λογοτύπου του, έχοντας απώτερο σκοπό το θύμα να βρεθεί σε ένα περιβάλλον που θα νιώσει οικία και γνώριμα.

Α'.6.1 Εγκατάσταση νέων σεναρίων επίθεσης

Όστε να δημιουργηθούν τα νέα σενάρια επιθέσεων χρειάζεται να ακολουθηθούν οι επόμενες ενέργειες προτού την εγκατάσταση του προγράμματος στο σύστημα. Αρχικά χρειάζεται ένα config.ini αρχείο το οποίο περιέχει σημαντικές πληροφορίες σχετικά με το κάθε ένα νέο σενάριο όπως το όνομά του, την περιγραφή ή και κάποιο payload. Στην περίπτωσή μας η προσθήκη ενός payload δεν χρειάζεται εφόσον δεν έχουμε σκοπό να εισάγουμε κάποιο κακόβουλο λογισμικό στο θύμα.

```

1  # This is a comment
2  [info]
3  Name: Cosmote
4  Description: A custom designed fake portal for Cosmote wifi victims.
```

Σχήμα Α'.8: Περιεχόμενα αρχείου config.ini.

Έπειτα, το αρχείο config.ini πρέπει να συνοδεύεται από τα αρχεία html και css που θέλει ο κακόβουλος χρήστης να δημιουργήσει για κάθε ξεχωριστό σενάριο. Τέλος όλα μαζί σε ένα φάκελο είναι απαραίτητο να βρίσκονται στο φάκελο “phishing-pages” του προγράμματος, μόλις όλες αυτές οι ενέργειες ολοκληρωθούν μπορούμε να προχωρήσουμε στην εγκατάσταση και τα σενάρια θα είναι έτοιμα για χρήση.

Παρακάτω υπάρχει ο πηγαίος κώδικας μιας περίπτωσης κλώνου, καθώς τα σημεία που παραμετροποιούνται για τους υπόλοιπους είναι μονάχα για το οπτικό μέρος της σελίδας. Το σημαντικό σημείο που παραμένει απαράλλαχτο είναι στην φόρμα εισαγωγής του κωδικού πρόσβασης, εκεί το wifiphisher επιτρέπει να δώσεις ένα όνομα συγκεκριμένο όνομα στην τιμή που θα κάνει καταγραφή ώστε να επιστρέψει στην οθόνη του επιτιθέμενου. Το όνομα της τιμής είναι “wphshr-password”.

```
index.html x
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="utf-8">
5   <meta name="viewport" content="width=device-width, initial-scale=0.7">
6   <title>Cosmote Wi-Fi Login Page</title>
7   <link rel="icon" type="image/x-icon" href="/static/cosmote-logo.ico">
8   <link rel="stylesheet" href="/static/styles.css">
9 </head>
10 <body>
11
12   <h1 id="container1">Cosmote Wi-Fi <br> Login Screen</h1><br>
13
14   <div id="container">
15     
16
17     <form>
18
19       <input type="password" name="wphshr-password" class="pass-area" placeholder="Wi-Fi Password">
20
21       <input type="submit" value="Συνδεση" class="btn-login">
22     </form>
23   </div>
24
25 </body>
26 </html>
```

Σχήμα Α'9: Κώδικας HTML σελίδας κλώνου.

```

C:\Users\John\Desktop> cosmote-custom-webpage > html > static > # styles.css > body
1  body {
2      background: linear-gradient(90deg, #000000, #000000 0%, #000000 82%);
3      background: linear-gradient(90deg, #000000, #000000 0%, #000000 82%);
4      font-family: 'Open Sans';
5  }
6
7  h1 {
8      text-align: center;
9      color: white;
10     font-family: 'Bree Serif';
11     font-size: 45px;
12     padding-top: 40px;
13 }
14
15 #container1 {
16     width: 400px;
17     height: 100px;
18     margin: 25px auto;
19     background: linear-gradient(90deg, #000000, #000000 0%, #000000 82%);
20     border-radius: 5px;
21     padding-bottom: 50px;
22     position: relative;
23 }
24
25 #container {
26     width: 400px;
27     height: 320px;
28     margin: 25px auto;
29     background: linear-gradient(90deg, #000000, #000000 0%, #000000 82%);
30     border-radius: 5px;
31     padding-bottom: 50px;
32     position: relative;
33 }
34
35 img {
36     height: 30%;
37     left: 140px;
38     top: -50px;
39     position: absolute;
40 }
41
42 input[type="password"] {
43     width: 300px;
44     height: 30px;
45     padding: 10px;
46     margin: 20px 0 5px 40px;
47     border-radius: 5px;
48     font-size: 18px;
49     text-align: center;
50 }
51
52 input[type="password"].pass-area {
53     margin-top: 135px;
54 }
55
56 input[type="submit"] {
57     width: 320px;
58     height: 50px;
59     margin: 20px 40px;
60     padding: 10px;
61     border: none;
62     border-radius: 5px;
63     background: linear-gradient(90deg, #000000, #000000 0%, #000000 82%);
64     color: white;
65     text-transform: uppercase;
66     cursor: pointer;
67 }
68
69 input[type="submit"]:hover {
70     background: linear-gradient(90deg, #000000, #000000 0%, #000000 82%);
71     border: 1px solid white;
72 }
73
74 a {
75     margin: 0 130px;
76     text-decoration: none;
77     color: white;
78 }
79
80 a:hover {
81     color: white;
82 }

```

Σχήμα Α'.10: Κώδικας CSS σελίδας κλώνου.

Κεφάλαιο Β'

Παρουσίαση επίθεσης

Με την ολοκλήρωση υλοποίησης κάθε ξεχωριστού σεναρίου η εκκίνηση της διαδικασίας των επιθέσεων μπορεί να ξεκινήσει. Οτιδήποτε αναλυθεί παρακάτω είναι ενέργειες που πραγματοποιήθηκαν στο εργαστήριο ασφάλειας NMSLAB της Πληροφορικής στο Πανεπιστήμιο. Ο χρόνος που διατέθηκε για κάθε μία ξεχωριστή επίθεση ήταν 15 με 20 λεπτά, αφήνοντας χρόνο στο θύμα ώστε να μπορέσει να καταλάβει την ύπαρξη του σημείου πρόσβασης κλώνου.

Β'.1 Πρώτα βήματα

Αναλυτικά ο τρόπος διεξαγωγής των επιθέσεων είναι ο εξής, με την εντολή "sudo wifiphisher --force-hostapd" χρησιμοποιείται για την εκτέλεση του εργαλείου Wifiphisher με την επιλογή "force-hostapd", η οποία αναγκάζει το εργαλείο να χρησιμοποιεί το ενσωματωμένο hostapd αντί για οποιαδήποτε έκδοση εγκατεστημένη στο σύστημα. Το Hostapd είναι ένα λογισμικό space daemon χρήστη που επιτρέπει τη δημιουργία ασύρματων σημείων πρόσβασης και διακομιστών ελέγχου ταυτότητας. Συνήθως χρησιμοποιείται για τη δημιουργία ενός σημείου ασύρματης πρόσβασης για νόμιμους σκοπούς, όπως σε δημόσιους χώρους ή σε περιβάλλον σπιτιού κ.α.. Ωστόσο, όταν χρησιμοποιείται για κακόβουλους σκοπούς, μπορεί να δημιουργεί ένα πλαστό σημείο πρόσβασης χρησιμοποιώντας ένα λογισμικό όπως το Wifiphisher με σκοπό να εξαπατήσει τους χρήστες να συνδεθούν με αυτό, και μπορεί να οδηγήσει σε κλοπή διαπιστευτηρίων ή άλλων ευαίσθητων πληροφοριών. Στην περίπτωση του Wifiphisher, η επιλογή "force-hostapd" διασφαλίζει ότι χρησιμοποιείται η ενσωματωμένη έκδοση του hostapd που παρέχεται με το εργαλείο, αντί για

οποιαδήποτε έκδοση εγκατεστημένη στο σύστημα που μπορεί να έχει ευπάθειες ή να είναι επιρρεπής σε σφάλματα. Η χρήση της ενσωματωμένης έκδοσης του hostapd που παρέχεται από το Wifiphisher μπορεί να βοηθήσει στη βελτίωση της συνολικής αποτελεσματικότητας του εργαλείου κατά την εκτέλεση επιθέσεων.

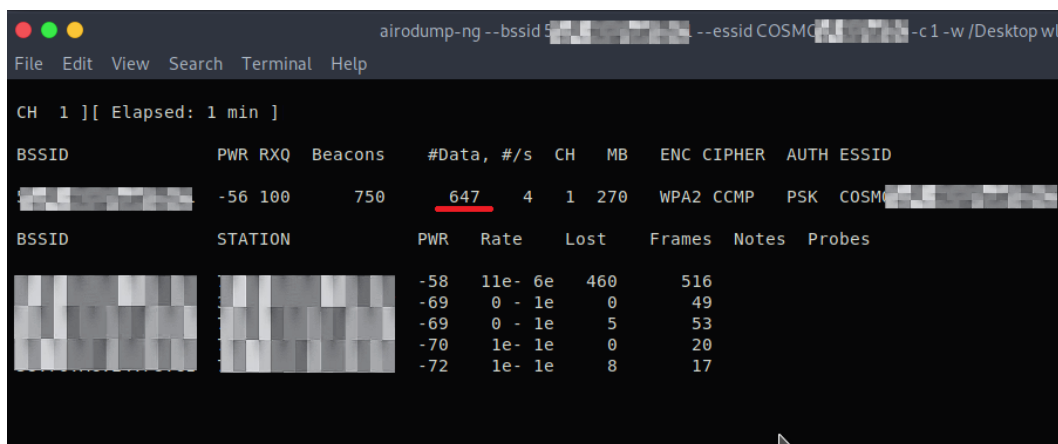
Το Hostapd (συντομογραφία του Host Access Point Daemon) είναι μια εφαρμογή λογισμικού ανοιχτού κώδικα που χρησιμοποιείται για τη δημιουργία σημείου ασύρματης πρόσβασης. Το εργαλείο Wifiphisher χρησιμοποιεί μια τροποποιημένη έκδοση του hostapd για να δημιουργήσει ένα πλαστό σημείο πρόσβασης που μιμείται ένα πραγματικό ασύρματο δίκτυο. Το ενσωματωμένο δυαδικό αρχείο hostapd που παρέχεται από το Wifiphisher έχει τροποποιηθεί ώστε να περιλαμβάνει πρόσθετες λειτουργίες και λειτουργίες που είναι απαραίτητες για τη δημιουργία και τη διαχείριση ενός πλαστού σημείου πρόσβασης για τους σκοπούς των επιθέσεων σε σημεία πρόσβασης. Οι δυνατότητες που μας ενδιαφέρουν σε μεγάλο βαθμό είναι η δυνατότητα χειρισμού συνδέσεων χρηστών και η δημιουργία του πλαστού σημείου πρόσβασης καθώς τροποποιεί την κεραία και κάνει μια εικονική “διαίρεση” χρησιμοποιώντας την μια κεραία σαν δύο ταυτόχρονα. Η μια χρήση για το deauthentication των θυμάτων και η άλλη για την δημιουργία του πλαστού σημείου πρόσβασης.

B'.2 Επιλογή δικτύου θύματος

Πλέον, έχοντας ολοκληρώσει την υλοποίηση κάθε ξεχωριστού σεναρίου επίθεσης εν συνεχεία και την εγκατάσταση του προγράμματος, με την εντολή “sudo wifiphisher --force-hostapd” που αναλύθηκε προηγουμένως τα πάντα είναι έτοιμα για την εκκίνηση της διαδικασίας της επίθεσης.

Κάνοντας ένα μικρό βήμα πίσω όμως, είναι θεμιτή να προηγηθεί η χρήση του εργαλείου airodump-ng για την αποφυγή επιθέσεων “στα τυφλά” μονάχα για ένα χαρακτηριστικό του, την ανίχνευση πακέτων που μεταδίδονται στο δίκτυο άρα

κατά συνέπεια ενεργή χρήση του δικτύου. Με τη στήλη #Data στο παρακάτω στιγμιότυπο οθόνης, ο αριθμός υποδεικνύει πόσα πακέτα δεδομένων έχουν συλλεχθεί. Όσο μεγαλύτερος είναι αυτός ο αριθμός, τόσο πιο πιθανό είναι από την πλευρά του επιτιθέμενου να ανακαλυφθούν ευαίσθητες πληροφορίες που μπορούν να χρησιμοποιηθούν κακόβουλα. Στην περίπτωση μας όμως δεν είναι αναγκαίο και η απλή πληροφορία ότι στο συγκεκριμένο δίκτυο υπάρχει κίνηση πακέτων, δηλαδή χρησιμοποιείται, είναι αρκετή.



```

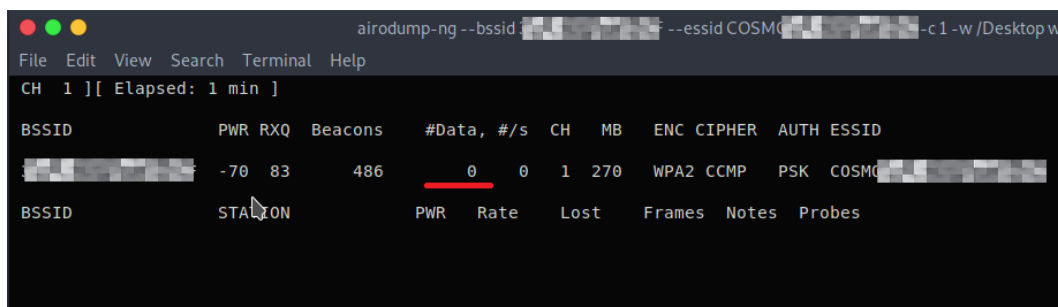
airodump-ng --bssid [redacted] --essid COSMO [redacted] -c 1 -w /Desktop w
File Edit View Search Terminal Help

CH 1 ][ Elapsed: 1 min ]

BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
[redacted]      -56 100   750    647   4  1 270 WPA2 CCMP  PSK  COSMO [redacted]

BSSID          STATION        PWR  Rate  Lost  Frames  Notes  Probes
[redacted]      [redacted]      -58  11e- 6e  460    516
[redacted]      [redacted]      -69   0 - 1e    0     49
[redacted]      [redacted]      -69   0 - 1e    5     53
[redacted]      [redacted]      -70   1e- 1e    0     20
[redacted]      [redacted]      -72   1e- 1e    8     17
  
```

Σχήμα Β'.1: Εργαλείο airodump-ng, έλεγχος κίνησης πακέτων, ενεργή κίνηση.



```

airodump-ng --bssid [redacted] --essid COSMO [redacted] -c 1 -w /Desktop w
File Edit View Search Terminal Help

CH 1 ][ Elapsed: 1 min ]

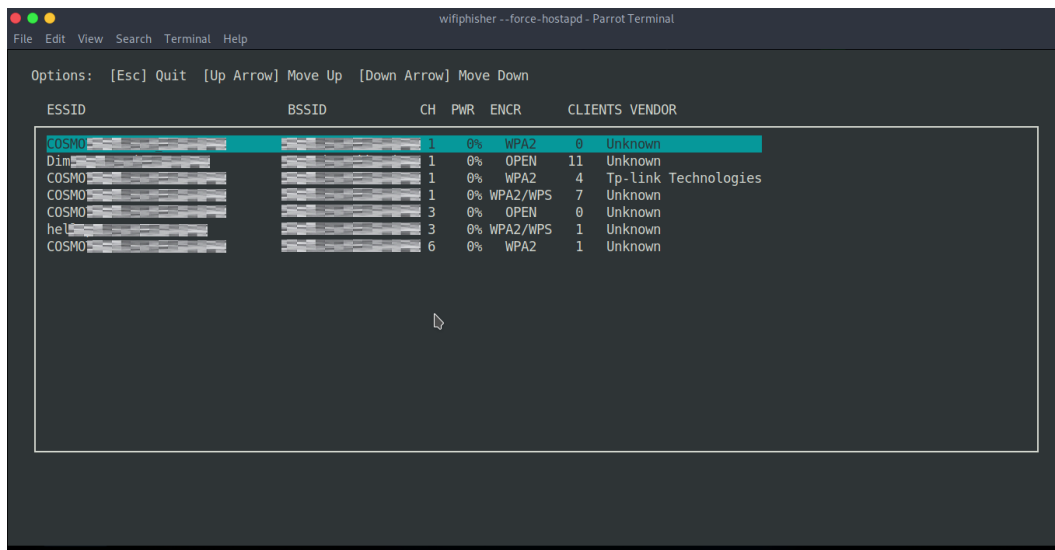
BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
[redacted]      -70  83   486     0   0  1 270 WPA2 CCMP  PSK  COSMO [redacted]

BSSID          STATION        PWR  Rate  Lost  Frames  Notes  Probes
[redacted]      [redacted]
  
```

Σχήμα Β'.2: Εργαλείο airodump-ng, έλεγχος κίνησης πακέτων, ανενεργή κίνηση.

Εχοντας βρει λοιπόν το δίκτυο που φαίνεται να έχει υψηλό αριθμό κίνησης πακέτων, συνεχίζουμε παρατηρώντας το στιγμιότυπο οθόνης από το wifiphisher παρακάτω, με αλλοιωμένες τις ευαίσθητες πληροφορίες του κάθε δικτύου (SSID

και MAC address), εμφανίζονται όλα τα διαθέσιμα δίκτυα της περιοχής έχοντας πληροφορίες σχετικά με το κανάλι εκπομπής του ρούτερ, τι είδους κρυπτογράφηση υπάρχει ως μέτρο ασφάλειας καθώς και το πόσες συσκευές είναι ενεργές στο εκάστοτε δίκτυο.



Σχήμα Β'.3: Wifiphisher, επιλογή δικτύου για επίθεση.

Β'.3 Επιλογή σεναρίου επίθεσης

Διαλέγοντας το επιθυμητό δίκτυο θύματος για επίθεση και έχοντας δημιουργήσει όλα τα διαφορετικά σενάρια προσαρμοσμένα για κάθε γνωστό πάροχο διαδικτύου, στο τελευταίο βήμα πριν την εκκίνηση μιας επίθεσης το μενού επιλογών φαίνεται όπως στην φωτογραφία παρακάτω και με την επιλογή ενός σεναρίου τίθεται σε εκκίνηση η επίθεση.

Τα “1 - Cosmote”, “2 - Cyt”, “4 - Nova”, “7 - Vodafone” και “9 - Wind” είναι τα προσαρμοσμένα σενάρια που υλοποιήθηκαν για τους σκοπούς που αναφέρθηκαν. Τα υπόλοιπα τέσσερα σενάρια, “3 - Firmware Upgrade Page”, “5 - OAuth Login Page”, “6 - Browser Plugin Update” και “8 - Network Manager Connect” είναι prebuilt σενάρια του προγράμματος wifiphisher, τα οποία δεν χρησιμοποιήθηκαν διότι δεν ταίριαζαν στις απαιτήσεις των επιθέσεων.

```

wifiphisher --force-hostapd - Parrot Terminal
File Edit View Search Terminal Help
Options: [Up Arrow] Move Up [Down Arrow] Move Down

Available Phishing Scenarios:

1 - Cosmote
  A custom designed fake portal for Cosmote wifi victims.

2 - Cyta
  A custom designed fake portal for Cyta wifi victims.

3 - Firmware Upgrade Page
  A router configuration page without logos or brands asking for WPA/WPA2 password due to a
  firmware upgrade. Mobile-friendly.

4 - Nova
  A custom designed fake portal for Nova wifi victims.

5 - OAuth Login Page
  A free Wi-Fi Service asking for social network credentials to authenticate via OAuth.

6 - Browser Plugin Update
  A generic browser plugin update page that can be used to serve payloads to the
  victims.

7 - Vodafone
  A custom designed fake portal for Vodafone wifi victims.

8 - Network Manager Connect
  The idea is to imitate the behavior of the network manager by first showing the
  browser's "Connection Failed" page and then displaying the victim's network manager window through the page
  asking for the pre-shared key.

9 - Wind
  A custom designed fake portal for Wind wifi victims.

```

Σχήμα Β'.4: Wifiphisher, επιλογή σεναρίου επίθεσης.

Β'.4 Από την οπτική του κακόβουλου χρήστη

Έχοντας ξεκινήσει την επίθεση ο κακόβουλος χρήστης αυτό που βλέπει στο τερματικό του εκτός από τη διεπαφή χρήστη που προσφέρει το πρόγραμμα όπως έχει παρουσιαστεί από τα αντίστοιχα σχήματα παραπάνω, φαίνεται στο επόμενο σχήμα. Το wifiphisher αρχικά διαπιστώνει την ζώνη ώρας ώστε να μπορέσει να θέσει το σωστό εύρος το καναλιών που θα χρησιμοποιήσει. Ανά τις χώρες τα WLAN κανάλια διαφέρουν. Έπειτα, πράττει έναν εικονικό διαχωρισμό στην μια και μοναδική κεραία που χρησιμοποιείται για την επίθεση, ορίζοντας τις απαραίτητες ενέργειες που είναι απαραίτητες να γίνουν. Η μια είναι το deauthentication και η άλλη η δημιουργία του πλαστού σημείου πρόσβασης. Αυτή η διαδικασία του εικονικού διαχωρισμού της κεραίας όπως αναφέρθηκε και σε προηγούμενη ενότητα επιτυγχάνεται λόγω του hostapd.

Εν συνεχεία το εργαλείο πλαστογραφεί το BSSID του αξιόπιστου σημείου πρόσβασης Wi-Fi, έτσι ώστε τα θύματα/χρήστες να εξαπατηθούν ώστε να συνδεθούν στο πλαστό σημείο πρόσβασης που δημιουργεί το εργαλείο, αντί για το πραγματικό. Αλλάζοντας τη διεύθυνση MAC, το εργαλείο μπορεί να δημιουργήσει ένα πλαστό σημείο πρόσβασης που φαίνεται να είναι το αξιόπιστο σημείο πρόσβασης, καθιστώντας πιο δύσκολο για τους χρήστες να διακρίνουν μεταξύ των δύο. Αυτή είναι μια σημαντική τεχνική που χρησιμοποιείται από το Wifiphisher για να παρασύρει τα θύματα/χρήστες να συνδεθούν στο πλαστό σημείο πρόσβασης.

Το `wpa_supplicant` είναι ένα πρόγραμμα που διαχειρίζεται συνδέσεις Wi-Fi. Χρησιμοποιείται για τον έλεγχο ταυτότητας και τη σύνδεση σε ασύρματα δίκτυα που απαιτούν διαπιστευτήρια, όπως κωδικό πρόσβασης. Όταν το εργαλείο Wifiphisher στέλνει ένα σήμα SIGKILL στη διαδικασία `wpa_supplicant`, το τερματίζει αναγκαστικά. Αυτή η ενέργεια πραγματοποιείται επειδή το εργαλείο Wifiphisher πρέπει να δημιουργήσει ένα πλαστό σημείο πρόσβασης για να εξαπατήσει τους χρήστες ώστε να συνδεθούν σε αυτό και η λειτουργία του νόμιμου `wpa_supplicant` θα μπορούσε να παρέμβει σε αυτήν τη διαδικασία.

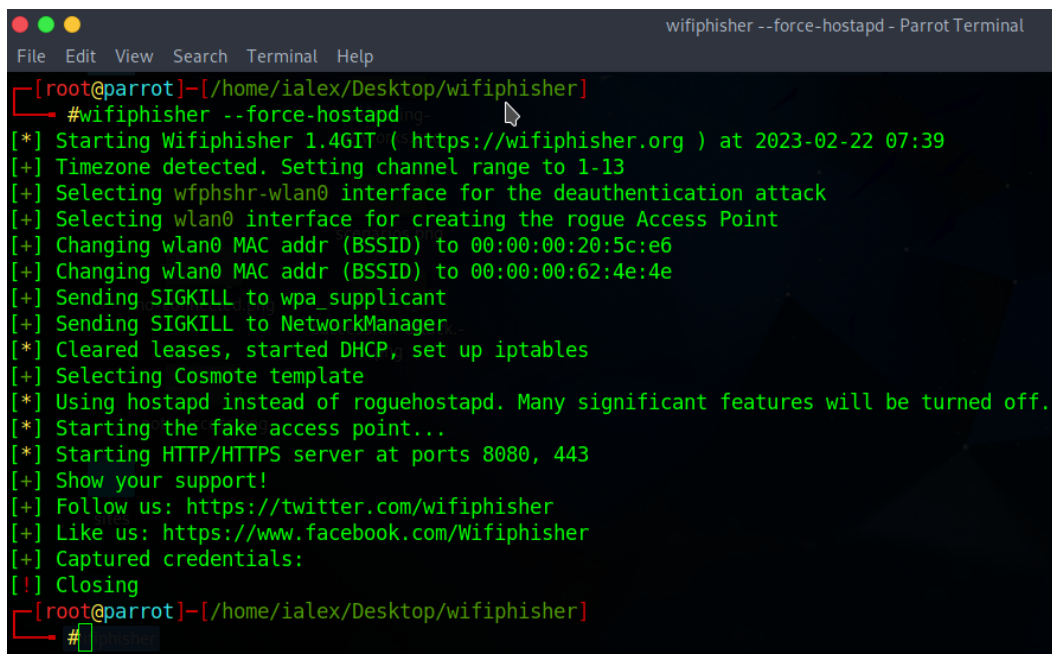
Το `NetworkManager` είναι και αυτό ένα πρόγραμμα που διαχειρίζεται τις συνδέσεις δικτύου. Είναι υπεύθυνο για τον εντοπισμό και τη διαμόρφωση συσκευών δικτύου και τη διαχείριση της συνδεσιμότητας της συσκευής σε διάφορα δίκτυα. Το εργαλείο Wifiphisher στέλνει ένα σήμα SIGKILL στο `NetworkManager` για να σταματήσει να παρεμβαίνει στη λειτουργία του εργαλείου. Αυτό συμβαίνει επειδή το `NetworkManager` μπορεί να προσπαθήσει να επανασυνδεθεί στο αρχικό δίκτυο και μπορεί να παρεμποδίσει το πλαστό σημείο πρόσβασης που δημιουργείται από το Wifiphisher.

Επιπλέον, η έξοδος του τερματικού δείχνει ότι το εργαλείο Wifiphisher διέγραψε τα DHCP leases και ξεκίνησε τη ρύθμιση DHCP, για να αρχίσει να εκχωρεί νέα leases σε θύματα/χρήστες που θα συνδεθούν στο ψεύτικο σημείο πρόσβασης.

Επιπροσθέτως δείχνει ότι το εργαλείο Wifiphisher δημιούργησε το `iptables`, το οποίο είναι ένα βοηθητικό πρόγραμμα τείχους προστασίας. Αυτό το βοηθητικό

πρόγραμμα μπορεί να χρησιμοποιηθεί για το φιλτράρισμα της κυκλοφορίας δικτύου αποκλείοντας ή επιτρέποντας συγκεκριμένους τύπους κίνησης με βάση διάφορες συνθήκες. Στο πλαίσιο του εργαλείου Wifiphisher, τα iptables μπορούν να χρησιμοποιηθούν για τον έλεγχο της κυκλοφορίας δικτύου προς και από το πλαστό σημείο πρόσβασης που δημιουργείται. Ακόμη φαίνεται και να δείχνει την επιλογή που έχουμε κάνει ανάμεσα στα διαφορετικά σενάρια επιθέσεων.

Τέλος, το εργαλείο δημιουργεί το πλαστό σημείο πρόσβασης που έχει το ίδιο όνομα (SSID) με το αξιόπιστο σημείο πρόσβασης που πλαστοπροσωπεί, γεγονός που μπορεί να δυσκολεύει τους χρήστες/θύματα να διακρίνουν μεταξύ των πραγματικών και των πλαστών δικτύων. Ο διακομιστής HTTP/HTTPS χρησιμοποιείται από το εργαλείο για την παροχή της πλαστής ιστοσελίδας στους χρήστες/θύματα που συνδέονται στο πλαστό σημείο πρόσβασης. Από προεπιλογή, το εργαλείο ρυθμίζει τον διακομιστή στις θύρες 8080 και 443.



```

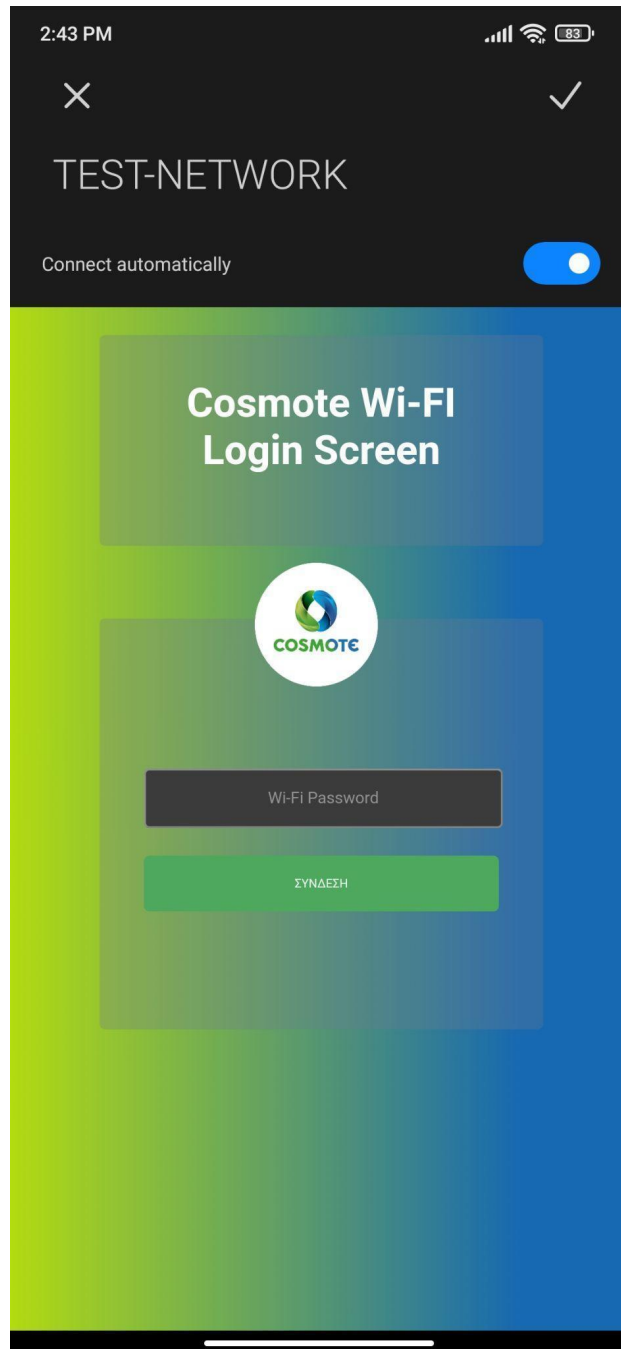
wifiphisher --force-hostapd - Parrot Terminal
File Edit View Search Terminal Help
[ root@parrot ] - [ /home/ialex/Desktop/wifiphisher ]
# wifiphisher --force-hostapd ng
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2023-02-22 07:39
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wifphshr-wlan0 interface for the deauthentication attack
[+] Selecting wlan0 interface for creating the rogue Access Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:20:5c:e6
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:62:4e:4e
[+] Sending SIGKILL to wpa_supplicant
[+] Sending SIGKILL to NetworkManager
[*] Cleared leases, started DHCP, set up iptables
[+] Selecting Cosmote template
[*] Using hostapd instead of roguehostapd. Many significant features will be turned off.
[*] Starting the fake access point...
[*] Starting HTTP/HTTPS server at ports 8080, 443
[+] Show your support!
[+] Follow us: https://twitter.com/wifiphisher
[+] Like us: https://www.facebook.com/Wifiphisher
[+] Captured credentials:
[!] Closing
[ root@parrot ] - [ /home/ialex/Desktop/wifiphisher ]
#

```

Σχήμα Β'.5: Τερματικός wifiphisher, απο την οπτική του κακόβουλου χρήστη.

B'.5 Από την οπτική του θύματος

Απο την πλευρά του θύματος/χρήστη τα πράγματα φαίνονται και είναι αναγκαίο να φαίνονται υπερβολικά πιο απλοποιημένα. Μόλις πατήσει να συνδεθεί στο πλαστό σημείο πρόσβασης η συσκευή τον προτρέπει να δει την phishing σελίδα και του ζητείται ο κωδικός πρόσβασης.



Σχήμα Β'.6: Phishing σελίδα, από την οπτική του θύματος.

B'.6 Επιτυχημένη περίπτωση επίθεσης

Με την ολοκλήρωση του βήματος επιλογής σεναρίου, βρισκόμαστε τώρα στην περίπτωση μιας επιτυχημένης επίθεσης. Μια επιτυχημένη επίθεση σημαίνει πως κάνοντας deauthentication όλες τις ασύρματες συσκευές του θύματος από το ρούτερ, ανακάλυψε την ύπαρξη του κλώνου σημείου πρόσβασης, πάτησε σε αυτό με σκοπό να συνδεθεί στο διαδίκτυο, έπειτα του εμφανίστηκε η προσαρμοσμένη σελίδα phishing και παραχώρησε τον κωδικό του στην φόρμα της σελίδας αυτής.

Όπως διακρίνεται κιάλας στο παρακάτω σχήμα, τα υπογραμμισμένα σημεία τονίζουν την απόκτηση του κωδικού σύνδεσης ρούτερ του θύματος.

```

wifiphisher --force-hostapd - Parrot Terminal
File Edit View Search Terminal Help

Extensions feed:
DEAUTH/DISAS - 74:f2: [redacted]
DEAUTH/DISAS - [redacted]
DEAUTH/DISAS - [redacted]
DEAUTH/DISAS - [redacted]
DEAUTH/DISAS - [redacted]
Connected Victims:
74:f2: [redacted] 10.0.0.87 Unknown Android
HTTP requests:
[*] GET request from 10.0.0.87 for http://connect.rom.miui.com/generate_204
[*] GET request from 10.0.0.87 for http://connect.rom.miui.com/generate_204
[*] GET request from 10.0.0.87 for http://connect.rom.miui.com/generate_204?wphshr-password=gg [redacted] 2m1
[*] GET request from 10.0.0.87 for http://connect.rom.miui.com/generate_204
[*] GET request from 10.0.0.87 for http://connect.rom.miui.com/generate_204

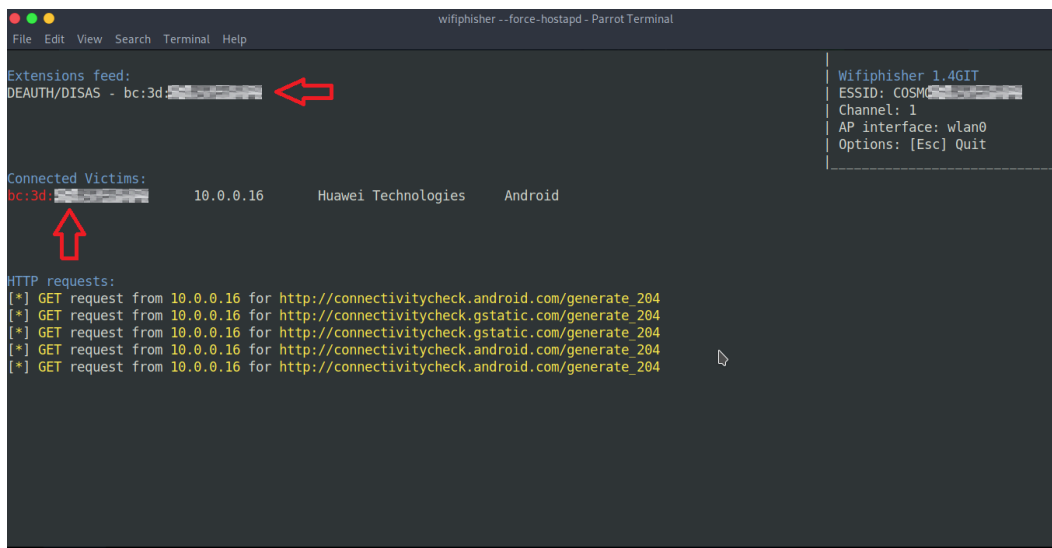
```

Σχήμα B'.7: Wifiphisher, deauthentication θύματος και απόκτηση κωδικού θύματος.

B'.7 Περίπτωση επίσκεψης phishing σελίδας

Φτάνοντας λοιπόν στην περίπτωση που το θύμα θα επισκεφτεί την phishing σελίδα, δηλαδή θα πατήσει στον κλώνο σημείο πρόσβασης, και δεν παραχωρήσει τα στοιχεία σύνδεσής του τότε ο επιτιθέμενος θα έχει στην οθόνη του μια εικόνα σαν το σχήμα παρακάτω.

Το deauthentication γίνεται κανονικά, φαίνεται η MAC address της συσκευής του θύματος που συνδέθηκε στον κλώνο και παρατηρείται κίνηση στα HTTP requests που υποδηλώνουν την εμφάνιση της phishing σελίδας στην συσκευή του.



```

wifiphisher --force-hostapd - Parrot Terminal

File Edit View Search Terminal Help

Extensions feed:
DEAUTH/DISAS - bc:3d: [redacted] ←

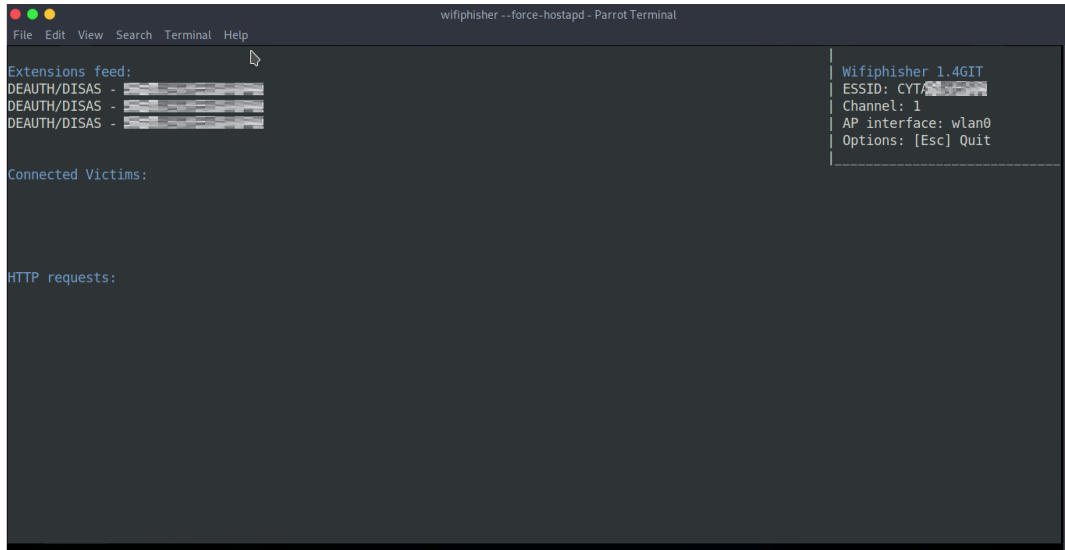
Connected Victims:
bc:3d: [redacted] 10.0.0.16 Huawei Technologies Android ↑

HTTP requests:
[*] GET request from 10.0.0.16 for http://connectivitycheck.android.com/generate_204
[*] GET request from 10.0.0.16 for http://connectivitycheck.gstatic.com/generate_204
[*] GET request from 10.0.0.16 for http://connectivitycheck.gstatic.com/generate_204
[*] GET request from 10.0.0.16 for http://connectivitycheck.android.com/generate_204
[*] GET request from 10.0.0.16 for http://connectivitycheck.android.com/generate_204
  
```

Σχήμα Β'.8: Wifiphisher, deauthentication θύματος με επίσκεψη στην phishing σελίδα χωρίς απόκτηση κωδικού θύματος.

Β'.8 Αποτυχημένη περίπτωση επίθεσης

Τέλος, δεν μπορεί να παραλειφθεί και η περίπτωση της αποτυχίας. Πρακτικά μια αποτυχία ισοδυναμεί με την αδυναμία εξαπάτησης του θύματος, δηλαδή την μη απόκτηση των διαπιστευτηρίων του. Το deauthentication λαμβάνει χώρα κανονικά, αλλά για πολλαπλούς λόγους, που θα αναλυθούν λεπτομερώς στο υπόλοιπο μέρος της εργασίας στο “κεφάλαιο Γ” παρουσίαση αποτελεσμάτων επίθεσης”, δεν καταλήγουμε σε υποκλοπή του κωδικού.



Σχήμα Β'9: Wifiphisher, deauthentication θύματος χωρίς επίσκεψη στην phishing σελίδα.

Κεφάλαιο Γ'

Παρουσίαση αποτελεσμάτων επίθεσης

Με βάση τα στοιχεία που συγκεντρώθηκαν από τις επιθέσεις Wi-Fi, τα ευρήματα της έρευνας υποδηλώνουν ότι ένα σημαντικό ποσοστό των ατόμων που στοχοποιήθηκαν ήταν ευάλωτα στις επιθέσεις, αν και το συνολικό ποσοστό επιτυχίας ήταν σχετικά χαμηλό.

Η διαπίστωση ότι τέσσερα άτομα έπεσαν θύματα των επιθέσεων και κοινοποίησαν τον κωδικό πρόσβασής τους υπογραμμίζει τη σημασία της λήψης κατάλληλων μέτρων ασφαλείας κατά την πρόσβαση σε δημόσια δίκτυα WiFi. Υπογραμμίζει τους πιθανούς κινδύνους και τις συνέπειες από την παράλειψή του. Τα δεδομένα τονίζουν την ανάγκη για αυξημένη επαγρύπνηση και προληπτικά μέτρα για την προστασία των προσωπικών πληροφοριών και των ευαίσθητων δεδομένων από ανοικτά δίκτυα. Επιπλέον, το γεγονός ότι έξι άτομα έκαναν κλικ στη σελίδα του σεναρίου phishing αλλά δεν παρείχαν τον κωδικό πρόσβασής τους υποδηλώνει ότι αναγνώρισαν την πιθανή απειλή και έλαβαν τα κατάλληλα μέτρα για να προστατεύσουν τα προσωπικά τους στοιχεία. Βέβαια, το σενάριο ήταν όσο το δυνατόν ρεαλιστικά, αλλά θα πρέπει να τονιστεί ότι οι χρήστες που συμμετείχαν στα πειράματα γνώριζαν ότι θα πραγματοποιηθεί κάποια επίθεση στο δίκτυο, και για αυτό να ήταν πιο επιφυλακτικοί και προσεκτικοί.

Γ'.1 Ανάλυση αποτελεσμάτων επιτυχημένης επίθεσης

Στην περίπτωση της επιτυχημένης επίθεσης όπως φαίνεται και στο σχήμα παρακάτω, ένα 5% των ανθρώπων που έπεσαν θύμα της επίθεσης παραχώρησαν τον κωδικό τους. Αξίζει να σημειωθεί πως κατά την διάρκεια των επιθέσεων 2

από τις 4 επιτυχημένες συνέβησαν την στιγμή που το θύμα είχε προσπαθήσει να κάνει επανεκκίνηση του ρούτερ του καθώς δεν είχε πρόσβαση στο διαδίκτυο απο το deauthentication που δεχόταν. Αυτό το περιστατικό έγινε εμφανή καθώς όλη την διάρκεια της επίθεσης με διαφορετική συσκευή υπήρξε συνεχής παρακολούθηση των διαθέσιμων δικτύων, και για μερικά λεπτά το δίκτυο του θύματος δεν βρισκόταν στην λίστα. Σε αυτό το χάσμα ενός-δύο λεπτών που το κάθε κοινό ρούτερ χρειάζεται ώστε να πραγματοποιηθεί η επανεκκίνηση, το θύμα είχε παραχωρήσει τον κωδικό του, πράγμα που αυξάνει κατά πολύ την πιθανότητα να μην κατάλαβε πως το πλαστό σημείο πρόσβασης δεν είναι το αυθεντικό και αυτός να είναι ο κύριος λόγος της επιτυχίας της επίθεσης.



Σχήμα Γ'.1: Επισημασμένο γράφημα αποτελεσμάτων επιτυχημένων επιθέσεων.

Γ'.2 Ανάλυση αποτελεσμάτων επίσκεψης phishing σελίδας

Φτάνοντας στην περίπτωση που το θύμα θα ανακαλύψει την ύπαρξη του πλαστού σημείου πρόσβασης και θα επισκεφτεί την phishing σελίδα αλλά δεν θα παραχωρήσει τον κωδικό του μας δίνει το συμπέρασμα πως ο συγκεκριμένος άνθρωπος πιθανόν να κατάλαβε την ύπαρξη κινδύνου και απέφυγε την οποιαδήποτε ενεργεία.

Γ'.3 Ανάλυση αποτελεσμάτων αποτυχίας επίθεσης

Τέλος, η τρίτη περίπτωση αποτελέσματος της επίθεσης είναι η αποτυχία, η οποία μπορεί να ερμηνευτεί καθώς και να δικαιολογηθεί με αρκετούς και διαφορετικούς λόγους.

Υπάρχουν διάφοροι λόγοι για τους οποίους κάποιος μπορεί να μην κάνει κλικ σε ένα πλαστό σημείο πρόσβασης, ακόμα κι αν δεν γνωρίζει τους πιθανούς κινδύνους ασφαλείας που σχετίζονται με τέτοια σημεία πρόσβασης. Μερικοί από τους πιθανούς λόγους είναι:

- Επιφυλακτικότητα ή έλλειψη ανάγκης: Το θύμα μπορεί να είναι προσεκτικό όταν χρησιμοποιεί δημόσιο Wi-Fi και να αποφεύγει τη σύνδεση με άγνωστα ή ύποπτα σημεία πρόσβασης. Μπορεί να προτιμά να χρησιμοποιεί το δικό τους πρόγραμμα δεδομένων από την κάρτα SIM ή ακόμη να περιμένει μέχρι να αποκατασταθεί το πρόβλημα στο αξιόπιστο δίκτυο Wi-Fi.
- Τεχνικές γνώσεις: Το θύμα μπορεί να έχει κάποιες τεχνικές γνώσεις και να είναι σε θέση να ανιχνεύσει πλαστά σημεία πρόσβασης ή να ξέρει πώς να ασφαλίσει τη συσκευή του όταν συνδέεται σε δημόσιο Wi-Fi. Ενδέχεται να γνωρίζει τους κινδύνους που συνδέονται με τα πλαστά σημεία πρόσβασης και να λαμβάνει τις απαραίτητες προφυλάξεις για την προστασία των ευαίσθητων πληροφοριών του.

- Άγνοια: Το θύμα ενδέχεται να μην έχει καταλάβει την ύπαρξη του πλαστού σημείου πρόσβασης, καθώς και την αδυναμία πλοήγησης στο διαδίκτυο.

Γ'.4 Συμπεράσματα

Συμπερασματικά, αυτά τα δεδομένα ενισχύουν τη σημασία της εκπαίδευσης των ατόμων σχετικά με τους κινδύνους που συνδέονται με τις διαδικτυακές δραστηριότητες και την κρισιμότητα της λήψης κατάλληλων μέτρων για την προστασία των προσωπικών πληροφοριών. Με την προώθηση της μεγαλύτερης ευαισθητοποίησης για ζητήματα διαδικτυακής ασφάλειας και την ενθάρρυνση των ατόμων να υιοθετήσουν προληπτικά μέτρα ασφαλείας, μπορεί να μειωθούν οι κίνδυνοι παραβιάσεων δεδομένων και άλλων περιστατικών διαδικτυακής ασφάλειας.

Βιβλιογραφία

- [1] Adel Ismail, Al-Alawi, "WiFi Technology: Future Market Challenges and Opportunities", Journal of Computer Science 2 (1): 13-18, 2006
- [2] H. Peng, "WIFI network information security analysis research," 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, China, 2012
- [3] Tom Rowan, "Negotiating WiFi security", Network Security, Volume 2010, Issue 2, 2010, Pages 8-12,
- [4] Alakshendra Sharma, Tushar Bhatia, Avijit Katyar, Samson Ebenezar U, "Wireless Security – An Introduction to Wireless Security Protocols and their Security Flaws", 2021 Annals of the Romanian Society for Cell Biology, 25(6), 11805–11812
- [5] Changhua He, John C. Mitchell, "Analysis of the 802.11i 4-way handshake", 2004 In Proceedings of the 3rd ACM workshop on Wireless security (WiSe '04), Association for Computing Machinery, New York, NY, USA, 43–50
- [6] B. Bhushan, G. Sahoo, A. K. Rai, "Man-in-the-middle attack in wireless and computer networking — A review", 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall), Dehradun, India, 2017, pp. 1-6
- [7] Avijit Mallik, "MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS", Department of Mechanical Engineering, Rajshahi University of Engineering & Technology, Rajshahi, Bangladesh 2018, Jurnal Pendidikan Teknologi Informasi Volume 2, Nomor 2, Oktober 2018, 109 - 134

- [8] Manesh Thankappana, Helena Rifà-Pousa, Carles Garrigues, “Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks: A State of the Art Review”, Center for Cybersecurity Research of Catalonia (CYBERCAT), Barcelona, Spain 2022
- [9] Keith Swiat, “The travelling menace: rogue hotspots”, Computer Fraud & Security, Volume 2006, Issue 12, 2006, Pages 13-15
- [10] Messier, R., “Social Engineering”, 2019, In CEH v10 Certified Ethical Hacker Study Guide, R. Messier (Ed.)
- [11] N. A. Al-Thani, "Adolescents' and social engineering: The role of psychometrics factors in determining vulnerability and designing interventions," 2022 9th International Conference on Behavioural and Social Computing (BESC), Matsuyama, Japan, 2022, pp. 1-5
- [12] S. Sabouni, A. Cullen and L. Armitage, "A preliminary radicalisation framework based on social engineering techniques," 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), London, UK, 2017, pp. 1-5
- [13] Kaouthar Chetoui, Birom Bah, Abderrahim Ouali Alami, Ayoub Bahnasse, Overview of Social Engineering Attacks on Social Networks, Procedia Computer Science, Volume 198, 2022, Pages 656-661, ISSN 1877-0509
- [14] Andy Amoordon, Virginie Deniau, Anthony Fleury, Christophe Gransart, “A single supervised learning model to detect fake access points, frequency sweeping jamming and deauthentication attacks in IEEE 802.11 networks”, Machine Learning with Applications, Volume 10, 2022, 100389, ISSN 2666-8270
- [15] Alotaibi B., Elleithy K, “Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions”, 2016, Wireless Pers Commun 90, 1261–1290
- [16] M. Conti, N. Dragoni and V. Lesyk, "A Survey of Man In The Middle Attacks," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027-2051, thirdquarter 2016

- [17] G. R. Hiertz, D. Denteneer, L. Stibor, Y. Zang, X. P. Costa and B. Walke, "The IEEE 802.11 universe," in IEEE Communications Magazine, vol. 48, no. 1, pp. 62-70, January 2010
- [18] Kaplanis Charalampos, "Detection and prevention of man in the middle attacks in Wi-Fi technology", Diss. Aalborg University, 2015
- [19] Volker Roth, Wolfgang Polak, Eleanor Rieffel, and Thea Turner, 2008, "Simple and effective defense against evil twin access points", In Proceedings of the first ACM conference on Wireless network security (WiSec '08), Association for Computing Machinery, New York, NY, USA, 220–235

Συντμήσεις

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
BWA	Broadband Wireless Access
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol
IP	Internet Protocol (address)
LLC	Logical Link Control
MIC	Message Integrity Check
OWE	Opportunistic Wireless Encryption
PTK	Pairwise Transient Key
PMK	Pairwise Master Key
PMF	Protected Management Frames
TKIP	Temporal Key Integrity Protocol
WLAN	Wireless Local-Area Network

Γλωσσάρι Ξενικών Όρων

ANonce	Τυχαίος αριθμός που δημιουργείται από ένα σημείο πρόσβασης
Baiting	Ένας κακόβουλος χρήστης χρησιμοποιεί ψευδή πληροφορία για να παρασύρει ένα θύμα σε μια παγίδα που μπορεί να κλέψει προσωπικές πληροφορίες
Beacons	Τακτικές μεταδόσεις από σημεία πρόσβασης με σκοπό την ενημέρωση των συσκευών χρήστη σχετικά με τις διαθέσιμες υπηρεσίες Wi-Fi και τα κοντινά σημεία πρόσβασης
Beacon packets	Η συνεχής μετάδοση σημάτων σε ένα δίκτυο beacon που διαφημίζει την παρουσία του σταθμού βάσης
Control packets	Χρησιμοποιείται από διάφορες λειτουργίες ρούτερ για τη δημιουργία και τη διατήρηση της απαραίτητης πληροφορίας σχετικά με την κατάσταση του δικτύου
Data packets	Δεδομένα που αποστέλλονται μέσω δικτύων υπολογιστών
Denial-of-service	Τύπος επίθεσης που καταστεί μια υπηρεσία απρόσιτη

DHCP lease	Μια προσωρινή εκχώρηση διεύθυνσης IP σε συσκευή στο δίκτυο
Group keys	Κρυπτογραφικό κλειδί που μοιράζεται μεταξύ μιας ομάδας χρηστών
Ieee	Συλλογή προτύπων δικτύωσης που καλύπτουν τις φυσικές προδιαγραφές και τις προδιαγραφές του επιπέδου σύνδεσης δεδομένων για τεχνολογίες όπως το Ethernet και το ασύρματο.
Initialization vector	Αυθαίρετος αριθμός που μπορεί να χρησιμοποιηθεί με ένα μυστικό κλειδί για κρυπτογράφηση δεδομένων για την αποτροπή επιθέσεων στον κυβερνοχώρο
Mac addresses	Μοναδικό αλφαριθμητικό χαρακτηριστικό 12 χαρακτήρων που χρησιμοποιείται για την αναγνώριση μεμονωμένων ηλεκτρονικών συσκευών σε ένα δίκτυο
Phishing	Τύπος επίθεσης που χρησιμοποιείται για την κλοπή δεδομένων χρήστη
Pre-Shared Key	Κωδικός πρόσβασης που χρησιμοποιείται για τον έλεγχο ταυτότητας ενός ατόμου που προσπαθεί να συνδεθεί σε ένα ασύρματο δίκτυο

Pretexting	Μορφή επίθεσης κοινωνικής μηχανικής όπου ο κακόβουλος χρήστης σκηνοθετεί ένα σενάριο που ξεγελά τα θύματα να παρέχουν πολύτιμες πληροφορίες
Pseudo-Random Generator	Πρόγραμμα που γράφτηκε και χρησιμοποιείται σε εφαρμογές πιθανοτήτων και στατιστικών όταν απαιτούνται μεγάλες ποσότητες τυχαίων ψηφίων
Rc4 algorithm	Γνωστός και ως Rivest Cipher 4, κρυπτογραφεί τα μηνύματα ένα byte τη φορά μέσω ενός αλγορίθμου
SNonce	Τυχαίος αριθμός που δημιουργείται από τη συσκευή χρήστη
Sniffing	Τύπος επίθεσης, συμβαίνει όταν ένας κακόβουλος χρήστης χρησιμοποιεί έναν ανιχνευτή πακέτων για να υποκλέψει και να διαβάσει δεδομένα που περνούν μέσα από ένα δίκτυο
Spoofing packets	Δημιουργία πακέτων πρωτοκόλλου Διαδικτύου (IP) με ψευδή διεύθυνση IP προέλευσης για την μίμηση ενός άλλου συστήματος υπολογιστή